Systemy Informacji Biznesowej

1 Definiowanie systemów informacyjnych

Ta część zawiera omówienie natury informacji i systemów.

1.1 Definiowanie danych i informacji

Ważne jest rozróżnienie danych i informacji. Dane są faktami surowymi i mogą przyjmować postać liczby lub stwierdzenia, na przykład daty lub miary. Konieczne jest, aby firmy wprowadziły procedury zapewniające rejestrację danych. Na przykład, aby zapewnić, że operator centrum obsługi klienta zawiera kod pocztowy każdego klienta, można go zapisać w swoim skrypcie, a weryfikacja sprawdzająca dokonana w celu sprawdzenia, czy dane zostały wprowadzone do systemu. Powszechną definicją informacji jest to, że są to dane przetworzone w sposób znaczący. Wymaga to procesu, który jest wykorzystywany do generowania informacji, która obejmuje zbieranie danych, a następnie poddawanie ich procesowi transformacji w celu tworzenia informacji. Niektóre przykłady informacji obejmują prognozę sprzedaży lub sprawozdanie finansowe. Jak stwierdzono, informacje są generowane poprzez transformację danych. Można to osiągnąć za pomocą szeregu różnych procesów transformacji lub danych. Niektóre przykłady procesów danych obejmują agregację, która podsumowuje dane za pomocą takich środków, jak pobieranie średniej wartości z grupy liczb. Klasyfikacja umieszcza dane w kategoriach takich jak terminowe i opóźnione dostawy. Sortowanie porządkuje dane, dzięki czemu przedmioty są umieszczane w określonej kolejności, na przykład wystawianie zamówień według daty dostawy. Obliczenia mogą być dokonywane na danych takich jak obliczanie wynagrodzenia pracownika przez pomnożenie liczby godzin przepracowanych przez stawkę godzinową. Wreszcie dane mogą być wybrane na podstawie zestawu kryteriów wyboru, takich jak lokalizacja geograficzna klientów. Chociaż informacje są przydatnym źródłem informacji dla osób i organizacji, nie wszystkie informacje można uznać za przydatne. Różnice między "dobrą" i "złą" informacją można zidentyfikować, rozważając, czy ma ona niektóre lub wszystkie cechy jakości informacji. Atrybuty mogą być związane z czasem, treścią i formą informacji. Terminowość odnosi się do tego, że informacje powinny być dostępne w razie potrzeby. Jeśli informacja zostanie dostarczona zbyt wcześnie, może przestać być aktualna po użyciu. Jeśli informacja zostanie dostarczona zbyt późno, nie będzie miała sensu. Również informacje powinny pokrywać prawidłowego okresu. Na przykład prognoza sprzedaży może zawierać informacje dotyczące wyników osiągniętych w przeszłości, bieżących wyników i przewidywanych wyników, aby odbiorca miał możliwość zapoznania się z przeszłością, teraźniejszością i przyszłymi okolicznościami. Treść informacji odnosi się do czynników, takich jak dokładność informacji i trafność informacji do konkretnej sytuacji i użytkownika. Forma informacji odnosi się do takich aspektów, jak przejrzystość informacji, które powinny być odpowiednie dla zamierzonego odbiorcy. Odbiorca powinien być w stanie szybko zlokalizować określone przedmioty i powinien być w stanie z łatwością zrozumieć te informacje. Informacje powinny również zawierać odpowiedni poziom szczegółowości, aby zaspokoić potrzeby informacyjne odbiorcy. Na przykład w niektórych przypadkach wymagane będą bardzo szczegółowe informacje, podczas gdy w innych konieczne będzie jedynie podsumowanie.

1.2 Definiowanie systemów

System można zdefiniować jako zbiór komponentów, które współpracują w celu osiągnięcia wspólnego celu. Celem systemu jest otrzymywanie danych wejściowych i przekształcanie ich na dane wyjściowe. W poprzedniej sekcji "Definiowanie danych i informacji" wykorzystano proces transformacji, aby wyjaśnić, w jaki sposób dane są przekształcane w informacje. Nie każdy system ma jeden cel, a często system zawiera kilka podsystemów z podprogramami, co przyczynia się do osiągnięcia ogólnego celu systemowego. Na przykład obszary finansowe, operacyjne i marketingowe organizacji powinny mieć

wszystkie cele, które razem pomagają osiągnąć ogólne cele korporacyjne. Widać, że w systemach dane są wykorzystywane jako dane wejściowe dla procesu, który tworzy informacje jako dane wyjściowe. W celu monitorowania wydajności systemu wymagany jest pewien mechanizm sprzężenia zwrotnego. Ponadto należy wywierać wpływ na kontrolę wszelkich występujących problemów i upewnić się, że system spełnia swój cel. Tak więc istnieje pięć komponentów ogólnego systemu pod względem wejścia, procesu, wyjścia, sprzężenia zwrotnego i sterowania.

1.3 Definiowanie systemów informacyjnych

Rola systemów informatycznych w przekazywaniu zarządzającym informacji, które umożliwią im podejmowanie decyzji zapewniających kontrolę nad organizacją. Organizacja będzie mieć kontrolę, jeśli spełnia potrzeby środowiska. W odniesieniu do systemów sterowania można je klasyfikować jako otwarte i zamknięte. System sterowania w pętli otwartej to taki, który nie ma możliwości zapewnienia spełnienia celów dla procesu. Oznacza to, że są nieodpowiednie w kontekście organizacyjnym ze względu na złożoność środowiska, w którym działają organizacje. Tak więc systemy z otwartą pętlą byłyby skuteczne tylko w osiąganiu celów systemu w przypadkach, w których z całą pewnością wiemy zdarzenia, które miałyby miejsce podczas procesu systemu. Systemy zamkniętej pętli mogą mieć dwa rodzaje mechanizmów kontrolnych, określane jako kontrola sprzężenia zwrotnego i sterowanie wyprzedzeniem. Systemy kontroli sprzężenia zwrotnego zwykle zapewniają sposób na kontrolowanie systemu. Negatywne sprzężenie zwrotne ma miejsce wtedy, gdy podejmowane są działania mające na celu odwrócenie wszelkich różnic między pożądanymi i rzeczywistymi wynikami. Słabością tego podejścia jest możliwość opóźnienia między rozbieżnością a działaniami podejmowanymi w celu jej zmniejszenia. Układy sterowania sprzężeniem wyprzedzającym próbują przezwyciężyć opóźnienie czasowe związane z układami sprzężenia zwrotnego poprzez włączenie elementu przewidującego w pętli sprzężenia zwrotnego sterowania. Systemy feedforward nie są tak powszechne, jak systemy opinii w ustawieniach biznesowych. Przykładami mogą tu być plany zarządzania projektami, które są realizowane z czasem, jakością i kosztami.

1.4 Systemy informacji biznesowej

Przy pomocy poprzednich definicji informacji i systemów możemy teraz zdefiniować system informacji biznesowych jako grupa powiązanych ze sobą komponentów, które wspólnie działają w celu realizacji działań wejściowych, przetwarzania, produkcji, przechowywania i kontroli w celu przekształcenia danych w produkty informacyjne, które mogą być wykorzystywane do wspierania prognozowania, planowania, kontroli, koordynacji, podejmowania decyzji i działania operacyjne w organizacji. Pod względem komponentów, które podejmują tę działalność, można je podzielić na pięć podstawowych zasobów: ludzi, sprzętu, oprogramowania, komunikacji i danych. Zasoby ludzkie obejmują użytkowników i programistów systemu informatycznego oraz tych, którzy pomagają w utrzymaniu i obsłudze systemu, takich jak menedżerowie IS i pracownicy pomocy technicznej. Do zasobów sprzętowych należą komputery i inne elementy, takie jak drukarki. Zasoby oprogramowania odnoszą się do programów komputerowych znanych jako oprogramowanie i związanych z nimi instrukcji obsługi. Zasoby komunikacyjne obejmują sieci oraz sprzęt i oprogramowanie niezbędne do ich obsługi. Zasoby danych obejmują dane, do których organizacja ma dostęp, na przykład komputerowe bazy danych i pliki papierowe. W większości organizacji Business Information Systems (BIS) szeroko korzystają z technologii informatycznych, takich jak komputery osobiste. Powody, dla których skomputeryzowane BIS stały się powszechne, są widoczne w ich zaletach, takich jak szybkość, dokładność i niezawodność. Mają także wysoki stopień elastyczności dzięki możliwości zaprogramowania ich do wykonywania różnorodnych zadań. Istnieją jednak pewne wady BIS, takie jak brak kreatywności, jaki posiadają ludzie, oraz trudności z włączeniem innych czynników do ich podejmowania decyzji, takich jak innowacja i intuicja.

1.5 Rodzaje systemu informacji biznesowej

Systemy informatyczne można podzielić na dwie kategorie systemów, które wspierają codzienną działalność biznesową organizacji i systemy wspierające podejmowanie decyzji menedżerskich. Systemy operacyjne (OIS) zajmują się głównie kontrolą procesów, przetwarzaniem transakcji i komunikacją. Systemy informacji zarządczej (MIS) zajmują się zapewnieniem wsparcia dla podejmowania decyzji menedżerskich. Niedawno ten podział BIS na systemy operacyjne i systemy zarządzania, choć użyteczny dla menedżerów dokonujących przeglądu typów używanych BIS, nie odzwierciedla obecnie dokładnie realiów systemów używanych w organizacji, szczególnie w związku ze zwiększonym wykorzystaniem międzyorganizacyjnego handlu elektronicznego i elektroniczna wymiana danych (EDI). Na przykład systemy e-biznesu i systemy planowania zasobów przedsiębiorstwa obejmują zarówno systemy operacyjne, jak i systemy zarządzania, aby zapewnić przedsiębiorstwom bardziej zintegrowane systemy informacyjne

2 Sprzęt

Sprzęt opisuje fizyczne składniki systemu komputerowego, które można zaklasyfikować jako urządzenia wejściowe, jednostkę centralną, urządzenia pamięci wewnętrznej i zewnętrznej oraz urządzenia wyjściowe (Beynon-Davis, 2009). Urządzenia wejściowe służą do przechwytywania lub wprowadzania danych do komputera. Centralna jednostka przetwarzania (CPU) wykonuje przetwarzanie, wykonując instrukcje podane w postaci programów komputerowych. Pamięć wewnętrzna jest wykorzystywana jako tymczasowy środek przechowywania danych i instrukcji, podczas gdy pamięć zewnętrzna zapewnia sposób przechowywania danych i programów poza komputerem. Urządzenia wyjściowe przekształcają wyniki przetwarzania na postać czytelną dla człowieka. Te komponenty sprzętowe zostaną teraz opisane bardziej szczegółowo.

2.1 Urządzenia wejściowe

Urządzenia wejściowe służą do wprowadzania danych lub instrukcji spoza komputera do komputera. Mysz i klawiatura to przykłady urządzeń wejściowych. Wybór urządzenia wejściowego często zależy od ilości danych, które należy wprowadzić. Wprowadzanie danych na małą skalę jest zwykle przeprowadzane przez ludzi, przy użyciu wielu znanych urządzeń wejściowych, takich jak mysz lub klawiatura. Komputerowy system informacyjny rzadko korzysta tylko z jednego urządzenia wejściowego. Nawet typowy komputer osobisty często oferuje kilka różnych metod wprowadzania danych, takich jak klawiatura, mysz, joystick i karta dźwiękowa.

2.2 Central Processing Unit (CPU)

Centralna jednostka procesora (CPU) lub procesor akceptuje instrukcje i dane i wykonuje je zapisując wyniki w pamięci. Zwiększona prędkość komputerów wynika przede wszystkim ze zwiększenia prędkości procesora. Szybkość procesora zależy od wielu różnych czynników. takie jak prędkość zegara i szerokość szyny. Szybkość zegara określa, ile instrukcji na sekundę może wykonać procesor. Szerokość magistrali opisuje, ile sztuk danych może być przesyłanych jednocześnie. W obu przypadkach im wyższa wartość, tym mocniejszy jest procesor. Szybkość zegara i wartości przepustowości mogą być pomocne przy próbie porównania procesorów w celu wybrania najbardziej odpowiedniego.

2.3 Pamięć wewnętrzna i zewnętrzna

Pamięć komputera jest zakwalifikowana jako pamięć wewnętrzna (zwana również pamięcią główną lub pamięcią podstawową), która jest przechowywana w komputerze i pamięci zewnętrznej (zwanej również pamięcią zewnętrzną), która jest przechowywana na oddzielnym urządzeniu, w którym informacja zostanie zachowana, nawet jeśli maszyna jest wyłączony. Pamięć komputera służy do

przechowywania danych oczekujących na przetwarzanie, instrukcji załadowanych z oprogramowania, które są używane do przetwarzania danych lub sterowania systemem komputerowym oraz danymi lub informacjami, które zostały przetworzone. Dyskietki i dyski twarde są przykładami pamięci zewnętrznej.

2.4 Urządzenia wyjściowe

Urządzenia wyjściowe wyświetlają wyniki przetwarzania komputerowego. Komputerowy system informacyjny wykorzystuje wiele urządzeń wyjściowych jako monitor, drukarkę i kartę dźwiękową.

2.5 Główne kategorie komputerów

Istnieją trzy podstawowe kategorie komputerów: komputer mainframe, minikomputer i mikrokomputer. Pokrótce przyjrzymy się cechom każdej kategorii, aby lepiej zrozumieć, w jaki sposób przemysł korzysta z technologii komputerowej.

2.5.1 Komputer główny

Komputery typu mainframe są tradycyjnie związane z dużymi, potężnymi maszynami przeznaczonymi do wielkoskalowych operacji przetwarzania danych. Wykorzystanie komputerów typu mainframe w przemyśle, które kiedyś były odpowiedzialne za duże przychody takich firm, jak IBM, spadło w ciągu ostatnich dwudziestu lat. IBM, Fujitsu i Unisys są obecnymi dostawcami. Postępy technologiczne umożliwiły mniejszym i tańszym systemom konkurowanie z systemami mainframe pod względem szybkości i mocy. Na przykład nowoczesny komputer osobisty można uznać za wielokrotnie potężniejszy niż jeden z najwcześniejszych systemów mainframe. W wielu organizacjach komputery typu mainframe są uznawane za systemy dotychczasowe, co oznacza, że chociaż menedżerowie zdają sobie sprawę, że istniejący system może nie być całkowicie odpowiedni do zaspokojenia potrzeb firmy, zmiana będzie trudna do wdrożenia.

2.5.2 Minikomputery

Minikomputer łączy w sobie niektóre cechy komputera mainframe i mikrokomputera. Obecnie są one często określane jako serwery przez firmy takie jak IBM (np. IBM AS / 400) i Hewlett-Packard (np. HP Alpha). Różne typy serwerów mogą mieć różne funkcje, takie jak zarządzanie siecią lub hostowanie bazy danych.

2.5.3 Mikrokomputery

Mikrokomputer wykorzystuje bardziej nowoczesną technologię, aby zapewnić stosunkowo duże możliwości obliczeniowe przy niskich kosztach. Mikrokomputery są obecnie często nazywane komputerami "klienta", które odbierają usługi i dane z maszyny "serwerowej". Niektóre z głównych cech mikrokomputera są małe, stosunkowo niedrogie i mogą być wykorzystywane do różnych celów.

3 Oprogramowanie

Ta część zawiera przegląd cech wspólnych dla szeregu nowoczesnych aplikacji oraz sposobu, w jaki oprogramowanie może być wykorzystywane do wspierania działalności biznesowej organizacji. Oprogramowanie można zdefiniować jako serię szczegółowych

instrukcje, które kontrolują działanie systemu komputerowego i istnieją jako programy opracowane przez programistów komputerowych. Istnieją dwie główne kategorie oprogramowania i aplikacji systemowych

3.1 Oprogramowanie systemowe

Oprogramowanie systemowe zarządza i steruje działaniem systemu komputerowego podczas wykonywania zadań w imieniu użytkownika. Oprogramowanie systemu składa się z trzech podstawowych kategorii: systemów operacyjnych, programów rozwoju oprogramowania i programów narzędziowych.

3.1.1 Systemy operacyjne (OS)

System operacyjny współdziała ze sprzętem komputera, monitorując i wysyłając instrukcje dotyczące zarządzania i kierowania zasobami komputera. System operacyjny działa jako pośrednik między funkcjami, które użytkownik musi wykonać, na przykład wyszukiwanie w bazie danych, i tym, jak przekładają się one na i od sprzętu w postaci reagowania na kliknięcia myszą i wyświetlania informacji na ekranie. Podstawowe funkcje systemu operacyjnego obejmują: przydzielanie i zarządzanie zasobami systemowymi, planowanie wykorzystania zasobów i monitorowanie działań systemu komputerowego.

3.1.2 Programy programistyczne

Programy do tworzenia oprogramowania umożliwiają użytkownikom tworzenie własnego oprogramowania w celu wykonywania zadań związanych z przetwarzaniem przy użyciu języków programowania. Języki programowania można opisać w kategoriach ich historycznej pozycji w rozwoju systemów programowania komputerowego. Język programowania pierwszej generacji lub język maszynowy wymaga od programisty jednego i zera do przedstawienia znaków i liczb. Te niezwykle czasochłonne zadania zostały nieco uproszczone za pomocą krótszych kodów i nazwano językiem asemblerowym. Znaczący postęp przyniosły języki trzeciej generacji, takie jak FORTRAN, COBOL, BASIC, Pascal i C, które znacznie skracają czas programowania programisty. Języki czwartej generacji, takie jak SQL, są zbudowane wokół systemu baz danych i sprawiają, że tworzenie kodu jest jeszcze łatwiejsze niż w przypadku języków trzeciej generacji.

3.1.3 Programy użytkowe

Programy narzędziowe udostępniają szereg narzędzi wspierających działanie i zarządzanie systemem komputerowym. Programy monitorujące wydajność systemu lub zapewniające zabezpieczenia są przykładami programów narzędziowych.

3.2 Oprogramowanie aplikacyjne

Oprogramowanie aplikacyjne można zdefiniować jako zestaw programów, które umożliwiają użytkownikom wykonywanie określonych czynności przetwarzania informacji. Oprogramowanie aplikacyjne można podzielić na dwie ogólne kategorie: uniwersalne i specyficzne dla aplikacji.

3.2.1 Zastosowania ogólnego zastosowania

Aplikacje ogólnego przeznaczenia to programy, które można wykorzystać do wykonywania szerokiego zakresu typowych zadań. Na przykład edytor tekstu jest zdolny do tworzenia różnorodnych dokumentów, które są odpowiednie do wielu różnych celów. Ten typ aplikacji jest często określany jako oprogramowanie produktywności, ponieważ pomaga poprawić wydajność jednostki. Oprogramowanie do przetwarzania tekstu obejmuje tworzenie różnych dokumentów wewnętrznych i zewnętrznych, w tym listy, raporty, faktury, notatki i protokoły z posiedzeń. Oprogramowanie arkusza kalkulacyjnego umożliwia przechowywanie, organizację i analizę danych liczbowych. Oprogramowanie baz danych pozwala na przechowywanie i wyszukiwanie informacji. Oprogramowanie multimedialne umożliwia pracę z mediami, takimi jak tekst, dźwięk, animacja i wideo.

3.2.2 Oprogramowanie specyficzne dla aplikacji

Oprogramowanie specyficzne dla aplikacji obejmuje programy przeznaczone do określonego celu lub realizujące jasno określone zadanie przetwarzania informacji. Oprogramowanie zaprojektowane do przeprowadzania przetwarzania listy płac lub zarządzania kontami jest przykładem programu specyficznego dla aplikacji.

4 Systemy baz danych

Celem bazy danych jest śledzenie rzeczy. Bazy danych mogą istnieć na papierze, na przykład w książce telefonicznej, ale są nieefektywne i kosztowne w utrzymaniu. Bazująca na komputerach baza danych oferuje zalety zaawansowanych funkcji wyszukiwania, które można wykorzystywać do lokalizowania i wyszukiwania informacji wielokrotnie szybciej niż metodami ręcznymi. Elektroniczna baza danych zapewnia użytkownikom możliwość dodawania, zmieniania lub usuwania rekordów zgodnie z wymaganiami. Funkcje indeksowania oznaczają, że te same podstawowe informacje mogą być przechowywane w wielu różnych kategoriach. Zapewnia to dużą elastyczność i umożliwia użytkownikom lokalizowanie, pobieranie i organizowanie informacji w razie potrzeby. Bazy danych używane w całej firmie są zwykle dostępne dla wielu różnych użytkowników w całym systemie sieciowym. Niektóre z zalet tego podejścia obejmują zminimalizowanie niepotrzebnego powielania informacji, spójność jest zachowywana przez zapewnienie, że wszelkie zmiany wprowadzone do informacji przechowywanych w bazie danych są odzwierciedlane dla wszystkich użytkowników i chociaż informacje są przechowywane w sposób uporządkowany, oprogramowanie bazy danych zwykle zapewnić wystarczającą elastyczność, aby spełnić różne wymagania poszczególnych użytkowników i działów.

4.1 Organizowanie danych w bazie danych

Dane w elektronicznej bazie danych są uporządkowane według pól i rekordów. Pole to pojedynczy element informacji, taki jak nazwa lub ilość. Rekord to zbiór powiązanych pól, a tabela to zbiór powiązanych rekordów. Aby zidentyfikować określony element informacji w bazie danych, wszystkie rekordy muszą zawierać unikalny identyfikator, zwykle nazywany polem kluczowym lub kluczem podstawowym. Pole kluczowe ma zazwyczaj postać numeru lub kodu i będzie inne dla każdego rekordu w bazie danych. Relacyjne bazy danych umożliwiają przechowywanie danych w wielu różnych tabelach i są najczęściej używanym typem bazy danych. Tabele w relacyjnej bazie danych można łączyć ze sobą za pomocą jednego lub więcej kluczy rekordów. Obejmuje to klucz podstawowy, a także inne klucze pomagające zlokalizować dane przechowywane w innej tabeli. Klucze rekordów zawarte w każdej tabeli mogą służyć do ustanowienia jednej lub więcej relacji między tabelami. Używając kombinacji rekordów można pobrać dane z kilku tabel jednocześnie. Pole używane do lokalizowania informacji w innej powiązanej tabeli jest często nazywane kluczem obcym.

4.2 Oprogramowanie bazy danych

Większość programów baz danych obsługuje tworzenie relacyjnych baz danych zawierających kilka połączonych tabel. Wiele programów, takich jak Microsoft Access, umożliwia automatyczne łączenie tabel w celu utworzenia wymaganych relacji. Wszystkie główne programy baz danych umożliwiają użytkownikom tworzenie i modyfikowanie formularzy wprowadzania danych. Formularz wprowadzania danych zapewnia wygodny sposób przeglądania, wprowadzania, edytowania i usuwania rekordów. Indeks przechowuje informacje dotyczące kolejności rekordów w bazie danych. Wszystkie nowoczesne programy bazodanowe oferują szereg wyrafinowanych funkcji bezpieczeństwa. Przykłady niektórych spośród najczęściej dostępnych funkcji, w tym szyfrowania i ochrony hasłem. Wreszcie wszystkie główne pakiety baz danych umożliwiają użytkownikom generowanie szerokiej gamy raportów. Wiele programów może automatycznie tworzyć proste raporty. Ponadto wiele

programów umożliwia użytkownikom wykonywanie obliczeń i innych działań podczas tworzenia raportu.

4.3 Pobieranie danych z bazy danych

Podczas korzystania z oprogramowania bazy danych dane są pobierane z bazy danych przy użyciu tak zwanego zapytania. Zapytanie umożliwia użytkownikowi zlokalizowanie, sortowanie, aktualizację lub wyodrębnienie rekordów z bazy danych. Użytkownicy projektują zapytanie, określając warunki, które muszą zostać spełnione, aby rekord mógł zostać wybrany. Istnieją dwa typy zapytań: kwerendy wyboru i kwerendy aktualizacji: kwerendę wyboru można użyć do zlokalizowania i wyświetlenia rekordów spełniających określone warunki. Żadne dane przechowywane w bazie danych nie zostały zmienione, a wszelkie rekordy niespełniające określonych warunków są po prostu tymczasowo ukrywane. Kwerendy aktualizacji mogą być używane do modyfikowania rekordów na różne sposoby, na przykład zgodnie z zestawem warunków określonych przez użytkownika. Typowe akcje wykonywane przez kwerendy aktualizacji obejmują aktualizowanie wartości przechowywanych w polach, usuwanie wszelkich niepotrzebnych rekordów, dołączanie nowych rekordów do bazy danych i generowanie nowych tabel zawierających wybrane rekordy lub informacje podsumowujące. Większość programów baz danych używa specjalnego strukturalnego języka zapytań (SQL) w celu tworzenia zapytań. Strukturalny język zapytań (SQL) zapewnia ustandaryzowaną metodę pobierania informacji z baz danych. Chociaż tradycyjnie używane do zarządzania dużymi bazami danych na komputerach typu mainframe i minikomputerach, stało się ono powszechnie używane popularne narzędzie do pakietów komputerów osobistych. Programy SQL są tworzone poprzez tworzenie serii instrukcji zawierających specjalne słowa kluczowe.

4.4 Business Intelligence

Systemy Business Intelligence (BI) są potrzebne ze względu na ogromne ilości danych przechowywanych obecnie w systemach informacji organizacyjnej oraz potrzebę wyciągnięcia użytecznych informacji z tego w postaci wzorców, trendów i przedstawienia tego w sposób zrozumiały dla decydentów. Systemy BI zazwyczaj koncentrują się na dostarczaniu aktualnych informacji na poziomie strategicznym w dużych organizacjach z dużymi zbiorami danych (stąd potrzeba hurtowni danych opisanej później). Systemy BI również generalnie zapewniają pośrednie wsparcie dla konkretnych decyzji, a nie specyficzne dla decyzji ukierunkowanie systemów wspomagania decyzji. System BI składa się z czterech głównych komponentów hurtowni danych, analityki biznesowej, zarządzania wydajnością biznesową (BPM) i interfejsu użytkownika. Dane są zbierane z różnych źródeł, a następnie przechowywane w specjalnym repozytorium baz danych określanym jako hurtownia danych w celu wspierania procesu decyzyjnego w organizacji. Repozytoria danych koncentrujące się na działach lub obszarach tematycznych nazywa się zbiorami danych. Eksploracja danych to rodzaj analizy, która ma na celu identyfikację wzorców w danych, które można wykorzystać do przewidywania przyszłych zachowań. Analizy biznesowe są używane do przeprowadzania analizy danych przechowywanych w hurtowni danych za pomocą narzędzi do raportowania i wysyłania zapytań. Zarządzanie wydajnością firmy obejmuje metody stosowane do mierzenia i zarządzania wydajnością firmy. Interfejs użytkownika integruje i wyświetla informacje z wielu obszarów biznesowych. Pulpity nawigacyjne zapewniają wizualną reprezentację w postaci wykresów porównujących rzeczywistą wydajność z pożądanymi celami skuteczności.

5 Sieci

Sieć łączy dwa lub więcej komputerów w celu współużytkowania danych lub zasobów. Pozwala to ludziom współpracować, a także pozwala na bardziej efektywny kosztowo udostępnianie sprzętu, takiego jak drukarki i faksy. Sieci są ważne dla organizacji, ponieważ pomagają nawiązać kontakt z

klientami, dostawcami i współpracownikami. Dzięki temu firma może szybciej i tanio zamawiać nowe surowce od swoich dostawców i może pozostać w kontakcie z potrzebami swoich klientów. Dalsze korzyści z sieci obejmują redukcję kosztów poprzez korzystanie z urządzeń takich jak poczta elektroniczna, skrócenie czasu przepływu informacji, na przykład porównywanie poczty e-mail z dostarczaniem pocztowym, możliwość udostępniania informacji przez dostęp do bazy danych poprzez system sieciowy, możliwość udostępniania urządzeń sprzętowych, takich jak: jako drukarki w sieci, używając narzędzi roboczych grupy do udostępniania dokumentów i innych informacji. Główne wady sieci to koszt instalacji sieci i zapewnienie bezpiecznej i niezawodnej usługi sieciowej.

5.1 Składniki sieciowe

Niektóre z głównych składników tworzących sieć są teraz opisane.

5.1.1 Serwery

Serwery kontrolują przepływ informacji w sieci i wykorzystują wyspecjalizowane oprogramowanie o nazwie sieciowy system operacyjny (NOS) do zarządzania siecią. Serwer i NOS umożliwiają współdzielenie informacji, oprogramowania i urządzeń sprzętowych, takich jak drukarki. Kontroluje również dostęp do informacji w plikach. W przypadku sieci składającej się z około 20 osób lub więcej, opisane powyżej funkcje mogą zostać podzielone między kilka serwerów w celu współdzielenia obciążenia. Może istnieć oddzielny serwer plików, serwer wydruku, serwer haseł i serwer bazy danych. W bardzo dużych firmach będzie wiele serwerów używanych do przechowywania danych. Będą one połączone siecią, aby zapewnić, że dane są dostępne dla wszystkich. Będą również odpowiedzialni za zapewnienie, poprzez proces zwany replikacją, że ta sama wersja danych istnieje na różnych serwerach. Przy użyciu wielu serwerów istnieje możliwość rozłożenia obciążenia obliczeniowego na te serwery, zamiast przeciążania jednej centralnej maszyny, co miało miejsce w czasach systemu mainframe. Dzielenie się funkcjami na kilku komputerach nosi nazwę "przetwarzania rozproszonego".

5.1.2 Komputery lub terminale użytkowników końcowych

Punkty dostępu dla użytkowników sieci znane są różnie jako klienci, węzły, stacje robocze lub, najczęściej, komputery osobiste. Aby pracować w sieci, każdy klient musi mieć zainstalowane oprogramowanie sieciowe, takie jak Novell Netware. Połączenie z siecią jest również wymagane przez kabel sieciowy podłączony do karty interfejsu sieciowego w jednym z gniazd PC lub przez system sieci bezprzewodowej.

5.1.3 Procesory telekomunikacyjne

Procesory telekomunikacyjne to elementy sprzętu, które służą do łączenia serwerów i klientów oraz różnych sieci. Są one zwykle określane przez ich konkretne nazwy, takie jak koncentratory, multipleksery, mosty i routery. W firmie, która musi korzystać z urządzeń gatewayowych, do ich utrzymania potrzebny jest specjalista. Koncentratory są używane do podłączenia do 20 komputerów osobistych do sieci w wygodny sposób za pomocą kabli połączeniowych (które wyglądają podobnie do kabli telefonicznych i gniazd) biegnących między tyłem komputera a hubem. Koncentrator może następnie zostać podłączony do serwera lub połączenia szkieletowego prowadzącego do serwera. Routery mogą wybrać najlepszą trasę dla przesyłanych pakietów i są również wykorzystywane w sieci szkieletowej i sieci rozległej, aby to osiągnąć. Chociaż urządzenia te były odrębne, teraz są produkowane jako hybrydy, które mają wspólne funkcje. Firmy przyłączone do Internetu zwykle używają routera jako bramy do przyłączenia swojej wewnętrznej sieci do Internetu. Często łączy się to z "zaporą ogniową", która ma na celu zmniejszenie ryzyka uzyskania przez osobę spoza firmy nieautoryzowanego dostępu do danych firmy.

5.1.4 Oprogramowanie pośrednie

Middleware to wyspecjalizowany typ oprogramowania, który umożliwia komunikację różnym aplikacjom. Działa jako warstwa pomiędzy innym oprogramowaniem, aby pomóc w przesyłaniu danych pomiędzy niekompatybilnymi systemami. Jest często opisywany jako "klej", który wiąże aplikacje do oprogramowania systemowego. Jest to ważne w świecie sieciowym, ponieważ zapewnia usługi tłumaczeniowe między oprogramowaniem działającym na różnych typach systemów komputerowych w różnych firmach. Przykładem oprogramowania pośredniego jest oprogramowanie bramki, które umożliwia wewnętrznemu systemowi poczty e-mail, takim jak Lotus cc: Mail, wysyłanie wiadomości do innych systemów poczty e-mail za pośrednictwem Internetu. Oprogramowanie pośredniczące jest również konieczne, aby umożliwić pojedynczą aplikację, taką jak przetwarzanie zamówień sprzedaży dostęp do różnych typów baz danych, takich jak Oracle, Informix lub Microsoft SQL Server, z których może korzystać duża firma. Oprogramowanie pośredniczące do pomocy w komunikacji można sklasyfikować zgodnie z siedmiowarstwowym modelem znanym jako model OSI

6 Internet i sieć WWW

Internet to rozległa sieć komputerów połączonych na całym świecie, które mogą współdzielić zarówno informacje, jak i przetwarzanie. Informacje są przesyłane z komputerów, których użytkownicy żądają usług na komputerach przechowujących informacje i hostujące aplikacje biznesowe, które dostarczają usługi w odpowiedzi na żądania. Komputery osobiste w domach i firmach są połączone z Internetem za pośrednictwem lokalnych dostawców usług internetowych (ISP), którzy z kolei są połączeni z większymi dostawcami usług internetowych z połączeniem z główną infrastrukturą lub szkieletami krajowymi i międzynarodowymi. Internet można opisać jako globalny system sieciowy złożony z mniejszych systemów. Internet powstał w 1969 roku przez amerykańską organizację wywiadowczą DARPA (Defense Advanced Research Projects). Internet zaczął osiągać obecną formę w 1987 roku, rozwijając się z systemów opracowanych przez DARPA i National Science Foundation (NSF).

6.1 Biznes z włączoną usługą internetową

Firmy z dostępem do sieci mogą być klasyfikowane przez podmioty uczestniczące w transakcjach biznesowych. Najczęstsze transakcje zidentyfikowane jako te, w których organizacja korzysta z Internetu w celu przeprowadzania transakcji z konsumentami, określane jako "biznes-konsument" (B2C) lub gdy firma dokonuje transakcji z innymi przedsiębiorstwami, określanymi jako "business-to-business" (B2B). Relacje między firmą a jej dostawcami i klientami mogą zostać radykalnie zmienione dzięki możliwościom, jakie daje Internet. Dzieje się tak, ponieważ Internet oferuje sposób na ominięcie niektórych partnerów kanału. Proces ten jest znany jako dezintermediacja lub "wycinanie pośrednika". Korzyści z dezintermediacji polegają na tym, że jest ona w stanie usunąć koszty sprzedaży i infrastruktury związane ze sprzedażą za pośrednictwem kanału. Niektóre z tych oszczędności mogą zostać przekazane klientowi w postaci obniżki kosztów. Chociaż rozpowszechnianie rozproszone jest szeroko rozpowszechnione, pojawił się również proces tworzenia nowych pośredników między klientami i dostawcami, nazywany re-pośrednictwem. Na przykład w firmach z branży turystycznej, takich jak Tripadvisor, można uzyskać informacje dotyczące miejsc docelowych i hoteli, a następnie podać linki do dostawców hotelowych.

6.2 Intranety i ekstranety

Większość usług internetowych jest dostępna dla każdej firmy lub konsumenta, który ma dostęp do Internetu. Jednak wiele aplikacji biznesowych, które uzyskują dostęp do poufnych informacji firmowych, wymaga, aby dostęp był ograniczony do osób uprzywilejowanych lub osób trzecich. Jeśli informacje są ograniczone do tych wewnątrz organizacji, sieć jest nazywana intranetem. Jeśli dostęp

zostanie rozszerzony na niektóre inne, ale nie wszystkie poza organizację, sieć określana jest jako ekstranet. Dostęp do ekstranetów mają autoryzowane osoby spoza firmy, takie jak współpracownicy, dostawcy lub główni klienci, ale informacje nie są dostępne dla wszystkich osób posiadających połączenie z Internetem, ale są ograniczone przy użyciu hasła. Intranety są również wykorzystywane do udostępniania informacji, takich jak spis telefonów pracowników, procedury personelu lub podręczniki jakości, informacje dla agentów, takie jak specyfikacje produktów, aktualna lista i obniżone ceny, informacje o konkurentach, harmonogramy fabryczne i poziomy magazynowania - wszystkie te informacje zwykle muszą być aktualizowane często i może być kosztowne. Extranety są szeroko stosowane w celu wspierania działań takich jak zamawianie od dostawców.

6.3. Sieć WWW

World Wide Web zapewnia standardową metodę wymiany i publikowania informacji w Internecie. Nośnik oparty jest na standardowych formatach dokumentów, takich jak HTML (hipertekstowy język znaczników), który został powszechnie przyjęty, ponieważ obsługuje szeroki zakres formatów ułatwiających czytanie dokumentów na różnych urządzeniach dostępowych. Zawiera również grafikę i animacje, które można zintegrować ze stronami internetowymi, a interakcja jest możliwa za pośrednictwem formularzy opartych na HTML, które umożliwiają klientom dostarczanie swoich danych osobowych w celu uzyskania większej ilości informacji o produkcie, wyszukiwania, zadawania pytań lub zgłaszania uwag. Jest to połączenie przeglądarek internetowych i HTML, które okazały się tak skuteczne w rozpowszechnionym korzystaniu z Internetu. Korzystanie z tych narzędzi zapewnia szereg korzyści, takich jak zwiększenie łatwości poruszania się między dokumentami za pomocą hiperłączy lub obrazów. To szybko staje się bardzo intuicyjnym sposobem nawigacji, który jest podobny we wszystkich witrynach internetowych i aplikacjach. Może zapewnić środowisko graficzne obsługujące multimedia, które jest popularne wśród użytkowników i zapewnia wizualne medium reklamowe. Standaryzacja narzędzi i wzrost popytu oznacza, że informacje można wymieniać z wieloma firmami i konsumentami.

6.4 Przeglądarki internetowe i serwery

Przeglądarki internetowe są aplikacjami używanymi do uzyskiwania dostępu do informacji w sieci WWW przechowywanych na serwerach internetowych. Serwery WWW służą do przechowywania, zarządzania i dostarczania informacji w sieci WWW. Głównymi przeglądarkami internetowymi są Microsoft Internet Explorer i Mozilla Firefox. Przeglądarki wyświetlają tekst i grafikę dostępną z witryn internetowych i udostępniają narzędzia do zarządzania informacjami z witryn internetowych. Przeglądarki internetowe komunikują się z serwerami WWW w następujący sposób. Żądanie z komputera jest wykonywane, gdy użytkownik wpisze adres internetowy, kliknie hiperłącze lub wypełni formularz online, taki jak wyszukiwanie. To żądanie jest następnie wysyłane do dostawcy usług internetowych i kierowane przez Internet do serwera docelowego przy użyciu mechanizmu opisanego w sekcji dotyczącej protokołów. Następnie serwer zwraca żądaną stronę WWW, jeśli jest to strona statyczna (stała) lub jeśli wymaga odniesienia do bazy danych, na przykład żądania informacji o produkcie, przekaże zapytanie do serwera bazy danych, a następnie zwróci to do klienta jako dynamicznie tworzonej strony internetowej. Informacje na temat wszystkich żądań stron są przechowywane w pliku dziennika transakcji, który rejestruje żądaną stronę, czas jej wykonania i źródło zapytania.

6.5 E-biznes

E-biznes obejmuje kilka kluczowych działań, w tym usprawnienie procesów biznesowych, usprawnienie komunikacji i zapewnienie środków do bezpiecznej realizacji transakcji biznesowych. E-biznes jest częścią szerszej gospodarki internetowej, która obejmuje wszystkie działania związane z

korzystaniem z Internetu w celach handlowych. Gospodarka internetowa składa się z następujących warstw:

- Infrastruktura internetowa. Firmy, które dostarczają sprzęt, oprogramowanie i inny sprzęt do Internetu. Przykłady: dostawcy usług internetowych, firmy sieciowe i producenci komputerów i serwerów.

- Infrastruktura aplikacji internetowych. Firmy, które oferują oprogramowanie ułatwiające transakcje internetowe. Ponadto firmy świadczące usługi tworzenia stron internetowych, projektowania i doradztwa. Przykłady: producenci oprogramowania do tworzenia stron internetowych, internetowych baz danych i wyszukiwarek.

- Intermedenci internetowi. Firmy łączące kupujących i sprzedających, na przykład poprzez dostarczanie treści lub tworzenie rynków, na których można prowadzić transakcje biznesowe. Przykłady: biura podróży, dostawcy treści i brokerzy online.

- Internet Commerce. Firmy, które sprzedają produkty i usługi konsumentom lub innym firmom. Przykłady: sklepy internetowe, subskrypcje lub usługi płatne oraz producenci sprzedający bezpośrednio do odbiorców.

Ogólnie rzecz biorąc, korzyści płynące z e-biznesu obejmują niższe koszty, większą wydajność i dostęp do większych rynków. Automatyzując wiele zadań administracyjnych związanych z zamawianiem, dostarczaniem i dostarczaniem towarów lub usług, koszt typowej transakcji biznesowej może zostać znacznie zredukowany. E-zamówienia są wykorzystywane do obniżenia kosztów administracyjnych i zakupu towarów po niższych cenach. Wspomniano wcześniej, że przyjęcie podejścia e-biznesowego może przyczynić się do wzmocnienia trzech głównych obszarów działalności: procesów produkcyjnych, procesów zorientowanych na klienta i wewnętrznych procesów zarządzania. Jeśli chodzi o procesy ukierunkowane na klienta, na przykład efektywność obsługi klienta może zostać poprawiona poprzez wprowadzenie help desk na stronie internetowej firmy. Oprócz pomagania klientom, taki zakład może również działać na rzecz obniżenia kosztów poprzez zmniejszenie presji na inne usługi wsparcia, takie jak telefony zaufania. Wreszcie, przyjęcie podejścia e-biznesowego może pomóc firmom w osiągnięciu większego, globalnego rynku. Jest to często jedna z korzyści restrukturyzacji relacji między producentem, detalistami i klientami.

6.6 E-commerce

Typową działalnością związaną z e-biznesem jest e-commerce, który można opisać jako wykorzystujący technologię do przeprowadzania transakcji biznesowych, takich jak kupowanie i sprzedawanie towarów i usług. Jednak e-commerce to coś więcej niż tylko

przeprowadzanie transakcji elektronicznych; obejmuje również szeroki zakres powiązanych działań, takich jak wsparcie posprzedażowe, a nawet logistyka. Działania związane z handlem elektronicznym można podzielić na pięć podstawowych typów:

- Business-to-business (B2B). Transakcje odbywają się między firmami. Około 80 procent całego handlu elektronicznego jest tego typu.

- Biznes-konsument (B2C). Firmy sprzedają produkty bezpośrednio konsumentom. B2C może obejmować takie działania, jak badania nad produktem (gdzie konsumenci zbierają informacje i porównują ceny) oraz dostawy elektroniczne (gdzie produkty informacyjne są dostarczane konsumentom za pośrednictwem poczty elektronicznej lub w inny sposób).

- Business-to-government (B2G). Transakcje odbywają się między firmami a organizacjami sektora publicznego.

- Konsument-konsument (C2C). Transakcje odbywają się między osobami prywatnymi. Być może najlepszym przykładem handlu C2C są internetowe serwisy aukcyjne i systemy peer-to-peer.

- Handel mobilny (m-commerce). M-Commerce to stosunkowo nowa inwestycja, która polega na sprzedaży towarów lub usług za pośrednictwem technologii bezprzewodowej, w szczególności telefonów komórkowych.

7 Pozyskiwanie systemów informatycznych

Główne wybory przy zakupie systemów informatycznych można zaklasyfikować jako gotowe (pakowane), niestandardowe aplikacje opracowane przez wewnętrzny dział IT lub software house i systemy opracowane przez użytkownika końcowego.

7.1 Indywidualny rozwój

Indywidualny rozwój odnosi się do tego, kiedy system informatyczny jest opracowywany przez specjalistę systemów informatycznych, aby odpowiadał wymaganiom biznesowym aplikacji. Specjaliści systemów informatycznych będą pracować dla firmy zwanej "wewnętrznym" opracowaniem na zamówienie lub dla strony trzeciej, takiej jak software house, która jest określana jako "outsourcing". Indywidualny rozwój ma tę zaletę, że produkuje oprogramowanie dostosowane do precyzyjnych wymagań firmy. Wady obejmują koszty, rozwój na zamówienie jest najdroższym sposobem tworzenia nowych systemów informatycznych. Pod względem czasu rozwój na zamówienie, zwłaszcza przy użyciu formalnych metodologii rozwoju strukturalnego, znany jest z przekroczenia czasu, z opóźnieniami miesięcy lub lat niezbyt często i jakości. Wreszcie pod względem jakości oprogramowanie na zamówienie zwykle nie jest wolne od błędów; Błędy oprogramowania mogą się wahać od trywialnych do katastroficznych, a te drugie często wynikają z niewłaściwej analizy wymagań

7.2 Oprogramowanie z półki

Opcjonalny zakup oprogramowania w pakiecie to metoda nabycia polegająca na bezpośrednim zakupie wstępnie napisanej aplikacji używanej przez więcej niż jedną firmę. Ten typ oprogramowania jest wstępnie napisany i jest dostępny dla całej gamy platform sprzętowych, od komputerów PC po komputery typu mainframe. Oprogramowanie "z półki" zostało napisane, aby oferować szeroką funkcjonalność, która będzie pasować do wielu różnych firm. Ten szeroki zakres funkcji ma tę zaletę, że spełnia wymagania dużej liczby firm. Może również oferować zbyt wiele funkcji dla konkretnej firmy, która może wtedy poczuć, że płaci za rzeczy, których nie będzie używać. Jednocześnie może wymagać od firm przetwarzania informacji w określony sposób, który jest sprzeczny z normalnym sposobem prowadzenia działalności. Ewentualnie, niektóre z gotowych pakietów oprogramowania mogą nie oferować wystarczające funkcje. Główną zaletą gotowych pakietów oprogramowania jest ich niski koszt w porównaniu z nabywaniem oprogramowania na zamówienie o tym samym poziomie funkcjonalności. Ponadto, ponieważ oprogramowanie do pakowania zostało opracowane na rynek komercyjny, jest mniej prawdopodobne, że będzie cierpieć z powodu błędów, które dotykają dostosowanego oprogramowania. W przypadku gotowego, gotowego, gotowego oprogramowania, wstępnie napisane oprogramowanie jest kupowane od dostawcy, ale możliwe jest skonfigurowanie go tak, aby był specyficzny dla firmy. W przypadku zakupu od ręki z półki, różne moduły mogą być kupowane od różnych dostawców i budowane razem.

7.3 Oprogramowanie opracowane przez użytkownika końcowego

Oprogramowanie opracowane przez użytkownika końcowego to oprogramowanie napisane przez specjalistów spoza SI, tj. Użytkowników biznesowych. Planowanie zasobów przedsiębiorstwa lub aplikacje instytucjonalne to te, które wpływają na ogólną działalność firmy, obejmują więcej niż jeden dział lub obszar funkcjonalny, lub systemy obejmujące dane organizacyjne przechowywane w korporacyjnych bazach danych. Przykłady obejmują systemy księgowe, systemy przetwarzania zamówień sprzedaży i planowanie wymagań materiałowych. Aplikacje użytkowników końcowych mają bardziej ograniczony zakres. Aplikacje mogą mieć charakter departamentalny lub osobisty i zazwyczaj są ukierunkowane na wyjście lub raport, a nie na nakłady. Aplikacje te mogą być napisane przez specjalistów IT lub samych użytkowników końcowych. Jeśli tak jest, często określa się je jako aplikacje opracowane przez użytkownika końcowego. Takie systemy mogą być proste, takie jak arkusz kalkulacyjny lub mała baza danych komputerów PC lub rzadziej mogą być bardziej zaawansowane, takie jak system planowania produkcji oparty na danych prognozowania sprzedaży z kilku oddziałów tej samej organizacji. Takie aplikacje są zwykle przeznaczone do użytku indywidualnego lub w departamencie, chociaż w przypadku drugiego przykładu system może mieć znaczenie dla całej firmy. Główną zaletą oprogramowania opracowanego przez użytkownika końcowego jest to, że jest on zwykle wykorzystywany przez tych, którzy go opracowują, a zatem wymagania te nie podlegają błędnemu tłumaczeniu ani dostarczaniu zbyt skomplikowanych rozwiązań. Negatywną stroną tego jest to, że w niektórych przypadkach można użyć nieodpowiednich narzędzi programistycznych, takich jak skomplikowane arkusze kalkulacyjne zamiast budowy bazy danych. Kolejną istotną kwestią związaną z rozwojem użytkowników końcowych jest to, że oprogramowanie może zostać zainfekowane błędami w wyniku cięcia narożnego, takiego jak słaby lub nieistniejący projekt, niewielkie lub żadne testy lub brak dokumentacji. Istnieje również szereg hybrydowych podejść do akwizycji. Grupa organizacji w tej samej działalności lub obszarze działalności może mieć wymagania systemów informatycznych, które indywidualnie mogą być bardzo kosztowne w rozwoju. Rozwiązaniem może być opracowywanie zindywidualizowanego systemu przez stronę trzecią, co pozwala rozłożyć koszty opracowania na wszystkie zaangażowane organizacje. Podobnie, gotowy pakiet może zapewnić 80 procent wymaganych funkcji, ale inne mogą wymagać dodania w wyniku indywidualnego opracowania przez specjalistów IS / IT lub użytkowników końcowych. Opisane powyżej podejścia do akwizycji systemów nie wykluczają się wzajemnie dla danego projektu lub wewnątrz organizacji. Tam, gdzie oprogramowanie jest ogólne dla wszystkich firm, tak jak ma to miejsce w przypadku oprogramowania systemowego i pakietów biurowych, zakupione zostanie oprogramowanie "z półki". Jeżeli firma ma bardziej konkretne potrzeby i pragnie osiągnąć przewagę konkurencyjną, zastosowane zostaną dostosowane do potrzeb i dostosowane do potrzeb podejście do przejęcia. W przypadku systemów e-biznesowych często istnieje potrzeba integracji wewnętrznych systemów i systemów zakupionych od różnych dostawców. Wykorzystuje to podejście blokowe różnych komponentów, w tym źródeł danych, które są ze sobą zintegrowane. Jest to określane jako integracja aplikacji dla przedsiębiorstw (EAI), a osiągnięcie tego jest poważnym wyzwaniem dla kierowników projektów i projektantów systemów.

7.4 Czynniki wpływające na akwizycję oprogramowania

Istnieje wiele czynników, które wpłyną na wybór metody akwizycji. Trzema krytycznymi kwestiami są czas, koszty i jakość. Jeśli organizacja ma naglący problem, który wymaga szybkiego uruchomienia nowego systemu informacyjnego, prawdopodobne jest, że będzie poszukiwany pakiet lub dostosowany pakiet. Podobnie, organizacja, która potrzebuje "rozwiązania w zakresie systemów jakości" może dobrze rozważyć trasę pakietu oprogramowania, zwłaszcza jeśli jego wymagania są proste. Różne opcje przejęcia mają różne mocne strony, gdy rozważa się je w kategoriach trzech krytycznych kryteriów. Jakość dostarczanego produktu jest rozpatrywana z dwóch powodów: liczba znalezionych błędów lub błędów oraz przydatność oprogramowania do spełnienia wymagań użytkownika biznesowego. Należy zauważyć, że dobra jakość pod względem liczby błędów, które

zazwyczaj występują w oprogramowaniu pakowanym, może pokrywać się z niską jakością pod względem dopasowania do potrzeb firmy. Zaletą oprogramowania w pakiecie jest to, że koszt opracowania i debugowania oprogramowania jest dzielony przez więcej niż jedną firmę. Skutkuje to niższymi kosztami i mniejszą ilością błędów niż rozwój na zamówienie dla pojedynczej firmy. Używanie oprogramowania w pakiecie przez więcej niż jedną firmę to także jego największa słabość, ponieważ jego funkcje muszą odpowiadać typowej firmie. W konsekwencji może nie odpowiadać potrzebom pojedynczej firmy. Inne czynniki wpływające na pozyskiwanie oprogramowania obejmują:

- Wielkość organizacji. Małe lub średnie przedsiębiorstwo będzie miało nieuchronnie stosunkowo ograniczone zasoby na zakup systemów informatycznych i technologii informacyjnej (IS / IT). Sugeruje to, że takie organizacje będą miały tendencję do faworyzowania zakupu gotowych pakietów lub ewentualnie opracowywania aplikacji dla użytkowników końcowych.

- Własna wiedza IS / IT. W przypadku niewielkiej ilości własnych doświadczeń IS / IT, zarówno w formie specjalistów IS / IT, jak i doświadczonych użytkowników końcowych, konieczne będzie korzystanie z usług stron trzecich przy nabywaniu nowych systemów informacji biznesowych. Mogą to być dostawcy oprogramowania dla gotowych pakietów oprogramowania, korzystanie z konsultantów i / lub domów oprogramowania. Dokładnie, jaka forma strony trzeciej zostanie wykorzystana, będzie zależeć od drugiej czynniki omówione tutaj.

- Złożoność wymaganego systemu informacji. W przypadku, gdy wymóg dotyczący systemu informacji biznesowych jest szczególnie złożony lub w przypadku nietypowej aplikacji niedostępnej jako rozwiązanie w pakiecie, możliwe jest, że można wyświetlić oprogramowanie na zamówienie (opracowane wewnętrznie lub przez stronę trzecią) jako jedyne opłacalne rozwiązanie. Jednak złożoność niekoniecznie oznacza "wyjątkowość". Na przykład można uznać system planowania wymagań materiałowych lub kompletny system rachunkowości za złożony, ale wiele pakietów istnieje dla różnych platform sprzętowych. Dlatego złożoność niekoniecznie jest wskaźnikiem, że należy wykluczyć gotowy pakiet.

- Unikalność obszaru biznesowego lub biznesowego, który ma być obsługiwany. Im wyższy stopień wyjątkowości w obsługiwanym obszarze, tym mniejsze jest prawdopodobieństwo znalezienia odpowiedniego gotowego pakietu. Jest to zatem oczywisty wskaźnik do pewnego rodzaju rozwoju na zamówienie. Tak jak poprzednio, nie wolno nam mylić wyjątkowości ze złożonością. Może się zdarzyć, że specjalista spoza IS / IT opracuje rozwiązanie za pomocą narzędzi dostępnych dla deweloperów końcowych. Oczywiście, jeśli wymagany system jest złożony i cechuje się wysokim stopniem unikalności, to zindywidualizowany rozwój przez specjalistów IS / IT jest prawdopodobnie najlepszą metodą pozyskiwania.

- Wiedza specjalistyczna w zakresie IS / IT wśród użytkowników końcowych. Pewien stopień wiedzy i umiejętności w zakresie IS / IT jest niezbędny, aby użytkownicy końcowi mogli tworzyć systemy informacyjne. Ponadto taka znajomość jest pożądana przy wyborze odpowiedniego gotowego oprogramowania "z półki", ponieważ może pomóc firmie bardziej precyzyjnie określić jej dokładne wymagania zarówno pod względem funkcjonalnym, jak i technologicznym. Jeśli organizacja ma niewielką wiedzę ekspercką IS / IT użytkownika końcowego, ale ma swój własny dział IT / IT, będzie w dużym stopniu zależna od rozwiązań dostarczanych przez specjalistów IS / IT z lub bez pomocy osób trzecich.

- Powiązania z istniejącym oprogramowaniem aplikacyjnym. Tam, gdzie nowe oprogramowanie biznesowe musi bardzo ściśle integrować się z istniejącymi systemami informacyjnymi, istnieje większe prawdopodobieństwo, że przynajmniej niektóre prace programistyczne zindywidualizowane będą musiały zostać wykonane w celu zintegrowania obu systemów. Ponadto wysoki stopień integracji może

oznaczać, że nowy system informacyjny musi zostać opracowany na miarę, aby osiągnąć pożądany poziom integracji. Mówiąc to, wielu dostawców oprogramowania dostarcza pakiety dla różnych obszarów biznesowych, które bardzo dobrze ze sobą integrują.

Patrząc na kombinacje powyższych, można wymyślić metodę "najlepszego dopasowania"

8 Rozwijanie systemów informacyjnych

8.1 Cykl rozwoju systemu

Cykl rozwoju rozwoju systemów (SDLC) to klasyczne podejście stosowane do opracowywania systemów informatycznych. W podejściu SDLC zdajemy sobie sprawę z tego, że systemy są tworzone w szeregu etapów lub faz i że każda faza musi zostać ukończona przed rozpoczęciem kolejnego. Uznaje się również fakt, że działanie programistyczne (część fazy budowy) powinno rozpocząć się dopiero po ustaleniu wymagań użytkownika i opracowaniu projektu systemu. Podsumujemy teraz podstawowe kroki, które podąża większość projektów rozwoju systemów.

8.1.1 Inicjacja

Faza inicjacji jest fazą inicjacji lub uruchomienia i jest pierwszą fazą projektu rozwoju systemów informatycznych. Jego celem jest ustalenie, czy projekt jest wykonalny, a następnie przygotowanie się do zapewnienia sukcesu projektu. Faza inicjacji zawiera bodziec, od którego powstaje potrzeba opracowania nowego BIS. Ten bodziec może powstać w wyniku jakiegoś zdarzenia zewnętrznego, takiego jak zmiana prawodawstwa, lub może wynikać z wewnętrznego dążenia do opracowania systemu informacji, który lepiej zaspokaja potrzeby biznesowe organizacji. Źródłem tego procesu inicjowania może być jeden z następujących elementów:

- Dyrektor zarządzający lub inne kierownictwo wyższego szczebla. Systemy zainicjowane od tego momentu prawdopodobnie będą miały wsparcie niezbędne do pomyślnego rozwoju.

- Dział systemów informatycznych. System może być tutaj inicjowany jako część ogólnej strategii IS / IT organizacji; aby zmaksymalizować szanse powodzenia, system nadal będzie potrzebował wsparcia zarządzania na wysokim poziomie.

- Funkcjonalny obszar biznesowy. Zainicjowany tutaj system będzie rywalizował o uwagę ze wszystkimi innymi projektami rozwojowymi podejmowanymi w tym czasie; często organizacja będzie miała komitet sterujący do decydowania o priorytetach rozwojowych.

8.1.2 Ocena wykonalności

Ocena wykonalności to działanie, które ma miejsce na początku projektu, aby zapewnić, że projekt jest realną propozycją biznesową. Raport wykonalności analizuje potrzebę i wpływ systemu i rozważa różne alternatywy dla nabywania oprogramowania. Ocenę wykonalności można uznać za część fazy początkowej. Ustalą, czy komputerowy system informacyjny pasuje do określonych kryteriów wykonalności. Zazwyczaj cytowane są trzy kryteria:

- Należy ustalić, czy system informatyczny jest technicznie wykonalny. Aby było to technicznie wykonalne, albo istnieje technologia, albo można ją utworzyć w celu obsługi wymaganego systemu.

- Aby być ekonomicznie wykonalnym, system informacyjny musi generować więcej korzyści niż koszt potrzebny do jego wytworzenia. Jednym z problemów jest to, że korzyści są często trudne do określenia ilościowo w kategoriach pieniężnych, a koszty są znacznie łatwiejsze do oszacowania.

- Zakładając, że proponowany system informatyczny jest zarówno wykonalny technicznie, jak i ekonomicznie, należy dokonać oceny, czy projekt jest wykonalny operacyjnie i organizacyjnie. Przez operacyjnie wykonalne rozumiemy, że system musi być zdolny do wykonywania w wymaganych parametrach prędkości, objętości, użyteczności i niezawodności. Aby proponowany system informacyjny był wykonalny dla organizacji, musi być zdolny do współdziałania z wzorcami pracy lub istniejące wzorce pracy muszą być przystosowane lub przeprojektowane tak, aby działały równolegle z nowym systemem informacyjnym. Wykonalność organizacyjna obejmie przegląd tego, jak potencjalne umiejętności i postawy użytkowników wpłyną na system.

Częścią procesu wykonalności może być zaproszenie do składania ofert dotyczące niektórych lub wszystkich elementów systemu informacyjnego. Mogą to być oprogramowanie aplikacyjne, sprzęt, oprogramowanie komunikacyjne lub oprogramowanie systemowe. Następnie zostaną ocenione różne alternatywy różnych dostawców. Dane wyjściowe z tego kroku (a zatem dane wejściowe do następnego etapu modelu) to przegląd etapowy i raport wykonalności, który zaleci kontynuację projektu lub ponowną ocenę projektu.

8.1.3 Analiza systemów

Analiza systemów polega na przechwytywaniu wymagań biznesowych systemu przez rozmowę z użytkownikami końcowymi lub ich obserwację oraz korzystanie z innych źródeł informacji, takich jak istniejąca dokumentacja systemu. Kiedy zostanie uzgodniony proponowany system informacyjny wykonalne, konieczne jest przeprowadzenie szczegółowych prac związanych z oceną dokładnych wymagań, które zamierzani użytkownicy mają dla nowego systemu. Należy zwrócić uwagę, że etap analizy systemów jest czasem określany jako krok określania wymagań lub etap badania systemów. Na tym etapie są trzy główne zadania. Po pierwsze, konieczne jest zrozumienie, jak działa obecny system informatyczny (skomputeryzowany lub oparty na papierze). Po drugie, opracowano schematyczny model bieżących procesów systemowych, aby zapewnić zgodność specjalistów IT i użytkowników systemu. Na koniec powstaje zestaw wymagań dla nowego systemu informacyjnego. Specyfikacja wymagań określi:

- funkcje, które musi zawierać nowy system (np. zdolność użytkowników końcowych do projektowania własnych raportów);

- zakres rozważanego systemu (np. czy system jest przeznaczony tylko dla jednego obszaru funkcjonalnego przedsiębiorstwa lub czy obejmuje wszystkie działania biznesowe?);

- zamierzeni użytkownicy nowego systemu;

- normy wydajności systemu, w tym czasy reakcji, czasy przetwarzania wsadowego (jeśli wymagane) i potrzeby niezawodności;

- wymagania środowiskowe, takie jak fizyczne środowisko pracy, system operacyjny i sprzęt, na którym będzie uruchomiony system. W tym ostatnim zadaniu może być pożądane wyprodukowanie innego schematu, tym razem wymaganego systemu informacji. Jeżeli w którymkolwiek momencie okaże się, że wymagania systemu określone przez potencjalnych użytkowników wydają się w pewnym sensie niewykonalne, konieczne będzie ponowne przeanalizowanie etapu wykonalności i przeprowadzenie dodatkowej analizy możliwych opcji. Dane wyjściowe z tego kroku w modelu będą dokumentem analizy wymagań użytkownika, który szczegółowo określa, co powinien zrobić proponowany system.

8.1.4 Projektowanie systemów

Faza projektowania systemu określa sposób działania systemu w kluczowych obszarach interfejsu użytkownika, modułów programu, zabezpieczeń i transakcji bazy danych. Dane wejściowe do tego etapu to zestawienie wymagań, które musi spełniać proponowany system informacyjny dostarczyć. Zadaniem etapu projektowania systemu jest przekształcenie tych wymagań w szereg alternatywnych projektów, z których wybrana zostanie najlepsza. W związku z tym etap projektowania dotyczy sposobu, w jaki proponowany system informacyjny zapewni to, co jest wymagane. Projektowanie systemów zajmuje się takimi sprawami, jak:

- wybór odpowiedniego systemu zarządzania bazami danych;

- ustanowienie ogólnych norm bezpieczeństwa systemów;

- decydowanie o metodach nawigacji systemowej (np. systemy menu i graficzne interfejsy użytkownika);

- ogólne standardy dotyczące drukowania raportów;

- standardy projektowania ekranu dla wejścia i wyjścia;

- wymagania dotyczące gromadzenia danych;

- wymagania dotyczące przechowywania danych.

Z drugiej strony, szczegółowy projekt da w wyniku schemat dla poszczególnych modułów systemu, które będą używane w następnym etapie budowy systemu. Szczegółowy projekt dodatkowo określi niektóre aspekty projektowania systemu, o których mowa powyżej. Jeśli w dowolnym momencie etapu projektowania okaże się, że wymagania przedstawione w etapie analizy nie mają rozwiązania projektowego (np. Z powodu sprzecznych lub niekompletnych wymagań), konieczne będzie ponowne przejrzenie etapu analizy i dokładniejsze określenie nowy system informacyjny ma do zrobienia pod tymi szczególnymi względami.

8.1.5 Kompilacja systemu

Kompilacja systemu to tworzenie oprogramowania przez programistów. Obejmuje pisanie kodu oprogramowania (programowanie), budowanie wersji oprogramowania, konstruowanie i zapełnianie bazy danych oraz testowanie przez programistów i użytkowników końcowych. Na tym etapie może również pojawić się dokumentacja i szkolenie. Termin "kompilacja" to taki, który będziemy używać oprócz bardziej zwyczajnego i niejednoznacznego terminu "implementacja", który znajduje się w wielu tekstach i metodologiach. Ten krok obejmuje trzy etapy: fizyczną budowę bazy danych, programowanie i testowanie. Fizyczna baza danych polega na konwersji projektu bazy danych z poprzedniego kroku na wymagane tabele i indeksy relacyjnej bazy danych. Podetap programowania obejmuje budowę kodu komputerowego, który będzie obsługiwał przechwytywanie, przechowywanie, przetwarzanie i przetwarzanie danych. Ponadto konieczne będzie zaprogramowanie różnych innych atrybutów operacyjnych wymaganego systemu (na przykład tych, które wynikają z projektu sterowania). Obok podetapu programowania i po jego zakończeniu będą miały miejsce różne formy testowania. Dane wyjściowe z etapu budowy będą testowane i będą dostępne do ostatecznej konwersji danych lub operacji "na żywo" i "na żywo". Jeśli podczas fazy budowy okaże się, że system nie spełnia pierwotnych wymagań określonych podczas etapu analizy, to tak będzie Konieczne jest ponowne przejrzenie etapu projektowania, aby sprawdzić, czy nie wystąpiły błędy w interpretacji wymagań systemowych. Jeśli brief projektowy został poprawnie zinterpretowany, ale system nadal zawiera błędy w dostarczaniu postrzeganych wymagań, konieczne będzie ponowne przeanalizowanie analizy w celu dokładniejszego określenia wymagań systemowych.

8.1.6 Wdrażanie systemu i przełączanie

Wdrożenie systemu obejmuje praktyczne kwestie, takie jak zapewnienie sprzętu i infrastruktury sieciowej dla nowego systemu; testowanie systemu; a także kwestie ludzkie dotyczące tego, jak najlepiej kształcić i szkolić pracowników, którzy będą wykorzystywać nowy system lub na niego wpływać. Wdrażanie obejmuje również przejście ze starego systemu do nowego. Ten krok w modelu kaskadowym zajmuje się przygotowaniem i przejściem ze starych do nowych systemów informatycznych. Jak można się spodziewać, etap wdrażania systemu napotyka na trudności. W tym miejscu zostanie odkryte, czy wszystkie poprzednie kroki zostały połączone, aby dostarczyć system informacyjny, który robi to, czego użytkownicy faktycznie chcą i który również działa prawidłowo. Dane zostaną przekształcone ze starych systemów informatycznych lub bezpośrednio wprowadzone do nowej bazy danych. Wreszcie, nowy system będzie działał od razu, w fazach lub po okresie równoległego działania. Jeśli napotkane zostaną błędy na etapie uruchamiania na żywo, system może kontynuować działanie, gdy błędy zostaną usunięte. Ewentualnie może być konieczne zawieszenie działania nowego systemu, podczas gdy najważniejsze błędy są naprawione. Taka korekta błędu może wymagać zmiany któregokolwiek z poprzednich kroków, w zależności od charakteru i wagi błędu (błędów). Z tej krótkiej dyskusji jasno wynika, że im później odkryte zostaną błędy związane z procesem rozwoju systemu, tym wyższy jest koszt ich prawidłowego wykonania. Najgorszy możliwy scenariusz jest prawdopodobnie taki, że system osiągnął etap na żywo tylko po to, aby odkryć, że wymagany system nigdy nie był naprawdę wykonalny.

8.1.7 Przegląd i konserwacja

Gdy system informacyjny działa w warunkach bieżącego działania, nieuniknione będzie, że zmiany będą wymagane z biegiem czasu. Faza konserwacji obejmuje dwa różne rodzaje konserwacji. Pierwsza, znana jako "nieproduktywna konserwacja", wynika z błędów lub niedopatrzeń w oryginalnym opracowaniu systemu, które jednak nie uniemożliwiają działania systemu do akceptowalnego poziomu, są nadal konieczne, aby poprawić zgodność z oryginalną specyfikacją. Druga forma utrzymania wiąże się z dodaniem nowych funkcji i udogodnień, które rozszerzają zakres i funkcjonalność systemu informatycznego. W początkowym okresie mogą one przybrać postać "sympatycznych do", "dzwonków i gwizdów", które nie były uważane za istotne dla systemu w momencie przejścia na nową. W dłuższej perspektywie system zostanie dostosowany i zmodyfikowany, aby sprostać zmieniającym się wymaganiom biznesowym. Należy również podjąć działania zwane przeglądem powdrożeniowym. Powinno to nastąpić około sześć miesięcy po przejściu na system i powinno sprawdzić, co było planowane w systemie informatycznym, w porównaniu z tym, co faktycznie się wydarzyło. Wnioski wyciągnięte z tego ćwiczenia będą niezwykle cenne podczas opracowywania kolejnego systemu.

9 Metodologie rozwoju systemów

9.1 SSADM

Metoda analizy strukturalnej systemów (SSADM) to ustrukturyzowana metoda rozwoju opracowana początkowo w latach 80. jako standardowa metoda rozwoju domeny publicznej. SSADM skupia się na aspektach wykonalności, analizy i projektowania cyklu rozwoju systemu. Zapewnia mniej wytycznych dotyczących aspektów zmiany i konserwacji projektu IS. Opisując SSADM w kilku szczegółach podkreśla metodyczne podejście wymagane dla dużych projektów, które niektórzy mogą określać jako biurokratyczne. Pokazuje także kontrast z alternatywnymi technikami, takimi jak RAD. SSADM ma strukturę pięciu modułów, w ramach której jest siedem etapów. Pięć modułów jest teraz omawianych.

9.1.1 Analiza wykonalności

Projekt będzie już w fazie planowania lub inicjacji, więc w tym momencie konieczne jest ustalenie, czy jest to technicznie i ekonomicznie wykonalne. Studium wykonalności podzielono na cztery etapy:

- przygotować się do studium wykonalności, oceniając zakres projektu;

- zdefiniować problem (co powinien zrobić nowy system, którego obecnie nie ma);

- wybrać najlepszą opcję wykonalności spośród dostępnych (zazwyczaj maksymalnie pięć opcji biznesowych i podobną liczbę opcji technicznych);

- złożyć raport wykonalności, zawierający uzasadnienie dla wybranej opcji.

Dane wyjściowe z tego etapu, raport wykonalności, stanowią teraz dane wejściowe dla następnego modułu; analiza wymagań.

9.1.2 Analiza wymagań

Ten etap jest niezwykle istotny, ponieważ służy do uzyskania pełnego zrozumienia tego, co jest wymagane od nowego systemu. Wszelkie błędy i pominięcia dokonane na tym etapie zostaną odzwierciedlone w pozostałej części procesu opracowywania systemu. Podejmowane są następujące kroki:

- Ustanowienie ram analizy. Zakres projektu jest ponownie oceniany, a następnie odpowiednio planowany.

- Zbadaj i określ wymagania. Szerokie wymagania zostaną zdefiniowane na etapie wykonalności: są one teraz rozszerzone na szczegółowy katalog wymagań systemowych.

- Zbadaj bieżące przetwarzanie. W studium wykonalności zostanie utworzony wstępny diagram przepływu danych, który został rozszerzony i obejmuje wszystkie istniejące procesy.

- Zbadaj aktualne dane. Logiczny model danych jest opracowywany w taki sposób, aby organizacja mogła uzyskać jasny obraz atrybutów zawartych w jednostkach danych i ich wzajemnych powiązań.

- Wyprowadź logiczny widok bieżących usług. Wymaga to zmiany logicznego modelu danych, tak aby odzwierciedlał logikę biznesową rozważanego systemu, a nie jego bieżącą fizyczną implementację.

- Zbierz wyniki badań. Jest to ostatni krok w analizie obecnego środowiska systemowego. Analitycy sprawdzą spójność i kompletność przed przejściem do następnego etapu.

Opracowano wiele możliwych rozwiązań systemowych dla postrzeganych wymagań biznesowych, a wpływ i korzyści każdego z nich zostaną ocenione. Wybrane rozwiązanie będzie najbardziej pasujące do wymagań firmy. Dwa kroki to:

- Zdefiniuj opcje systemów biznesowych. Działania w tym zakresie obejmą ustanowienie minimalnych systemów

wymagania, rozwój szkieletu formy alternatywnej, przygotowanie krótkiej listy opcji, a wreszcie pełna ocena każdej alternatywnej opcji krótkiej listy, w tym analiza kosztów i korzyści, analiza wpływu oraz plan rozwoju i integracji dla każdego z nich.

- Wybierz opcję systemu biznesowego. Dokładny sposób, w jaki zostanie to zrobione, będzie różny dla różnych organizacji. Cel jest jednak taki sam: dla odpowiednich menedżerów użytkowników wybór opcji systemu biznesowego na podstawie dowodów przedstawionych przez zespół analityczny.

9.1.3 Specyfikacja wymagań

Ten moduł ma jeden etap, który z kolei jest podzielony na osiem dyskretnych kroków.

- Określ wymagane przetwarzanie systemu. W tym miejscu elementy istniejącego systemu, które mają pozostać częścią nowego systemu, są dodawane do szczegółów zawartych w katalogu wymagań.

- Opracuj wymagany model danych. Nadmiarowe elementy z modelu danych istniejącego systemu są usuwane (jeśli istnieją) i dodawane są dodatkowe wymagane elementy. Ponadto sprawdzane są relacje między starymi i nowymi podmiotami.

- Wyprowadzanie funkcji systemowych. Tutaj procesy, które zostaną zidentyfikowane i włączone do diagramów przepływu danych, zostaną zidentyfikowane bardziej precyzyjnie i odpowiednio udokumentowane.

- Poprawić wymagany model danych. Wymagany model danych opracowany wcześniej został teraz wzmocniony poprzez przeprowadzenie analizy danych relacyjnych i normalizację; wynikiem powinien być zestaw tabel, które można zaimplementować za pomocą systemu zarządzania relacyjnymi bazami danych.

- Opracuj prototypy specyfikacji. Obejmuje to tworzenie prototypów dla wybranych części specyfikacji, tak aby dokładne wymagania mogły być zatwierdzone przez docelowych użytkowników końcowych; takie elementy jak menu, przykładowe ekrany wprowadzania danych i raporty mogą być konstruowane.

- Opracuj specyfikacje przetwarzania. Analityk na tym etapie zajmuje się przedstawieniem wpływu czasu na dane poddane różnym działaniom (tj. Tworzenie, odczytywanie, aktualizowanie i usuwanie); dwa narzędzia, które są tu stosowane, to analiza historii istnienia jednostki i wykresy zależności korespondencji. Są to narzędzia wykorzystywane przez profesjonalnych analityków systemów i wykracza to poza zakres tego tekstu.

- Potwierdź cele systemowe. Przedostatnim zadaniem jest przeprowadzenie formalnego przeglądu wymagań systemowych, aby zapewnić, że ostateczna specyfikacja wymagań jest kompletna i w pełni zrozumiana zarówno przez użytkowników, jak i deweloperów.

- Zestaw specyfikacji wymagań. Na koniec, różne komponenty (w tym wymagany systemowy logiczny model danych, definicje funkcji, katalog wymagań i inne elementy) są montowane w końcowym dokumencie specyfikacji wymagań, który następnie zapewnia dane wejściowe do następnego modułu i etapu.

9.1.4 Logiczna specyfikacja systemu

Tutaj ustala się wszelkie ograniczenia wyboru środowiska technicznego (np. Bezpieczeństwo, wydajność, łatwość aktualizacji). Wybrano odpowiednią opcję techniczną; musi być zgodny z wymaganymi kryteriami strategicznymi i operacyjnymi, które zostały już ustalone. Proces opracowywania specyfikacji systemów jest kontynuowany, a wynikiem jest zestaw możliwych do wdrożenia komponentów. Poszczególne kroki są następujące:

- Zdefiniuj dialogi użytkownika. Dotyczy to definiowania sposobów interakcji użytkownika z systemem (na przykład menu i nawigacja systemów).

- Zdefiniuj procesy aktualizacji. Tutaj ustala się definicję transakcji, które będą zmieniać dane (w celu wsparcia tego etapu wykorzystywane są historie życia jednostki).

- Określ procesy zapytania. Oprócz nawigacji i aktualizacji, użytkownicy będą chcieli wykonać zapytania dotyczące danych przechowywanych w systemie.

- Złóż logiczny projekt. Jest to w zasadzie kontrola spójności i kompletności. Gdy projekt logiczny zostanie ukończony i zostanie "podpisany", można zająć się ostatnim etapem.

9.1.5 Projekt fizyczny

Ten etap dotyczy dostarczenia ostatecznego projektu, z którego można opracować i wdrożyć system. Należy ukończyć siedem etapów:

- Przygotuj się na fizyczny projekt. Badane jest środowisko implementacji, opracowywane są standardy opracowywania aplikacji i uzgodniona fizyczna strategia projektowania.

- Utwórz fizyczne projektowanie danych. Wymagany jest logiczny model danych (LDM) i opracowywany jest projekt danych specyficznych dla danej firmy.

- Utwórz mapę implementacji komponentu funkcji. Komponenty każdej funkcji systemu są rysowane. Obejmuje to ich związek z fizycznymi komponentami funkcji (rzeczywistymi działaniami biznesowymi), które obsługują.

- Optymalizacja projektowania fizycznych danych. Projekt fizycznych danych jest testowany pod kątem wymaganych celów wydajności i optymalizowany, jeśli to konieczne.

- Pełny projekt specyfikacji funkcji. Dotyczy to dowolnych komponentów funkcji, które wymagają programowania.

- Konsolidacja interfejsu danych procesowych. Interfejs danych procesowych znajduje się między fizycznym projektem bazy danych a projektem procesu. Pomaga to odwzorować bazę danych na potrzeby przetwarzania (szczególnie ważne, gdy zmieniono bazę danych lub zmodyfikowano wymagania przetwarzania).

- Zmontuj fizyczny projekt. Ten etap i cały cykl życia SSADM są zakończone tym krokiem. Dostarczono wiele produktów, w tym definicje funkcji, zoptymalizowany projekt danych fizycznych, katalog wymagań oraz szacunki czasu i przestrzeni.

9.2 Szybkie tworzenie aplikacji (RAD)

Dowody z niepowodzeń projektów w projektach w latach 80. i 90. XX w. Wskazują, że tradycyjne metodologie strukturalne mają tendencję do dostarczania systemów, które przybywają zbyt późno i dlatego nie spełniają już swoich pierwotnych wymagań. Tradycyjne metody mogą zawieść na kilka sposobów:

- Luka w zrozumieniu między użytkownikami i programistami. Użytkownicy mają mniejszą wiedzę na temat tego, co jest możliwe i praktyczne z punktu widzenia technologii, podczas gdy programiści mogą być mniej świadomi kwestii związanych z podejmowaniem decyzji biznesowych, które stanowią wyzwanie dla rozwoju systemu.

- Tendencja programistów do odizolowania się od użytkowników. Historycznie rzecz biorąc, twórcy systemów byli w stanie ukryć się za ścianą żargonu, co sprawia, że społeczność użytkowników znajduje się w niekorzystnej sytuacji podczas omawiania problemów z IS / IT. Podczas gdy niektóre żargony mogą być konieczne, jeśli punkty mają być zwięzłe, często są wykorzystywane do ukrywania słabych postępów w konkretnym projekcie deweloperskim. Tendencję do izolacji wzmacnia fizyczne oddzielenie personelu komputerowego we własnych klimatyzowanych pomieszczeniach komputerowych. Deweloperzy mogą argumentować w swojej obronie, że użytkownicy mają również swój własny żargon związany z domeną, co zwiększa problem z odszyfrowywaniem wymagań.

- Jakość mierzona bliskością produktu do specyfikacji. Jest to podstawowa trudność - spostrzeżenie, że "system wykonuje dokładnie to, co określona w specyfikacji", oznacza, że system nadal nie dostarcza informacji, których użytkownicy potrzebują do celów decyzyjnych. Rzeczywisty nacisk powinien być położony na porównanie wyników z wymaganiami, a nie na wyniki ze specyfikacją, która była odzwierciedleniem postrzeganej potrzeby w określonym momencie.

- Długie czasy rozwoju. Spojrzenie wstecz na poprzednią sekcję na temat SSADM i modelu wodospadu ujawni, że procesy analizy i projektowania mogą być bardzo pracochłonne i czasochłonne. Czasu na rozwój nie pomaga fakt, że organizacja może borykać się z szybko zmieniającymi się warunkami biznesowymi, a wymagania również mogą ulec zmianie. Istnieje ryzyko, że syndrom "ruchomych bramek" spowoduje spustoszenie z tradycyjnym podejściem do rozwoju systemów.

- Potrzeby biznesowe zmieniają się w trakcie procesu rozwoju. Nawiązuje się do powyższego. Potrzebna jest metoda, w której możliwe są kolejne iteracje w procesie rozwoju, tak aby można było uwzględnić najnowsze wymagania.

- To, co otrzymują użytkownicy, niekoniecznie jest tym, czego chcą. Pierwszy użytkownik może zobaczyć nowy system informacyjny na etapie testowania lub szkolenia. W tym momencie okaże się, czy system dostarczony przez profesjonalistów IS / IT jest tym, czego faktycznie potrzebuje użytkownik. Odpowiednią analogią jest tutaj zakup domu lub samochodu, po prostu na podstawie rozmów z agentem nieruchomości lub garażem, zamiast przez faktyczne odwiedzenie domu lub prowadzenie samochodu. Jest mało prawdopodobne, że coś zakupione w ten sposób doprowadzi do zadowolenia klienta i nie ma powodu przypuszczać, że systemy informacyjne opracowane w podobny sposób będą bardziej skuteczne.

Nie tylko istnieje presja ze strony użytkowników końcowych na szybsze tworzenie systemów, ale same działy IS / IT coraz częściej dostrzegają potrzebę bardziej efektywnego wykorzystania ograniczonych zasobów ludzkich w swoich działach, a jednocześnie szybko dostarczają systemy zapewniające korzyści biznesowe. Wszystko to w klimacie szybkiej zmiany biznesu, a zatem szybko zmieniających się potrzeb informacyjnych. Szybkie tworzenie aplikacji (RAD) jest możliwym rozwiązaniem tych problemów i presji. Wykorzystuje to prototypowanie do angażowania użytkowników i zwiększania szybkości rozwoju. Rapid Application Development (RAD) to metoda opracowywania systemów informatycznych wykorzystujących prototypy w celu osiągnięcia zaangażowania użytkownika i szybszego rozwoju w porównaniu z tradycyjnymi metodami, takimi jak SSADM. Prototypowanie tworzy wstępną wersję części lub ramy wszystkich systemów informatycznych, które mogą być przeglądane przez użytkowników końcowych. Prototypowanie jest procesem iteracyjnym, w którym użytkownicy sugerują modyfikacje przed dalszymi prototypami i buduje się ostateczny system informacyjny.

9.3 Model spiralny

Model spiralny jest iteracyjnym modelem rozwoju systemów opracowanym przez Boehm (1988), który obejmuje ocenę ryzyka. Model spiralny został opracowany z uwagi na fakt, że projekty rozwoju systemów mają tendencję do powtarzania etapów analiza, projektowanie i kod w ramach procesu prototypowania. Każda spirala składa się z czterech głównych działań, którymi są:

- Planowanie. Ustalanie celów projektu, definiowanie alternatyw.

-- Ocena ryzyka. Analiza rozwiązań alternatywnych oraz identyfikacja i rozwiązanie ryzyka.

-- Inżynieria. Odpowiednik fazy budowy SDLC z kodowaniem i testowaniem.

- Ocena klienta. Testowanie produktu przez klientów.

Model jest ściśle powiązany z RAD, ponieważ implikuje iteracyjny rozwój z możliwością przeglądu po każdej iteracji lub spirali, co odpowiada produkcji jednej wersji prototypowej lub przyrostowej. Przed rozpoczęciem pierwszej spirali tworzony jest plan wymagań, więc można zauważyć, że model spiralny nie opisuje fazy inicjacji i analizy SDLC, koncentrując się na projektowaniu i budowaniu. Chociaż model spiralny nie był powszechnie stosowany w przemyśle, zwolennicy tego modelu twierdzą, że obejmuje ono najlepsze cechy zarówno klasycznego SDLC, jak i podejścia do prototypowania. Dodaje również walidację wymagań i projektu, wraz z analizą ryzyka, która jest często pomijana w projektach RAD.

9.4 Model dojrzałości zdolności

Kolejny wpływowy model najlepszych praktyk w rozwoju BIS to Model Dojrzałości Pojemności dla Oprogramowania. Ten model, który został zrewidowany w latach 90. i w nowym tysiącleciu, zmusza organizacje do przeglądu procesu opracowywania systemów. Stanowi on ramy dla menedżerów do oceny obecnego zaawansowania procesu opracowywania systemów. Model ma pięć etapów. Są one opisane przez instytut jako:

-- Inicjał. Proces oprogramowania jest określany jako ad hoc, a czasami nawet chaotyczny. Niewiele procesów jest zdefiniowanych, a sukces zależy od indywidualnego wysiłku i heroizmu.

- Powtarzalny. Podstawowe procesy zarządzania projektami są ustalane w celu śledzenia kosztów, harmonogramu i funkcjonalności. Konieczna jest dyscyplina procesowa, aby powtórzyć wcześniejsze sukcesy w projektach o podobnych aplikacjach.

- Zdefiniowany. Proces oprogramowania do zarządzania i inżynierii jest udokumentowany, ustandaryzowany i zintegrowany ze standardowym procesem oprogramowania dla organizacji. Wszystkie projekty wykorzystują zatwierdzoną, dostosowaną wersję standardowego procesu oprogramowania organizacji do tworzenia i utrzymywania oprogramowania.

-Zarządzane. Szczegółowe pomiary procesu oprogramowania i jakości produktu są gromadzone. Zarówno proces oprogramowania, jak i produkty są ilościowo rozumiane i kontrolowane.

- Optymalizacja. Ciągłe doskonalenie procesów jest możliwe dzięki ilościowym informacjom zwrotnym z procesu oraz pilotowaniu innowacyjnych pomysłów i technologii.

10 Bezpieczeństwo systemów informatycznych

Rolą komputerowych mechanizmów kontrolnych i bezpieczeństwa jest ochrona systemów przed przypadkowymi niefortunnymi przypadkami oraz celową kradzieżą i korupcją danych i aplikacji, a także pomoc organizacjom w zapewnieniu, że ich działania informatyczne są zgodne z prawem oraz z oczekiwaniami pracowników i klientów w zakresie prywatności. W tej sekcji omówiono zagrożenia bezpieczeństwa dla systemów informatycznych przed wprowadzeniem metod ochrony systemów informatycznych przed tymi zagrożeniami. Szczególny nacisk położono na obszary wirusów komputerowych i zagrożeń dla usług internetowych.

10.1 Zagrożenia bezpieczeństwa w systemach informatycznych

Kontrola nad systemami informatycznymi opiera się na dwóch podstawowych zasadach: konieczności zapewnienia dokładności danych przechowywanych przez organizację oraz potrzeby ochrony przed utratą lub uszkodzeniem. Najczęstsze zagrożenia napotykane przez systemy informacji organizacyjnej można umieścić w następujących kategoriach wypadków, klęsk żywiołowych, sabotażu (przemysłowego i indywidualnego), aktów wandalizmu, kradzieży, nieuprawnionego użycia (hakowania) i wirusów komputerowych, które zostaną teraz opisane.

10.1.1 Wypadki

Szereg szacunków sugeruje, że 40-65% wszystkich szkód wyrządzonych systemom informatycznym lub danych korporacyjnych powstaje w wyniku błędu ludzkiego. Oto kilka przykładów sposobów, w jakie mogą wystąpić ludzkie błędy:

- Niedokładne wprowadzanie danych. Jako przykład rozważ typowy system zarządzania relacyjnymi bazami danych, w którym kwerendy aktualizacji służą do zmiany rekordów, tabel i raportów. Jeśli zawartość zapytania jest niepoprawna, mogą wystąpić błędy we wszystkich danych manipulowanych przez zapytanie. Chociaż ekstremalne, znaczące problemy mogą być spowodowane przez dodanie lub usunięcie pojedynczego znaku do zapytania.

- Próby wykonania zadań wykraczających poza zdolność pracownika. W mniejszych komputerowych systemach informatycznych częstą przyczyną przypadkowego uszkodzenia są użytkownicy próbujący instalować nowe elementy sprzętowe lub aplikacje. W przypadku aplikacji, istniejące dane mogą zostać utracone, gdy program zostanie zainstalowany lub program może nie działać zgodnie z oczekiwaniami.

- Niezastosowanie się do procedur korzystania z organizacyjnych systemów informatycznych. Tam, gdzie procedury organizacyjne są niejasne lub nie pozwalają przewidzieć potencjalnych problemów, użytkownicy często mogą ignorować ustalone metody, działać z własnej inicjatywy lub nieprawidłowo wykonywać zadania.

- Niewykonanie procedur tworzenia kopii zapasowych lub weryfikacja kopii zapasowych danych. Oprócz regularnego tworzenia kopii zapasowych ważnych danych biznesowych konieczne jest również sprawdzenie, czy wykonane kopie zapasowe są dokładne i wolne od błędów.

10.1.2 Klęski żywiołowe

Wszystkie systemy informacyjne są podatne na uszkodzenia spowodowane przez zjawiska naturalne, takie jak burze, uderzenia pioruna, powodzie i trzęsienia ziemi. W Japonii i Stanach Zjednoczonych przykłada się wielką wagę do ochrony krytycznych systemów informatycznych przed skutkami trzęsień ziemi. Chociaż takie zagrożenia stanowią mniejszy problem w znacznej części Europy, odpowiednio zaprojektowane systemy uwzględniają nieoczekiwane klęski żywiołowe.

10.1.3 Sabotaż

W odniesieniu do systemów informacyjnych sabotaż może być celowy lub niezamierzony i przeprowadzany indywidualnie lub jako akt sabotażu przemysłowego. Indywidualny sabotaż jest zwykle przeprowadzany przez niezadowolonego pracownika, który chce dokonać jakiejś formy zemsty na swoim pracodawcy. Bomba logiczna (czasami określana jako "bomba zegarowa") jest dobrze znanym przykładem tego, jak pracownik może spowodować celowe uszkodzenie systemów informatycznych organizacji. Bomba logiczna to destrukcyjny program, który aktywuje się w określonym czasie lub w reakcji na określone wydarzenie. W większości przypadków bomba logiczna jest aktywowana kilka miesięcy po opuszczeniu organizacji przez pracownika. Zwykle skutkuje to odsunięciem podejrzenia od pracownika. Inny znany przykład nazywa się tylnymi drzwiami. Tylne drzwi to sekcja kodu programu, która umożliwia użytkownikowi obejście procedur bezpieczeństwa w celu uzyskania pełnego dostępu do systemu informacyjnego. Chociaż tylne drzwi mają uzasadnione zastosowania, takie jak testowanie programów, mogą również służyć jako narzędzie sabotażu. Należy jednak zauważyć, że indywidualny sabotaż staje się coraz mniejszy ze względu na przepisy takie jak ustawa o komputerowym nadużyciu. Sabotaż przemysłowy uważany jest za rzadki, chociaż w ciągu ostatnich kilku lat pojawiło się wiele głośnych spraw. Sabotaż przemysłowy jest zwykle przeprowadzany w celu uzyskania pewnego rodzaju korzyści konkurencyjnych lub finansowych.

Działania zaangażowanych stron są zazwyczaj wysoce zorganizowane, ukierunkowane na konkretne obszary działalności konkurencyjnej organizacji i wspierane przez dostęp do znacznej bazy zasobów. Sabotaż przemysłowy jest uważany za poważniejszy niż sabotaż indywidualny, ponieważ chociaż liczba wystąpień jest stosunkowo niewielka, poniesione straty są wyjątkowo wysokie. Zamiarem spowodowania utraty lub uszkodzenia nie musi być obecność, aby mógł nastąpić sabotaż. Wyobraźmy sobie przypadek organizacji wprowadzającej nowy system informacyjny w krótkim czasie i bez odpowiednich konsultacji z personelem. Pracownicy mogą czuć się zagrożeni przez nowy system i mogą chcieć uniknąć korzystania z niego. Typową reakcją może być niepoprawne wprowadzanie danych w celu zdyskredytowania nowego systemu. Alternatywnie pracownik może nadal wykonywać zadania ręcznie (lub ze starszym systemem), twierdząc, że jest to bardziej skuteczny sposób pracy. W takich przypadkach główną motywacją pracownika jest zabezpieczenie swojej pozycji, że uszkodzenie lub utrata systemu informatycznego organizacji jest uboczna w stosunku do tego celu

10.1.4 Wandalizm

Umyślne uszkodzenia sprzętu, oprogramowania i danych uważane są za poważne zagrożenie dla bezpieczeństwa systemów informatycznych. Zagrożenie związane z wandalizmem polega na tym, że organizacji tymczasowo odmawia się dostępu do niektórych jej zasobów. Nawet stosunkowo niewielkie uszkodzenie części systemu może mieć znaczący wpływ na organizację jako całość. Na przykład w małym systemie sieciowym uszkodzenie serwera lub współużytkowanego urządzenia pamięci masowej może skutecznie zahamować pracę wszystkich podłączonych do sieci. W większych systemach ograniczony przepływ pracy przez jedną część organizacji może tworzyć wąskie gardła, zmniejszając ogólną produktywność całej organizacji. Uszkodzenie lub utrata danych może mieć poważniejsze skutki, ponieważ organizacja nie może korzystać z danych, dopóki nie zostanie zastąpiona. Koszty związane z wymianą uszkodzonych lub utraconych danych mogą znacznie przewyższyć wszelkie straty wynikające z uszkodzenia sprzętu lub oprogramowania. Przykładowo, opóźnienia spowodowane koniecznością wymiany sprzętu lub danych mogą sprawić, że organizacja nie będzie w stanie konkurować o nowe firmy, co zaszkodzi ogólnej rentowności firmy. W ostatnich latach wandalizm został rozszerzony na Internet. Pojawiło się wiele incydentów, w których witryny firmowe zostały zniszczone.

10.1.5 Kradzież

Podobnie jak w przypadku wandalizmu utrata ważnych urządzeń, oprogramowania lub danych może mieć znaczący wpływ na efektywność organizacji. Kradzież można podzielić na dwie podstawowe kategorie: kradzież fizyczna i kradzież danych. Kradzież fizyczna, jak to się mówi, obejmuje kradzież sprzętu i oprogramowania. Kradzież danych zwykle wiąże się z wykonywaniem kopii ważnych plików bez powodowania szkody dla oryginałów. Jeśli jednak oryginalne pliki zostaną zniszczone lub uszkodzone, wartość skopiowanych danych zostanie automatycznie zwiększona. Organizacje usługowe są szczególnie narażone na kradzież danych, ponieważ ich działania polegają głównie na dostępie do korporacyjnych baz danych. Wyobraź sobie konkurenta uzyskującego dostęp do listy klientów należącej do organizacji sprzedaży. Bezpośrednim skutkiem takiego wydarzenia byłoby umieszczenie obu organizacji na zasadniczo równych zasadach. Jednak w dłuższej perspektywie pierwsza organizacja nie będzie już cieszyć się przewagą konkurencyjną i ostatecznie może przestać istnieć. Zarówno kradzież danych, jak i kradzież fizyczna mogą przybierać różne formy. Przykładem jest rosnący niepokój związany z kradzieżą informacji o klientach, takich jak dane karty kredytowej, z witryn firmowych.

10.1.6 Nieautoryzowane użycie

Jednym z najczęstszych zagrożeń bezpieczeństwa w stosunku do skomputeryzowanych systemów informacyjnych jest niebezpieczeństwo nieuprawnionego dostępu do poufnych danych. Wbrew

powszechnemu przekonaniu, które zachęcają media, ryzyko hakerów, uzyskanie dostępu do systemu informacji korporacyjnych jest stosunkowo niewielki. Większość naruszeń bezpieczeństwa związanych z poufnymi danymi można przypisać pracownikom organizacji. W wielu przypadkach naruszenia są przypadkowe, ponieważ pracownicy nie są świadomi, że określone zestawy informacji są ograniczone. Celowe naruszenia są zazwyczaj wynikiem pracownika, który chce uzyskać jakąś osobistą korzyść z wykorzystania uzyskanych informacji. Jednak musimy wziąć pod uwagę, że zagrożenie, jakie stwarzają hakerzy, zaczyna się zwiększyć, ponieważ coraz więcej organizacji korzysta z Internetu w celach biznesowych. Ponadto należy zauważyć, że nawet stosunkowo niewielka liczba incydentów hakerskich może stanowić poważne straty dla przemysłu. Haker to osoba, która próbuje uzyskać nieautoryzowany dostęp do komputerowego systemu informacyjnego, zwykle za pośrednictwem łącze telekomunikacyjne. Jednak jest to popularne użycie tego terminu i wielu specjalistów IT uważa je za nieprawidłowe. Tradycyjnie "hakowanie" odnosiło się do procesu pisania kodu programu, więc hakerzy byli niczym więcej niż wykwalifikowanymi programistami komputerowymi. Nawet dzisiaj wielu ludzi uważa się za "hakerów" tradycyjnego rodzaju, a niechęć do skojarzenia ze stereotypem przestępcy komputerowego. Ponadto wiele osób wprowadza rozróżnienia między nimi którzy usiłują uzyskać nieautoryzowany dostęp do komputerowych systemów informatycznych ze szkodliwych przyczyn i z innymi motywacjami. Osoba uzyskująca dostęp do systemu informatycznego ze szkodliwych przyczyn jest często określana jako cracker, a nie haker. Podobnie, wiele osób twierdzi, że używa hakerów do celów etycznych, takich jak pomoc firmom w identyfikacji wad bezpieczeństwa lub pomoc organom ścigania w zatrzymywaniu przestępców. Ogólnie rzecz biorąc, większość ludzi uważa hakerów za jedną z trzech kategorii tych, którzy chcą zademonstrować swoje umiejętności obsługi komputera, przechytrzając projektantów określonego systemu, tych, którzy chcą uzyskać jakąś formę korzyści (zwykle finansowej) przez kradzież, zmianę lub usuwanie informacji poufnych i tych, którzy chcą wyrządzić szkodę systemowi informatycznemu, być może jako akt zemsty na byłym pracodawcy. Zrozumiałe jest, że najczęstsze przestępstwo popełniane przez hakerów wiąże się z oszustwami telekomunikacyjnymi. Najwyraźniej pierwszym zadaniem większości hakerów jest uzyskanie bezpłatnych połączeń telefonicznych, aby czasochłonne zadanie włamania do danego systemu można było wykonać bez ponoszenia ogromnych kosztów. Jednak rozwój cyfrowej technologii komunikacyjnej oznacza, że możliwe jest wprowadzenie środków zaradczych przeciwko hakerstwu.

10.1.7 Wirusy komputerowe

Istnieje kilka różnych rodzajów wirusów komputerowych. Niektóre przykłady obejmują:

- Wirus linków dołącza się do struktury katalogów na dysku. W ten sposób wirus może manipulować informacjami o plikach i katalogach. Wirusy linków mogą być trudne do usunięcia, ponieważ zostają osadzone w danych, których dotyczy problem. Często próby usunięcia wirusa mogą spowodować utratę danych.

- Pasożytnicze wirusy umieszczają swoje kopie w legalnych programach, takich jak pliki systemu operacyjnego, często nie starając się ukryć swojej obecności. W ten sposób za każdym razem, gdy uruchamiany jest plik programu, również wirus. Ponadto większość wirusów jest tworzona jako programy rezydentne i rezydentne (TSR). Po aktywacji wirus pozostaje w pamięci komputera wykonując różne operacje w tle. Operacje takie mogą obejmować tworzenie dodatkowych kopii lub usuwanie plików na dysku twardym.

- Wirusy makr tworzone są przy użyciu wysokopoziomowych języków programowania znajdujących się w pakietach e-mail, przeglądarkach internetowych i aplikacjach, takich jak edytory tekstu. Technicznie, takie wirusy są wyjątkowo prymitywne, ale mogą powodować znaczne szkody.

Z możliwym wyjątkiem antywirusów (opisanych bardziej szczegółowo później), wszystkie wirusy należy uznać za szkodliwe. Nawet jeśli program antywirusowy nie robi nic więcej niż sam się reprodukuje, może nadal powodować awarie systemu i utratę danych. W wielu przypadkach uszkodzenia spowodowane przez wirus komputerowy mogą być przypadkowe, powstałe jedynie w wyniku złego programowania. Istnieją również dowody sugerujące, że wirusy mogą powodować fizyczne uszkodzenia elementów sprzętowych. Możliwe jest na przykład skonstruowanie wirusa, który nakazuje kontrolerowi dysku podjęcie próby odczytania nieistniejącej ścieżki, powodując natychmiastowe i nieodwracalne uszkodzenie dysku twardego. Do niedawna uważano, że wirusów komputerowych nie można dołączać do plików danych, takich jak dokumenty do edycji tekstu lub wiadomości e-mail. Jednak wbudowane języki programowania występujące w wielu nowoczesnych aplikacjach oznaczają, że pliki danych mogą być teraz używane do przesyłania wirusów. Jednak prawdą jest, że wirusy nie mogą być przesyłane za pomocą zwykłej wiadomości e-mail. Wirus może być przesyłany tylko jako załącznik do wiadomości lub jeśli używany pakiet e-mail zezwala na aktywną zawartość. Dwa inne rodzaje programów są związane z wirusami komputerowymi; robaki i trojany. Robak to mały program, który porusza się w systemie komputerowym losowo zmieniając lub zastępując fragmenty danych podczas ich przenoszenia. Trojan pojawia się jako legalny program w celu uzyskania dostępu do systemu komputerowego. Trojany są często używane jako systemy dostarczania wirusów komputerowych.

10.2 Ograniczanie zagrożeń do systemów informatycznych

Ogólnie rzecz biorąc, istnieją cztery główne podejścia, które można zastosować w celu zapewnienia integralności systemu informacyjnego. Są to powstrzymywanie, odstraszanie, zaciemnianie i odzyskiwanie. Chociaż każda strategia jest omawiana osobno, należy zauważyć, że skuteczna polityka bezpieczeństwa będzie opierać się na różnych koncepcjach i technikach.

10.2.1 Ograniczanie

Strategia powstrzymywania próbuje kontrolować dostęp do systemu informacyjnego. Jedno podejście polega na tym, aby potencjalne cele były możliwie nieatrakcyjne. Można to osiągnąć na kilka sposobów, ale wspólna metoda polega na stworzeniu wrażenia, że docelowy system informacji zawiera dane o niewielkiej wartości lub o zerowej wartości. Byłoby bezcelowe, na przykład, próba kradzieży danych, które zostały zaszyfrowane, dane byłyby faktycznie bezużyteczne dla nikogo poza właścicielem. Druga technika polega na stworzeniu skutecznej serii obrony przed potencjalnymi zagrożeniami. Jeśli wydatek, czas i wysiłek wymagany do uzyskania dostępu do systemu informacyjnego są większe niż korzyści wynikające z uzyskania dostępu, ingerencja staje się mniej prawdopodobna. Należy jednak nieustannie ulepszać i ulepszać mechanizmy obronne, aby nadążać za postępem technologicznym i rosnącą wyrafinowaniem hakerów. Tak więc, podejście takie wydaje się być kosztowne pod względem zasobów organizacyjnych. Trzecie podejście polega na usunięciu docelowego systemu informacji z potencjalnych zagrożeń. Typowe sposoby, w jakie można to osiągnąć, obejmują dystrybucję aktywów na dużym obszarze geograficznym, dystrybucję ważnych danych w całej organizacji lub izolowanie ważnych systemów.

10.2.2 Odstraszanie

Strategia oparta na odstraszaniu wykorzystuje groźbę kary, aby zniechęcić potencjalnych intruzów. Ogólnym podejściem jest przewidywanie i przeciwdziałanie motywacjom osób, które najprawdopodobniej zagrażają bezpieczeństwu systemu. Powszechna metoda polega na ciągłym reklamowaniu i wzmacnianiu kar za nieautoryzowany dostęp. Nierzadko zdarza się, że pracownik jest zwolniony z pracy w celu uzyskania dostępu do poufnych danych. Podobnie nierzadko zdarza się organizacjom wnieść prywatne oskarżenia przeciwko osobom, które spowodowały szkody lub straty w

ważnych systemach informatycznych. Próby naruszenia bezpieczeństwa systemu informatycznego są zniechęcane przez nagłaśnianie udanych działań przeciwko pracownikom lub innym stronom. Drugie podejście polega na próbie wykrycia potencjalnych zagrożeń tak wcześnie, jak to możliwe, na przykład poprzez monitorowanie wzorców korzystania z systemu informacyjnego i badanie wszystkich anomalii. Jednakże, chociaż taka technika może zapobiec niektórym atakom i zmniejszyć szkody spowodowane przez innych, może być kosztowna pod względem zasobów organizacyjnych. Trzecia stosowana technika zazwyczaj polega na przewidywaniu prawdopodobnych obszarów ataku, a następnie wprowadzaniu odpowiednich zabezpieczeń lub środków zaradczych. Jeśli organizacja odczuwa na przykład, że jest szczególnie podatna na wirusy komputerowe, może zainstalować oprogramowanie do skanowania antywirusowego w całej organizacji.

10.2.3. Obfuskacja

Obfuscation zajmuje się ukrywaniem lub dystrybucją aktywów, tak aby wszelkie spowodowane szkody mogły być ograniczone. Jednym ze sposobów realizacji takiej strategii jest monitorowanie wszystkich działań organizacji, a nie tylko tych związanych z korzystaniem z jej systemów informacyjnych. Zapewnia to bardziej kompleksowe podejście do bezpieczeństwa niż powstrzymywanie lub odstraszanie, ponieważ zapewnia również środek ochrony przed kradzieżą i innymi zagrożeniami. Druga metoda polega na przeprowadzaniu regularnych audytów danych, sprzętu, oprogramowania i środków bezpieczeństwa. W ten sposób organizacja ma pełniejszy przegląd swoich systemów informatycznych i może dokładniej oceniać zagrożenia. Na przykład regularny audyt oprogramowania może skutkować zmniejszeniem użycia nielegalnego oprogramowania. To z kolei może zmniejszyć liczbę infekcji wirusowych w organizacji, uniknąć potencjalnych sporów z firmami zajmującymi się oprogramowaniem i wykryć nielegalne lub nieautoryzowane korzystanie z programów i danych. Rozproszenie zasobów w kilku lokalizacjach może być wykorzystane do zniechęcenia potencjalnych intruzów i może również ograniczyć szkody spowodowane przez udany atak. Zastosowanie innych technik, takich jak procedury tworzenia kopii zapasowych, może zostać wykorzystane do dalszego ograniczenia zagrożeń.

10.2.4 Odzyskiwanie

Strategia oparta na odzyskiwaniu uznaje, że bez względu na to, jak dobrze się broni, w końcu dojdzie do naruszenia bezpieczeństwa systemu informatycznego. Taka strategia w dużej mierze dotyczy zapewnienia normalnego działania informacji system zostanie przywrócony tak szybko, jak to możliwe, z jak najmniejszymi zakłóceniami w organizacji, jak to możliwe. Najważniejszym aspektem strategii opartej na odzyskiwaniu jest staranne planowanie organizacyjne. Opracowanie procedur awaryjnych, które dotyczą szeregu nieprzewidzianych wypadków, jest niezbędne, jeżeli ma nastąpić pomyślne wyleczenie. Przewidując uszkodzenie lub utratę, duży nacisk kładzie się na procedury tworzenia kopii zapasowych i środki odzyskiwania. W dużych organizacjach może zostać utworzona strona zapasowa, dzięki czemu przetwarzanie danych może zostać natychmiast przełączone na witrynę dodatkową w razie sytuacji awaryjnej. Mniejsze organizacje mogą korzystać z innych środków, takich jak urządzenia RAID lub usługi hurtowni danych.

10.3 Rodzaje kontroli

Istnieje pięć głównych kategorii kontroli, które można zastosować w systemach informatycznych. Są to: ochrona fizyczna, kontrola biometryczna, kontrola telekomunikacyjna, kontrola awarii i audyt.

10.3.1 Ochrona fizyczna

Ochrona fizyczna obejmuje stosowanie fizycznych barier mających na celu ochronę przed kradzieżą i nieuprawnionym dostępem. Uzasadnienie takiego podejścia jest niezwykle proste: jeśli dostęp do pomieszczeń i sprzętu jest ograniczony, ryzyko kradzieży i wandalizmu jest ograniczone. Ponadto, uniemożliwiając dostęp do sprzętu, jest mniej prawdopodobne, że nieupoważniony użytkownik uzyska dostęp do poufnych informacji. Zamki, bariery i łańcuchy bezpieczeństwa są przykładami tej formy kontroli.

10.3.2 Kontrola biometryczna

Kontrole te wykorzystują unikalne cechy osób w celu ograniczenia dostępu do newralgicznych informacji lub sprzętu. Skanery sprawdzające odciski palców, odciski głosu, a nawet wzory siatkówki są przykładami kontroli biometrycznych. Do niedawna wydatki związane z biometrycznymi systemami kontroli umieszczały je poza zasięgiem wszystkich poza największymi organizacjami. Ponadto wiele organizacji wyraziło zastrzeżenia dotyczące dokładności metod rozpoznawania stosowanych do identyfikacji konkretnych osób. Jednak wraz z wprowadzeniem bardziej zaawansowanego sprzętu i oprogramowania, oba te problemy zostały w dużej mierze rozwiązane. Wiele organizacji zaczęło teraz szukać metod, dzięki którym biometryczne systemy kontroli mogą być wykorzystywane do ograniczania przypadków oszustw.

10.3.3 Kontrola telekomunikacyjna

Te elementy sterujące pomagają zweryfikować tożsamość konkretnego użytkownika. Typowe elementy kontroli komunikacji obejmują hasła i procedury sprawdzania poprawności użytkowników.

10.3.4 Kontrola awarii

Mechanizmy zapobiegania awariom próbują ograniczyć lub uniknąć uszkodzeń spowodowanych awarią systemu informatycznego. Typowe przykłady obejmują procedury odzyskiwania i regularne tworzenie kopii zapasowych danych. Kopie zapasowe są objaśnione bardziej szczegółowo w dalszej części.

10.3.5 Audyt

Audyt polega na regularnym analizie procedur, sprzętu, oprogramowania i danych. W odniesieniu do oprogramowania i danych, audyty mogą być przeprowadzane automatycznie za pomocą odpowiedniego programu. Oprogramowanie do audytu działa poprzez skanowanie dysków twardych dowolnych komputerów, terminali i serwerów podłączonych do systemu sieciowego. Po zeskanowaniu każdego dysku twardego, nazwy wszystkich znalezionych programów są dodawane do dziennika. Ten dziennik można następnie porównać do listy programów, które są prawnie własnością organizacji. Ponieważ dziennik zawiera informacje dotyczące miejsca pobytu każdego znalezionego programu, stosunkowo łatwo jest określić lokalizację nieautoryzowanych programów. W wielu organizacjach programy audytowe są również wykorzystywane do śledzenia licencji na oprogramowanie i umożliwiają firmom zapewnienie, że działają zgodnie z warunkami umów licencyjnych.

10.3.6 Wykrywanie i zapobieganie infekcji wirusowej

Ryzyko infekcji wirusowej można zredukować do minimum poprzez wdrożenie stosunkowo prostego zestawu środków bezpieczeństwa:

- nieuprawniony dostęp do maszyn i oprogramowania powinien być w miarę możliwości ograniczony;

- maszyny i oprogramowanie powinny być regularnie sprawdzane za pomocą programu do wykrywania wirusów;

- wszystkie nowe dyski i oprogramowanie pochodzące z zewnętrznego źródła powinny zostać sprawdzone przed użyciem za pomocą programu wykrywającego wirusy;

- dyskietki powinny być chronione przed zapisem, gdy tylko jest to możliwe, ponieważ fizycznie niemożliwe jest skopiowanie wirusa na dysk chroniony przed zapisem;

- należy regularnie tworzyć kopie zapasowe danych i plików programów w celu zminimalizowania szkód spowodowanych zainfekowaniem systemu przez wirus.

Skanery antywirusowe mają za zadanie wykrywać, a następnie bezpiecznie usuwać programy antywirusowe z systemu komputerowego. Najczęstsza metoda wykrywania używana przez te programy obejmuje skanowanie sygnatur poszczególnych wirusów. Często można zlokalizować wirusa, po prostu przeszukując każdy plik na zainfekowanym dysku pod kątem tych charakterystyk identyfikacyjnych. Jednakże, ponieważ nowe wirusy są wykrywane dość często, lista sygnatur zawartych w programie wykrywania szybko staje się przestarzała. Z tego powodu większość programistów twierdzi, że regularne aktualizacje programów są niezbędne. Jednak wprowadzenie nowych rodzajów wirusów, takich jak wirusy polimorficzne i ukryte, oznacza, że samo sprawdzanie podpisu nie może być dłużej uważane za całkowicie bezpieczną metodę wykrywania. Z tego powodu większość skanerów antywirusowych wykorzystuje kombinację technik zwiększających ich efektywność. Wśród stosowanych metod są sumy kontrolne, osłony wirusów, antywirusy, heurystyki i inokulacja. Tarcze wirusa to programy TSR, które stale monitorują i kontrolują dostęp do urządzeń pamięci masowej systemu. Każda nietypowa próba modyfikacji pliku lub zapisu na dysku spowoduje aktywację komunikatu z prośbą o autoryzację operacji. Podobne zadanie wykonują urządzenia wykrywające wirusy sprzętowe. Nowoczesne urządzenia zabezpieczające sprzęt mogą być bardzo wyrafinowane, z wykorzystaniem własnych procesorów, kontrolerów dysków i innych kosztownych komponentów. Jednak pomimo roszczeń producentów tych urządzeń, niewiele jest dowodów sugerujących, że są one bardziej skuteczne niż rozwiązania programowe. Po wykryciu wirusa istnieją trzy metody jego usunięcia. Pierwsza, dezynfekcja, próbuje przywrócić uszkodzone pliki i struktury katalogów do ich pierwotnego stanu. Jednak we wszystkich przypadkach dezynfekcja nie jest możliwa. Druga technika polega na zastąpieniu programu antywirusowego tak, aby został trwale i nieodwracalnie usunięty z dysku. Trzecią i ostatnią metodą usuwania wirusa jest przywrócenie kopii zapasowej zainfekowanego dysku do systemu. Proces zapisywania plików na dysk skutecznie zastępuje wirusa i przywraca system do pierwotnego stanu. Pomimo wyrafinowania programów skanujących, żaden nie jest w stanie zapewnić pełnej ochrony przed infekcjami. Przeprowadzono wiele testów w celu określenia wydajności określonych programów do skanowania antywirusowego. We wszystkich tych testach żaden program nie osiągnął jeszcze doskonałej oceny.

10.4 Techniki sterowania systemami informatycznymi

Niektóre z najpopularniejszych technik wykorzystywanych do sterowania komputerowymi systemami informatycznymi to: formalne zasady bezpieczeństwa, hasła, szyfrowanie plików, procedury organizacyjne regulujące korzystanie z komputerowych systemów informatycznych, techniki weryfikacji użytkowników i procedury tworzenia kopii zapasowych. Poniżej opisano każdą z tych technik bardziej szczegółowo.

10.4.1 Formalna polityka bezpieczeństwa

Być może najprostszą i najskuteczniejszą kontrolą jest sformułowanie kompleksowej polityki bezpieczeństwa. Spośród wielu różnych pozycji, taka polityka określi, co jest uważane za dopuszczalne użycie systemu informacyjnego, co jest uważane za niedopuszczalne korzystanie z systemu informacyjnego, sankcje dostępne w przypadku, gdy pracownik nie przestrzega zasad bezpieczeństwa

oraz szczegółowe informacje na temat istniejących kontroli, w tym ich formy i funkcji oraz planów dalszego ich rozwoju. Po sformułowaniu polityki należy ją opublikować, aby stała się skuteczna. Ponadto wsparcie kierownictwa jest niezbędne, aby zapewnić przestrzeganie przez pracowników wytycznych zawartych w polityce.

10.4.2 Hasła

Hasło stanowi jedną z najczęstszych form ochrony komputerowych systemów informatycznych. Oprócz zapewnienia prostych, niedrogich sposobów ograniczania dostępu do sprzętu i poufnych danych, hasła zapewniają także szereg innych korzyści. Wśród nich jest to, że dostęp do systemu można podzielić na poziomy poprzez wydawanie pracownikom różnych haseł na podstawie ich pozycji i wykonywanej pracy. Również działania pracownika mogą być regulowane i nadzorowane poprzez monitorowanie użycia hasła. W końcu, jeśli hasło zostanie wykryte lub skradzione przez stronę zewnętrzną, powinno być możliwe ograniczenie ewentualnych szkód wynikających z tego. Korzystanie z haseł może zachęcić pracowników do wzięcia części odpowiedzialności za ogólne bezpieczeństwo systemu.

10.4.3 Szyfrowanie

Dodatkową warstwę ochrony wrażliwych danych można zapewnić za pomocą technik szyfrowania. Nowoczesne metody szyfrowania polegają na użyciu jednego lub większej liczby kluczy. Bez prawidłowego klucza żadne zaszyfrowane dane nie mają znaczenia, a zatem nie mają wartości dla potencjalnego złodzieja.

10.4.4 Procedury organizacyjne

W normalnych okolicznościach zestaw procedur korzystania z systemu informacyjnego powstanie w wyniku formalnej polityki bezpieczeństwa. Takie procedury powinny szczegółowo opisywać prawidłowe działanie systemu i obowiązki użytkowników. Ponadto procedury powinny uwypuklać kwestie związane z bezpieczeństwem, powinny wyjaśniać niektóre uzasadnienia, a także opisywać kary za nieprzestrzeganie instrukcji.

10.4.5 Walidacja użytkownika

Znaczenie dla telekomunikacji polega na użyciu technik walidacji użytkownika. Konieczna jest weryfikacja tożsamości użytkowników próbujących uzyskać dostęp do systemu spoza organizacji. Hasło jest niewystarczające do zidentyfikowania użytkownika, ponieważ mogło zostać skradzione lub przypadkowo ujawnione innym. Jednakże, pytając o datę urodzenia lub inne dane osobowe, tożsamość użytkownika może zostać potwierdzona. Alternatywnie, jeśli lokalizacja użytkownika jest znana, system może spróbować wywołać użytkownika z powrotem w ich bieżącej lokalizacji. Jeśli użytkownik jest oryginalny, połączenie zostanie poprawnie nawiązane, a użytkownik uzyska dostęp do systemu. Chociaż takie metody nie zapewniają całkowitego bezpieczeństwa, ryzyko nieautoryzowanego dostępu może zostać dramatycznie zmniejszone.

10.4.6 Procedury tworzenia kopii zapasowych

Skutki nagłej utraty danych mogą wpływać na działalność firmy w różny sposób. Zakłócenia spowodowane normalną działalnością firmy mogą skutkować znacznymi stratami finansowymi spowodowanymi takimi czynnikami, jak stracone szanse, dodatkowe koszty handlowe i niezadowolenie klientów. Skumulowane skutki utraty danych mogą okazać się szkodliwe dla obszarów tak różnych, jak wizerunek firmy i morale pracowników. Być może najważniejszym powodem wprowadzenia skutecznych procedur tworzenia kopii zapasowych jest po prostu koszt związany z

odtwarzaniem utraconych danych. Jedną z najczęstszych metod ochrony cennych danych jest wykorzystanie techniki "ojciec-ojciec, syn". W tym przypadku wykorzystywany jest obrotowy zestaw dysków lub taśm zapasowych, dzięki czemu trzy różne wersje tych samych danych są przechowywane jednocześnie. Aby zilustrować tę metodę, wyobraź sobie jednego użytkownika pracującego z komputerem osobistym i używającego trzech dyskietek do przechowywania danych. Każdego dnia wszystkie przetwarzane dane są kopiowane na dysk zawierający najstarszą wersję ("dziadek") tych danych. Tworzy to ciągły cykl, który gwarantuje, że najstarsza kopia zapasowa nie będzie miała więcej niż trzy dni. Warto zwrócić uwagę na kilka ogólnych uwag dotyczących tworzenia kopii zapasowych danych:

- Czas, wysiłek i wydatki związane z tworzeniem kopii zapasowych zostaną zmarnowane, chyba że zostaną wykonane w regularnych odstępach czasu. To, jak często tworzone są kopie zapasowe, zależy w dużej mierze od ilości pracy przetworzonej w danym okresie. Ogólnie rzecz biorąc, kopie zapasowe będą tworzone częściej, ponieważ liczba transakcji wykonywanych każdego dnia wzrasta.

- Kopie zapasowe danych powinny być sprawdzane za każdym razem, gdy są produkowane. Wadliwe urządzenia pamięci masowej i nośniki mogą czasami powodować niekompletne lub zniekształcone kopie danych. Ponadto należy podjąć środki ostrożności przeciwko wirusom komputerowym, aby zapobiec uszkodzeniu przechowywanych danych.

- Zabezpieczenie kopii zapasowych należy zapewnić, przechowując je w bezpiecznym miejscu. Zazwyczaj organizacja produkuje dwa zestawy kopii zapasowych; jeden do przechowywania w zakładzie, drugi do usunięcia z lokalu i przechowywany w innym miejscu. W ten sposób poważna awaria, taka jak pożar w siedzibie firmy, nie spowoduje całkowitego zniszczenia danych organizacji. Warto zauważyć, że nie wszystkie dane muszą być archiwizowane w regularnych odstępach czasu. Aplikacje, na przykład, można normalnie szybko i łatwo przywrócić z oryginalnego nośnika. W podobny sposób, jeśli utworzono kopię zapasową danego elementu danych, tworzenie dodatkowych kopii może nie być konieczne. W celu skrócenia czasu potrzebnego na tworzenie kopii zapasowych wiele organizacji korzysta z oprogramowania, które umożliwia tworzenie przyrostowych kopii zapasowych. Początkowo tworzona jest kopia zapasowa wszystkich plików danych i dokłada się starań, aby zapewnić dokładność kopii. Ta początkowa, kompletna kopia zapasowa jest zwykle nazywana pełną kopią zapasową (czasami nazywaną również archiwalną kopią zapasową). Od tego momentu wyspecjalizowane oprogramowanie do tworzenia kopii zapasowych służy do wykrywania i kopiowania tylko tych plików, które zmieniły się w jakiś sposób od czasu utworzenia ostatniej kopii zapasowej. W przypadku utraty danych uszkodzone pliki można zastąpić, najpierw przywracając pełną kopię zapasową, a następnie przyrostowe kopie zapasowe. Jedną z głównych zalet tworzenia przyrostowych kopii zapasowych jest możliwość prześledzenia zmian dokonanych w plikach danych

czas. W ten sposób można zlokalizować i przywrócić dowolną wersję danego pliku.

10.5 Zagrożenia bezpieczeństwa dla usług internetowych

Pojawiło się wiele istotnych nowych zagrożeń dla systemów informacji organizacyjnych związanych z rosnącym zaufaniem do intranetów i Internetu jako podstawowych narzędzi do przeprowadzania transakcji z partnerami, dostawcami i klientami. Chociaż poniższe materiały koncentrują się na Internecie, wiele z nich ma również znaczenie dla firmowych sieci intranetowych.

10.5.1 Odmowa usługi (DoS)

Ponieważ firmy zaczynają polegać na technologii sieciowej, aby obniżyć koszty, stają się bardziej narażone na pewne ryzyko. Na przykład, więcej szkód może powstać, gdy dana osoba uzyskuje dostęp

do serwera sieciowego, niż gdy tylko uzyskuje dostęp do pojedynczegp komputera. Podobnie firmy polegające na Internecie w celu komunikacji biznesowej mogą podlegać atakom typu "odmowa usługi". Zazwyczaj te ataki obejmują blokowanie kanałów komunikacyjnych używanych przez firmę. Na przykład, system e-mail może zostać zaatakowany, wysyłając do firmy miliony długich wiadomości. Inne techniki obejmują zmianę stron internetowych firmy lub atakowanie systemów używanych do przetwarzania transakcji online. W takich przypadkach firmy są zazwyczaj zmuszane do zamykania usług do czasu rozwiązania problemu. Wpływ ataku typu "odmowa usługi" może być bardzo poważny, szczególnie w przypadku organizacji, które w dużym stopniu polegają na Internecie w zakresie handlu elektronicznego.

10.5.2 Trojany

Ostatnio gwałtownie wzrosło wykorzystanie trojanów do zakłócania działalności firmy lub uzyskania dostępu do poufnych informacji. Większość trojanów napotykanych przez organizacje biznesowe ma na celu zbieranie informacji i przekazywanie regularnych raportów właścicielowi. Zazwyczaj trojan będzie zawierał funkcję rejestrowania kluczy (czasami nazywaną "rejestratorem klawiszy") w celu przechwycenia wszystkich danych wprowadzanych z klawiatury z danego komputera. Przechwytywanie danych z klawiatury umożliwia właścicielowi trojana gromadzenie wielu informacji, takich jak hasła i zawartość wszystkich wychodzących wiadomości e-mail. Niektóre trojany zostały zaprojektowane w celu zapewnienia właścicielom kontroli nad docelowym systemem komputerowym. W rzeczywistości trojan działa jako aplikacja do zdalnego sterowania, umożliwiając właścicielowi wykonywanie czynności na komputerze docelowym tak, jakby siedzieli przed nim. Czasami właściciel trojana nie podejmuje żadnych działań, aby ukryć swoje działania: ofiara widzi podejmowane działania, ale nie może interweniować, nie wyłączając komputera. Częściej jednak trojan działa po cichu, a ofiara nie zdaje sobie sprawy, że na ich komputerze działają programy, usuwa pliki, wysyła wiadomości e-mail i tak dalej. Niektóre programy mają na celu zakłócenie działań firmy poprzez inicjowanie ataków typu "odmowa usługi" lub atakowanie serwerów firmowych. Jednak zdarzenia z udziałem tego rodzaju trojana są rzadkie, ponieważ często wymagają bardzo wysokiego poziomu dostępu do systemów firmy.

10.5.3 Kradzież tożsamości i nadużycia związane z marką

Kradzież tożsamości polega na wykorzystywaniu tożsamości innej osoby do przeprowadzania czynności, które obejmują wysyłanie zniesławiających wiadomości e-mail do dokonywania nieuczciwych zakupów. Uważa się za stosunkowo łatwe podszywanie się pod inną osobę w ten sposób, ale o wiele trudniej udowodnić, że komunikacja nie pochodzi od ofiary. W przypadku organizacji biznesowych istnieje zagrożenie podszywania się pod pracowników w celu składania fałszywych zamówień. Alternatywnie, firma może być zakłopotana, jeśli plotki lub fałszywe informacje prasowe są przesyłane przez Internet. Pojęcie nadużywania marki służy do objęcia szerokiej gamy działań, począwszy od sprzedaży podrobionych towarów, na przykład oprogramowania, po wykorzystanie dobrze znanej marki w celach komercyjnych. Na przykład nazwa dobrze znanej firmy może być osadzona na specjalnej stronie internetowej, dzięki czemu strona zyskuje wysoką pozycję w wyszukiwarce. Użytkownicy, którzy szukają nazwy firmy, zostaną prawdopodobnie przekierowani na specjalną stronę internetową, na której zamiast tego zostaną im zaoferowane towary konkurencji.

10.5.4 Wymuszenia

Do wyłudzania pieniędzy od firm takich jak cybersquatting i groźba ujawnienia informacji o klientach można zastosować różne podejścia. Cybersquatting obejmuje rejestrację domeny internetowej, którą prawdopodobnie chce posiadać firma lub celebryta. Chociaż sama rejestracja domeny nie jest sama w sobie nielegalna, niektóre osoby próbują wymuszać na różne sposoby pieniądze od firm lub celebrytów. Zazwyczaj właściciel domeny prosi o dużą kwotę w celu przeniesienia domeny do

zainteresowanej strony. Czasami jednak żądaniom dotyczącym pieniędzy mogą towarzyszyć groźby, takie jak zagrożenie, z którego domena zostanie wykorzystana w sposób, który zaszkodzi reputacji ofiary, chyba że zapłata zostanie zrealizowana. Chociaż istnieje ustalony mechanizm rozwiązywania sporów dotyczących nazw domen, wiele ofiar cybersquatting decyduje się nie korzystać z tych procedur, ponieważ nie chcą przyciągać negatywnej reklamy. Bardziej powszechna forma wymuszeń ma miejsce zwykle po naruszeniu bezpieczeństwa, w wyniku którego uzyskano poufne dane firmy. Często zagrożenie polega na udostępnianiu informacji konkurentom lub opinii publicznej, chyba że dokonano płatności.

10.5.5 Nadużycie zasobów

Organizacje zawsze musiały zapewniać, że pracownicy nie korzystają z zasobów firmy z przyczyn osobistych. Chociaż niektóre działania, takie jak wysyłanie okazjonalnych osobistych wiadomości e-mail, są tolerowane przez większość firm, zwiększona dostępność dostępu do Internetu i urządzeń poczty elektronicznej zwiększa ryzyko, że takie urządzenia mogą być nadużywane. Dwa przykłady zagrożeń związanych ze zwiększonym dostępem do Internetu obejmują oszustwa i cyberstalking. Cyberstalking to stosunkowo nowa forma przestępczości polegająca na nękaniu osób za pośrednictwem poczty elektronicznej i Internetu. Interesy dla organizacji biznesowych to fakt, że wielu prześladowców korzysta z urządzeń firmowych w celu prowadzenia swojej działalności. Zdarzały się również przypadki "stalkingu korporacyjnego", w którym organizacja wykorzystywała swoje zasoby do nękania osób lub konkurentów biznesowych. W przypadku organizacji konsekwencją cyberstalking może być utrata reputacji i groźba działania karnego i cywilnego.

10.5.6 Inne zagrożenia

W tej części omówiono dwa dodatkowe przykłady pojawiających się zagrożeń: cyberterroryzm i oszustwa giełdowe. Cyberterroryzm opisuje ataki na systemy informatyczne, które są motywowane przekonaniami politycznymi lub religijnymi. Organizacje zaangażowane w przemysł obronny często są ofiarami takich ataków. Jednak wiele innych firm jest również zagrożonych atakami o podłożu politycznym. Na przykład firmy handlujące w krajach, które są w zawirowaniach politycznych lub firmy z partnerami biznesowymi w tych krajach, również są narażone na takie ataki. Wiele niedawnych przypadków uwidoczniło niebezpieczeństwo rozpowszechniania w internecie niedokładnych lub wprowadzających w błąd informacji. Oszustwa giełdowe online polegają na sztucznym zwiększaniu lub zmniejszaniu wartości akcji poprzez rozpowszechnianie ostrożnie zaprojektowanych plotek na tablicach ogłoszeń i w pokojach rozmów. Chociaż takie działania mogą wydawać się stosunkowo nieszkodliwe, firmy mogą ponosić znaczne straty. Przypadki oszustw giełdowych w Internecie podkreślają niezwykle ważną kwestię: organizacje są narażone na ryzyko związane z dystrybucją fałszywych informacji przez Internet. Ważne jest, aby pamiętać, że skutki oszustw giełdowych online nie ograniczają się jedynie do wpływania na ceny akcji. Wyobraźmy sobie na przykład, co mogłoby się stać, gdyby fałszywe informacje prasowe zaczęły się pojawiać, gdy firma była w trakcie negocjacji fuzji lub strategicznego sojuszu. Zapobieganie pojawianiu się niedokładnych lub wprowadzających w błąd informacji w Internecie jest trudne. Sama wielkość Internetu oznacza, że monitorowanie stron internetowych, czatów i serwisów informacyjnych stanowi niedopuszczalne obciążenie dla zasobów nawet największych organizacji.