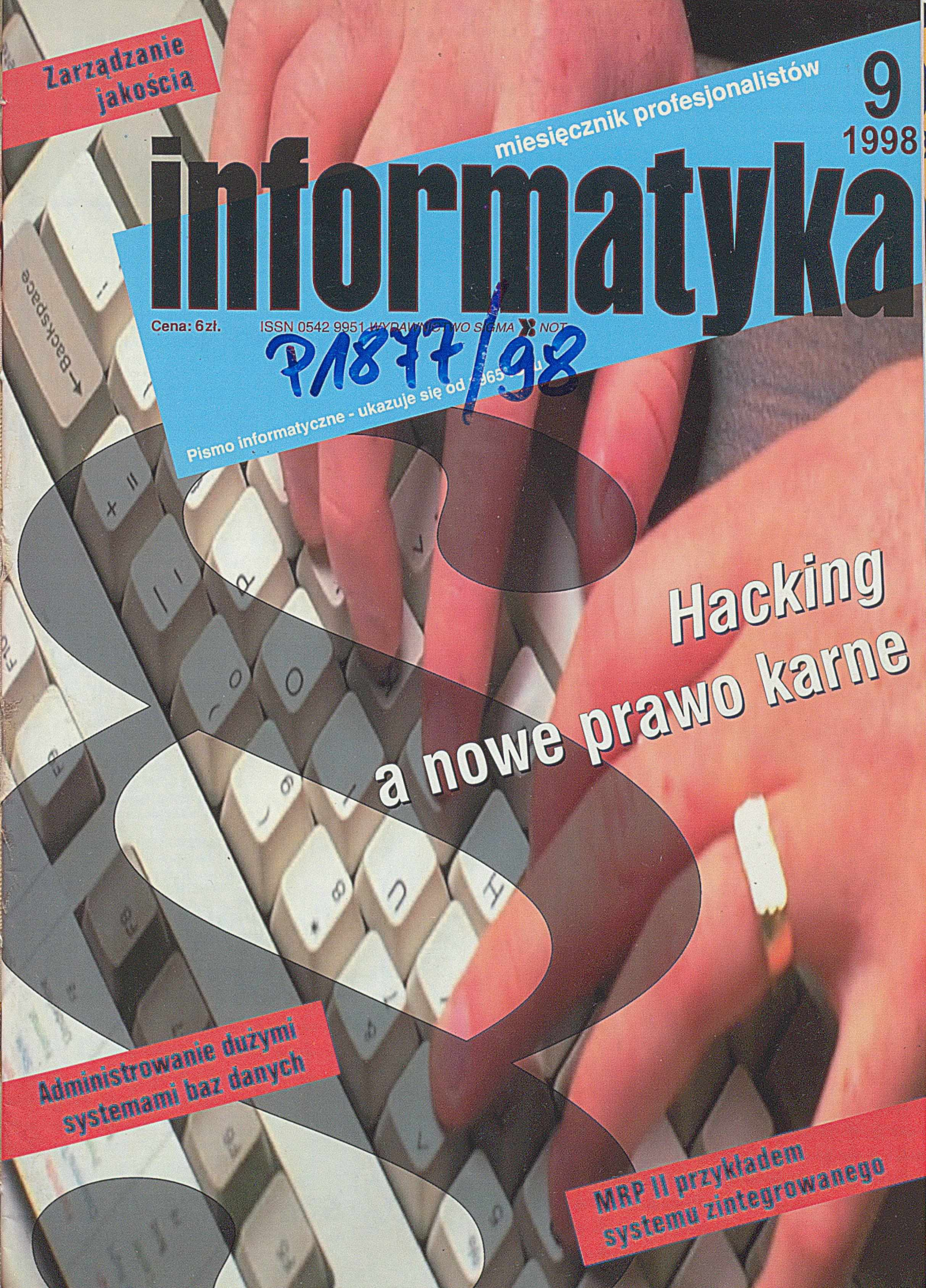


Zarządzanie jakością

miesięcznik profesjonalistów

9
1998

informatyka

Cena: 6 zł. ISSN 0542 9951 WYDAWNICTWO SIGMA NOT

Pismo informatyczne - ukazuje się od 1965 r.

Hacking a nowe prawo karne

Administrowanie dużymi systemami baz danych

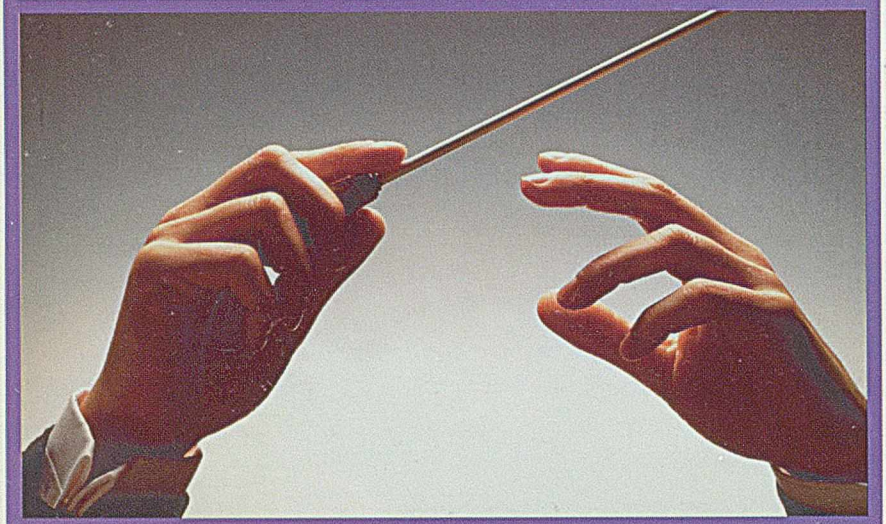
MRP II przykładem systemu zintegrowanego

Nowoczesny system zdalnej obsługi operacji pomiędzy bankiem a jego klientami, cechujący się wysokim bezpieczeństwem danych oraz łatwością obsługi.

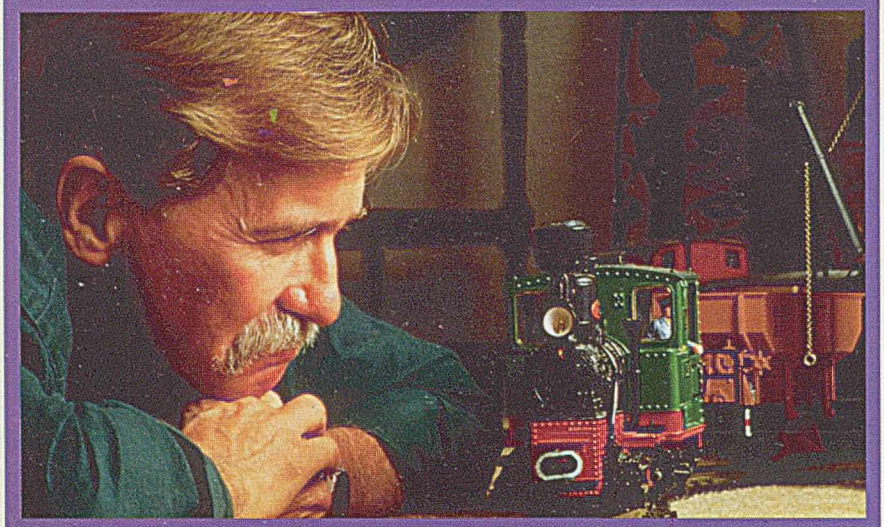
Zakres funkcjonalny obejmuje:
- możliwość integracji z systemem finansowo-księgowym przedsiębiorstwa
- dyspozycje bankowe i informacje o nich
- pocztę elektroniczną i wiele innych.

Klienci PKO BP, PBG Grupa PeKaO S.A., Banku Zachodniego S.A., BIG Banku Gdańskiego S.A. i wielu innych – domagajcie się instalacji systemu ***Net*Bank 2**!

***Net* BANK 2®**



Całkowita kontrola•



Absolutne bezpieczeństwo••

Niezwykła łatwość•••

• nad własnymi pieniędzmi
•• dokonywanych operacji
••• dostępu do środków informacji

SOFTBANK® S.A.
BANKOWOŚĆ I SYSTEMY BANKOWE
02-146 WARSZAWA, ul. 17 Stycznia 72a, tel. 878 62 00, fax 878 63 00

informatyka

Miesięcznik
ISSN 0542-9951
INDEKS 36124

nr 9 1998
Wrzesień
Rok wydania XXXIV

WYDAWCA:
Wydawnictwo Czasopism i Książek
Technicznych SIGMA NOT Spółka z o.o.
ul. Ratuszowa 11
00-950 WARSZAWA
skrytka pocztowa 1004

REDAKCJA:
00-950 Warszawa,
ul. Ratuszowa 11, p. 644, 628
skrytka pocztowa 1004
tel., fax: 619-11-61
tel.: 619-22-41 w. 159
e-mail: informat@pol.pl
www.pol.pl/informatyka/

PRENUMERATA:
tel. 40-35-89, 40-30-86
Prenumeratę przyjmujemy również
w sieci INTERNET:
WWW.pol.pl./sigma_not
E-mail: kolpor.sigma@pol.pl

Okładka:
AGAT, Jerzy Burski i Andrzej Jacyszyn
Łamanie:
Alina Klepacz, program PageMaker

Druk:
Drukarnia SIGMA NOT Sp. z o.o.

W numerze:

Uprzejmie informujemy, że począwszy od września br. w Internecie będą zamieszczane spisy treści kolejnych zeszytów czasopism, wydawanych przez Wydawnictwo SIGMA-NOT.

Czy jest w tym domu gospodarz?

Tylko wtedy czujemy, że jesteśmy we własnym domu, gdy możemy kontrolować to, co do niego przybywa oraz co ubywa. Nasz kraj jest domem, w którym nie tylko nie kontrolujemy przepływu towarów, ale nawet nie mamy pełnej wiedzy o tym, co, kto i kiedy do nas przywozi lub wywozi. Służby celne bez scentralizowanego systemu komputerowego są we współczesnym świecie bezradne.

Choć nikt tego nie zauważa, ogłoszona właśnie klapa systemu informatycznego dla służb celnych to poważny cios dla naszej gospodarki. W kraju będącym korytarzem handlowym dla Europy, Rosji i Azji po prostu nie da się kontrolować i analizować przepływu tak wielkiej ilości towarów (m.in. około 6 tys. ciężarówek dziennie) wyłącznie za pomocą kartek, kalki, spinaczy i długopisów. Gdy celnicy dysponują tylko takimi narzędziami, o polskiej gospodarce decydują: firmy i rządy innych krajów, mafie i przypadek. Same tylko bezpośrednie straty budżetu, wynikające z braku ścisłej kontroli celnej, wynoszą około 10 mld USD rocznie. Jak widać, nawet bardzo drogi system informatyczny dla służb celnych, gdy działa, amortyzuje się zaledwie w ciągu kilku miesięcy.

Często zdarza się, że dematerializują się przesyłki tranzytowe albo są eksportowane towary nie przekraczając granicy. A oto kilka przykładów celnej fikcji:

- na jednym tylko transporcie „wyeksportowanego" alkoholu straciliśmy 2 mln zł;
- w urzędach komunikacji zarejestrowano w ub. r. o 41 tysięcy więcej nowych samochodów, niż było ich w dokumentach celnych;
- deklarowana cena sprowadzonych do nas masowo tekstyliów jest wielokrotnie niższa niż wartość użytego do ich produkcji surowca.

Oszustwa zagranicznych dostawców, brak ustawy antydumpingowej oraz nieistniejąca polityka celna państwa powodują, że bankrutują uczciwi, krajowi producenci (przytoczenie ich pełnej listy przekracza przysługującą mi objętość). Gdy dojdzie do bankructwa polskiego przedsiębiorstwa, szamani jedynie słusznej (znowu to przerabiamy) opcji ekonomicznej twierdzą, że leniwi pracownicy polskich fabryk przegrywają z lepszą zagraniczną konkurencją.

W 1994 r. zdecydowano się zbudować Ogólnopolski System Informatyczny Administracji Celnej (OSIAC). Już sam przebieg przetargu na jego wykonawcę wskazywał, że będzie to kolejna, do tego największa i najważniejsza, katastrofa informatyzacji administracji państwowej. Przeanalizowana przez NIK dokumentacja tego przetargu to przerażający obraz amatorszczyzny organizacyjnej, braku rozsądku i świadomości wagi celu.

Po mętnych procedurach przetargowych wygrała niemiecka firma CGK, własność Siemens Nixdorf, gdyż oferowała ponoć lepsze warunki finansowe i krótszy czas wykonania systemu. Jak krótki był to czas, każdy widzi. Po prawie trzech latach GUC zdołał jedynie położyć kable.

Wielcy przegrani tego przetargu mieli doświadczenie, zaplecze fachowe, kapitał i dobre referencje. Zrobili działające już od kilku lat krajowe systemy informatyczne dla służb celnych: AT&T GIS w Rosji i Szwajcarii, a IBM w Norwegii, Danii i Austrii. W obu tych koncernach do dziś nie rozumieją, dlaczego przegrali z firmą nieprodukującą oprogramowania ani sprzętu, bez służb serwisowych, o zdolności kredytowej w wysokości 1/100 wartości kontraktu.

Może pewien wpływ na taki wybór miał list Ministra Gospodarki Niemiec napisany do polskiego Ministra Współpracy Gospodarczej z Zagranicą. Zapoznali się z nim członkowie komisji przetargowej przed podjęciem ostatecznej decyzji. Czytamy w nim m.in.: ... *wygranie przetargu przez firmę CGK w znacznym stopniu mogłoby się przyczynić do zwiększenia inwestycji przedsiębiorstw z jej kraju w Polsce. W tym kontekście chciałbym Pana prosić o* ***obiektywne*** *(podkr. aut.) rozpatrzenie i ocenę oferty, jak również polecić ją Pana bezpośredniej uwadze.* W rezultacie, także obiektywnie, system nie istnieje.

Dlaczego nie mamy niezbędnych do rządzenia państwem, krajowych systemów informatycznych? Odpowiedź na to pytanie sugeruje spostrzeżenie prof. Jadwigi Staniszkis (cytuję z pamięci): *jest w naszym kraju tyle głupoty, że aż trudno uwierzyć, że to tylko przypadek.* Lobby cwaniaków oraz oszustów krajowych i zagranicznych są tak silne, że to one decydują o tym, czy powstanie krajowy system informatyczny - celny, podatkowy, rejestracji pojazdów czy gruntów.

Naiwni sądzą, że teraz się to skończy. Prezes GUC, Janusz Paczocha obiecuje, że powstanie system informatyczny dla służb celnych. Na początek organizuje wzorcowy, jak twierdzi, przetarg na dostawę około 3 tys. komputerów PC. Prezes GUC pewnie nie wie, że metoda: „najpierw kupimy komputery, a potem się zobaczy", już się sprawdziła przy Poltaxie.

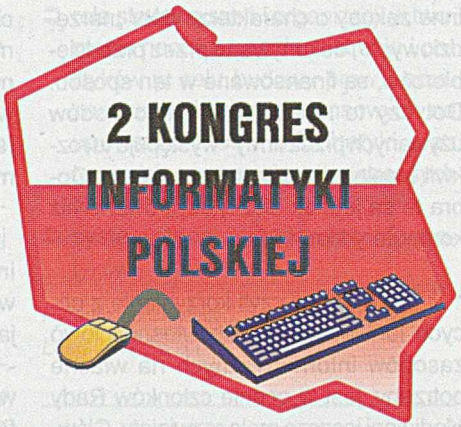
Nie wróży też nic dobrego pohukiwanie prezesa GUC na dziennikarzy. Waldemar Pawlak również chciał komputeryzować kraj, też nie lubił pismaków i był, oceniając jego politykę celną, tak samo dobrym gospodarzem, jak jego poprzednicy i - niestety - następcy.

Leszek Jaworek

2 Kongres Informatyki Polskiej

http://kongres.org.pl

Poznań, 30 listopada - 2 grudnia 1998 r.



„Informatyka" – patron medialny

Rada Medialna 2 Kongresu Informatyki Polskiej

Została utworzona Rada Medialna Kongresu. W skład Rady weszli dziennikarze z czołowych pism informatycznych oraz redakcji, zajmujących się tematami informatycznymi. Celem Rady jest wskazywanie zagadnień dotyczących informatyki i jej upowszechnianie. Rada będzie ściśle współpracować z Komitetem Programowym Kongresu. Dotychczas nie istniało w Polsce forum umożliwiające dziennikarzom, zajmującym się problematyką informatyczną, regularną wymianę poglądów.

Skład Rady Medialnej 2 Kongresu Informatyki Polskiej:

Zbigniew Blewoński – „PCKurier"
Michał Bonarowski – „Gazeta Bankowa"
Andrzej Horodeński – „MRK"
Tomasz Kulisiewicz – „TeleInfo"
Marek Młynarski – „TelekomFORUM"
Andrzej J. Piotrowski - Rzecznik Prasowy 2 Kongresu
Tadeusz Rogowski – „NetFORUM"
Stanisław M. Stanuch – „Gazeta Wyborcza"
Lesław Wawrzonek – „Informatyka"
Tomasz Zieliński – CRN
Marek Zimnak – „Chip" Vogel Verlag
Zbigniew Zwierzchowski – „Rzeczpospolita"

Na spotkaniu ustalono, że autorytet poszczególnych Członków Rady Medialnej gwarantuje, że ich publikacje będą mogły być opatrywane logo Kongresu. Nie wyklucza to oczywiście podejmowania tematyki kontrowersyjnej i wyrażania własnego zdania autorów publikacji. Do zadań Członków Rady należy jednak budowanie merytorycznego charakteru dyskusji toczącej się przed Kongresem. Skład Rady jest otwarty dla innych redakcji, które zaakceptują uzgodnione kryteria.

Rada zdecydowała także, że poszczególne wydawnictwa będą mogły zaprezentować swój wkład w dyskusję przedkongresową uczestnikom i gościom 2 Kongresu Informatyki Polskiej poprzez tzw. reprinty publikacji (lub w innej postaci odpowiedniej dla danego medium). Szczegóły tego zamierzenia będą jeszcze przedmiotem dalszych ustaleń.

Kontakt Andrzej J. Piotrowski
tel. +(22) 7731746, fax +(22) 7731729
E-mail: A_J_P@it.com.pl

W gronie członków Rady Medialnej odbywają się comiesięczne dyskusje o problemach, które będą przedmiotem zainteresowania 2 KIP. Poniżej przedstawiamy podsumowanie wypowiedzi członków Rady na dwóch kolejnych spotkaniach.

Informatyka i pieniądze

Pytanie 1. Jeśli przedsiębiorstwa uchylają się od podawania konkretnych danych finansowych co do korzyści gospodarczych (zwiększenia potencjału rynkowego, redukcji kosztów lub redukcji strat firmy), osiąganych w wyniku zastosowania narzędzi informatycznych, to co stanowi siłę napędową dla rozwoju rynku informatycznego?

Zdaniem członków Rady Medialnej odpowiedzi na to pytanie należy poszukiwać zarówno w warstwie merytorycznej, jak i w mentalności osób podejmujących decyzje. Podstawowym problemem jest brak nawyku ścisłego kontrolowania kosztów prowadzenia działalności przedsiębiorstw w Polsce, w tym szczególnie - liczenia kosztów związanych z informatyką. Jednocześnie, brakuje postrzegania informatyki jako narzędzia do zwiększania efektywności - dlatego że jeszcze bardzo niewielu menedżerów dokładnie wie, jakie korzyści wynikają ze stosowania zaawansowanej technologii teleinformatycznej. Jako jeden ze stymulatorów popytu należy wskazać konkurencję między poszczególnymi podmiotami. Część menedżerów sądzi, że skoro konkurenci się informatyzują, oni też powinni podejmować kroki w tym kierunku. Ma to aspekt czysto praktyczny - zdarza się często, że komputeryzacja przynosi efekty w postaci szybszego i łatwiejszego zdobywania klientów.

Czynniki psychologiczne rozwoju rynku informatycznego opierają się na modzie na informatyzację, dosadniej mówiąc - jest to owczy pęd do informatyzowania wielu sfer działalności, bez wnikania w sensowność inwestycji.

Pytanie 2. W jaki sposób efektywnie pozyskiwać środki na finansowanie własnych potrzeb informatycznych przedsiębiorstw - dlaczego stosowanie powszechnych (w innych branżach) instrumentów finansowych (kredyty, leasing, dzierżawa lub wręcz zakup usług obsługi informatycznej - outsourcing) nie cieszy się w Polsce popularnością?

Według opinii członków Rady Medialnej kredyty bankowe są obecnie zbyt drogie, a leasing zbyt niepewny prawnie (głównie w warstwie podatkowej: VAT i cło), by te formy finansowania zakupów rozpatrywać jako realną możliwość dla polskich przedsiębiorstw. Co prawda, w wypadku mniejszych przedsiębiorstw leasing komputerów jest stosowany, ale nie spotyka się tej formy w dużych projektach.

Członkowie Rady zwracają uwagę, że mimo wspomnianych problemów

inne zakupy o charakterze dóbr „narzędziowych", dokonywane przez przedsiębiorców, są finansowane w ten sposób. Dotyczy to na przykład samochodów używanych przez firmy - występuje tu rozkwit leasingu i kredytu bankowego. Dobra te są jednak dłużej użytkowane niż komputery klasy PC.

Outosourcing, czyli korzystanie z obcych funkcjonalnie i/lub własnościowo zasobów informatycznych na własne potrzeby, jest w ocenie członków Rady Medialnej jeszcze mało rozwinięty. Główne problemy to brak dobrej oferty na rynku, ryzyko, związane z nieuprawnionym wglądem do danych przedsiębiorstwa (szczególnie dotyczy to poufnych danych bankowych), brak możliwości korzystania z usług większej liczby dostawców - czyli możliwość uzależnienia się od jednego usługodawcy. Członkowie Rady zwracają jednak uwagę, że uzależnianie się od zewnętrznego dostawcy może być mniej groźne niż zakup na własność dużych systemów informatycznych. W takim wypadku związanie się z jedną technologią, a szczególnie z jednym dostawcą, jest obciążone dużym ryzykiem.

Pytanie 3. W jaki sposób finansować rozwój firm z branży teleinformatycznej przy wysokim koszcie kapitału, schematach inwestycyjnych dyskryminujących rozwój firm nowatorskich i kreatywnych, klasyfikacji w grupie wysokiego ryzyka? Czy rzeczywiście branża informatyczna w Polsce to branża wysokiego ryzyka (patrz: Computer-Land, Prokom, Optimus, Telekomunikacja)?

Podstawowe pytanie brzmi: czy branża komputerowa jest istotnie tak zyskowna, jak się powszechnie sądzi. Zdaniem członków Rady Medialnej trudno jest przekonać potencjalnych inwestorów, że informatyka to zyskowny interes. Co prawda - przykłady dużych firm, których akcje notowane są na giełdzie papierów wartościowych pokazują, że na informatyce można zarobić, ale w jaki sposób przekonać inwestorów, że małe firmy też przyniosą zysk w krótkim czasie? Symptomatyczne jest, że wśród inwestorów instytucjonalnych, obecnych w Polsce, firmy informatyczne nie cieszą się popularnością. Jeśli tak, to być może analitycy z tych firm nie są przekonani o racjonalności takiej inwestycji, choćby ze względu na duże ryzyko. Niemniej jednak, według członków Rady, możemy być świadkami wzrostu niewielkich firm komputerowych, zajmujących się prostymi usługami lub montażem komputerów PC.

Pytanie 4. Kto (i jak) ma płacić za informatyzację administracji państwowej i samorządowej, służb publicznych, jak wojsko, policja, szpitale, szkoły itd., - - szczególnie gdy duża liczba finansowanych z budżetu projektów kończy się fiaskiem?

Ministerstwo Spraw Wewnętrznych i Administracji podjęło pracę nad standaryzacją procedur zakupów informatycznych w administracji. Zdaniem członków Rady Medialnej odgórna formalizacja procedury zakupów może nie przynieść spodziewanych efektów. Pojawiła się także propozycja przerzucenia odpowiedzialności za powodzenie projektów na dostawców. Za nieudane projekty płaciliby wykonawcy, jeśli niepowodzenie nie byłoby wynikiem obiektywnych trudności. Czy outsourcing może być rozwiązaniem dla polskiej administracji? Częściowo tak, ale ponieważ oferta nie jest bogata (por. pytanie 2), trudno spodziewać się, by outsourcing w adminstracji szybko stał się popularny.

Pytania kolokwium i resume opracował: Michał Bonarowski („Gazeta Bankowa")

Informatyka a państwo

W czasie omawiania na forum Rady Medialnej 2KIP programu Kongresu pojawiła się wątpliwość: czy temat „Rola państwa w rozwoju społeczeństwa informacyjnego" jest potrzebny?

Dość popularny jest pogląd, iż ogólnoświatowy rozwój informatyki w znacznej mierze wynika z faktu, że ...administracje poszczególnych krajów nie mieszają się do tej dziedziny. Również w Polsce, ciężko doświadczonej za sprawą okresu centralnego planowania, modne jest przekonanie, że państwo powinno się jak najmniej wtrącać do gospodarki. Czy zagadnienie to jest jednak aż tak proste? Jakich działań (odniesionych do rozwoju informatyki) ze strony administracji powinni domagać się obywatele w zamian za płacone podatki?

Problematyka rozwoju sektora informatycznego i oczekiwań w stosunku do państwa stała się tematem kolejnego kolokwium „Informatyka a państwo".

Jaka jest rola państwa?

Zebrani członkowie Rady Medialnej zgodzili się że niezależnie od zróżnicowanych doktryn politycznych państwo jest (w mniejszym lub w większym stopniu) organizatorem poczynań, które przekraczają możliwości działania jednostki i z jakiś względów (np. politycznych) nie są lub nie mogą być realizowane przez organizacje pozarządowe. Patrząc na problem pragmatycznie: skoro godzimy się płacić podatki, więc przynajmniej domagajmy się aby nasze pieniądze wydawano sensownie. Oczywiste jest, że taka teza dotyczy również wszelkich działań skorelowanych z informatyką.

Uczestnicy kolokwium zgodzili się, że w krajach o niekwestionowanej gospodarce rynkowej rola państwa we wspomaganiu finansowym i prawnym upowszechnienia informatyki i przemysłu nowoczesnych technologii jest duża i znacznie większa niż u nas. Świadczą o tym na przykład następujące fakty:

- Internet powstał z pieniędzy budżetowych USA,
- projekt sieci WWW powstał w ośrodku badawczym CERN - dotowanym z budżetu państw UE,
- Komisja Unii Europejskiej koordynuje ogromny pakiet przedsięwzięć związanych z pracami badawczo-rozwojowymi i wdrożeniami produktów informatycznych istotnych dla realizacji koncepcji społeczeństwa informacyjnego; firmy są wspierane dofinansowaniami w wysokości nawet 50% nakładów na tego typu prace,
- prawa podatkowe wielu krajów sprzyjają przedsiębiorstwom innowacyjnym; ma to szczególne znaczenie dla rozwoju sektora informatycznego,
- w USA są państwowe i prywatne fundusze dla przedsiębiorstw zwiększonego ryzyka inwestycyjnego,
- rząd RFN sfinansuje dostęp do Internetu w 10 tys. niemieckich szkół,
- rząd Wielkiej Brytanii sponsoruje niedochodowe, specjalistyczne książki z dziedziny informatyki, jak też bardzo kosztowny projekt edukacji informatycznej w szkołach,

- prawa imigracyjne w USA są łaskawsze dla specjalistów komputerowych,
- Ambasada Kanadyjska „kaperuje" w Polsce informatyków,
- Ambasada USA organizuje spotkania polskich i amerykańskich biznesmenów, spełniając rolę katalizatora dla prywatnych przedsięwzięć.

Waga, jaką rządy innych krajów przywiązują do wspierania rozwoju informatyki, pozwala przypuszczać, że pasywna postawa naszej administracji sprawi, iż rozwój informatyki w Polsce będzie uzależniony od decyzji podejmowanych poza naszymi granicami. W efekcie staniemy się w tej dochodowej dziedzinie wyłącznie importerem. Dotyczyć to będzie zarówno technologii, jak i sił fachowych. Prawdopodobne jest, że uzyskanie dostępu do różnorodnych rozwiązań będzie powiązane z koniecznością dopasowywania się Polski do obcych wzorców - nawet jeśli będzie to powiązane z wieloma niedogodnościami. Z pewnością będzie to bardziej kosztowne niż edukacja.

Edukacja

Zdaniem członków RM, uwzględniając możliwości budżetu, realizowane przez rząd zadania oraz skalę priorytetów najważniejszą sferą, w której państwo powinno stymulować rozwój informatyki w kraju, jest edukacja użytkowników, specjalistów i kadry nauczającej. Wśród ważkich zadań należy wymienić:

- kształcenie nauczycieli;
- dotowanie niedochodowych (z racji niskich nakładów) książek dla specjalistów;
- utrzymywanie bibliotek;
- wspieranie lokalnych inicjatyw dokształcania informatycznego dorosłych.

Państwo powinno mieć wieloletni program edukacyjny w zakresie informatyki dla całego społeczeństwa. Jego przygotowanie należy zlecić fachowcom, a zaopiniowanie odpowiednim stowarzyszeniom i organizacjom.

Polityka, finanse, programy

Państwo może szkodzić, jak i sprzyjać, upowszechnianiu technik informatycznych za pomocą polityki celnej i podatkowej. W tym roku na przykład przyhamowano tempo informatyzacji, podnosząc cła na podzespoły elektroniczne i likwidując ulgi podatkowe na zakup sprzętu komputerowego. Równocześnie statystyki podają, że tempo wzrostu rynku informatycznego było w Polsce znacznie niższe niż na przykład w Czechach (np. tyle samo sprzedanych PC przy czterokrotnie mniejszej liczbie ludności) i na Węgrzech - jeszcze przed ww. „przedsięwzięciami".

Polska jest krajem zbyt biednym, aby korzystać z programów upowszechniania informatyki i rozwoju przemysłu teleinformatycznego realizowanych w bogatszych krajach. Powinny powstać programy dopasowane do naszych możliwości. Obecnie nie ma żadnych.

Urzędy państwowe

Wśród urzędników administracji pokutują trzy mity:

- mała informatyzacja = PC + oprogramowanie MS Office;
- duża informatyzacja = przyłączenie do Internetu;
- informatyka jest tak zaawansowaną dziedziną, że może się nią zajmować tylko Komitet Badań Naukowych. Dla innych resortów jest „zbyt mądra".

Zdaniem RM bardzo ważnym sposobem upowszechniania informatyki jest rutynowe i oparte na racjonalnych przesłankach korzystanie przez instytucje administracji rządowej i samorządowej z technik informatycznych. Upowszechnienie informatyki powinno się zacząć od urzędników administracji, tak aby uznali ją za niezbędne narzędzie swojej pracy. W przedsięwzięciach informatycznych administracji należy też położyć nacisk na usprawnienie relacji urząd-obywatel. Dotąd projekty informatyczne koncentrowały się jedynie na obsłudze „wewnętrznych" zadań administracji.

Z kręgu ważnych zagadnień, związanych z udziałem państwa w rozwoju informatyki pozostawiono do dyskusji w innym terminie:

- analiza nieudanych krajowych przedsięwzięć informatycznych w celu uniknięcia powtarzania błędów,
- normowanie i certyfikowanie systemów informatycznych i oprogramowania. Czy i kto powinien opracować normatywne wymagania dla projektu i jego realizacji, takie jak: bezpieczeństwo, błędy i warunki testowania, zgodność z prawem,
- rola stowarzyszeń i organizacji w tworzeniu nacisku na administrację i polityków w celu budowy praw i przeznaczania środków finansowych na upowszechnienie informatyki oraz tworzenie przemysłu nowoczesnych technologii,
- system stopni zawodowych informatyków.

Pytania kolokwium i resume opracował: Lesław Wawrzonek

---

2 Kongres Informatyki Polskiej

Poznań, 30 listopada - 2 grudnia 1998 r.

WARSZAWA – 3 lipca 1998 r.
Komitet Programowy 2 Kongresu Informatyki Polskiej podjął decyzję o zmniejszeniu liczby sesji roboczych Kongresu. Ustalono, że odbędzie się dziewięć sesji tematycznych. Za każdą sesję roboczą odpowiada członek Komitetu Programowego.

Zdecydowano, że Komitet wystąpi do przedstawicieli Rządu RP, z prośbą o przedstawienie uczestnikom Kongresu założeń polityki w odniesieniu do sektora informatycznego oraz zagadnień wynikających z procesu integracji z Unią Europejską. Zaproszenie wystosowane będzie również do przedstawicieli Sejmu, z prośbą o zaprezentowanie uczestnikom inicjatyw i prac legislacyjnych, których zakres obejmuje zagadnienia związane z informatyką. W pierwszym dniu Kongresu zaplanowano również dyskusję panelową nad Raportem z 1 Kongresu Informatyki Polskiej i wystąpienie podsumowujące 50-lecie Informatyki w Polsce.

Odbywające się w drugim dniu sesje robocze Kongresu będą miały charakter dyskusji panelowych. Do udziału w poszczególnych panelach tematycznych zaproszone zostaną osoby o uznanym autorytecie w danej dyscyplinie. Komitet Programowy uznał, że ważne jest również włączenie do dyskusji osób reprezentujących młodsze pokolenie (np. wyróżniający się studenci).
Uwzględniając znaczący dorobek poszczególnych firm sponsorujących 2 Kongres Informatyki, Komitet Programowy uznał, że merytoryczny udział przedstawicieli sponsorów w gronie panelistów będzie cennym wzbogaceniem dyskusji. Nie przewiduje się jednak prezentacji o charakterze komercyjnym. Przyjęto także założenie, że co najmniej połowa czasu poszczególnych sesji zostanie zarezerwowana na głosy „z sali" pozostałych uczestników Kongresu.

Do składu Komitetu Programowego została włączona pani Agnieszka Boboli. Do czasu wyjaśnienia spraw personalnych zawieszony został udział „Polskiej Społeczności Internetu (PSI)" w gronie organizatorów Kongresu.

Do Komitetu Honorowego 2 Kongresu zaproszono Prezydenta Miasta Poznania i Przewodniczącego Związku Miast Polskich Wojciecha Szczęsnego-Kaczmarka.

Sekcja Polska

IEEE THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

Warszawa, dn. 23.04.1998 r.

Szanowny Pan
prof. dr hab. Jerzy Buzek
Prezes Rady Ministrów

List otwarty w sprawie strategii rozwoju przemysłu elektronicznego w Polsce

Strategia rozwoju gospodarki

W każdym okresie rozwoju techniki są takie jej działy, w których przejście na wyższy poziom rozwoju warunkuje rozwój pozostałych jej obszarów. Dział taki jest wtedy strategiczny w danym okresie czasu dla rozwoju gospodarki każdego państwa. Dostrzeżenie dostatecznie wcześnie obszarów strategicznych i inwestycja w ich rozwój daje nieporównywalne z nakładami korzyści ekonomiczne w całej gospodarce i przewagę nad innymi konkurencyjnymi, zagranicznymi gospodarkami.

W Polsce, chociaż już od dziewięciu lat głęboko reformowanej, nie znane są społeczeństwu decyzje strategiczne na szczeblach państwa dotyczące rozwoju działów polskiej gospodarki. Z tego względu nasze Stowarzyszenie zawodowe chce nakłonić decydentów państwowych do prowadzenia aktywnej polityki gospodarczej w sensie tworzenia strategii rozwoju wybranych dziedzin gospodarki. Nie ulega wątpliwości, że wśród nich powinny znaleźć się pewne działy przemysłu elektronicznego, bez rozwoju których wiele innych dziedzin gospodarczych jest nieefektywnych, nienowoczesnych, a przez to niskodochodowych i niekonkurencyjnych.

Ekonomia oparta na prawach wolnego rynku w żadnym razie nie może oznaczać braku troski ze strony organów państwowych co do kierunków i możliwości rozwoju przemysłu i nauki we własnym kraju, w szczególności w sytuacji gdy jest on pod tak ścisłym działaniem konkurencyjnych firm i organizacji zagranicznych. Dowodem na to, że taka troska jest niezbędna w każdym kraju, osiągającym wysokie wskaźniki gospodarcze, są inicjatywy promocyjne w gospodarce podejmowane od wielu lat przez Kongres USA lub MITI w Japonii, nie wspominając już o wielokierunkowych analogicznych działaniach prowadzących do tego samego celu w krajach azjatyckich.

Działanie promocyjne ze strony Rządu dla nielicznych, szczególnie ważnych dla całej gospodarki dziedzin przemysłu w żadnym razie nie oznacza naruszenia zasad konkurencyjności przemysłu. Natomiast oznacza, że preferencje te powinny się zmieniać w czasie i dotyczyć ciągle nowych, innowacyjnych technologii i wyrobów, które wpływają na tworzenie nowoczesnej infrastruktury przemysłowej, ważnej dla rozwoju gospodarczego całego kraju.

Polski przemysł elektroniczny

Elektryka, a w szczególności elektronika, stanowią jedną z najważniejszych dziedzin techniki nowoczesnego świata, należą do działu tzw. high technology i wciąż są wyznacznikami postępu cywilizacyjnego świata. Kraj, który nie bierze udziału w toczącym się w tej dziedzinie wyścigu dokonań naukowych i technicznych skazuje się na kosztowny import, ekonomiczną i społeczną marginalizację, a w dalszej perspektywie na pozbawienie suwerenności gospodarczej. Są to fakty na tyle oczywiste, że byłoby nietaktem ich przywoływanie gdyby nie to, że proces upadku elektryki w Polsce ma miejsce od wielu już lat i obecnie nic nie wskazuje na to, aby miał być powstrzymany.

Szczególnie jaskrawym, negatywnym dowodem na brak strategii rozwoju elektroniki w Polsce w minionych latach jest obecnie konieczność zakupienia z zagranicy wyposażenia elektronicznego dla śmigłowca wojskowego typu Huzar. Polska ma potencjał kadrowy i w dużym stopniu wyposażenie techniczne, aby urządzenia elektroniczne tego typu i podobne produkować w Polsce na poziomie identycznym jak w państwach wysokouprzemysłowionych. Dowodem na to jest produkcja radarów wojskowych (na najwyższym światowym poziomie), detektorów na podczerwień, komputerów personalnych (stanowiących 20% rynku europejskiego) i wielu innych produktów elektronicznych. W Polsce są już zalążki nowoczesnego przemysłu elektronicznego, głównie aparaturowego i sprzętowego - poszerzenie skali tych pozytywnych przykładów wymaga jednak prowadzenia dobrze określonej strategii rozwoju gospodarki. ***Za wysoce niebezpieczne dla przyszłości ekonomicznej i cywilizacyjnej kraju uważamy zadowalanie się płytko pojętym, wtórnym rozwojem elektryki i elektroniki*** *(głównie obsługi urządzeń i systemów elektronicznych produkowanych za granicą, obsługi komputerów i ich serwisu* ***zamiast opracowywania i produkcji*** *urządzeń, systemów i oprogramowania).*

Polska ma jeszcze rzeszę dobrze wykształconych inżynierów i techników, ma dobre uczelnie kształcące elektryków i elektroników. Pozostały również pewne urządzenia technologiczne w jednostkach badawczych i produkcyjne w działających jeszcze nielicznych fabrykach. Ten potencjał dzisiaj może być jeszcze wykorzystany. Jutro będzie zmarnowany.

Polska Sekcja IEEE

Międzynarodowe stowarzyszenie elektryków i elektroników - The Institute of Electrical and Electronics Engineers - IEEE skupia na całym świecie ponad 350.000 członków. Amerykańska Sekcja IEEE jest regularnym konsultantem Kongresu i Prezydenta USA przy podejmowaniu strategicznych decyzji gospodarczych.

Polska Sekcja IEEE liczy ponad 400 członków i skupia elitę naukową i techniczną elektryków i elektroników polskich. Działa w Polsce od 26 lat.

Nasze wystąpienie wynika nie z chęci zabiegania o finansowanie reprezentowanej przez nas dziedziny nauki i techniki, ale z poczucia obowiązku naukowców i techników informowania ośrodków decyzyjnych kraju o tych dziedzinach wiedzy, nowych technikach i nowych technologiach, które mogą mieć istotny wpływ na rozwój gospodarczy kraju.

Oczekiwania społeczne

Społeczeństwo polskie, a inteligencja techniczna w szczególności, oczekuje od Rządu i Sejmu Rzeczpospolitej Polskiej pilnego opracowania strategicznych kierunków rozwoju przemysłu polskiego i ich czynnego wspierania (finansowego, promocyjnego czy protekcyjnego).

Zaniedbanie tych obecnie pilnych działań postawi wkrótce Polskę na progu Wspólnoty Europejskiej jako kraju bez porównywalnej, nowoczesnej infrastruktury przemysłowej, skazanego na odgrywanie roli podrzędnej.

Polska Sekcja IEEE oczekuje rzetelnego i poważnego ustosunkowania się do naszego apelu i wyraża głęboką nadzieję, że działania nad stworzeniem warunków szybkiego rozwoju wybranych działów ***high technology*** *polskiej elektryki i elektroniki rozpoczną się w najbliższej przyszłości.*

Za Zarząd Polskiej Sekcji IEEE:

Wiceprzewodniczący
prof. dr hab. inż. Bohdan Mroziewicz

Przewodniczący
prof. dr hab. inż. Ryszard S. Jachowicz

Autorzy listu do dziś nie otrzymali odpowiedzi Prezesa Rady Ministrów prof. dr hab. Jerzego Buzka.

SAP na Nowojorskiej Giełdzie

Od sierpnia br. SAP A.G. będzie notowany na Nowojorskiej Giełdzie Papierów Wartościowych. Ze swoimi 9000 klientami w ponad 90 państwach SAP ma około 28% rynku systemów klasy ERP. Przyczyną wejścia na nowojorską giełdę nie jest głównie chęć zdobycia pieniędzy, a raczej zwrócenie uwagi na firmę klientów z największego rynku. W USA firma SAP uzyskuje 35% dochodów ze sprzedaży, a z tego kraju pochodzi ponad 20% inwestorów.

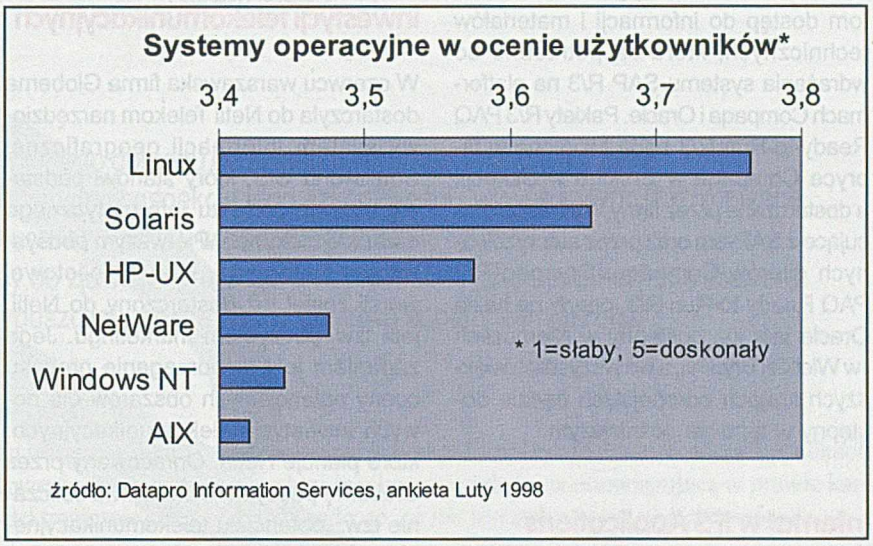
Znawcy rynku oprogramowania są ciekawi czy presja Wall Street na uzyskiwanie co kwartał dobrych wyników nie wpłynie na długookresową strategię firmy, znanej z planowania swoich celów w perspektywie znacznie dłuższej niż kwartał.

Wiadomo, że we Frankfurcie cena akcji SAP podwoiła się od początku br. Przy wzroście zatrudnienia 32%.

Pewnym zagrożeniem dla przyszłości SAP-a może być jego stosunek do problemu serwisu, gdyż nie stanowi on najmocniejszej strony niemieckich przedsiębiorstw. Pomimo powolnego rozwoju sieci konsultantów w większości wypadków SAP działa za pośrednictwem partnerów. Dopóki oprogramowanie klasy ERP dobrze się sprzedaje, SAP nie musi się martwić zyskami z usług serwisowych. Jednak wraz z upływem czasu najprawdopodobniej będzie musiał zainteresować się tą kwestią.

Ekspansja Linuxa

Do tej pory Linux był pomijany przez prasę branżową i używany przez pracowników nauki, inżynierów, studentów i ... hackerów. Teraz ma szansę wejść w główny nurt rynku komputerowego jako konkurencja dla komercyjnych systemów unixowych a przede wszystkim dla Windows NT. Nawet najwięksi producenci w dziedzinie IT zainteresowali się Linuxem. Na przykład Oracle i Informix wprowadzają Linuxową wersję swoich programów, Sun już używa Linuxa jako systemu operacyjnego dla końcowych stacji roboczych, IBM może niedługo dołączy do tej listy.



Nawet bez poparcia „wielkich" świata informatyki Linux odniósł swoisty sukces. W ciągu kilku lat wyewoluował z zabawki *hackera* do systemu, przynajmniej częściowo, lepszego technicznie od Windows NT. „Ojcem" systemu jest Linus Torvalds, który w 1991 roku jako student napisał pierwszą wersję programu. Udostępniając źródła programu w Internecie, zachęcił innych do pracy nad systemem. Tysiące młodych programistów z całego świata stara się udoskonalić Linuxa. Tylko najlepsze, dokładnie przetestowane poprawki są dołączane do kolejnych wersji. Każdy może, za darmo, ściągnąć pełną wersję systemu z Internetu, używać go i wprowadzać własne modyfikacje.

Pomimo hackerskiego pochodzenia Linux jest systemem godnym zaufania. Trudno oszacować liczbę użytkowników, jako że program jest bezpłatny, a wielu inżynierów instaluje go bez informowania o tym swoich przełożonych. Linux jest używany przez większość firm oferujących dostęp do Internetu, a poza Ameryką staje się najpopularniejszą wersją Unixa. Według badań Datapro użytkownicy ocenili Linuxa wyżej niż wszystkie pozostałe systemy komercyjne.

Jednak, aby móc poważnie konkurować z Microsoftem, Linux potrzebuje wsparcia dużych firm. Jak dotąd tylko Netscape i Corel zadeklarowały pełne poparcie. Jeśli pozostałe firmy softwareowe się przyłączą, to Linux stanie się bardzo poważną alternatywą systemową dla kosztownych produktów komercyjnych.

SAP R/3 w Zakładzie Energetycznym Toruń S.A.

Zakład Energetyczny Toruń S.A. zawarł umowę na zakup licencji i wdrożenie zintegrowanego oprogramowania do zarządzania przedsiębiorstwem SAP R/3. ZE Toruń zakupił system R/3 w pełnej konfiguracji dla ponad 300 użytkowników końcowych. Pierwszy etap wdrożenia rozpoczętego 1 lipca 1998 r. powinien zakończyć się w połowie lutego 1999 r. startem produktywnym modułów finansowych. Prace wdrożeniowe będzie prowadzić zespół konsultantów SAP Polska oraz firm partnerskich SAP.

Docelowo R/3 ma pracować również w spółkach zależnych od ZE Toruń – sieci sklepów Spółki - Energohandel, Elektrowni Wodnej Włocławek oraz Ciepłowni Grudziądz.

Współpraca Compaq i Oracle

Compaq i Oracle będą współpracować w regionie EMEA (Europa, Bliski Wschód i Afryka) przy opracowaniu gotowych do użytku pakietów R/3 do SAP R/3. Com-

paq zamierza obsługiwać bazy danych Oracle w swoich rozwiązaniach pakietowych R/3PAQ Ready-to-Run R/3. Zgodnie z warunkami zawartej umowy Compaq i Oracle będą oferowały wspólne seminaria szkoleniowe i prezentacje, mające na celu promocję nowych produktów. Seminaria mają umożliwić klientom dostęp do informacji i materiałów technicznych, które są potrzebne do wdrażania systemu SAP R/3 na platformach Compaqa i Oracle. Pakiety R/3 PAQ Ready-to-Run R/3 będą tworzone w fabryce Compaqa w Erskine w Szkocji, a dostarczane przez firmy VAR współpracujące z SAP-em oraz przez autoryzowanych dilerów Compaqa. Compaq R/3 PAQ Ready-to-Run R/3, oparty na bazie Oracle jest już dostępny w Niemczech i w Wielkiej Brytanii, a we wszystkich większych krajach europejskich będzie dostępny w terminie późniejszym.

Internet w IFS Applications

IFS i Microsoft rozpoczęły współpracę dotyczącą rozwoju drugiej generacji funkcji internetowych współdziałajacych z systemami IFS Applications. Celem współpracy jest rozszerzenie funkcjonalności oprogramowania przyspieszającego i ułatwiającego dostęp i korzystanie z Internetu. Wspólnie również prowadzone będą akcje marketingowe w Skandynawii, ojczyźnie IFS.

Komputery w magazynach

We wrześniu rozpocznie się promocja nowego produktu firmy Quantum Software S.A. – systemu wspomagającego zarządzanie magazynami – Qquar.

W Polsce pojawia się coraz więcej przedsiębiorstw dystrybucyjnych oraz produkcyjno-dystrybucyjnych, których podstawowym środkiem działania są magazyny. Wielu przedsiębiorców całą swoją uwagę poświęca wyglądowi magazynu (kosztowne wyposażenie), nieliczni zaś zastanawiają się nad stratami wynikającymi z błędnej wysyłki towaru, nie mówiąc o już o czasie, który traci się na poszukiwanie danego towaru. W celu zmniejszenia takich strat powstał system Qquar. Pozwala on kontrolować przepływ towaru od momentu jego zamówienia poprzez magazynowanie, aż po wysyłkę do klienta. Modułowa budowa pozwala łatwo skonfigurować system, dostosować go do sposobu pracy magazynu czy wreszcie przypisać pracownikom prawa do realizacji określonych funkcji. Qquar będzie prezentowany podczas tegorocznego SOFTARGU w Katowicach

Wspomaganie planowania inwestycji telekomunikacyjnych

W czerwcu warszawska firma Globema dostarczyła do Netii Telekom narzędziowy system informacji geograficznej Smallworld GIS, który stanowi podstawę dużego projektu informatycznego o nazwie Netgraph. Pierwszym podsystemem Netgrapha, który w pilotowej wersji został już dostarczony do Netii, jest tzw. podsystem marketingu. Jego zadaniem jest wspomaganie procesu oceny potencjalnych obszarów dla nowych inwestycji telekomunikacyjnych, które planuje Netia. Opracowany przez Globemę podsystem umożliwia obliczanie tzw. „potencjału telekomunikacyjnego" dowolnego obszaru na podstawie szczegółowych danych o poszczególnych budynkach, które w tym obszarze występują. Smallworld razem z rozwiniętym przez Globemę modułem Business Toolkit zajmuje się odpowiednią agregacją danych, ich prezentacją w różnych formach i wykonuje przestrzenne analizy zebranych danych (na mapach w różnych układach geograficznych), co umożliwia typowanie najbardziej obiecujących obszarów inwestycyjnych.

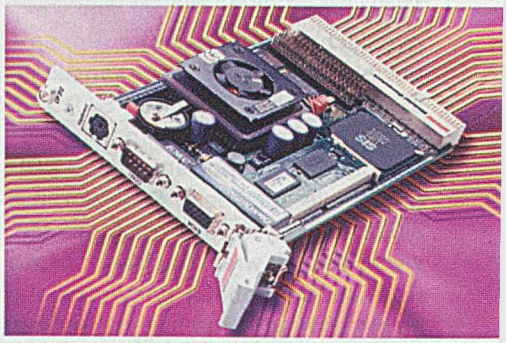
Moduł przesyłania danych dla notebooków

Aparat d50 Motoroli jest pierwszym modelem pełniącym funkcję zarówno telefonu GSM, jak i przenośnego modułu do transmisji danych, który wyposażony jest we własne źródło zasilania i zaawansowaną technologię kompresji danych. Przy użyciu standardowej baterii litowo-jonowej, dostarczanej z aparatem d50, urządzenie może zaoferować do czterech godzin pracy ciągłej (komunikacja głosowa/dane) lub do 60 godzin w stanie gotowości do pracy. W razie potrzeby urządzenie to może pobierać zasilanie z gniazda komputera głównego (H/PC lub PDA). Technologia kompresji danych Digital Data Fast (DDF) pozwala na przesyłanie danych z szybkością do 36 000 bps.

Moduł d50

CP312 – nowy szybki procesor dla przemysłu

PEP Modular Computers wprowadza na rynek nową jednostkę centralną dla komputerów przemysłowych zgodnych ze standardem CompactPCI 2.1. CP312 jest obecnie najszybszą jednostką centralną tej klasy, może być wyposażona w procesor typu Socket 7 aż do 300 MHz (Intel, AMD, Cyrix). Standardowo karta wyposażona jest m.in. w dwa układy watchdog'a dla aplikacji czasu rzeczywistego. Procesor wraz z zestawem kart przeszedł pozytywnie testy zgodności z takimi systemami jak: MS-



Procesor CP312

DOS, Windows'95, Windows NT, Windows'98, QNX. Podstawową zaletą systemów CompactPCI, w stosunku do standardowych PC jest ich wysoka odporność na wibracje i wstrząsy, dodatkowo przy projektowaniu płyt CPCI bierze się pod uwagę możliwość ich pracy w rozszerzonych zakresach temperatur: -40°C +85°C.

Oprac. Rafał Maślana

Hacking a nowy kodeks karny

Andrzej Adamski

Uzyskanie nieuprawnionego dostępu do systemu komputerowego (*hacking*) jest zachowaniem rozmaicie ocenianym w aspekcie jego szkodliwości i wywołującym zróżnicowane reakcje ustawodawców w poszczególnych krajach. Stosunek polskiego ustawodawcy do zjawiska *hackingu* określić można jako umiarkowanie liberalny. Należy jednak przypuszczać, że nie jest to postawa w pełni zamierzona.

Nowy kodeks karny (n.k.k.), który wchodzi w życie w dniu 1 września 1998 r., zawiera w rozdziale XXXIII przepisy przewidujące karalność zamachów na bezpieczeństwo elektronicznie przetwarzanej informacji. Mają one umożliwić pociągnięcie do odpowiedzialności karnej sprawców najbardziej klasycznych przestępstw komputerowych, takich jak: *hacking* (art. 267 § 1), naruszenie integralności komputerowego zapisu informacji (art. 268 § 2) oraz podsłuch (art.267 § 2) i sabotaż komputerowy (art. 269 § 1 i 2).

O tym, czy tak się stanie i czy wejście w życie nowego kodeksu karnego istotnie oznaczać będzie „koniec pogody dla hackerów" czy raczej tylko „przelotne zachmurzenie bez większych opadów"[1], będzie decydować w praktyce wiele czynników. Jednym z nich jest jakość samego prawa. Ściślej zaś mówiąc - zakres prawnokarnej ochrony informacji przed zagrożeniem, jakie dla jej dostępności, poufności i integralności niesie ze sobą każdy atak *hackera*, każda próba uzyskania dostępu do systemu komputerowego przez osobę do tego nieuprawnioną.

Niniejsze opracowanie jest próbą analizy art. 267 § 1 n.k.k., który przewiduje karalność *hackingu*, w aspekcie funkcji ochronnej tego przepisu. Celem poniższych rozważań jest ustalenie, na czym polega istota czynu zabronionego przez ten przepis i jakie formy zamachów na bezpieczeństwo systemów komputerowych będą naruszać jego dyspozycję. Ogólne stwierdzenie, iż po 1 września 1998 r. *hacking* będzie w Polsce ścigany jako przestępstwo, ma w istocie niewielką wartość informacyjną. Sugeruje bowiem, że każda postać tego zachowania będzie traktowana jako naruszenie prawa uzasadniające reakcję karną. Jest więc stwierdzeniem mało precyzyjnym i w gruncie rzeczy dezinformującym. Należy bowiem uświadomić sobie, że pod rządem nowego kodeksu karnego naruszanie poufności informacji lub integralności zapisu informacji przechowywanej w komputerze będzie miało w wielu wypadkach charakter legalny ze względu na obowiązującą w prawie karnym zasadę: *to, co nie jest zabronione, jest dozwolone*.

Hacking w ujęciu n.k.k.

Stosunek polskiego ustawodawcy do *hackingu* wyraża treść art. 267 § 1 n.k.k.:

Kto bez uprawnienia uzyskuje informację dla niego nieprzeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

W myśl najprostszej interpretacji tego przepisu *hacker* ponosi odpowiedzialność karną za zapoznanie się z treścią przechowywanej w systemie komputerowym informacji (np. cudzej korespondencji elektronicznej lub planów marketingowych konkurencyjnego przedsiębiorstwa), jeżeli uzyska do niej dostęp na skutek przełamania zabezpieczeń. Określenie „uzyskanie informacji" - jest bowiem tradycyjnie interpretowane w doktrynie prawa karnego jako zapoznanie się z jej treścią[2]. W tym kontekście o art. 267 § 1 n.k.k. mówi się jako o przepisie penalizującym „kradzież informacji"[3]. Mimo że taka wykładnia omawianego przepisu wydaje się z logicznego punktu widzenia całkowicie poprawna, w praktyce może ona jednak okazać

[1] Dotychczasowa wymiana poglądów na ten temat oscyluje pomiędzy tego typu prognozami: por. J. Wojciechowski, *Koniec pogody dla hackerów*, „Rzeczpospolita", 2 października 1997 r., A. Adamski, *Komputery i paragrafy*, „Rzeczpospolita", 30 października 1997 r.

[2] Por. S. Glaser i A. Mogilnicki (*Kodeks karny - komentarz*, Kraków 1934, s. 831), którzy interpretując znamiona ustawowe przestępstwa naruszenia tajemnicy korespondencji na gruncie art. 253 § 1 kk z 1932 r.,stwierdzają, że przez podstępne „uzyskanie" wiadomości telefonicznej lub telegraficznej nieprzeznaczonej dla sprawcy rozumie się „zapoznanie się z treścią danej wiadomości."

[3] Por. W. Wróbel, *Przestępstwa przeciwko ochronie informacji*, „Rzeczpospolita", nr 206 (3550) z 3 września 1993 r.

się mało użyteczną metodą inkryminowania *hackingu*, z co najmniej dwóch powodów.

Po pierwsze, nie wszyscy sprawcy włamań do sieci komputerowych poszukują informacji. Znane są przypadki włamań dokonywanych wyłącznie w celu wykazania nieskuteczności zabezpieczeń lub dokonania „kradzieży czasu pracy komputera"[4]. Po drugie, sprawcy działającemu w celu uzyskania informacji trudno będzie udowodnić, że taką informację uzyskał. Chociaż większość serwerów sieciowych automatycznie rejestruje wszystkie polecenia wydawane przez ich użytkowników i pozwala na ustalenie, które pliki czytali, to wyłączenie rejestracji tych poleceń i usunięcie *logów* wskazujących na korzystanie z uprawnień dostępu do poszczególnych katalogów i plików nie przedstawia dla wprawnego użytkownika szczególnej trudności[5].

Ponadto, uzależnienie odpowiedzialności *hackera* od warunku „uzyskania (przez niego) informacji" ma jeszcze jedną wadę, która poważnie osłabia funkcję ochronną omawianego przepisu. Okazuje się bowiem, że samo skopiowanie przez sprawcę plików danych zawierających informacje, z którymi nie zdążył się on jeszcze zapoznać, nie wyczerpuje znamion ustawowych omawianego przestępstwa. Tym samym, szczególnie groźna forma *hackingu,* polegająca na „kradzieży" informacji na cudze zlecenie, pozostawałaby praktycznie poza zakresem penalizacji art. 267 § 1 n.k.k.

Aby do tego nie dopuścić i zapewnić wyższy standard ochrony poufności informacji narażonej na ataki *hackerów*, można zaproponować alternatywną interpretację analizowanego przepisu. Interpretacja ta wychodzi z założenia, że dostęp do systemu informatycznego jest zazwyczaj zabezpieczony hasłem. Łamiąc zabezpieczenie w postaci hasła, *hacker* często zapoznaje się z nieprzeznaczoną dla niego informacją, jaką jest treść hasła. Jeżeli tak się dzieje[6] - zachowanie sprawcy wyczerpuje znamiona ustawowe przestępstwa z art. 267 § 1 n.k.k.

Przyjęcie takiej interpretacji omawianego przepisu oznacza, że nie musi wcale dojść do użycia „złamanego" hasła i penetracji systemu komputerowego, aby można było *hackerowi* postawić zarzut popełnienia przestępstwa. Karalna bowiem staje się już czynność *de facto* przygotowawcza, jaką jest uzyskanie informacji warunkującej „wejście" do cudzego systemu komputerowego, nie zaś uzyskanie - dzięki tej informacji - nieuprawnionego dostępu do znajdujących się tam danych i programów komputerowych.

Powyższa interpretacja art. 267 § 1 n.k.k. niewątpliwie wzmacnia funkcję ochronną tego przepisu, który w porównaniu ze swym poprzednikiem - art. 172 § 1 k.k. z 1969 r. (chroniącym tajemnicę korespondencji) zapewnia o wiele słabszą ochronę prawną **poufności** informacji, będącą indywidualnym przedmiotem ochrony przestępstwa określonego w art. 267 § 1 n.k.k.

Na gruncie art. 172 § 1 kk z 1969 r. zapoznanie się z treścią chronionej informacji nie stanowi warunku koniecznego dokonania przestępstwa. Przepis ten bowiem posługuje się obiektywnymi kryteriami karalności i za naruszenie tajemnicy korespondencji uznaje (między innymi) samo otwarcie zamkniętego pisma lub przyłączenie się do przewodu służącego do podawania wiadomości[7].

Natomiast w ujęciu art. 267 § 1 n.k.k. takie czynności wykonawcze jak „otwarcie zamkniętego pisma", „podłączenie się do przewodu służącego do przekazywania informacji" oraz „przełamanie elektronicznych, magnetycznych albo innych szczególnych zabezpieczeń" nie stanowią już obiektywnych kryteriów naruszenia poufności informacji, lecz charakteryzują sposób uzyskania przez sprawcę informacji, do której nie jest on uprawniony. W konsekwencji, aby przypisać sprawcy winę, nie wystarczy, tak jak poprzednio, udowodnić mu na przykład, że bez zgody osoby uprawnionej otworzył on cudze pismo zamknięte, lecz że pismo to otworzył i przeczytał. Podobnie jest z karalnością *hackingu*. Dlatego też druga z przedstawionych wyżej interpretacji przepisu art. 267 § 1 n.k.k. może okazać się szczególnie przydatna w jego ściganiu.

Problem polega jednak na tym, że *modus operandi* hackerów nie ogranicza się wyłącznie do „przełamywania" zabezpieczeń broniących dostępu do informacji, lecz obejmuje bogaty repertuar technik, za pomocą których dokonują oni infiltracji systemów komputerowych bez forsowania zabezpieczeń. Mogą oni w tym celu użyć podstępu (*social engineering, IP spoofing*), przechwycić hasło lub inną informację w czasie jej transmisji (*sniffing*) albo wykorzystać lukę (*bug*) w istniejących zabezpieczeniach. Spróbujmy zatem przeanalizować wyżej wymienione metody uprawiania *hackingu* pod kątem bezprawności ich stosowania w rozumieniu przepisów n.k.k.

Hacking z użyciem podstępu

Inteligentni *hackerzy* nie włamują się do systemów komputerowych[8]. Potrzebne im informacje, np. takie jak hasła dostępu, uzyskują podstępem od użytkowników lub administratorów systemu, a stosowaną w tym celu metodę działania nazywają „inżynierią społeczną" (*social engineering*). Najczęściej polega ona na wprowadzeniu w błąd dysponenta poszukiwanej przez *hackera* informacji co do tożsamości nadawcy wiadomości przesłanej pocztą elektroniczną (*fake mail*) lub rozmawiającej z nim przez telefon osoby. W ten sposób *hacker,*

---

[4] Przykładem mogą tu być notowane w Stanach Zjednoczonych AP przypadki „kradzieży czasu pracy" superkomputerów Cray przez *hackerów,* którzy po uzyskaniu nieuprawnionego dostępu do tych maszyn uruchamiali na nich programy do łamania haseł. Wykorzystując w ten sposób moc obliczeniową superkomputerów do celów nielegalnych, „kradli" jednocześnie czas ich pracy, którego wartość szacowano na znaczne kwoty, sięgające niekiedy kilku tysięcy dolarów.

[5] Zob. A. Frisch, *UNIX. Administracja systemu*, Warszawa 1996, s. 193-199.

[6] W praktyce złamanie hasła odbywa się często w sposób w pełni zautomatyzowany i *hacker* jest powiadamiany przez system nie o treści złamanego hasła, lecz o przełamaniu zabezpieczeń i uzyskaniu dostępu do atakowanego systemu.

[7] Por. np.J.Bafia, K.Mioduski, M.Siewierski, *Kodeks karny. Komentarz*, Warszawa 1987, s.146.

[8] A.Berg, *Cracking a Social Engineer*, LANTimes Online 11/6/1995. <http://www.lantimes.com/lantimes/95nov/511a140a.html>

podszywający się pod prawowitego, lecz roztargnionego właściciela konta, który rzekomo zapomniał swojego hasła, uzyskuje informację umożliwiającą mu wejście do cudzego systemu frontowymi drzwiami - bez potrzeby forsowania zabezpieczeń.

Uzyskanie tą drogą wiadomości nieprzeznaczonej dla *hackera* można traktować jako naruszenie art. 172 § 1 k.k. z 1969 r. Przepis bowiem ten uznaje za jedną z form naruszenia tajemnicy korespondencji „podstępne uzyskanie nieprzeznaczonej (dla sprawcy) wiadomości nadanej przy użyciu środków telekomunikacji", co według poglądów przedstawicieli doktryny prawa karnego może zdarzyć się, gdy „sprawca uzyskuje nieprzeznaczoną dla niego wiadomość, podając się za inną osobę"[9].

Próżno by natomiast szukać w nowym kodeksie karnym przepisu umożliwiającego inkryminowanie „inżynierii społecznej". Oznacza to, że od 1 września 1998 r. wprowadzenie innej osoby w błąd w celu uzyskania od niej zastrzeżonej dla sprawcy informacji nie będzie już czynem zabronionym[10].

Czynem prawnie dozwolonym pozostanie natomiast penetrowanie cudzych systemów komputerowych przy użyciu haseł, które po „złamaniu" lub przechwyceniu są kolportowane przez członków „podziemia komputerowego" za pośrednictwem piracki BBS-ów lub *hackerskich* stron WWW. Ocenę taką uzasadnia treść art. 267 § 3 n.k.k., z którego wynika wyłącznie zakaz ujawnienia innej osobie nielegalnie uzyskanej informacji. Wspomniany przepis nie penalizuje natomiast wykorzystania takiej informacji przez inną osobę do celów sprzecznych z prawem lub niegodziwych, co należy uznać za ewidentną lukę prawną.

Element podstępu występuje także w popularnej obecnie wśród *hackerów* metodzie inflitracji systemów komputerowych za pośrednictwem Internetu, jaką jest atak typu *IP spoofing*[11]. W odróżnieniu od „inżynierii społecznej" obiektem manipulacji jest w tym wypadku nie człowiek, lecz system komputerowy. W szczególności zaś ta część systemu, która ma czuwać na bezpieczeństwem sieci i nie wpuszczać do niej wszystkich przychodzących z zewnątrz pakietów danych, lecz tylko te o określonym adresie IP. *Hacker* potrafi jednak „zmylić" mechanizmy filtrujące ruch w sieci. Dokonuje tego, przerabiając adresy IP na pakietach danych, tak aby zostały one rozpoznane jako pochodzące z sieci, do której faktycznie dopiero usiłuje się dostać. Zabieg ten na ogół pozwala mu uniknąć procedury autentyzacyjnej. Niepytany zatem przez system o hasło, dzięki swoistej mistyfikacji, uzyskuje dostęp do sieci i znajdujących się w niej zasobów informacji[12].

Kwalifikacja prawna tej postaci *hackingu* wcale nie jest oczywista. Sprawca bowiem nie oddziaływuje bezpośrednio na istniejące zabezpieczenia i nie usuwa ich - co semantycznie odpowiadałoby pojęciu „przełamania", jakim posługuje się art. 267 § 1 n.k.k., lecz dokonuje obejścia zabezpieczeń, co jest czynnością wykonawczą, której nie wymienia treść omawianego przepisu[13]. Z drugiej strony, sprawcy nie można postawić zarzutu naruszenia dyspozycji przepisu art. 268 § 2 n.k.k., który (między innymi) chroni integralność zapisu informacji przed nieautoryzowanymi modyfikacjami. *Hacker,* preparując za pomocą specjalnego oprogramowania adres źródłowy IP w nagłówku pakietu danych, nie ingeruje w żaden sposób w treść zapisu znajdującego się na komputerowym nośniku informacji, co jest warunkiem karalności na podstawie art. 268 § 2 n.k.k.

Generowanie pakietów IP o zmienionym adresie źródłowym odbywa się w czasie ich transmisji i nie pozostawia żadnych śladów na twardym dysku zarówno komputera będącego obiektem ataku, jak i maszyny używanej przez *hackera*. W konsekwencji, przypisanie mu odpowiedzialności za popełnienie czynu określonego w art. 268 § 2 n.k.k. nie może wchodzić w grę, skoro zachowanie się sprawcy nie wypełnia znamion ustawowych tego przestępstwa.

Z analogicznych powodów należałoby również wykluczyć możliwość pociągnięcia do odpowiedzialności karnej na podstawie art. 268 § 2 n.k.k. *hackera* posługującego się takimi technikami uzyskiwania nieuprawnionego dostępu do systemów komputerowych, jak przechwycenie sesji legalnego użytkownika (*session hijacking*) czy fragmentacja-reasemblacja pakietów. Obie te techniki polegają na podszywaniu się pod uprawnionego użytkownika systemu i mają więcej wspólnego z podstępem niż z włamaniem. A jednak, w każdej z wyżej wymienionych sytuacji istnieją możliwości postawienia *hackerowi* zarzutu popełnienia przestępstwa. Możliwości te wynikają z treści art. 267 § 2 n.k.k. i wiążą się z okolicznością, iż zastosowanie którejkolwiek z omawianych metod uprawiania *hackingu* (*IP spoofing*, *session hijacking* i fragmentacja-reasemblacja pakietów) wymaga użycia specjalnego, dedykowanego oprogramowania.

Z tego samego względu przepis art. 267 § 2 n.k.k. umożliwia penalizację przechwytywania haseł dostępu metodą *password sniffer*. Spróbujmy zatem przedstawić argumenty przemawiające na rzecz wyżej zaprezentowanego stanowiska na przykładzie ostatniej z wymienionych metod.

Hacking z zastosowaniem podsłuchu

Odpowiedzialność karną na podstawie art. 267 § 2 n.k.k. ponosi ten, „kto w celu uzyskania informacji, do której nie jest upraw-

[9] L.Gardocki, *Prawo karne*, Warszawa 1996, s. 271.

[10] Z wyjątkiem sytuacji, w której sprawca w celu podstępnego uzyskania informacji posłuży się urządzeniem podsłuchowym, wizualnym lub innym urządzeniem specjalnym (art. 267 § 2 n.k.k.). Tego rodzaju czyn nie będzie już jednak „inżynierią społeczną" w czystej postaci.

[11] Nazwa ta oznacza spreparowanie adresu źródłowego IP w nagłówku pakietu danych przesyłanych Internetem (IP - skrót od *Internet Protocol* - nazwa jednego z protokółów komunikacyjnych, umożliwiających przesyłanie danych Internetem).

[12] Opis ataku techniką *IP spoofing* podaję za: D. Icove, K. Seger, W. VonStroch, *Computer Crime. A Crimefighter's Handbook*, O'Reilly & Associates, Inc., Sebastopol, CA 1995, s.50.

[13] Na tę ułomność definicji prawnej *hackingu* zwracałem uwagę, analizując projekt kodeksu karnego z 1993 r. (zob. A. Adamski, *Przestępstwa komputerowe w projekcie kodeksu karnego na tle europejskich standardów normatywnych*, w: *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z konferencji naukowej*, Poznań, 20-22 kwietnia 1994, Toruń 1994, s. 152).

niony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym". Oczywiście program komputerowy trudno byłoby uznać za desygnat pojęcia „urządzenie", jakim posługuje się ten przepis[14]. Program komputerowy bowiem jest zespołem instrukcji napisanych w języku „zrozumiałym" dla urządzenia, jakim jest komputer, by ten wykonywał określone zadania. Sam program nie posiada jednak atrybutów urządzenia i bez udziału komputera nie jest zdolny do wykonywania żadnych funkcji.

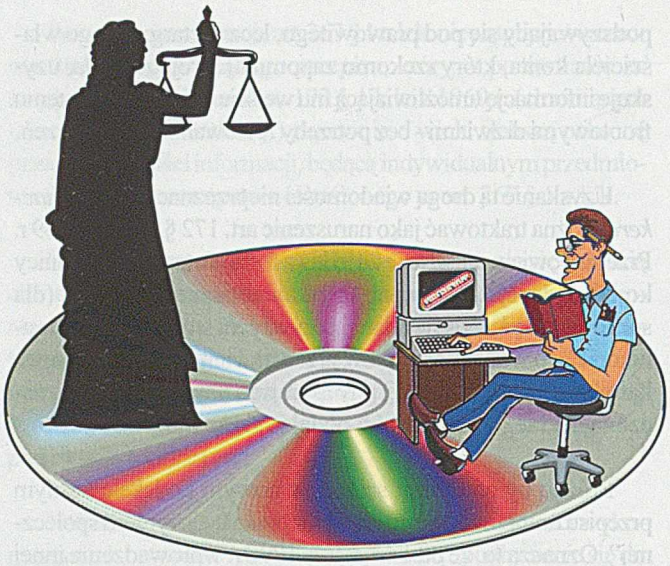
To samo można powiedzieć o komputerze, który w zależności od rodzaju zainstalowanego w nim oprogramowania może być wykorzystywany do różnych zadań. Z tego powodu należy przyjąć, że komputer wyposażony w specjalny program umożliwiający uzyskanie zastrzeżonej dla sprawcy informacji jest urządzeniem, o którym mówi przepis art. 267 § 2 n.k.k.

Nie ulega wątpliwości, że programem takim jest *password sniffer*, który umożliwia monitorowanie ruchu w danej sieci i przechwytywanie początkowej sekwencji bajtów każdej sesji, które zawierają identyfikatory i hasła użytkowników monitorowanej sieci. Posłużenie się *snifferem* pozwala *hackerowi* na uzyskanie informacji, do której nie jest on uprawniony. Stanowi więc czyn zabroniony w rozumieniu art. 267 § 2 n.k.k.

W podobny sposób można uzasadnić karalność stosowania *spoofingu* i innych technik podszywania się pod uprawnionego użytkownika w celu uzyskania nielegalnego dostępu do systemu komputerowego. Trzeba jednak podkreślić, że ze względu na brzmienie art. 267 § 2 n.k.k. warunkiem zastosowania tego przepisu wobec *hackera* uprawiającego *spoofing* jest możliwość wykazania mu, iż celem jego działania było uzyskanie informacji znajdujących się w atakowanym przez niego systemie, nie zaś na przykład chęć wypróbowania programu umożliwiającego *spoofing* lub sprawdzenie własnych *hackerskich* umiejętności. W aspekcie praktycznym oznacza to spore szanse na uchylenie się przed odpowiedzialnością karną przyłapanego na gorącym uczynku *hackera*, któremu nie będzie można przedstawić dowodów wskazujących na działanie w zamiarze uzyskania informacji.

Hacking z wykorzystaniem luk bezpieczeństwa

Wszelkie słabości systemów operacyjnych, potokołów sieciowych i programów aplikacyjnych są bezlitośnie eksploatowane przez *hackerów* - najczęściej w celu zamanifestowania ich logistycznej przewagi nad profesjonalnymi twórcami i producentami *softwaru*. Zarówno Internet[15], jak i literatura przedmiotu[16], obfitują w szczegółowe informacje i opisy na ten temat. Zamiast więc



cytować znajdujące się tam opisy, przejdźmy od razu do konkluzji uwzględniającej prawny aspekt tego zagadnienia.

O popełnieniu przestępstwa określonego w art. 267 § 1 n.k.k decyduje sposób uzyskania zastrzeżonej informacji, nie zaś samo jej uzyskanie. Jeżeli następuje to bez przełamywania zabezpieczeń - przestępstwa nie ma. Jeżeli sprawca wykorzystuje błąd programisty i wchodzi do systemu przez „dziurę" w konfiguracji lub oprogramowaniu systemowym po to, by uzyskać znajdującą się w systemie informację - nie można mu nawet przypisać usiłowania przestępstwa, o którym mówi art. 267 § 1 n.k.k. Jeżeli „przechodzenie przez dziurę" nie wymaga od *hackera* ingerencji w zapis na komputerowym nośniku informacji lub korzystania ze specjalnego oprogramowania - zachowanie takie w ogóle nie jest karalne.

❖ ❖ ❖

Jak więc widać z powyższego - bynajmniej niewyczerpującego - wyliczenia, uzyskanie dostępu przez osobę nieuprawnioną do cudzego systemu komputerowego i skopiowanie znajdującego się tam zapisu informacji, nie zawsze będzie prowadzić do kolizji z przepisami nowego kodeksu karnego. Spostrzeżenie to wydaje się istotne dla co najmniej trzech kategorii podmiotów.

Ustawodawcę powinno inspirować do ulepszenia prawa. Organom, które prawo to będą stosować, uświadamia potrzebę korzystania w szerokim zakresie z opinii biegłych, głównie na okoliczność: „czy zarzucany sprawcy czyn wypełnia znamiona ustawowe przestępstwa?" Dla potencjalnych sprawców zamachów na nienaruszalność i poufność informacji przetwarzanej w systemach komputerowych może natomiast stanowić swoiste *memento*. „Sędziowie - jak głosi art. 178 ust.1 Konstytucji RP - w sprawowaniu swego urzędu są niezawiśli i podlegają tylko Konstytucji oraz ustawom". Trzeba się więc liczyć z ewentualnością, że ich punkt widzenia na wykładnię omawianych przepisów może różnić się od zareprezentowanego w niniejszym wystąpieniu.

Andrzej Adamski jest pracownikiem Katedry Prawa Karnego i Polityki Kryminalnej Uniwersytetu Mikołaja Kopernika w Toruniu
e-mail: aadamski@law.uni.torun.pl

[14] Urządzenie to: „rodzaj mechanizmu lub zespół elementów, przyrządów służących do wykonywania określonych czynności, uławiający pracę." (*Słownik jezyka polskiego,* pod red. M.Szymczaka, t.III, Warszawa 1992).

[15] Np. http://oliver.efri.hr/~crv/security/bugs/list.html

[16] Zob. np.: W. R. Cheswick, S. M. Bellovin, *Firewalls and Internet Security*, Addison-Wesley, 1994; S. Garfinkel, G. Spafford, *Bezpieczeństwo w Unixie i Internecie*, Warszawa 1997.

Parę uwag o prawie i bezpieczeństwie systemów komputerowych

Tomasz Ryś

Egzekwowanie prawa w Polsce pozostawia wiele do życzenia, a zwłaszcza prawa „nowego". Problem bezpieczeństwa sieci komputerowych nie ogranicza się oczywiście tylko do zagadnień prawnych.

Ustawa o prawach autorskich funkcjonuje już parę lat. Przez ten czas – w odniesieniu do oprogramowania – mieliśmy w Polsce tak naprawdę tylko jedną „grubą" aferę, w której chodziło o legalną sprzedaż w Polsce oprogramowania kupionego legalnie w USA. Cały problem w swojej istocie sprowadzał się do braku możliwości „odcinania kuponów" przez europejskie (polskie) przedstawicielstwo producenta tego oprogramowania, bowiem sprzedaż realizowana była poza „oficjalnym" kanałem dystrybucyjnym. Wiele firm dawno rozwiązało ten problem i przestało bawić się w rozróżnianie amerykańskich i europejskich wersji. Szary import (bo z tym mieliśmy w zasadzie do czynienia) był i będzie, a jedyną przed nim obroną jest opieka i wsparcie techniczne oferowane tylko „legalnym" klientom. „Afera" ta w sumie miała bardzo mało wspólnego z ustawą o prawie autorskim, mimo że zaangażowano niebagatelne siły policyjne. Poza tym w dwu innych przypadkach prokuratora zwróciła się do nas o identyfikację sprzedawanych programów zawartych w liście złapanego „kopiarza" dysków CD. I to wszystko – sami niewinni !?! Kontrastuje to wyraźnie z informacjami producentów oprogramowania, którzy twierdzą, że Polska to raj dla piratów i tracą tutaj grube miliony dolarów.

Zarówno organy ścigania jak i użytkownicy systemów komputerowych muszą się dopiero nauczyć jak rozpoznawać włamania i identyfikować ich skutki. Wymaga to sporo czasu, wysokich kwalifikacji, ogromnego doświadczenia i odpowiedniego prawa.

Podobnie, choć tak naprawdę jeszcze gorzej, będzie z funkcjonowaniem przepisów prawa dotyczących *hackingu* bowiem problem jest znacznie bardziej delikatny i dużo trudniej wykrywalny. Zarówno organy ścigania jak i użytkownicy systemów komputerowych muszą dopiero nauczyć się jak rozpoznawać włamania i identyfikować ich skutki. Wymaga to sporo czasu, wysokich kwalifikacji, ogromnego doświadczenia i odpowiedniego prawa. W krajach, które borykają się z tym problemem od lat wykrywalność tego typu przestępstw jest nadal niezbyt imponująca, a *hackerzy* są czasami poszukiwani latami. Jedynym pocieszającym faktem jest to, że jest ustawa (lepsza lub gorsza), która pozwoli w ogóle zacząć działać.

Tak naprawdę to w Polsce mamy do czynienia w odniesieniu do *hackingu* z problemem społecznym. Wiele organizacji nadal traktuje włamania do systemów komputerowych jako coś wstydliwego i ma ogromne poczucie winy, bliskie syndromowi dorastającego chłopca, w wypadku stwierdzenia włamania. W opinii społecznej panuje bowiem mylne przekonanie o tym, że z komputerem można zrobić wszystko co się tylko da. Jak coś się nie udaje to trudno, ale jak można przeczytać listy kolegi bo zapomniał ustawić hasło – to jest to w porządku. Nic bardziej mylnego. Musimy zdać sobie sprawę z tego, że włamania do systemów komputerowych są dokładnie tym samym co włamanie do naszych mieszkań. Skopiowanie pliku nie należącego do mnie jest dokładnie tym samym, co włamanie się do biurka kolegi i wykradnięcie stamtąd taśmy czy dyskietki. Jeżeli ktoś okradnie nasze mieszkanie zgłaszamy ten proceder na policję, rozgłaszamy na lewo i prawo – a wszyscy nam współczują. Dokładnie tak samo powinno być w przypadku włamań do systemów komputerowych. Powinnyśmy mówić o tym głośno i wyraźnie. Przecież nie ukrywamy włamania do naszych mieszkać tylko z tego powodu, że zostawiliśmy otwarte okno balkonowe na trzecim piętrze. Im więcej będzie informacji o dokonanych włamaniach tym więcej osób dostrzeże ten problem i pozna najprostsze metody zabezpieczeń.

Przeważająca większość włamań do systemów komputerowych realizowana jest na bazie inżynierii społecznej. *Hacker* sprytem, inwencją i tupetem wchodzi w posiadanie identyfikatora i hasła, które otwiera mu wrota do systemu. Czasami wystarczy telefon do mało rozgarniętej sekretarki i powołanie się na jakiegoś dyrektora i sytuację krytyczną. W innym wypadku wystarczy pogadać przy piwie z „przypadkowym" człowiekiem na hałaśliwej dyskotece. Można także po prostu wejść do pokoju administratora, który zostawił pracujący terminal z uprawnieniami administratora i właśnie wyszedł na godzinny *lunch*. Te proste metody okazały się bardzo skuteczne w realizacji wielkich włamań.

Ochrona systemów komputerowych to nie tylko zapora ogniowa (*firewall*). Problem bezpieczeństwa jest niezwykle złożony, a opracowanie „prawdziwej" polityki bezpieczeństwa dla określonej organizacji wymaga sporo czasu i nakładów. Należy bowiem wziąć pod uwagę wszystko: zabezpieczenie pomiesz-

czeń, sposób realizacji kopii bezpieczeństwa, przepływ informacji, wersje oprogramowania, itd. Nie wystarczy po prostu kupić *firewall*-a. To tak jakby kupić do domu zamek do drzwi bo nazywa się „zamek". Nieważne, że można go otworzyć wytrychem zrobionym z drutu – mamy przecież *firewall*. W innym przypadku możemy też założyć skomplikowany zamek szyfrowy, opancerzyć drzwi, ale kompletnie zignorować fakt, że mieszkamy na parterze i domownicy, często wychodząc z domu, zostawiają otwarte drzwi balkonowe bo jest potworny upał. Podobnie jest z zaporami ogniowymi. Nie każde oprogramowanie mające w nazwie *firewall* jest prawdziwym zabezpieczeniem. Nie wystarczy ustawić zaporę na dostęp z Internetu, bowiem przeważająca większość włamań w dużych organizacjach realizowana jest z jej wnętrza. Przykłady: obrażony pracownik usuwa bardzo ważne dane, aby zemścić się na dyrekcji bo nie dostał podwyżki; dział techniczny swobodnie przegląda listy płac, które powinny być dostępne tylko dla działu finansowego, itp. Często też zdarza się, że mamy doskonale zabezpieczony system, ale zapominamy o tym, że dysk może po prostu się zepsuć. Nie archiwizujemy danych w odpowiednim reżimie ślepo wierząc w doskonałość współczesnej techniki. Mamy *firewall*, tyle że tracimy wszystkie dane – zupełnie bez udziału *hackera*. Odpowiedni systemem *backup*-ów może być jedynym ratunkiem w wypadku destrukcyjnych włamań. Dobra organizacja archiwizacji, odpowiedni sprzęt i oprogramowanie pozwolą odbudować zniszczony system w ciągu paru godzin.

Ochrona systemów komputerowych to nie tylko zapora ogniowa (*firewall*). Problem bezpieczeństwa jest niezwykle złożony, a opracowanie „prawdziwej" polityki bezpieczeństwa dla określonej organizacji wymaga sporo czasu i nakładów.

Hacker hobbysta może jednak być bardzo przydatny jako specjalista analizujący stan zabezpieczenia naszego systemu. Zatem nie każdy członek listy dyskusyjnej o _hackingu_ musi być od razu przestępcą.

Odrębnym zagadnieniem jest także monitorowanie włamań. Nie każdy *firewall* pozwala natychmiast wykryć, że następuje właśnie włamanie i określić jakie szkody wyrządził *hacker*. Często włamywacz tygodniami buszuje po naszym systemie, aż zdecyduje się na jakiś krok rozpaczy, aby ktoś to w końcu zauważył. *Firewall* powinien mieć mechanizmy zbliżone do kamery telewizyjnej. Mimo, że włamywacz pracował w rękawiczkach, to jednak możemy się o nim coś dowiedzieć analizując zapis „wideo". Wielu *hackerów* traktuje włamania do systemów komputerowych jak jeszcze jedną grę komputerową typu *Red Alert*: „udało mi się złamać ten system – wygrałem". Robią to po prostu „dla sportu", choć włamanie do systemu bankowego i możliwość przelania sporych pieniędzy na własne konto może skusić każdego. Wtedy *hacker* staje się prawdziwym przestępcą i już musi być ścigany – w grę wchodzą spore pieniądze. Musimy jednak zdać sobie sprawę, że pozyskanie poufnych danych (np. jakiegoś listu, opisu projektu), może być brzemienne w skutki - dla nas prywatnie lub dla całej firmy. *Hacker* hobbysta może jednak być bardzo przydatny jako specjalista analizujący stan zabezpieczenia naszego systemu. Zatem nie każdy członek listy dyskusyjnej o *hackingu* musi być od razu przestępcą.

W czasach, w których telefon w Polsce nie jest już czymś wyjątkowym, a z Internetem możemy połączyć się z praktycznie dowolnego mieszkania, coraz więcej osób dostrzega problem ochrony systemów komputerowych. Wielu też zaczyna rozumieć, że nawet modem, pozostawiony bez zabezpieczeń wewnątrz firmy, jest potencjalnym zagrożeniem dla bezpieczeństwa danych. Coraz więcej osób zauważa, że są *firewalle* i dobre *firewalle*. Dostrzegamy problem poufności danych, utajniania bitów w komputerze i konstrukcji alarmów poza solidnymi „zamkami". Nas, jako dystrybutorów oprogramowania CheckPoint Firewall-1, bardzo to cieszy, bowiem sprzedaż tego systemu wzrosła w ostatnim roku o ponad 300%.

Mam nadzieję, że dobry system zaporowy razem z wchodzącą ustawą przyczynią się skutecznie do zwiększenia wykrywalności *hackerów*-przestępców i tym samym do poprawy bezpieczeństwa sieci komputerowych. Problemu nie da się już dłużej ignorować w czasach kiedy komputerami w naszych domach zaczynają się bawić pięcioletnie urwisy.

Tomasz Ryś jest dyrektorem działu dystrybucji oprogramowania krakowskiej firmy CLICO
E-mail: tomasz.rys@clico.pl
http://www.clico.pl

Hack w Nowym Kodeksie Karnym - nihil novi

Kornel Rozpara

Po zapoznaniu się z treścią Nowego Kodeksu Karnego, zwłaszcza z przepisami dotyczącymi przestępstw komputerowych, zastanawialiśmy się z przyjaciółmi, jaki będzie on miał wpływ na działalność polskich *hackerów*? Początkowo przeraziły nas przewidywane kary, ale po namyśle i dokładnej analizie przepisów n.k.k. doszliśmy do wniosku, że „nie taki diabeł straszny, jak go malują.

1 września wchodzi w życie nowy kodeks karny, który przewiduje surowe kary za przestępstwa komputerowe.
Czy hackerzy powinni się bać tej daty?
Aby na to pytanie odpowiedzieć należy zdefiniować różnych „maniaków komputerowych". Należy pamiętać, że nie każdy, uważany przez społeczeństwo za hackera, jest nim naprawdę. Kto więc powinien się bać, a kto może w spokoju robić swoje w świecie systemów komputerowych?

Definicje, czyli o czym mówimy?

Prawdziwy *hacker* nie jest przestępcą, dlatego nie martwią go przepisy n.k.k., ponieważ nie zamierza ich łamać. Omija on zabezpieczenia systemów, aby ujawnić coś, co obrazowo nazywamy "dziurami". Czy jest to przestępstwo, jeśli wejdę do czyjegoś mieszkania przez dziurę w ścianie, której właściciel nie zauważył, i zostawię mu kartkę z napisem: „Drogi Panie, w ścianie jest ogromna dziura. Ma Pan tu taki bałagan, że z pewnością jej Pan nie dostrzeże. Warto ją zamurować, ponieważ jutro może przyjść złodziej i wynieść wszystko z mieszkania. Życzliwy." Tak więc prawdziwy hacker nie wchodzi do czyjejś „wirtualnej posesji" w celu zniszczenia czy kradzieży danych, tylko po to, by wykazać, że włożył wiele pracy aby odnaleźć dziurę i dowieść, że jest lepszym fachowcem niż producent i administrator. Jeśli dodatkowo pomoże administratorowi (właścicielowi) usunąć błąd w systemie i w ten sposób zablokuje dostęp do niego, to raczej zasługuje na nagrodę niż karę. *Hacker* zatem nie jest przestępcą wedle przepisów n.k.k.

W naszym środowisku są to sprawy oczywiste. *Cracker* jest to osoba, która nie szuka błędów i niedoróbek systemowych (nazywamy je *bugami*), lecz kradnie plik z hasłami i próbuje złamać któreś z nich. Jeśli przyjmiemy, że hasło samo w sobie jest informacją prywatną, wtedy jej deszyfracja i odczytanie jest przestępstwem (art.267 par. 1). Podobnie jest z *carderami*. Są to osoby, które w nieuczciwy sposób zdobywają numery kart kredytowych i używają ich w celu osiągnięcia korzyści majątkowych. Jest to oczywiste przestępstwo, które, moim zdaniem, powinno być karane nawet jeszcze bardziej surowo niż obecnie. Ponieważ zarówno *carderzy,* jak i *crackerzy,* nie cieszą się sympatią tzw. dobrych *hackerów*, to uważamy, że 1 września 1998 roku jest dniem sukcesu zarówno polskiego prawa, jak i osób zajmujących się wyszukiwaniem „bugów" w systemach operacyjnych. W swoim imieniu i moich kolegów wyrażam zadowolenie, iż n.k.k odstraszy czy może ograniczy działalność młodych „chakerów", zwanych także lamerami, których działalność powoduje, że prawdziwi fachowcy, czyli my, jesteśmy postrzegani przez władze, media oraz zwykłych ludzi jako przestępcy. Nie ukrywam, iż nowy kodeks będzie miał wpływ na niektóre nasze działania praktykowane dotychczas, mające na celu dostanie się do czyjegoś systemu.

Motywacje *hackera*

Przypomnijmy sobie, jakie są motywacje hackera, który chce dokonać „włamania" do cudzej sieci. Pierwszą jest chęć zaspokojenia swoich ambicji. Wykazanie błędu lub niedoróbki w systemie operacyjnym jest nie lada osiągnięciem, zatem trudno się dziwić, iż młodzi ludzie pragną udowodnić, że są lepsi od administratorów czy producentów oprogramowania, którzy biorą przecież za swoją pracę niemałe pieniądze. Lecz jest coś, co przewyższa uczucie triumfu po znalezieniu „buga", coś wiąże

się z pojęciami „hack", „hacker", „hacking". Skąd wywodzi się ta nazwa? Aby to wyjaśnić musimy cofnąć się do przełomu lat 70. i 80. Otóż właśnie w tamtych czasach, ludzi zajmujących się komputerami, zagłębiających się w ich tajemnice nazwano *hackerami* (*hacker* - osoba wynajmowana do bardzo ciężkiej pracy). Porównywano ich z osobami karczującymi lasy, z pionierami ciężko pracującymi, aby ucywilizować nowe tereny. To jest odpowiedź na pytanie, jaki jest główny motor działań *hackerów* – zamiłowanie do ciężkiej pracy. Jeśli któryś z moich kolegów w ciągu pięciu minut włamie się do kilku słabo zabezpieczonych systemów, a ja będę przez dwa tygodnie pracował nad naprawdę trudnym serwerem, to kto będzie miał większą satysfakcję? Dlatego im wyższe poprzeczki stawiają nam producenci, administratorzy i prawodawcy, tym większa jest nasza satysfakcja i radość z osiągniętego sukcesu.

Nowe prawo, nowa strategia

Czy n.k.k. jest zatem długo wyczekiwanym przez *hackerów* rozwiązaniem? Otóż nie wygląda to tak różowo. Problem polega na tym, że nie wiem, na jakiej podstawie przedstawiane będą zarzuty popełnienia przestępstwa? Jeśli dowodem mają być logi systemowe, to istnieje prawdopodobieństwo powstania swoistego chaosu podczas ścigania „włamywacza". Wyobraźmy sobie sytuację, kiedy hacker, nie naruszając przepisów, dostaje się do *hosta* - ofiary. Znajduje „buga" i zostawia list informujący o znalezionej dziurze w systemie. Większość administratorów to ludzie ambitni i traktują „buszującego" w ich sieci bez uprawnień jak osobistego wroga. Gdy zechcą komuś zaszkodzić, to w każdej chwili mogą spreparować logi (dużo łatwiej niż dokument papierowy) i „wrobić" w poważne (wg n.k.k.) przestępstwo często niewinną osobę. Dlatego po 1 września *hacker* będzie musiał zacierać dokładnie ślady. Jak to zrobić, aby nie złamać przy tej okazji przepisu z art. 268 par. 1 i 2? Czy mam zatem wybrać legalny *hacking*, nie usuwać logów i pozwolić, by administrator, znający mój adres IP, wykorzystał tę wiedzę przeciwko mnie? Wobec tego wykrycie prawdziwego przestępcy będzie niezwykle trudne i wymagać będzie dokładności i ogromnej wiedzy ze strony organów ścigania. *Hackerów* może pocieszać fakt, iż w n.k.k. w art.115 par.14 istnieje wyraźna definicja dokumentu elektronicznego, a art.270 par.1 stwierdza, iż przerabianie lub podrabianie takiego dokumentu w celu użycia go jako autentycznego podlega karze ograniczenia lub pozbawienia wolności od 3 miesięcy do 5 lat. Co się z tym wiąże? Każdy administrator naraża się na poważne konsekwencje, preparując na przykład logi systemowe. Jak wspomniałem, jest to problem poważny i musimy poczekać na proces precedensowy, by ustalić taktykę działania.

Spójrzmy teraz okiem *hackera* na przepisy dotyczące przestępstw komputerowych w n.k.k. i zastanówmy się, co hacker może, a czego mu nie wolno. Nowy kodeks karny określa wyraźnie, iż przestępstwem jest jedynie przeczytanie, zniszczenie lub ingerencja w zawartość dokumentu przez osobę do tego nieuprawnioną (art. 267 par.1 i art. 268 par.1 i 2). Podczas mojej *hackerskiej* działalności, jedynymi dokumentami, które trwale zmieniałem, były logi systemowe. Jednak według nowego prawa, wiedząc, że nie robię niczego złego, mogę chyba zaprzestać czyszczenia logów, modląc się jednocześnie, by ambitny administrator (zwany przez nas adminem) nie zrobił ze mnie złodzieja cennych informacji. Choć to wówczas on dokonuje przestępstwa. Równie dobrze mogę dostać się do systemu ofiary z jakiegoś zagranicznego. Jeśli nie naruszę prawa i nie spowoduję szkód na serwerze, to ufam, że ambitny administrator nie będzie ścigał niewinnego Yokashiru Kashimoto, z którego konta dostałem się do atakowanego systemu.

Zastanówmy się nad atakami typu DoS (*Denial of Service*). Art. 165 par 1 p.4 n.k.k stwierdza, że *L'nie wolno sprowadzać niebezpieczeństwa dla na przykład mienia o wielkich rozmiarach poprzez zakłócanie lub uniemożliwianie przetwarzania, gromadzenia lub przesyłania informacji*. Ataki DoS mają na celu wyłączenie, ewentualnie zawieszenie systemu komputera - ofiary spełniają zatem często kryteria poszkodowanych opisanych w tym artykule. Dlatego też uważam, iż młodzi „chakerzy", którzy dla zabawy wysyłają tzw. teardropa w celu unieruchomienia poważnego serwisu, powinni mieć się na baczności. Choć moje pytanie brzmi: jak udowodnić komuś zdalne zakłócanie pracy serwera, podczas gdy ataki komputerowe nie obowiązują korelacje czasowe i trudno określić miejsce, z którego dokonano przestępstwa.

Art. 267 par. 2 zabrania używać wszelkich urządzeń, dzięki którym osoba nieuprawniona może uzyskać dostęp do pewnej informacji. Zrezygnować zatem należy z niektórych programów. Pragnę jednak podkreślić, że najczęściej nie służą one do uzyskiwania dostępu do danych, lecz wykonują wiele operacji, które umożliwią osobie atakującej uzyskanie uprawnień administratora.

Reasumując, nie ulega wątpliwości, że sam proces dostania się do systemu i otrzymania praw administratora nie zawsze jest przestępstwem w rozumieniu n.k.k. Z przestępstwem mamy do czynienia, gdy włamanie było przeprowadzone w celu uzyskania informacji przechwytywanych za pomocą komputera. Nowy kodeks karny być może odstraszy wielu podszywających sie pod *hackerów* przestępców, dzięki czemu popularny obraz prawdziwego *hackera* stanie się bardziej pozytywny. Warto jednak pamiętać, że żadne przepisy nie wyeliminują zjawiska *hackingu* całkowicie, a mogą jedynie zmniejszyć liczbę „wybryków" osób czyniących wielkie szkody w systemach komputerowych. Wprowadzany obecnie kodeks karny może tylko ucieszyć nas - *hackerów*, jak i zapewne administratorów. Wątpliwy może być jedynie proces uzyskania bezspornego dowodu winy, a czy w tej kwestii n.k.k. spełni swe zadanie, przekonamy się w przyszłości.

Kornel Rozpara jest tegorocznym maturzystą, organizatorem pierwszego zlotu *hackerów* w Polsce Hacking in Poland 1998 – HiP'98 (Informatyka 6/98).
e-mail: m0rbius@multi-ip.com.pl

Administrowanie dużymi systemami baz danych

Wojciech Czujowski, Jacek Gruber

Systemy informatyczne w organizacjach służą głównie do eksploatacji baz danych. Bardzo istotne jest zapewnienie właściwego poziomu dostępności i niezawodności systemów bazodanowych, ponieważ są one systemami produkcyjnymi. Można to osiągnąć, stosując właściwe procedury administrowania oparte na wiedzy o budowie i środowisku działania systemów baz danych. Wielkość oraz rozproszenie tych systemów znacznie komplikują procedury i problemy administrowania.

Wzrastającą wagę zagadnień eksploatacji i administrowania dużymi bazami danych potwierdza organizowanie dorocznych światowych konferencji naukowo-technicznych im poświęconych [2], jak również czasopismo omawiające wyłącznie tę problematykę [1].

Całościowe spojrzenie na problematykę administrowania dużymi bazami danych umożliwia sformułowanie katalogu zaleceń przydatnych w pracy administratorów.

Administrowanie systemem zarządzania bazą danych (SZDB) polega na utrzymaniu możliwie wysokiej wydajności przetwarzania oraz dostępności i bezpieczeństwa danych systemów baz danych (SBD), które pracują pod kontrolą systemów SZBD. System SBD to baza danych wraz z jedną lub kilkoma aplikacjami, które z tych danych korzystają.

System SBD, który nie jest właściwie i starannie administrowany, nie może w sposób zadowalający dostarczać usług, których się od niego oczekuje. Często jest to przyczyną wielu komplikacji, a nawet poważnych strat finansowych.

W praktyce administrator bazy danych (ABD) nie ma żadnego wpływu na fazy tworzenia i rozwoju w cyklu życia systemu SBD. Administrowanie bazą danych odbywa się jedynie podczas eksploatacji oraz utrzymania SBD. ABD może natomiast wpływać na konserwację i pielęgnację przez optymalizację wydajności, niezawodności [8] i bezpieczeństwa systemu SBD.

Brak jest precyzyjnego kryterium określającego, które bazy danych można sklasyfikować jako duże. Pod tym pojęciem rozumie się zwykle te z nich, w których ilość przechowywanych w relacjach krotek jest znaczna lub bardzo duża. W takich bazach dużą rolę odgrywają czynniki, które w małych bazach nie są istotne, a tym bardziej krytyczne [2].

Wielkość bazy danych jest dość ściśle związana z optymalizacją wydajnościową i niezawodnościową, które z kolei zależą od odpowiedniej alokacji danych bazy.

Duża baza jest najczęściej rozproszoną bazą danych (RBD). Rozproszony system bazy danych (RSBD) to system całościowy, tzn. baza danych wraz z jedną lub kilkoma aplikacjami korzystającymi z jej danych. Natomiast system zarządzania rozproszonymi bazami danych (SZRBD) to środowisko programowe funkcjonowania systemów RSBD. Przetwarzanie danych może odbywać się pod kontrolą jednego lub wielu SZRBD, które mogą być niezależne albo homo- lub heterogeniczne.

Poprzez odpowiednią fragmentację bazy danych można zwiększyć efektywność przetwarzania. Poprawę efektywności dostępu do danych oraz niezawodności systemu bazodanowego można również osiągnąć, stosując replikacje RBD.

W wymienionych tu rozwiązaniach powstaje problem utrzymywania spójności bazy, czyli propagacji modyfikacji danych bazy RBD. W celu utrzymania spójności scentralizowanych (lokalnych) baz danych stosuje się algorytmy dwufazowego zatwierdzania (*two-phase commit - 2PC*) transakcji. Algorytmy stosowane dla baz rozproszonych wymagają jeszcze jednej fazy. Nazywamy je algorytmami trzyfazowego zatwierdzania (*three-phase commit - 3PC*) transakcji. W celu zapewnienia spójności baz RBD i niezawodności systemów RSBD stosuje się także algorytmy odtwarzająco-naprawcze transakcji zakłócanych przez uszkodzenia miejsc sieciowych systemu bazy danych.

Charakterystyka topologii stosowanych do zarządzania dużymi bazami danych

Omawiając możliwie precyzyjnie zagadnienia administrowania dużymi bazami danych, dokonamy krótkiego przeglądu wpływu stosowanych topologii środowisk operacyjnych i sieciowych na zarządzanie takimi bazami. Uwzględnimy przy tym zastosowania tych topologii zarówno do scentralizowanych, jak i rozproszonych baz danych.

Scentralizowane bazy danych

Baza scentralizowana to lokalna baza danych, w której dane są przechowywane na jednym komputerze. Możliwy jest zdalny dostęp do danych. Do zarządzania scentralizowaną bazą danych stosuje się zwykle jeden system SZBD. Optymalizacja dostępu do danych bazy scentralizowanej polega na odpowiedniej indeksacji danych. Dla dużych baz danych zalecane jest tworzenie i utrzymywanie indeksów dla dużych relacji. Relacje o małej ilości krotek mogą być nieindeksowane. Indeksowanie znacznie przyspiesza wyszukiwanie danych.

Ważnym czynnikiem jest odpowiednia konstrukcja zapytań pochodzących zarówno z aplikacji (wpływ administratora jest ograniczony), jak i definiowanych przez użytkownika lub administratora w sposób bezpośredni (wpływ administratora bywa znaczący).

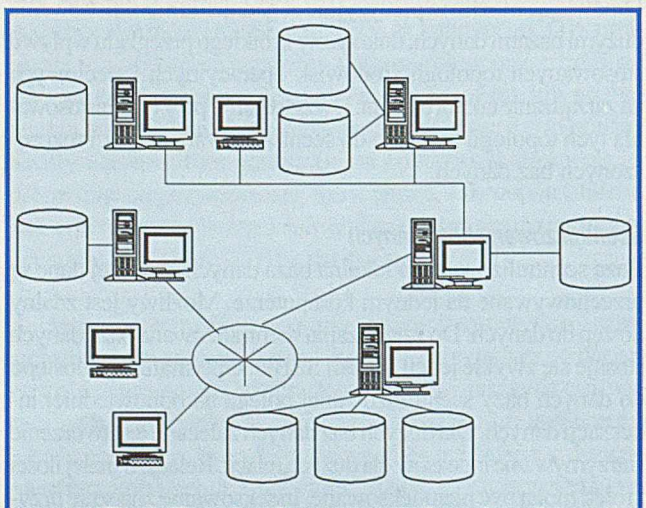
Jednym z głównych zadań systemu SZBD jest kontrola i utrzymywanie spójności danych zarówno w czasie normalnego funkcjonowania SZBD, jak i w razie awarii. „Pilnowanie" wielu spośród różnorodnych więzów bazy danych jest implementowane z zastosowaniem wyzwalaczy, czyli procedur uruchamianych w wypadku określonych działań na bazie danych. W celu utrzymania spójności danych wykorzystuje się również przetwarzanie transakcyjne. Przy przetwarzaniu transakcji w scentralizowanych SZBD stosuje się protokoły dwufazowego zatwierdzania [8]. Niezawodność scentralizowanej bazy danych jest w dużej mierze zależna od sprzętu i oprogramowania systemowego oraz zarządzającego bazą danych. W celu zabezpieczenia danych stosuje się również archiwizację. Konieczne jest określenie procedur postępowania archiwizacji i odtwarzania danych w wypadku awarii. Proces archiwizacji i odtwarzania dla dużych baz danych jest zwykle bardzo czasochłonny.

Administrowanie dużą, scentralizowaną bazą danych sprowadza się zatem do utrzymania spójności oraz odpowiedniego poziomu zabezpieczeń dostępu. Nie można natomiast uzyskać optymalnych rozwiązań problemu dostępu do danych. Zatem również poziom niezawodności takiej bazy jest zwykle niezadowalający. W celu zwiększenia wydajności, dostępności i bezpieczeństwa buduje się rozproszone bazy danych.

Rozproszone bazy danych

Rozproszona baza danych RBD jest zbiorem zwielokrotnionych, pozostających ze sobą w logicznej relacji, w dużym stopniu autonomicznych baz danych, znajdujących się w wielu miejscach sieci komputerowej (rys. 1). Bazy te mogę być zarządzane przez wiele SZRBD.

Powodem stosowania rozproszonych baz danych jest łatwość ich dopasowania do struktury dużych, rozproszonych terytorialnie organizacji. Rozproszona baza danych jest postrzegana przez użytkownika jako baza o pewnym schemacie, ale całkowicie scentralizowana. Systemy rozproszonych baz danych realizują te same zadania co systemy scentralizowane, lecz bardziej wydajnie (zwiększona dostępność) i bezpiecznie.



Rys.1. Zarządzanie rozproszoną bazą danych

Zarządzanie rozproszoną bazą danych może odbywać się w sposób scentralizowany lub rozproszony.

Scentralizowane zarządzanie rozproszoną bazą danych polega na wykorzystaniu jednego SZBD. Poszczególne SZBD komunikują się z centralnym SZBD, który posiada informacje o wszystkich fragmentach i replikach oraz ich wykorzystaniu.

Rozproszone zarządzanie rozproszoną bazą danych polega na zwiększeniu autonomiczności poszczególnych SZBD, które komunikują się między sobą w celu wspólnej realizacji określonych zadań. SZBD wchodzące w skład systemu zarządzania rozproszoną bazą danych SZRBD nie muszą być homogeniczne.

Ważną cechą SZRBD jest wykorzystywanie w nich architektury klient-serwer. W SZRBD wykorzystuje się te modele architektury, które zapewniają zdalne zarządzanie danymi, rozproszone zarządzanie danymi oraz rozproszone przetwarzanie.

Analiza przykładowych mechanizmów stosowanych w systemach zarządzania dużymi bazami danych

Mimo że administrator nie może wpływać ani na początkowe fazy cyklu życia SBD, związane z jego tworzeniem, ani na metody optymalizacji procesu przetwarzania stosowane wewnątrz SZBD, to znajomość tych zagadnień może mu jednak pomóc w rozwiązywaniu problemów administrowania.

Przedstawimy krótko mechanizmy przetwarzania i optymalizacji zapytań i na podstawie ich analizy podamy ogólne zalecenia dotyczące konstruowania zapytań. Na podstawie własności protokołów przetwarzania transakcji podamy zalecenia dla administratora odnośnie do obsługi transakcji w dużych bazach danych.

Przetwarzanie i optymalizacja zapytań - wydajność przetwarzania i dostępność danych

Zapytanie może pochodzić od systemu bazy danych lub bezpośrednio od użytkownika. Najczęściej spotykanymi kryteriami optymalizacji zapytań są [3]:

- dla baz scentralizowanych
  - ✓ minimalizacja kosztu całkowitego zapytania,
  - ✓ minimalizacja czasu przetwarzania i objętości tworzonych tymczasowo relacji roboczych,
- a dla baz rozproszonych dodatkowo
  - ✓ minimalizacja ruchu sieciowego wywołanego przetwarzaniem zapytania.

Nie mając wpływu na zapytania pochodzące z zaprojektowanych aplikacji, administrator może jednak konstruować zapytania służące np. do tworzenia bieżących raportów oraz - w wypadku bazy rozproszonej - modyfikacji globalnej bazy danych. Istnieją ogólne zalecenia dotyczące konstruowania zapytań [4]:

- należy tworzyć zapytania korzystające ze złączeń i półzłączeń zamiast z podzapytań;
- w zapytaniach należy unikać operatorów negacji, sumy, różnicy.

Sposób przetwarzania oraz optymalizacja zapytań należą do podstawowych problemów w dużych bazach danych. Zagadnienia te są znacznie trudniejsze do rozwiązania w bazach rozproszonych niż w scentralizowanych ze względu na znacznie większą ilość parametrów wpływających na wydajność realizacji zapytań rozproszonych. Administrator dużej bazy danych powinien znać

zasady konstrukcji i dekompozycji zapytań, lokalizacji danych oraz przynajmniej zasady znajdowania rozwiązań stosowane w algorytmach ich przetwarzania i optymalizacji.

Ponieważ do specyfikowania dostępu do danych używa się zwykle nieproceduralnych języków obliczeń relacyjnych, to nie ma możliwości wskazania sposobu poszukiwania odpowiedzi na zadawane zapytanie. Do systemów zarządzania bazami danych jest wbudowany procesor zapytań (*query processor*), który pośredniczy między zapytaniem użytkownika a manipulowaniem danymi na poziomie fizycznym. Należy podkreślić, że do specyfikacji i rozwiązywania problemów optymalizacji zapytań używa się algebry obliczeń relacyjnych. Algebrą tą posługuje się również procesor zapytań. Przetwarza on zapytanie wysokiego poziomu wyrażone w postaci obliczeń relacyjnych na operacje bazodanowe wyrażone w języku algebry relacyjnej, uwzględniając działania na fragmentach relacji. W tym celu zapytanie obliczeniowe jest dekomponowane na sekwencję operacji relacyjnych nazywanych zapytaniem algebraicznym.

W wypadku bazy rozproszonej dane muszą być jeszcze zlokalizowane, a zapytanie algebraiczne musi być rozszerzone o operacje komunikacji, ponieważ operacje algebraiczne na danych są realizowane lokalnie. Następnie minimalizuje się koszt wykonania zapytania względem kryterium wymaganych zasobów obliczeniowych, czyli operacji dyskowych zapisu, odczytu, zasobów procesora, a w wypadku rozproszonej bazy danych również kosztu komunikacji sieciowej. Przez transformacje realizowane w procesorze zapytań osiąga się poprawność i efektywność. Jednakże zapytania obliczeń relacyjnych mogą mieć wiele równoważnych i poprawnych transformacji do algebry relacji. Głównym problemem jest więc wybór strategii zużywającej minimum zasobów.

W wypadku stosowania SZRBD należy zwrócić uwagę na miejsce przetwarzania danych, ponieważ zwiększa to przestrzeń możliwych rozwiązań wyboru strategii przetwarzania. Wskazane jest korzystanie z relacji tymczasowych i widoków roboczych, gdyż zwiększa to efektywność kolejnych zapytań.

Celem globalnym optymalizacji zapytań jest minimalizacja funkcji kosztu całkowitego, na który składają się: koszty przetwarzania, operacji wejścia/wyjścia, zasobów procesora, a dla rozproszonej bazy danych dodatkowo koszty komunikacji sieciowej. W scentralizowanych bazach danych głównym składnikiem całowitego kosztu są koszty zasobów procesora oraz operacji wejścia/wyjścia. Należy pamiętać, że dla systemów bazodanowych pracujących w środowiskach sieci lokalnych najbardziej znaczące są takie koszty przetwarzania, jak: koszt dostępu i złączeń. W sieciach rozległych dominują koszty komunikacyjne, w których szacowaniu trzeba uwzględniać: szerokość kanałów komunikacyjnych, szybkość transmisji, koszty związane ze stosowanym protokołem transmisji danych. Natomiast pozostałe czynniki nie są w większości algorytmów uwzględniane.

Wyniki optymalizacji czasu odpowiedzi na zapytanie mogą być sprzeczne z wynikami optymalizacji kosztowej. Należy wziąć więc pod uwagę możliwość przetwarzania operacji bazodanowych równolegle w różnych miejscach sieci.

Przejrzyste przedstawienie zagadnienia przetwarzania i optymalizacji zapytań można osiągnąć, wyrażając własności tego procesu przetwarzania za pomocą oszacowania złożoności odpowiednich operacji algebry relacyjnej. Złożoność ta wpływa na czas realizacji przetwarzania zapytania. Stąd łatwo opracować reguły, które zawsze uwzględnia w swym działaniu procesor zapytań. W tabeli przedstawiono w porządku rosnącym złożoność relacyjnych operacji unarnych i binarnych. Zgodnie z nim rośnie również czas przetwarzania [3].

Operacja	Złożoność
Selekcja Projekcja (bez eliminacji duplikatów)	O(n)
Projekcja (bez eliminacji duplikatów) Grupowanie	O(n log n)
Złączenie Półzłączenie Podział Operatory zbiorowe	O(n*log n)
Produkt kartezjański	$O(n^2)$

Złożoność operacji algebry relacyjnej

Złożoność jest zależna od liczby relacji. Dlatego najpierw powinny być wykonywane operacje najbardziej selektywne, redukujące tę liczbę. Operacje powinny być wykonywane kolejno od najmniej złożonych, aby unikać tworzenia produktów kartezjańskich lub je opóźniać.

Procesory zapytań scentralizowanych i rozproszonych systemów zarządzania bazami danych różnią się pod wieloma względami. Optymalizacja zapytań ma na celu wybór najlepszego rozwiązania strategii przetwarzania. Przykładowo, w tzw. metodzie bezpośredniej sprawdza się wszystkie możliwe rozwiązania względem kryterium minimalizacji kosztu. Jest ona efektywna przy wyborze najlepszej strategii, jednakże może być przyczyną znacznych narzutów na przetwarzania samej optymalizacji. Takie przypadki zdarzają się, gdy istnieje wiele strategii równoważnych albo przy optymalizacji zapytań z udziałem dużej ilości relacji.

W praktyce często stosuje się metody heurystyczne, które zalecają m.in.: grupowanie wspólnych wyrażeń, wykonywanie selekcji przed projekcją, zastępowanie złączeń przez serie półzłączeń i zapisywanie wyników operacji pośrednich w relacjach tymczasowych. Jednakże heurystyki nie dają rozwiązań optymalnych.

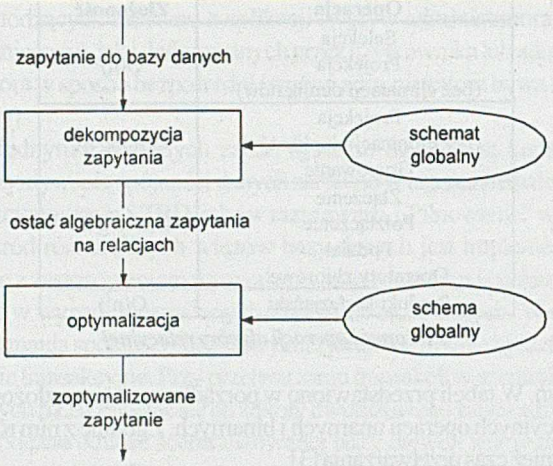
Optymalizacja zapytań obejmuje optymalizację czasową pojedynczych zapytań oraz grup zapytań, które można rozpatrywać pod względem ich powiązań i możliwości ich wykorzystania. Przy jednoczesnej optymalizacji wielu zapytań przestrzeń możliwych rozwiązań rośnie.

Optymalizacja czasowa zapytania może być statyczna, dynamiczna lub hybrydowa. Optymalizacja statyczna jest wykonywana w czasie kompilacji przed wykonaniem zapytania. Optymalizacja dynamiczna jest wykonywana na etapie przetwarzania zapytania. Optymalizacja hybrydowa jest podobna do optymalizacji statycznej, ale używa algorytmu opartego na statystyce.

Statystyki bazy danych wpływają na jej optymalizację. Ważna jest liczność relacji, wielkość rekordów, udział rekordów w złączeniach z innymi relacjami. Dla atrybutów rozpatruje się ich dziedziny oraz ilość różnych wartości.

W optymalizacji zapytania do scentralizowanej bazy danych bierze udział tylko jedno miejsce decyzyjne. Podobnie, w scentralizowanym zarządzaniu rozproszoną bazą danych strategię przetwarzania zapytania generuje jedno miejsce. Podejście scentralizowane jest stosunkowo proste (rys. 2), chociaż wymaga wiedzy o całej rozproszonej bazie danych.

Przy zastosowaniu podejścia rozproszonego do określania strategii przetwarzania zapytań do bazy rozproszonej, konieczna jest jedynie informacja o lokalnym schemacie bazy, zaś resztę



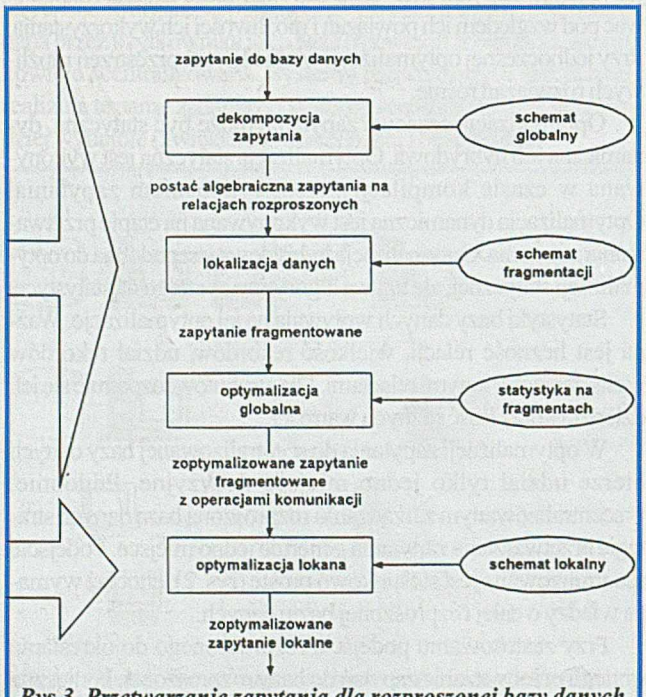
Rys.2. Przetwarzanie zapytania dla scentralizowanej bazy danych

informacji uzyskuje się poprzez współpracę pomiędzy miejscami. Niekiedy stosuje się podejście hybrydowe, w którym jedno miejsce podejmuje decyzję, a inne, zaangażowane w przetwarzanie zapytania, optymalizują podzapytania lokalne.

Przetwarzanie i optymalizacja zapytania przebiegają etapowo. Dla scentralizowanej bazy danych są to: dekompozycja oraz optymalizacja.

W rozproszonych bazach danych istnieje jeszcze etap - lokalizacji, a optymalizacja jest podzielona na globalną i lokalną (rys. 3).

Techniki dekompozycji są takie same dla scentralizowanych i rozproszonych SZBD. W dekompozycji są wykorzystywane jedynie informacje o schemacie globalnym bazy opisującym relacje globalne. Na tym etapie brakuje informacji o rozproszeniu danych. Zapytania są traktowane zawsze jako złożone i wymagające upraszczania. Bardzo istotne jest zatem, jak są one zbudowane. Kolejnym krokiem w dekompozycji jest analiza, która wyklucza zapytania błędne i nieprawidłowe semantycznie. Zapytanie jest błędne, jeżeli odwołuje się do relacji i atrybutów relacji, których nazwy nie są zdefiniowane lub gdy wykryty zostanie błąd typu. Algorytmy



Rys.3. Przetwarzanie zapytania dla rozproszonej bazy danych

analizy są w tym wypadku takie same, jak w językach programowania. Zapytanie jest nieprawidłowe semantycznie, jeżeli otrzymany graf zapytania jest niespójny. Następnie, na podstawie reguł logiki, eliminowana jest redundancja.

Po dekompozycji w SZRBD wykonuje się lokalizację danych. Podstawą jest tu schemat fragmentacji oraz zapytanie wyrażone w algebrze relacji rozproszonych. Ustala się, które fragmenty są wymagane i zastępuje kolejne części zapytania globalnego jego odwołaniami lokalnymi, czyli przekształca się zapytanie wyrażone w algebrze relacji rozproszonych na zapytanie w algebrze relacji na fizycznych fragmentach. Odpowiednio zaprojektowana alokacja bazy danych zwiększa dostępność danych dla zapytania. Administrator może zmieniać schemat fragmentacji i replikacji. Zagadnienie alokacji danych nie będziemy obecnie omawiać.

Po dekompozycji i lokalizacji następuje optymalizacja zapytania. Permutacja uporządkowania operacji wewnątrz zapytania może dawać wiele równoznacznych strategii jego wykonania. Znalezienie optymalnego uporządkowania tych operacji dla danego zapytania jest główną rolą warstwy optymalizacji zapytań. Celem optymalizacji jest znalezienie strategii przydatnych do dalszej optymalizacji i odrzucenie strategii złych. Jako kryterium oceny przyjmuje się koszt całkowity lub czas przetwarzania.

Istnieją statyczne i dynamiczne algorytmy optymalizacji zapytań baz relacyjnych, np. algorytm INGRES i Algorytm R [5, 6].

Pożądane jest, aby kierując zapytanie bezpośrednie do bazy danych, administrator brał pod uwagę własności wymienionych algorytmów optymalizacji i poprzez sekwencje zapytań „wzmacniał" podatność zapytań na optymalizację albo tę optymalizację wprowadzał.

Możemy określić *kilka szczegółowych zaleceń, które ułatwiają administratorowi konstruowanie zapytań dobrze zbudowanych i możliwie optymalnych*:

- W celu zmniejszenia złożoności obliczeniowej należy korzystać ze złączeń i półzłączeń zamiast z podzapytań oraz unikać operatorów negacji, sumy i różnicy;
- Korzystanie z relacji tymczasowych i widoków roboczych zmniejsza koszt i przyspiesza przetwarzanie zapytania;
- Aby ułatwić dekompozycję zapytania, należy w klauzuli WHERE stosować postać znormalizowaną predykatu;
- Należy pamiętać, że zapytania błędne lub nieprawidłowe semantycznie również zajmują zasoby SZBD;
- Korzystne jest stosowanie pośredniego rozdzielenia i uproszczenia zapytań, ponieważ zmniejsza się w ten sposób koszt przetwarzania zapytania;
- Przyspieszenie przetwarzania zapytań można uzyskać przez ułożenie sekwencji zapytań -rosnąco - w kolejności liczności złączeń.

Przetwarzanie i optymalizacja transakcji, niezawodność baz i bezpieczeństwo danych

Transakcja jest zbiorem operacji wykonywanych na bazie danych tak, aby zachować spójność danych. Dlatego może być ona zakończona przez: (1) zatwierdzenie (*commit*) lub (2) odrzucenie (*abort*). Transakcja rozproszona aktualizuje kilka baz danych i może być zatwierdzona tylko w wypadku pomyślnego zatwierdzenia transakcji lokalnych będących całością transakcji rozproszonej. Przetwarzanie transakcyjne musi spełniać cztery warunki (ACID): atomowość (*atomcity*), spójność (*consistency*), niezależność (*isolation*), trwałość (*durability*). Baza może być niespójna jedynie w

trakcie wykonywania transakcji. Atomowość gwarantuje, że musi być wykonane „wszystko albo nic". Spójność zapewnia nienaruszalność zasad integralności. Utrzymanie spójności bazy polega na zachowaniu reguł integralności dla wszystkich replik i fragmentów bazy rozproszonej. Niezależność transakcji polega na tym, że jedna nie uwzględnia działania innych. Po zakończeniu transakcji zmiany w bazie są utrwalone i nie mogą być z bazy danych usunięte, co gwarantuje trwałość.

Transakcje, które są definiowane przez administratora za pomocą języków dostępu do baz danych (za pośrednictwem SZBD albo w inny sposób), nazywamy transakcjami bezpośrednimi. Mogą to być transakcje modyfikujące znaczną część danych.

Dzięki wiedzy o mechanizmach i protokołach transakcyjnych można przewidywać i naprawiać występujące w czasie przetwarzania uszkodzenia bazy danych, z którymi nie radzi sobie SZBD albo nie ma w ogóle takiej możliwości systemowej. Uszkodzenia takie są zwykle dotkliwe i wymagają odtwarzania danych. Na podstawie wiedzy o stosowanym przez SZBD i SBD protokole transakcyjnym można wyspecyfikować procedury naprawy i odtwarzania bazy danych po awarii.

Transakcja może być przerwana przez błąd danych wejściowych, np. wykrycie blokady (*deadlock*). W tym wypadku utrzymywanie cech ACID transakcji nazywamy odtwarzaniem transakcji (*transaction recovery*). Transakcja może być też przerwana w wyniku awarii miejsca (*site system failure*), np. nośnika danych, zasilania. Zapewnienie własności transakcyjnych w tym wypadku nazywamy odtwarzaniem po awarii (*crash recovery*).

W dużych bazach danych zagadnienie awarii podczas przetwarzania transakcji jest szczególnie ważne ze względu na rozproszenie, a w konsekwencji, również awarii wynikających z transmisji pomiędzy zaangażowanymi miejscami przetwarzania. Uszkodzenia komunikacyjne (*line failures*) mogą powodować podział sieci na dwie lub więcej. Przy rozważaniu własności protokołów zakłada się, że każde miejsce potrafi odróżnić uszkodzenie samego siebie od uszkodzenia powodującego podział sieci. Uszkodzenie miejsca objawia się brakiem komunikatu, złą składnią lub niepoprawną sekwencją komunikatów. Uszkodzenie komunikacyjne może się objawiać zaburzeniem sekwencji komunikatów lub zaginięciem komunikatu.

Przetwarzanie transakcji może odbywać się w sposób scentralizowany lub rozproszony i jest ono realizowane przez menedżera transakcji (*transaction manager*). Lokalnie za aktualizację danych odpowiada tzw. lokalny menedżer odtwarzania LMO (*local recovery manager - LRM*). Do aktualizacji danych używa się dwóch metod: w miejscu (*in-place*) oraz poza miejscem (*out of place*) [8]. Przy aktualizacji w miejscu dane poprzednie pozycji wykonywanej akcji są tracone. Dlatego niezbędne jest zachowanie informacji o zmianie stanu bazy danych, która umożliwi przywrócenie spójności po uszkodzeniu. W tym celu stosuje się log bazy danych, który dla pojedynczej transakcji zapamiętuje niezbędne o niej informacje. Log bazy danych może być zapisywany synchronicznie i asynchronicznie. Do tego celu służy protokół utrzymania logu z zapisem w przód (*write-ahead logging - WAL*).

Przy aktualizacji poza miejscem stosuje się technikę cieni lub tworzenie plików różnicowych. W technice cieni jest tworzony obraz pozycji z nowymi wartościami. Natomiast poprzednia wartość jest zachowywana dla potrzeb odtwarzania. Technika plików różnicowych polega na tworzeniu pliku zawierającego wartość różnicową poprzedniej i nowej wartości pozycji. Zatwierdzenie transakcji polega na wpisaniu nowych wartości na podstawie pliku różnicowego.

Głównym celem przetwarzania transakcyjnego realizowanego przez SZBD jest zwiększenie niezawodności operacji bazodanowych. Szczególnie ważnymi miarami w bazodanowym modelu niezawodnościowym są: dostępność, wydajność oraz spójność [7]. Niezawodnościowe protokoły zatwierdzania, zakończenia oraz odtwarzania są próbą zapewnienia kompletu własności przetwarzania transakcyjnego i polepszenia kompletu miar niezawodnościowych.

Protokół 2PC jest stosowany zarówno w scentralizowanych, jak rozproszonych bazach danych. Wyróżnia się scentralizowany, liniowy i rozproszony protokół 2PC. W każdym wypadku zasada protokołu jest ta sama. W pierwszej fazie koordynator zbiera potwierdzenia gotowości do zapisu transakcji od uczestników. W drugiej następuje zapisanie wyników transakcji do bazy danych.

Koordynator odrzuca transakcję, gdy nie uzyska potwierdzeń wszystkich uczestników w określonym czasie. Odrzucenie transakcji odbywa się zgodnie z protokołami zakończenia (przeterminowania), które muszą być nieblokujące. Jeżeli zebrano wszystkie potwierdzenia, koordynator zatwierdza transakcję. Protokoły zatwierdzania i zakończenia zapewniają atomowość transakcji. Protokoły odtwarzania są wykorzystywane po awarii miejsca w momencie restartu.

Protokół 2PC z głosowaniem zapewnia atomowość transakcji przez rozszerzenie atomowego zatwierdzania lokalnego transakcji na transakcje rozproszone. W rozproszonych bazach danych występują uszkodzenia miejsc i łączy komunikacyjnych. Dlatego powinno stosować się protokoły nieblokujące zakończenia i niezależne odtwarzania. W wypadku uszkodzeń powodujących podział wielokrotny sieci, nie ma możliwości utrzymania spójności bazy danych. Dlatego należy zapewnić niezależność protokołów.

W wypadku uszkodzenia koordynatora transakcji uczestnik transakcji może zostać zablokowany. Niestety, dla protokołu 2PC nie jest możliwa realizacja nieblokującego protokołu zakończenia. Protokół 2PC odtwarzania nie gwarantuje również niezależnego odtworzenia rozproszonej bazy danych do postaci spójnej.

Protokół 3PC stosowany w rozproszonych bazach danych jest algorytmem nieblokującym. Dla protokołu zatwierdzania blokowanie nie zachodzi, ponieważ, w przeciwieństwie do 2PC, przeterminowanie z powodu braku koordynatora powoduje przejście do wyboru nowego koordynatora, który kończy transakcję. Protokół zakończenia obsługuje przeterminowanie oczekiwania na potwierdzenie od miejsc biorących udział w transakcji. Protokoły odtwarzania są podobne do odpowiedników w 2PC, wymagają jednak wymiany większej liczby komunikatów, aby unikać blokowania. Protokoły 2PC i 3PC zapewniają atomowość i trwałość przetwarzania transakcji po wystąpieniu uszkodzeń.

Procedury przywracania spójności baz danych

Znając własności protokołów 2PC i 3PC, można wykonać analizę ich działania w kierunku opracowania *zaleceń i procedur do wykorzystywania przez administratora w wypadkach występowania awarii miejsc lub podziału sieci prowadzących do stanów awaryjnych - czyli niespójności - bazy*.

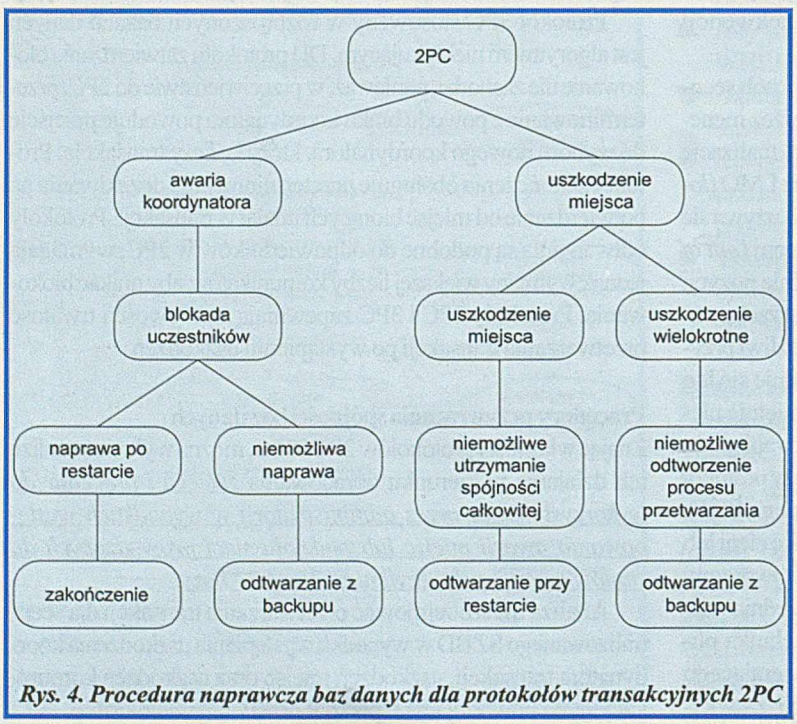
Analiza musi obejmować przetwarzania transakcji dla scentralizowanego SZBD w wypadku wystąpienia uszkodzenia koordynatora transakcji, uszkodzeń miejsc oraz uszkodzeń komunikacyjnych powodujących podział prosty lub wielokrotny.

Aby wykonać naprawę bazy danych, administrator powinien posiadać wiedzę o stosowanym przez SZBD protokole przetwarzania transakcji oraz fragmentacji i replikacji bazy danych.

Jeżeli SZBD używa protokołu 2PC, to w wypadku awarii koordynatora transakcji nastąpi blokada uczestników. Sukces naprawy koordynatora transakcji oraz restart miejsca prowadzi do uruchomienia protokołu zakończenia transakcji. W przeciwnym wypadku - gdy naprawa nie powiedzie się - uczestnicy nie mogą podjąć decyzji dalszego przetwarzania transakcji. Następuje blokada i w rezultacie nie jest zachowana spójność bazy danych, ponieważ transakcja nie zostanie zakończona. Ostatecznym rozwiązaniem jest odtworzenie bazy danych z kopii archiwalnej. Jeżeli nastąpi uszkodzenie miejsca, nie jest możliwe utrzymanie spójności bazy danych, nawet jeżeli powiedzie się odtwarzanie przy ponownym uruchomieniu. W wypadku uszkodzeń wielokrotnych miejsc przy przetwarzaniu protokołu 2PC również następuje blokada i dlatego nie mogą zadziałać protokoły odtwarzania. Również w tym wypadku rozwiązaniem jest odtworzenie bazy danych z kopii archiwalnej. *Procedurę naprawczą przywracania spójności baz danych w wypadku stosowania transakcyjnego protokołu 2PC przedstawiono na rys. 4.*

Protokół 3PC przetwarzania transakcji jest bardziej złożony. W wypadku awarii koordynatora transakcji następuje wybór nowego, który prowadzi przetwarzanie transakcji do zakończenia. Nie gwarantuje to jednak spójności bazy danych, ponieważ nie jest zachowana atomowość przetwarzania transakcji.

Uszkodzenia miejsc uczestników transakcji przy przetwarzaniu protokołu 3PC należy rozpatrywać osobno dla baz replikowanych i niereplikowanych. W wypadku replikowanej bazy danych działają protokoły kontroli replik, które mimo zatwierdzenia transakcji mogą powodować nietrwałość. Dla niereplikowanej bazy danych działają protokoły zakończenia i odtwarzania. Nie zapewniają one globalnej atomowości transakcji i globalnej spójności bazy danych. Odtwarzanie niezależne jest możliwe w mniejszej liczbie przypadków niż unikanie blokowania w procesie zakańczania transakcji.



Rys. 4. Procedura naprawcza baz danych dla protokołów transakcyjnych 2PC

Dla uszkodzeń komunikacyjnych przy przetwarzaniu protokołu 3PC, w wypadku podziału wielokrotnego, może dojść do blokady. Przetwarzanie w poszczególnych partycjach nie zapewnia spójności bazy. Przetwarzanie transakcji może przywrócić spójność, jednak nie jest możliwe zagwarantowanie nieblokującego przetwarzania protokołów zakończenia transakcji. W tym wypadku podobnie, jak dla protokołu 2PC, również rozwiązaniem jest odtworzenie bazy danych z kopii archiwalnej.

Podział prosty gwarantuje spójne lokalnie zakończenie transakcji. Procedury zakończenia mogą realizować strategię pesymistyczną lub optymistyczną. Strategia pesymistyczna zakłada, że transakcje, które nie gwarantują utrzymania spójności, nie mogą być wykonywane. Dla strategii optymistycznej najważniejsza jest dostępność danych, nawet kosztem spójności. W wypadku pełnej replikacji bazy danych - gdzie, jak już stwierdziliśmy - działają protokoły kontroli replik, mogą one powodować nietrwałość transakcji. Dla niereplikowanej lub częściowo replikowanej bazy danych realizowana jest strategia pesymistyczna. W scentralizowanych protokołach zakończenia stosowany jest algorytm miejsca głównego (*primary site*) i kopii głównej (*primary copy*). Stosowane są algorytmy głosowania większościowego oraz głosowania z kworum. Protokoły odtwarzania, przywracając bazę do stanu poprawnego, mogą stosować kryterium poprawności semantycznej lub syntaktycznej danych. Procedurę naprawczą przywracania spójności baz danych w wypadku stosowania transakcyjnego protokołu 3PC przedstawiono na rys. 5.

Niezależność transakcji i blokady, dostępność danych

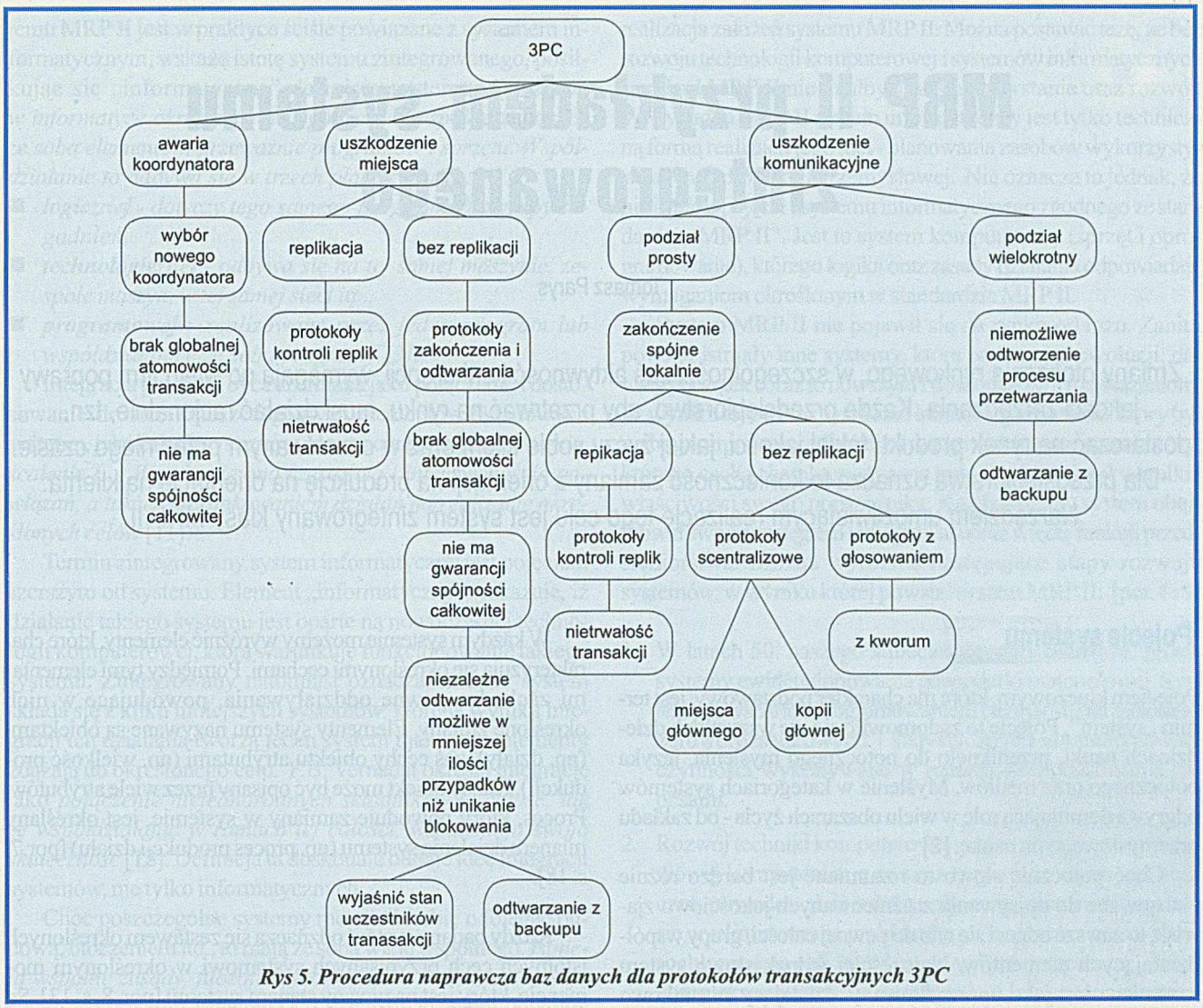
Niezależność transakcji wprowadza warunek nieuwzględniania działania innych transakcji w tym sensie, że transakcje nie mogą wzajemnie wpływać na modyfikowanie współdzielonych przez siebie danych. Blokowanie danych może prowadzić do blokad (*deadlock*) w wykonywaniu transakcji. Blokowanie danych na poziomie krotki, fragmentu relacji lub relacji zależy od własności SZBD oraz rodzaju transakcji.

Blokowanie zmniejsza dostępność danych. Można ją zwiększyć przez odpowiednią konstrukcję transakcji lub alokację danych. Administrator może mieć wpływ tylko na transakcje definiowane bezpośrednio. Należy pamiętać, aby blokować tylko niezbędne dla transakcji krotki, fragmenty relacji lub relacje.

Podsumowując działania, które może podjąć administrator w wypadku awarii dla poszczególnych protokołów oraz podając inne zalecenia wynikające z optymalizacji przetwarzania transakcji, zakładamy, jak poprzednio, że miejsce odróżnia uszkodzenie samego siebie od uszkodzenia komunikacyjnego oraz że awaria miejsca następuje w czasie pracy SZBD i ujawnia się natychmiast.

Uwagi i zalecenia dla ABD dużej bazy danych przy obsłudze transakcji:

- Protokół zakończenia (przeterminowania) 2PC w wypadku awarii uczestnika powoduje odrzucenie transakcji.
- W wypadku awarii koordynatora może dojść do blokady, ponieważ protokół 2PC nie przewiduje wyboru nowego koordynatora, który będzie kontynuował zatwierdzanie transakcji. ABD musi podjąć działania w celu usunięcia



Rys 5. Procedura naprawcza baz danych dla protokołów transakcyjnych 3PC

blokady. Nie jest zachowana spójność całościowa bazy danych. Jeżeli nie zrobi tego SZBD w procesie odtwarzania, należy przyjąć strategię obierania miejsca głównego.

- Protokół odtwarzania 2PC nie gwarantuje niezależnego odtwarzania, dlatego niemożliwe jest utrzymanie spójności całościowej bazy danych. ABD musi pamiętać, że w tym wypadku również może dojść do blokady.
- W wypadku podziałów wielokrotnych nie ma możliwości obsługi transakcji zarówno dla protokołów 2PC, jak i 3PC. Należy wtedy podjąć decyzję, czy odtwarzać bazę danych z kopii archiwalnej. Innym rozwiązaniem jest usunięcie danych niespójnych czy też wybór miejsca głównego.
- W replikowanych bazach danych istnieją protokoły kontroli replik. Ich działanie może prowadzić do nietrwałości transakcji. Zatwierdzone zmiany mogą być odwołane w wypadku niezgodności replik.
- W wypadku uszkodzeń wielokrotnych w momencie łączenia partycji działają protokoły odtwarzania, które mogą uruchomić protokoły zakończenia.
- Protokoły zakończenia w replikowanych bazach danych opierają się na strategii miejsca głównego lub bazy głównej. W wypadku uszkodzeń wielokrotnych należy posłużyć się odtworzeniem bazy z kopii archiwalnej. W wypadku dużych baz danych jest to jednak szczególnie czasochłonne.
- Ponieważ blokady zmniejszają dostępność, należy pamiętać przy konstruowaniu transakcji bezpośrednich, aby blokować tylko niezbędne dla transakcji krotki, fragmenty relacji lub relacje. Dostępność można zwiększyć, dokonując zmian w alokacji bazy danych.

Literatura

[1] *VLDB - The International Journal of Very Large Data Bases*, Springer Berlin Heidelberg, 1996-1998.

[2] Informix, Conference Large Database Administration, Informix Inc., San Jose, 1995.

[3] Ozsu M. T., Valduriez P., ***Distributed Database Management***, Edmonton 1994.

[4] Rodgers U., ***Oracle. Przewodnik projektanta baz danych***, *WNT*, Warszawa, 1985.

[5] Stonebraker M., Kreps P., Wong W., Held G., ***The Design and Implementation INGRES***, ACM Trans. Database Syst., 1976.

[6] Epstein R., Stonebraker M., Wong W., ***Query Processing in a Distributed Relational Databases System***, ACM SIGMOND Int. Conference on Management of Data, Austin, Texas, 1978.

[7] Marciniak J. J., ***Encyclopedia of Software Engineering***, Wiley Interscience, 1994.

[8] Gruber J., ***Mechanizmy podwyższania niezawodności w rozproszonych bazach danych***, II Kr. Konf. Nauk.-Techn. - Niezawodność Systemów Czasu Rzeczywistego, Łagów, 1997.

Wojciech Czujowski jest pracownikiem Silicon & Software Systems, Dublin, Irlandia
Jacek Gruber jest pracownikiem Wydziałowego Zakładu Informatyki Politechniki Wrocławskiej

MRP II przykładem systemu zintegrowanego

Tomasz Parys

Zmiany otoczenia rynkowego, w szczególności zaś aktywność konkurencji, wymagają od wielu firm poprawy jakości zarządzania. Każde przedsiębiorstwo, aby przetrwać na rynku, musi działać racjonalnie, tzn. dostarczać na rynek produkt takiej jakości, jakiej życzy sobie klient oraz w oczekiwanym przez niego czasie. Dla przedsiębiorstwa oznacza to konieczność zamiany z orientacji na produkcję na orientację na klienta. Narzędziem umożliwiającym realizację tego celu jest system zintegrowany klasy MRP II.

Pojęcie systemu

Pojęciem kluczowym, które ma charakter podstawowy, jest termin „system". Pojęcie to zadomowiło się we wszystkich dziedzinach nauki, przeniknęło do potocznego myślenia, języka potocznego oraz mediów. Myślenie w kategoriach systemów odgrywa dominującą rolę w wielu obszarach życia - od zakładu przemysłowego po naukę. [2]

Choć potocznie słowo to rozumiane jest bardzo różnie i stosowane do opisywania zróżnicowanych jakościowo zjawisk, to zawsze odnosi się ono do pewnej całości, grupy współdziałających elementów. Najczęściej jednak słowo system rozumiane jest jako uporządkowany, działający stosunkowo sprawnie mechanizm, który zapewnia realizację określonych zadań.

E. Yourdon w swojej pracy *Współczesna analiza strukturalna* podaje następujące definicje terminu system: [13]

1. *Regularnie współpracująca lub współzależna grupa elementów tworzących jednolitą całość (...)*
2. *Zorganizowany zbiór doktryn, idei lub prawideł, zwykle przewidziany do objaśnienia budowy lub działania pewnej usystematyzowanej całości (...)*
3. *Uporządkowana lub zorganizowana procedura (...)*
4. *Sposób klasyfikacji, symbolizacji lub schematyzacji (...)*
5. *Harmonijne rozmieszczenie lub wzór: PORZĄDEK*
6. *Zorganizowane społeczeństwo lub sytuacja społeczna traktowana jako trwała ORGANIZACJA.*

System zdefiniowany może zostać także jako *zbiór obiektów powiązanych określonymi wzajemnymi zależnościami lub oddziaływaniami* [7].

A. K. Koźmiński w swoich pracach rozumie system jako *zestaw składników, między którymi zachodzą wzajemne stosunki i gdzie każdy składnik jest połączony z innym bezpośrednio lub pośrednio* [8, s. 13].

W każdym systemie możemy wyróżnić elementy, które charakteryzują się określonymi cechami. Pomiędzy tymi elementami zachodzą pewne oddziaływania, powodujące w nich określone zmiany. Elementy systemu nazywane są obiektami (np. działy), zaś cechy obiektu atrybutami (np. wielkość produkcji). Każdy obiekt może być opisany przez wiele atrybutów. Proces, który powoduje zamiany w systemie, jest określany mianem działania systemu (np. proces produkcji działu) [por.7, s. 18].

Każdy badany system odznacza się zestawem określonych istotnych cech przypisanych systemowi w określonym momencie, który jest nazywany stanem systemu [por. 8, s. 13]. Są to zatem wszystkie obiekty, atrybuty oraz działania wraz z ich opisem [por. 7, s. 18].

Z systemem związanych jest kilka pojęć, które mają zasadnicze znaczenie dla zrozumienia działania systemu oraz jego właściwego opisu. Pojęciami tymi są: [8, s. 13 i n.]

- *zdarzenie* - określane jako zmiana jednej lub kilku cech systemu uznanych za ważne,
- *czyn systemu* - jest to mające miejsce w systemie zdarzenie, dla którego żadne inne zdarzenie w systemie lub jego otoczeniu nie jest warunkiem koniecznym ani wystarczającym do jego wystąpienia,
- *reakcja systemu* - zachodzące w systemie zdarzenie, dla którego warunkiem wystarczającym jest inne mające miejsce w nim lub jego otoczeniu zdarzenie,
- *zachowanie systemu* - obejmuje jedno lub więcej zdarzeń, które są konieczne lub wystarczające do wywołania w nim lub jego otoczeniu innego stanu. Zachowanie systemu jest zamianą systemu, która powoduje inne zdarzenia,
- *proces* - jest to pasmo zachowań powiązanych ze sobą i pełniących funkcję wywoływania zdarzenia, które jest celem systemu.

Terminem, który pozostał jeszcze do zdefiniowania, jest system zintegrowany. Biorąc pod uwagę fakt, że działanie sys-

temu MRP II jest w praktyce ściśle powiązane z systemem informatycznym, wskażę istotę systemu zintegrowanego, posiłkując się „informatyczną" definicją systemu. *Systemem w informatyce określa się na ogół zespół współdziałających ze sobą elementów, przeważnie programów i sprzętu. Współdziałanie to odbywa się w trzech płaszczyznach:*

- ***logicznej** - dotyczy tego samego programu lub grupy zagadnień,*
- ***technologicznej** - odbywa się na tej samej maszynie, zespole maszyn, w tej samej sieci itp.,*
- ***programowej** - realizowane przez jeden program lub współdziałające ze sobą programy [3].*

Integracja powinna być rozumiana jako połączenie i dostosowanie do siebie poszczególnych elementów składowych systemu, jak i całych systemów. Integracja oznacza *zespolenie, scalenie (...) Wyraża się ona częstością i intensywnością powiązań, a także ukierunkowaniem działań na realizację określonych celów* [11].

Termin zintegrowany system informatyczny jest pojęciem szerszym od systemu. Element „informatyczny" wskazuje, iż działanie takiego systemu jest oparte na nowoczesnej technologii komputerowej, która warunkuje funkcjonowanie takiego systemu. Zintegrowany natomiast oznacza, iż dany system składa się z kilku mniejszych systemów, które w wyniku integracji ich działania tworzą jeden system i jako jego elementy zdążają do określonego celu. F.B. Vernadat określa integrację jako *połączenie niejednorodnych składników w całość, tak że współdziałając w ramach tej całości, wzmacniają swoją skuteczność* [12]. Definicja ta doskonale oddaje ideę integracji systemów, nie tylko informatycznych.

Choć poszczególne systemy mogą od siebie odbiegać budową, otoczeniem itd., to mają ze sobą wiele wspólnego. *Istnieją wspólne zasady, filozofie i teorie, które doskonale stosują się do wszystkich systemów* [13]. Analizując zatem dowolny system (typ systemu), na przykład informatyczny, można stosunkowo często wykorzystać wiedzę i doświadczenia zdobyte podczas analizy innych systemów.

MRP II jako system zintegrowany

MRP II (*Manufacturing Resource Planning* - planowanie zasobów produkcyjnych) jest metodyką planowania zasobów wykorzystywanych w produkcji przemysłowej. W literaturze przedmiotu można spotkać różne tłumaczenia tego terminu na język polski. I. Durlik używa terminu „planowanie i sterowanie zasobami produkcyjnymi" [por. 5], zaś A. Popończyk nazywa MRP II „planowaniem zasobów gospodarczych" [por. 9]. Niezależnie jednak od tłumaczenia termin zasób służy do określania urządzeń, zapasów, środków trwałych, środków pieniężnych oraz ludzi, którzy są zaangażowani w proces produkcyjny.

Bardzo często system klasy MRP II jest utożsamiany z systemem informatycznym (komputerowym). Takie rozumowanie jest jednak błędne. Chociaż funkcjonowanie systemu klasy MRP II jest niemożliwe bez właściwego, przystosowanego do jego wymogów systemu informatycznego, na który składają się zarówno sprzęt, jak i oprogramowanie, to jednak MRP II nie jest takim systemem. System informatyczny dostarcza jedynie środków technicznych oraz narzędzi, dzięki którym możliwa jest realizacja założeń systemu MRP II. Można postawić tezę, że bez rozwoju technologii komputerowej i systemów informatycznych standard MRP II nie miałby szans na powstanie oraz rozwój. W wypadku MRP II system informatyczny jest tylko techniczną formą realizacji jego idei - planowania zasobów wykorzystywanych w produkcji przemysłowej. Nie oznacza to jednak, że nie istnieje pojęcie „systemu informatycznego zgodnego ze standardem MRP II". Jest to system komputerowy (sprzęt i oprogramowanie), którego logika oraz zasady działania odpowiadają wymaganiom określonym w standardzie MRP II.

System MRP II nie pojawił się na rynku od razu. Zanim powstał istniały inne systemy, które podlegając ewolucji, dawały początek coraz to nowszym i doskonalszym rozwiązaniom. W wyniku tej ewolucji na bazie istniejącego systemu, który był wzbogacany o nowe funkcje i właściwości, powstawał nowy, którego cechą charakterystyczną było to, iż zawierał wszelkie właściwości swego poprzednika. Każdy kolejny system obejmował swoim zasięgiem i integrował coraz więcej funkcji przedsiębiorstwa. Można wyróżnić następujące etapy rozwoju systemów, w wyniku której powstał system MRP II: [por.4 i 9]

1. W latach 50. naszego stulecia powstały pierwsze, proste systemy ewidencjonowania gospodarki materiałowej. Systemy te wsparte oprogramowaniem bazującym na metodach zdroworozsądkowych i statystycznych automatyzowały czynności wykonywane w ramach gospodarowania zapasami.

2. Rozwój techniki komputerowej oraz wzrost mocy obliczeniowej komputerów, a co się z tym wiąże szybkości obliczeń, powodował, iż wraz z upływem czasu możliwe stało się wyeliminowanie problemów związanych z praco- i czasochłonnością obliczeń. Umożliwiło to połączenie w jeden kompleksowy system takich działań, jak: prognozowanie, określanie wielkości produkcji i zamówień, określanie stanów magazynowych itd. W wyniku takich przeobrażeń powstał system MRP (*Material Requirements Planning* – planowanie potrzeb materiałowych).

3. MRP jest systemem wspomagającym planowanie i harmonogramowanie produkcji. Przygotowany harmonogram jest łączony z materiałami, które są niezbędne do jego wykonania. MRP śledzi także stany zapasów magazynowych i tak ustala ich poziom, aby minimalizować ich ilość oraz czas składowania przy zachowaniu ciągłości produkcji.

4. Prawdziwy rozwój systemów MRP rozpoczął się na początku lat 60. wraz z przyjęciem ilościowych metod zarządzania popartych techniką komputerową [por. 5].

5. Wraz z upływem czasu system MRP był wzbogacany o coraz to nowe funkcje. Do planowania materiałowego, realizowanego w ramach MRP, dołączono planowanie oraz sterowanie innymi czynnikami produkcji. Spowodowało to, iż harmonogram produkcji był dokładniejszy, gdyż oprócz zapotrzebowania materiałowego uwzględniał także takie czynniki jak praca, energia, kapitał itd. Kolejnym, naturalnym etapem było połączenie informacji o przebiegu produkcji oraz sprzedaży ze sterowaniem tymi procesami. Następnie system został wzbogacony o sprzężenie zwrotne pomiędzy procesami planowania, sterowania oraz wy-

twarzania. Posiadając takie właściwości oraz zakres działania, system stał się zamknięty, objął swym zasięgiem całe przedsiębiorstwo. Systemowi nadano nazwę *Manufacturing Resource Planning*. Ponieważ jednak akronim tej nazwy był identyczny jak dla poprzednika, dla ich odróżnienia dodano rzymską II i tak powstał znany dziś system MRP II.

W literaturze są wyróżniane jeszcze systemy klasy ERP (*Enterprise Resource Planning*) określane także jako MRP II Plus lub MRP III (*Money Resource Planning*). Wszystkie te terminy opisują system planowania zasobów finansowych przedsiębiorstwa, w których realizowane w MRP II zostały uzupełnione o procedury finansowe, na przykład rachunkowość zarządczą, *cash flow*, rachunek kosztów. W chwili obecnej standard ten nie jest do końca opisany, nie ma jego formalnej definicji [por. 1].

Standard MRP II został opracowany przez amerykańskie stowarzyszenie APICS (*American Production and Inventory Control Society* - amerykańskie stowarzyszenie sterowania produkcją i zapasami). Według tego opublikowanego pod koniec lat 80. standardu, MRP II obejmuje następujące funkcje [10]:

- ***Planowanie biznesowe*** (*Business Planning*);
- ***Planowanie produkcji i sprzedaży*** (SOP - *Sales and Operation Planning*);
- ***Harmonogramowanie planu produkcji*** (MPS - *Master Production Scheduling*);
- ***Zarządzanie popytem*** (DEM - *Demand Management*);
- ***Planowanie potrzeb materiałowych*** (MRP - *Material Requirements Planning*);
- ***Podsystem struktur wyrobów*** (*Bill of Material Subsystem*);
- ***Podsystem transakcji materiałowych*** (INV - *Inventory Transaction Subsystem*);
- ***Podsystem harmonogramów spływu*** (SRS - *Scheduled Receipts Subsystem*);
- ***Sterowanie produkcją*** (SFC - *Shop Floor Control*);
- ***Planowanie zdolności produkcyjnych*** (CRP - *Capacity Requirements Planning*);
- ***Zarządzanie środowiskiem roboczym*** (*Input/Output Control*);
- ***Zaopatrzenie*** (PUR - *Purchasing*);
- ***Planowanie dystrybucji*** - (DRP - *Distribution Resource Planning*);
- ***Pomoce warsztatowe*** (*Tooling*);
- ***Interfejs do planowania strategicznego*** (*Financial Planning Interface*);
- ***Symulacja*** (*Simulation*);
- ***Pomiar działania systemu*** (*Performance Mea - Surement*).

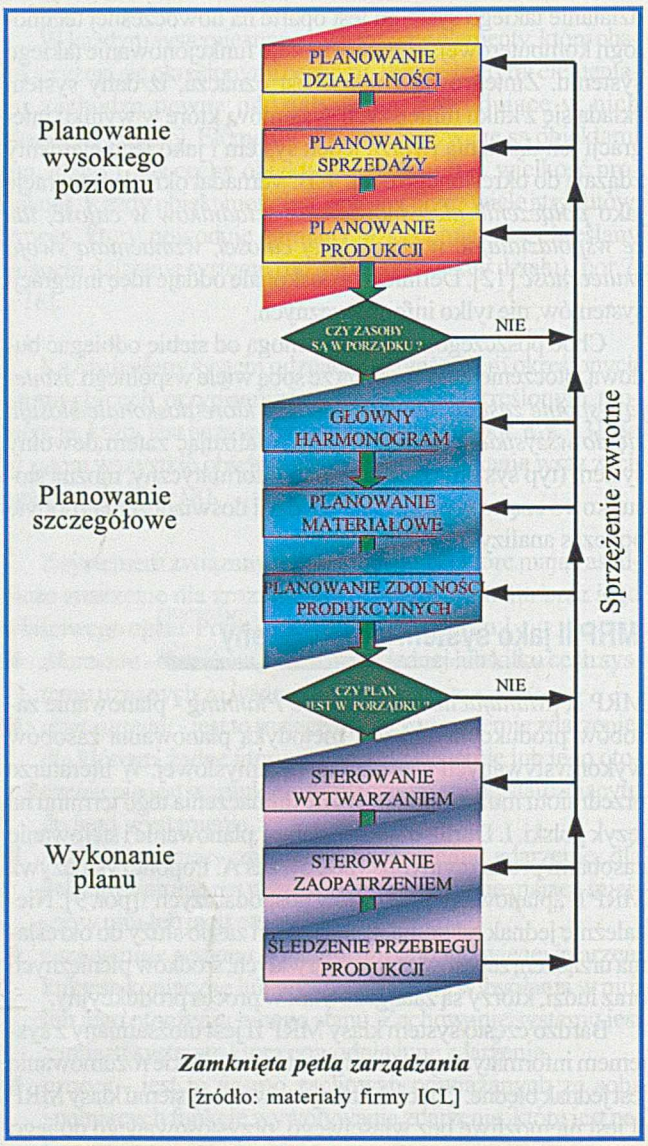
System MRP II jest modelem realnego procesu kierowania działalnością w rozbiciu na fazę planowania i sterowania. System MRP II pomaga w rozwiązaniu tzw. uniwersalnego równania produkcji, które sprowadza się do odpowiedzi na cztery pytania [6]:

1. Co mamy wyprodukować (jakie wyroby i w jakim terminie), aby wyznaczony popyt został zaspokojony ?
2. Czym musimy dysponować i w jakim czasie (zdolności produkcyjne, surowce itd.), żeby wykonać tę produkcję ?
3. Co z tego, czego potrzebujemy, posiadamy obecnie (jakimi dysponujemy zdolnościami produkcyjnymi w kolejnych okresach, jakie mamy zapasy produkcji w toku, półfabrykatów, surowców) ?
4. Co musimy jeszcze kupić (usługi i surowce), aby wykonać tę produkcję ?

Uniwersalne równanie produkcji należy zatem traktować jako podstawę prowadzenia działalności przedsiębiorstwa.

MRP II jest to metoda analizy kompletnych planów działalności przedsiębiorstwa (*Business Plan*) aż do wyników. Jest to sprzężenie zwrotne pomiędzy procesem planowania a procesem produkcji. MRP II integruje działania wykonywane w przedsiębiorstwie jednocześnie na trzech poziomach zarządzania, tj. na poziomie strategicznym, taktycznym i operatywnym [por. 5].

W MRP II zakłada się tzw. zamkniętą pętlę zarządzania (*Closed Loop*) [por. rys.], której założeniem jest integracja danych otrzymywanych na wymienionych poziomach zarządzania.



Zamknięta pętla zarządzania
[źródło: materiały firmy ICL]

Integracja danych w wypadku zamkniętej pętli zarządzania oznacza wymianę danych, swobodny ich przepływ oraz wykorzystanie we wszystkich etapach planowania i sterowania pro-

dukcją. W zamkniętej pętli zarządzania działa mechanizm przekazujący określone wytyczne „w dół" do poszczególnych działów funkcjonalnych przedsiębiorstwa. Jednocześnie, dzięki sprzężeniom zwrotnym, działa mechanizm przekazywania danych „w górę". W efekcie jego działania na wyższe etapy są przekazywane dane o realizacji planów produkcji i sprzedaży, a wraz z nimi informacje o występujących kłopotach i zakłóceniach w realizacji tych planów. Działanie mechanizmu sprzężeń zwrotnych możliwe jest dzięki istnieniu w MRP II bazy danych, do której dane wprowadza i pobiera sam system. Zapewnia to spójność oraz aktualność danych gromadzonych w bazie.

Każda z funkcji systemu może zostać zaklasyfikowana w zamkniętej pętli zarządzania do jednej z trzech faz (poziomów) planowania i sterowania przedsiębiorstwa: [por.10]

1. faza tworzenia planu działalności (planowanie wysokiego poziomu)
2. faza planowania szczegółowego
3. faza wykonania zadań.

Funkcje wykonywane w ramach tych faz są ze sobą połączone, przy czym połączenia w obrębie poszczególnych faz mają zdecydowanie silniejszy charakter niż te pomiędzy fazami. Celem MRP II jest integracja wyszczególnionych powyżej poziomów planowania i sterowania produkcją w jeden spójny system, uzyskiwany przez sprzężenia zwrotne pomiędzy poszczególnymi fazami i funkcjami. Sprzężenie zwrotne oznacza w tym wypadku bezpośrednie powiązanie planu wyższego szczebla z planem na szczeblu niższym, tak że planowanie na niższym szczeblu oparte jest na wynikach planu szczebla wyższego. Plan stworzony na danym poziomie możliwy jest do realizacji dzięki wynikom analizy zdolności produkcyjnych. Należy zauważyć, że MRP II jest rozwiązaniem metodycznym, opisującym procedury i algorytmy działania, podającym przedsiębiorstwom wskazówki do działania. Nie jest to gotowe oprogramowanie, które wystarczy wdrożyć, aby uzyskać rozwiązanie wszystkich bolączek przedsiębiorstwa.

Integracja poszczególnych funkcji oraz faz działania w ramach MRP II ma również na celu wyznaczenie zapotrzebowania na surowce i moce produkcyjne potrzebne do wyprodukowania określonych wyrobów. Idea MRP II zakłada wspieranie tego procesu. Zapotrzebowanie to jest wyznaczane na podstawie planów produkcyjnych (przygotowywanych na podstawie prognoz względem przyszłych potrzeb rynku) oraz danych konstrukcyjnych o strukturze wyrobów. MRP II ma za zadanie umożliwić przedsiębiorstwu elastyczne reagowanie na zmieniające się potrzeby rynku przy jednoczesnym zachowaniu optymalnego poziomu zapasów, co następuje w wyniku dokładnego zaplanowania ich ilości oraz czasu, kiedy będą potrzebne w procesie produkcji. Integracja funkcji ułatwia także proces planowania oraz modyfikacji już opracowanych planów bez względu na rodzaj produkowanych wyrobów. MRP II jest adresowane do przedsiębiorstw o różnym profilu produkcji, od produkcji masowej, przez produkcję na zamówienie po produkcję niskoseryjną.

W MRP II integracja dotyczy także danych zgromadzonych w bazie danych. Wspomagana komputerowo, wspólna dla wszystkich modułów MRP II baza danych jest w stanie szybko dostarczać im niezbędnych informacji. Baza danych, którą posługuje się MRP II, jest także przydatna w badaniach symulacyjnych. Pozwala to określać przyszłe wielkości na dostawie symulowanych warunków. W MRP II można zatem symulować alternatywne plany produkcyjne i analizować jakość decyzji jeszcze zanim zostaną one podjęte [por.5].

Przy omawianiu zagadnienia integracji pamiętać należy, że w wypadku konkretnego przedsiębiorstwa, w zależności od jego specyfiki działania oraz zastosowanych rozwiązań organizacyjnych, różnie rozkłada się punkt ciężkości integracji modułów systemu. Inaczej będzie w wypadku przedsiębiorstw produkcyjnych, inaczej zaś w sferze usług czy handlu [por. 1].

Aleksander Popończyk zauważa, że MRP II jest narzędziem integrującym przedsiębiorstwo i jest ono przeznaczone dla jednego człowieka - dyrektora generalnego. Dyrektor naczelny bowiem jest odpowiedzialny za koordynację działań całego przedsiębiorstwa, jednoczy firmę [9]. Na dyrektorze spoczywa trud podejmowania, akceptowania decyzji oraz ponoszenia za nie odpowiedzialności. MRP II jest narzędziem, które wspomaga decydenta w wykonywanych przez niego pracach. Od jego decyzji zatem zależy, w jakim stopniu zalety systemu zostaną wykorzystane.

MRP II wspiera ludzi przy podejmowaniu decyzji gospodarczych warunkujących działanie i rozwój przedsiębiorstwa. W ostatecznym rozrachunku to od ludzi, a nie od systemu, zależą decyzje podejmowane w przedsiębiorstwie, a tym samym jego działania i pozycja na rynku.

Literatura

[1] Adamczewski A., *Wdrażanie systemu zintegrowanego jako złożone przedsięwzięcia informatyczne*, „Informatyka", wydanie specjalne styczeń/96.

[2] Bertalanfy L., *Ogólna teoria systemów*, Warszawa 1984.

[3] Chmielarz W., *Systemy informatyczne wspomagające zarządzanie. Aspekt modelowy w budowie systemów*, Warszawa 1996.

[4] Maciejec L., *Czy programowanie w przedsiębiorstwie ma przyszłość?*, „Computerworld" 1996, nr 38.

[5] Durlik I., *Inżynieria zarządzania. Strategia i projektowanie systemów produkcyjnych*, Warszawa 1995.

[6] Greniewski M., *MRP II a planowanie strategiczne*, w: *Human-Computer Interaction. Materiały konferencyjne*, red. Kubiak B.F. i Korowicki A., Gdańsk 1997.

[7] Gordon G., *Symulacja systemów*, Warszawa 1974.

[8] Koźmiński A. K., *Analiza systemowa organizacji*, Warszawa 1976.

[9] Popończyk A., *Dwa w jednym, czyli system informatyczny i system MRP II w przedsiębiorstwie*, „Informatyka", wydanie specjalne - czerwiec 1996.

[10] Popończyk A., *Elementy składowe systemu MRP II*, „Informatyka", wydanie specjalne - czerwiec 1996.

[11] Santarek K., *Computer Integrated Manufacturing*, w: *CIM-ARIS Computer Integrated Manufacturing, Architecture of Integrated Information Systems*, red. Kasprzak T., 1995.

[12] Vernadat F.B., *Enterprise Modeling and Integration Principles and Applications*, London 1996.

[13] Yourdon E., *Współczesna analiza strukturalna*, Warszawa 1996.

Tomasz Parys
Zakład Systemów Informacyjnych Zarządzania
Wydział Zarządzania UW
E-mail: parys@ocelot.wz.uw.edu.pl

Polityka bezpieczeństwa informacji

Janusz Górski

W wielu zastosowaniach informatyki bezpieczeństwo informacji jest jednym z podstawowych kryteriów rozstrzygających o praktycznej przydatności systemu. Polityka bezpieczeństwa informacji organizacji określa cele bezpieczeństwa oraz zasady, odpowiedzialność i środki służące osiąganiu postawionych celów. W ramach artykułu przedstawiono zakres zagadnień związanych ze zdefiniowaniem i wdrożeniem polityki bezpieczeństwa informacji w instytucji, której funkcjonowanie jest uzależnione od systemu informatycznego.

Pojęcie bezpieczeństwa informacji

Pod pojęciem systemu komputerowego (lub krócej, systemu) będziemy rozumieli strukturę, na którą składają się węzły generujące, składujące i/lub przetwarzające informację oraz środki komunikacyjne służące przesyłaniu informacji. Informacja stanowi podstawowy zasób takiego systemu. Będziemy posługiwali się pojęciem *podmiotu* dla określenia jakiegokolwiek obiektu (użytkownik, komputer, program aplikacyjny, itp.), który może uzyskać dostęp do informacji przechowywanej, przetwarzanej lub przesyłanej w systemie. Dostęp jest rozumiany szeroko, może on polegać na bezpośrednim odczytaniu, wywnioskowaniu (z innych, posiadanych już informacji), modyfikacji lub zniszczeniu rozważanej informacji. *Podmiot upoważniony* to taki, który ma prawo do dostępu. Zakładamy, że istnieje zbiór kryteriów pozwalających na wyróżnienie podmiotów upoważnionych. Kryteria te reprezentują punkt widzenia właściciela systemu.

Tradycyjnie, *bezpieczeństwo informacji* jest rozumiane w terminach następujących atrybutów:

- *Integralność* (ang. *integrity)* - informacja w systemie nie może zostać zmieniona lub zniszczona przez podmioty nieupoważnione.
- *Dostępność* (ang. *availability)* - informacja jest dostępna (w określonym miejscu, czasie i postaci) podmiotom upoważnionym.
- *Poufność* (ang. *security)* - informacja nie jest udostępniana podmiotom nieupoważnionym.

Nie wszystkie informacje w systemie podlegają ochronie w tym samym stopniu. Tak więc, celowym jest dokonanie klasyfikacji zasobów informacyjnych, a następnie określenie wymaganego poziomu ich zabezpieczenia. Klasyfikacji takiej dokonuje się w odniesieniu do wartości jaką ma dany zasób informacyjny dla wykorzystującej go instytucji. Punktem wyjścia przy rozważaniach dotyczących stopnia zabezpieczenia zasobów jest pojęcia *ochrony niezbędnej*. Ochrona niezbędna wynika z obowiązujących ogólnych aktów prawnych (np. z ustawy o ochronie dóbr osobistych obywateli) lub umów szczegółowych, zawartych np. pomiędzy daną instytucją i jej klientami. Przykładem może tu być np. informacja o adresach, informacja o płaconych rachunkach, informacja o dochodach, itp. Zakres ochrony wykraczający poza ochronę niezbędną wynika z oceny znaczenia rozważanego zasobu informacyjnego dla danej instytucji. Często stosuje się tu podział na kategorie, w ramach których określane są szkody związane z utratą bezpieczeństwa.

Zakres polityki bezpieczeństwa

Z każdym systemem (w tym również informatycznym) związany jest jego *cykl życia*, który w najogólniejszym ujęciu obejmuje okres czasu od powzięcia zamiaru wytworzenia tego systemu, poprzez wszystkie etapy związane z konkretyzacją tej idei, projektowaniem, realizacją, instalacją w środowisku docelowym, eksploatacją, dokonywaniem zmian i udoskonaleń, a skończywszy na wycofaniu systemu z użytkowania i jego całkowitej dematerializacji. Bezpieczeństwo jest atrybutem całego systemu i dlatego musi być brane pod uwagę w ramach wszystkich etapów cyklu życia i w odniesieniu do wszystkich jego części składowych (a nie wyłącznie w odniesieniu do segmentu technicznego). Oznacza to w szczególności, że skuteczne zabezpieczenie wymaga podejścia systemowego, obejmującego oprócz części technicznej, również zagadnienia organizacji, zarządzania, personelu i infrastruktury oraz że oprócz zagadnień związanych z projektowaniem, implementacją i użytkowaniem należy również brać pod uwagę problemy pielęgnacji, współpracy z kontrahentami, instalacji, likwidacji czy też zgodności z obowiązującym prawem.

Nie ma systemów absolutnie bezpiecznych. Również zabezpieczanie wszystkiego i wszędzie nie jest działaniem sensownym i może w efekcie doprowadzić do nadmiernych kosztów i sparaliżować normalne funkcjonowanie danej organizacji. Bezpieczeństwo jest w znacznym stopniu uzależnione od ludzi, ich świadomości i woli współdziałania. Ludzie ci funkcjonują w ra-

mach struktur organizacyjnych i realizują zadania wynikające z przydzielonych im funkcji i związanej z tym odpowiedzialności. Dlatego niezbędne jest jawne sformułowanie *polityki bezpieczeństwa* danej organizacji, która określa sposób rozumienia bezpieczeństwa, stanowi podstawę do dalszych analiz w kierunku konkretnych rozwiązań technicznych, ustala odpowiedzialność i jasno wyraża intencje władz organizacji odnośnie wspierania wszelkich działań zmierzających do realizacji tej polityki.

Racjonalny wybór zabezpieczeń musi być oparty o analizy, których wyniki stanowią podstawę do wyznaczenia sensownego poziomu nakładów oraz wskazują kierunki, gdzie nakłady te będą wykorzystane w sposób najbardziej efektywny. Bez przeprowadzenia takich analiz nie jest możliwy uzasadniony wybór środków bezpieczeństwa i konkretnych rozwiązań technicznych. Dla przykładu, inwestycja w szyfrowanie sygnałów przesyłanych liniami komunikacyjnymi może okazać się zupełnie chybiona jeżeli aplikacje końcowych użytkowników, korzystające z deszyfrowanej już informacji, będą narażone na łatwy do przeprowadzenia atak prowadzący do utraty poufności. Działania związane z ustaleniem zagrożeń istniejących w kontekście danej aplikacji i ich potencjalnych skutków są objęte *analizą bezpieczeństwa.*

Zestaw zabezpieczeń wynikających z przeprowadzonych analiz bezpieczeństwa znajduje swój materialny wyraz w postaci *systemu ochrony*, który obejmuje całość środków, struktur organizacyjnych i procedur postępowania służących zapewnieniu bezpieczeństwa informacji w danej organizacji.

W nawet w najlepiej zabezpieczonym systemie trzeba liczyć się z sytuacją, w której dojdzie do utraty bezpieczeństwa chronionych zasobów. Wtedy, wielkość poniesionych strat będzie zależeć od zdolności danej organizacji do zidentyfikowania i ograniczenia skutków takiego incydentu, podjęcia działań zmierzających do przywrócenia poprzedniego poziomu bezpieczeństwa oraz kontynuacji normalnej działalności. Sprawność tych działań zależy od tego czy organizacja ta jest do takiej sytuacji przygotowana. Umożliwia to *plan zapewnienia ciągłości funkcjonowania,* który zawiera scenariusze działań związanych z sytuacjami awaryjnymi. Plan taki jest więc istotnym elementem kompleksowego systemu bezpieczeństwa.

W bezpieczeństwie systemu znaczącą rolę odgrywa czynnik czasu. Nawet bardzo dobrze zabezpieczony system (względem określonej grupy zagrożeń) może utracić bezpieczeństwo na skutek pojawienia się nowych zagrożeń, które nie były poprzednio wzięte pod uwagę (np. nowe postaci wirusów) lub utraty skuteczności istniejących zabezpieczeń (np. poprzez ujawnienie ich sekretów). Może również zaistnieć sytuacja gdzie (dobrze dobrany) zbiór zabezpieczeń staje się nieefektywny ponieważ nie są one w praktyce stosowane. Niezbędne jest więc ciągłe zbieranie danych nt. nowych zagrożeń, inwentaryzacja prób ataków na system i innych zdarzeń związanych z bezpieczeństwem oraz ponawianie analizy bezpieczeństwa i weryfikacja skuteczności istniejących zabezpieczeń. Oznacza to, że niezbędne jest *zarządzanie bezpieczeństwem* systemu mające na celu ciągłe utrzymywanie (odnawianie) pożądanego poziomu bezpieczeństwa. Istotnym elementem jest tu *audyt* czyli działania kontrolne oceniające stan zabezpieczeń w systemie.

Powyższe rozważania wskazują na szeroki zakres pojęcia bezpieczeństwa systemu, daleko wykraczający poza zagadnienia czysto techniczne. Wynika również z nich, że w wielu wypadkach, przyjęcie konkretnych rozwiązań technicznych powinno być poprzedzone analizami przeprowadzonymi w odniesieniu do całego systemu i związanej z nim aplikacji.

Cykl życia bezpieczeństwa systemu

Cykl życia bezpieczeństwa systemu obejmuje całość działań dotyczących bezpieczeństwa i związanych z rozpatrywanym systemem. W szczególności, w jego zakres wchodzą następujące obszary:

- *Wytwarzanie systemu.*
  - Polityka bezpieczeństwa systemu, która jest wykorzystana jako punkt odniesienia przy ocenie bezpieczeństwa.
  - Specyfikacja funkcjonalna, która precyzuje wymagania odnośnie bezpieczeństwa systemu.
  - Analiza funkcjonalna systemu wykazująca w jaki sposób funkcje wymuszające bezpieczeństwo są powiązane z zagrożeniami.
  - Analiza „mocy" mechanizmów bezpieczeństwa, poprzez ocenę tworzących je algorytmów, przyjętych założeń oraz wynikających stąd własności.
  - Identyfikacja poziomu bezpieczeństwa komponentów systemu. W obecnym stanie technologii, system jest często „składany" z istniejących elementów, których

własności z punktu widzenia bezpieczeństwa mogą się różnić w znaczący sposób.
- Analiza integracyjna, która określa zdolność do harmonijnego współdziałania funkcji i mechanizmów bezpieczeństwa obecnych w systemie.
- Analiza i ocena słabych stron konstrukcji systemu, polegająca na ich identyfikacji, ocenie wynikających stąd skutków oraz propozycji środków zaradczych.
- Wybór i ocena architektury systemu ochrony określającej dyslokację i sposób dostępu do funkcji i mechanizmów wymuszających bezpieczeństwo.
- Szczegółowy projekt funkcji i mechanizmów bezpieczeństwa.
- Weryfikacja, walidacja i testowanie bezpieczeństwa systemu.

- *Środowisko wytwórcze:*
  - Zarządzanie konfiguracją zarówno w aspekcie wytwarzanego systemu jak i w aspekcie środowiska wytwórczego (w szczególności chodzi tu o ochronę i kontrolę dostępu do elementów konfiguracji oraz tworzonych wersji systemu).
  - Bezpieczeństwo użytych narzędzi (np. języki programowania i ich kompilatory).
  - Bezpieczeństwo związane z personelem zaangażowanym w proces wytwórczy.
  - Bezpieczeństwo procesu produkcji systemu.

- *Użytkowanie systemu:*
  - Łatwość użytkowania. Dotyczy to nie tylko sytuacji „normalnych" ale również sytuacji związanych z błędem systemu oraz procedurami powrotu do stanu normalnego i wynikającymi stąd skutkami dla bezpieczeństwa.
  - Niestabilność warunków operacyjnych systemu i wynikające stąd skutki dla bezpieczeństwa oraz możliwe środki zaradcze.
  - Dokumentacja użytkowa w zakresie bezpieczeństwa systemu.
  - Bezpieczne dostarczenie systemu w miejsce przeznaczenia oraz bezpieczeństwo instalacji systemu.
  - Bezpieczeństwo inicjalizacji i konfigurowania systemu.

- *Pielęgnacja:*
  - Stosowane strategie pielęgnacji systemu.
  - Ilość i bezpieczeństwo personelu mającego dostęp do systemu w trakcie jego konserwacji.
  - Efekty wynikające z aktualizacji jednego podsystemu i ich wpływ na inne podsystemy z nim współpracujące.
  - Bezpieczeństwo testowania po zabiegach konserwatorskich.
  - Usuniecie „kanałów dostępu" związanych z testowaniem systemu.

Proces zapewniania bezpieczeństwa informacji

Zapewnienie bezpieczeństwa nie jest aktem jednorazowym. Jest to proces, który powinien mieć jasno zdefiniowany zakres i cele, przypisaną odpowiedzialność oraz przydzielane zasoby. Ponieważ proces ten przebiega w zmiennych warunkach, musi on podlegać zarządzaniu.

Uruchomienie procesu zapewniania bezpieczeństwa w organizacji wymaga podjęcia następujących akcji:

- *Definicja celów bezpieczeństwa.* Cele lub zadania organizacji jak również istniejące uregulowania prawne nakładają określone wymagania dotyczące wykorzystania istniejących w niej systemów informatycznych. Wymagania te są podstawą do sformułowania celów bezpieczeństwa. Tak więc, cele bezpieczeństwa stanowią wymagania, których wypełnienie gwarantuje właściwe i bezpieczne wykorzystanie systemów informatycznych na rzecz osiągania celów i wypełniania zadań stawianych przed całą organizacją.

- *Uruchomienie funkcji zarządzania bezpieczeństwem.* Zarządzanie bezpieczeństwem zmierza do osiągnięcia i utrzymywania w czasie poziomu bezpieczeństwa adekwatnego do jawnie sformułowanych celów bezpieczeństwa. Wymaga to określonych działań organizacyjnych, dekompozycji i przydziału zadań i odpowiedzialności oraz koordynacji i nadzoru nad bezpieczeństwem.

- *Opracowanie polityki bezpieczeństwa informacji.* Polityka bezpieczeństwa określa sposoby osiągania bezpieczeństwa, na podstawie analizy zagrożeń i związanego z nimi ryzyka oraz poprzez dobór odpowiedniego zestawu środków ochronnych.
- *Implementacja systemu ochrony wynikającego z przyjętej polityki bezpieczeństwa.* Poprzez ustalanie priorytetów, planowanie zadań i przydzielanie odpowiedzialności związanej z ich realizacją, zestaw zabezpieczeń objęty systemem ochrony podlega wdrożeniu w ramach istniejących ograniczeń zasobów.

- *Zdefiniowanie programu szkoleń.* Program szkoleń musi uwzględniać potrzeby podniesienia kompetencji personelu czynnie zaangażowanego w procesie zapewniania bezpieczeństwa oraz ogólną potrzebę rozbudzenia świadomości i zrozumienia wśród załogi w zakresie przyjętych środków ochrony.

- *Nadzór nad bezpieczeństwem.* Proces zapewniania bezpieczeństwa nie kończy się z momentem wprowadzenia w życie systemu ochrony. Bezpieczeństwo musi podlegać nadzorowi i okresowym sprawdzeniom. W sytuacjach pojawienia się nowych zasobów, zagrożeń, wykrycia luk w systemie ochrony, itp., działania objęte powyższymi punktami są muszą być ponowione.

Janusz Górski jest pracownikiem Politechniki Gdańskiej, Katedry Zastosowań Informatyki
e-mail: jango@pg.gda.pl

Trzeci wymiar w Internecie – język VRML 97

Stanisław Polak

Po co VRML?

Jesteś właścicielem firmy budowlanej lub projektowej. Chcesz być nowoczesny, więc wizytówkę swojej firmy w postaci strony WWW umieszczasz w Internecie. W swojej ofercie masz trzy rodzaje domów. Aby użytkownik Internetu mógł je obejrzeć, dołączasz do zdjęcia każdy z nich. A jeżeli potencjalny nabywca chciałby zobaczyć wnętrza domów? Cóż, można go zaprosić do siedziby firmy i pokazać prospekt. Chyba, że zamiast zdjęć zamieścisz trójwymiarowe modele domów, które potencjalny nabywca będzie mógł zobaczyć, nie ruszając się od swojego komputera.

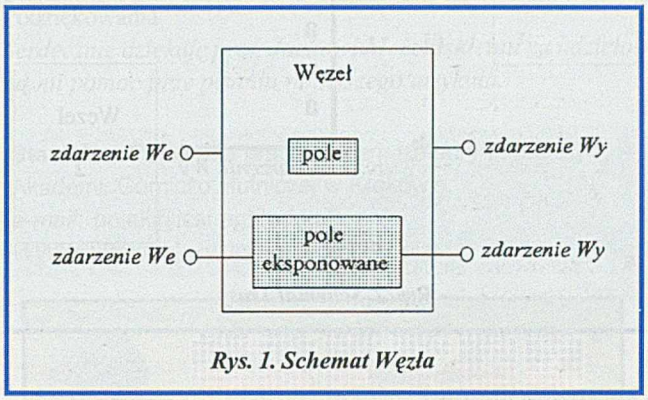
Co on na tym zyska? Może obejrzeć dom z każdej strony; wystarczą tylko ruchy myszką. Wycieczka po wirtualnym domu może wyglądać następująco: naciskamy myszką przycisk dzwonka, drzwi otwierają się bezszelestnie. Wchodzimy. W przedpokoju automatycznie zapala się światło. Wejdźmy do pokoju. Pokój jest jasno oświetlony przez słońce wpadające przez okno. Jeżeli oświetlenie jest zbyt słabe, możemy włączyć żyrandol. Zwiedzając pokój, mamy na przykład możliwość otwierania szaf, zaglądania w różne zakamarki itp.

Wszystko to można zrealizować w prosty sposób za pomocą języka VRML (*Virtual Reality Modeling Language*), czyli języka do tworzenia trójwymiarowych obiektów, które można prezentować w Internecie.

Niniejszy artykuł nie ma być kursem języka VRML, a tylko zachęcić Czytelnika do zainteresowania się nim.

Podstawy języka

VRML jest językiem młodym (jego historia rozpoczyna się w 1994 roku), ciągle rozwijanym i ... wciąż jeszcze mało znanym. Podstawowymi elementami służącymi do budowy trójwymiarowych obiektów są **Węzły** (*Nodes*). VRML zawiera pewną ilość zdefiniowanych węzłów. Użytkownik może tworzyć nowe węzły za pomocą już istniejących. Każdy węzeł zawiera pewną ilość **Pól** (*Fields*). Przy czym rozróżniamy dwa rodzaje pól: zwykłe (*field*) oraz eksponowane (*exposed field*). Każdy węzeł może przyjmować pewną liczbę **Zdarzeń wejściowych** (*eventIn*), które zmieniają stan węzła. Węzeł ma również możliwość wysyłania **Zdarzeń wyjściowych** (*eventOut*), które oznaczają, że coś w danym węźle zostało zmienione. Mechanizm ten umożliwia wzajemną komunikację pomiędzy poszczególnymi węzłami. Dzięki temu na przykład węzeł odpowiedzialny za wykrycie obecności obserwatora może przesłać odpowiednią informację do węzła odpowiedzialnego na przykład za włączenie światła muzyki, jak w naszym przykładzie.



Rys. 1. Schemat Węzła

Węzły

Możemy wyróżnić następujące rodzaje węzłów:

- **Geometryczne** umożliwiają tworzenie obiektów geometrycznych za pomocą brył (kula, stożek, sześcian, walec), umieszczanie tekstów itp.;
- **Własności** służą do zmiany koloru obiektów, nałożenia tekstury na obiekt, wygładzania obiektów itp.;
- **Wyglądu** służą do zmiany takich parametrów, jak: rodzaj nakładanej na obiekt tekstury, rodzaj materiału, z którego jest zbudowany obiekt itp.;
- **Sensory** wykrywają działania użytkownika, takie jak: dotknięcie obiektu, wejście do zadanego obszaru i wiele innych;
- **Interpolatory** służą do animacji obiektów;
- **Inne** umożliwiają m.in.: dodanie dźwięku do oglądanej sceny, dodanie efektu mgły, ustalenie punktu widokowego, umieszczenie własnego skryptu (np. Java, JavaScript) i wiele innych;

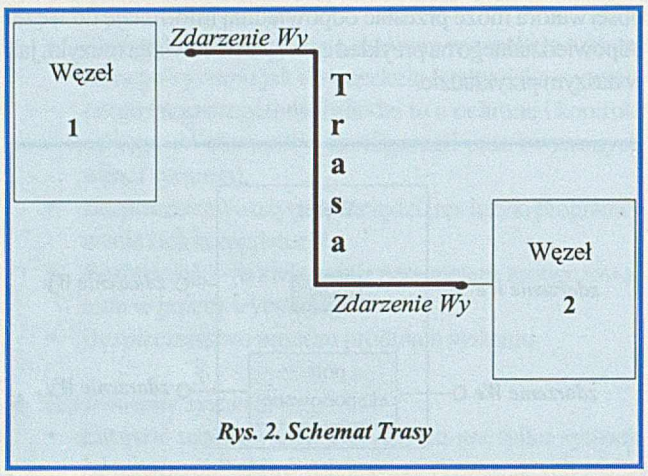
Pola

Pola to części składowe węzłów lub inaczej parametry, które odróżniają węzły tego samego typu. Pola służą do definicji stanu początkowego danego węzła, czyli na przykład ustalamy, że sześcian (węzeł *Box*) ma rozmiary: 4 x 5 x 6 metrów. Różnica między polem zwykłym a polem eksponowanym jest taka, że

w wypadku zwykłych pól nie mamy możliwości późniejszego zmieniania stanu początkowego węzła. Wartości parametrów ustalone podczas definiowania obiektu są niezmienne. Obrazuje to rysunek - do pola zwykłego nie ma dostępu z zewnątrz. W wypadku pól eksponowanych (rysunek) przez wysłanie odpowiedniego zdarzenia można zmieniać wartości parametrów ustalonych w trakcie definicji obiektu.

Zdarzenia

Węzły mogą komunikować się ze sobą przez przyjmowanie/wysyłanie zdarzeń. Jeżeli połączymy wyjście jednego z wejściem innego, otrzymamy tzw. **Trasę** (*Route*). Zdarzenia zapewniają interakcję z użytkownikiem. Poszczególne węzły mogą przesyłać między sobą informacje, które pozwalają w miarę wiernie odtworzyć rzeczywiste zachowania się rzeczy bądź osób.



Rys. 2. Schemat Trasy

No to zaczynamy

Jeżeli już poznaliśmy podstawowe pojęcia języka VRML, to spróbuję pokrótce omówić sposób stworzenia wymienionego na początku artykułu modelu domu. Ściany zbudujemy za pomocą sześcianu i załóżmy, że nasz dom ma wysokość 5 m, zaś długość ścian wynosi 30 m.

```
Box
{
    size 30 5 30
}
```

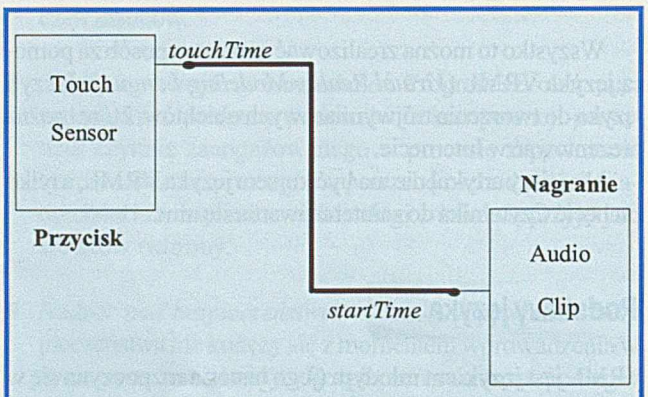
W powyższym przykładzie *Box* jest nazwą węzła, zaś *size* nazwą pola. Węzeł *Box* ma tylko jedno pole, które umożliwia określenie rozmiarów sześcianu. Do budowy wnętrza domu użyjemy pozostałych elementów geometrycznych, takich jak: walec, sfera itp.

Naciśnięcie przycisku przy drzwiach ma spowodować brzęczenie dzwonka. Przycisk dzwonka zrobimy podobnie jak ściany naszego budynku, czyli za pomocą sześcianu o odpowiednio niewielkich rozmiarach. Sam odgłos dzwonka musimy wcześniej nagrać i umieścić w pliku typu **MIDI** lub **WAVE**. VRML ma zdefiniowany węzeł, który pozwala na dodanie dźwięku do oglądanej sceny. Węzeł ten pozwala m.in. sterować zmianą natężenia dźwięku w zależności od odległości pomiędzy obserwatorem a źródłem dźwięku.

Aby stwierdzić fakt naciśnięcia przycisku, należy użyć jeszcze jednego węzła, a mianowicie **sensora dotyku** (*TouchSensor*). Sensory pozwalają wykryć takie zachowania obserwatora, jak: dotknięcie, przesuwanie, obracanie przedmiotu itp. Ostatni etap to odpowiednie połączenie omawianych węzłów, co może wyglądać następująco:

```
Group
{
    children
    [
        Shape { geometry Box {...} }   #węzeł nr 1
        DEF Przycisk TouchSensor {}  #węzeł nr 2
         Sound                          #węzeł nr 3
         {
             source DEF Nagranie AudioClip
              {
                  url „dzwonek.mid”
              }
         }
    ]
}
ROUTE Przycisk.touchTime TO Nagranie.startTime
```

W węźle grupującym *Group* zdefiniowałem następujące trzy węzły. Węzeł numer 1 definiuje przycisk dzwonka - sześcian o odpowiednim rozmiarze. Drugi węzeł definiuje sensor dotyku. Dodatkowo temu węzłowi nadaję nazwę (za pomocą słowa kluczowego DEF), aby można jej było później użyć. Wreszcie trzeci węzeł zawiera definicję źródła dźwięku. Na rys. 3 pokazano realizację połączenia miedzy sensorem dotyku a węzłem odtwarzającym dźwięk. W trakcie definicji węzłów niektórym z nich nadawałem nazwę, dzięki temu mogę określić, które węzły mają być ze sobą połączone. Konstrukcja: **ROUTE Przycisk.touchTime TO Nagranie.startTime** określa połączenie



Rys. 3. „ROUTE Przycisk.touchTime TO Nagranie.startTime”

między sensorem dotyku a węzłem odtwarzającym dźwięk. Równocześnie określamy, że moment aktywacji sensora dotyku jest początkiem odtwarzania dźwięku. Dlatego dźwięk dzwonka usłyszymy natychmiast po naciśnięciu przycisku. Zostaje jeszcze jedna kwestia. Jak to się dzieje, że dotknięcie przycisku jest wykrywane przez sensor dotyku. Proszę zauważyć, że sensor dotyku, jak i kształt przycisku dzwonka, są definiowane w tym samym węźle grupującym. Sensor dotyku wykrywa dotknięcie

obiektu (geometrii), który jest zdefiniowany w tej samej grupie i tak jest w tym wypadku. Jeżeli zdefiniowalibyśmy jakiś obiekt poza tą grupą, wtedy sensor dotyku nie wykryje dotknięcia.

Następny problem to ożywienie naszego świata. W języku VRML są do dyspozycji specjalne węzły zwane **interpolatorami**. Interpolatory umożliwiają m.in. cykliczne przesuwanie, obracanie, zmianę koloru obiektu itp. Interpolatory umożliwiają symulację prostych, cyklicznych ruchów. Jeżeli nas to nie satysfakcjonuje, możemy użyć węzła zwanego **skryptem**.

Węzeł ten daje nowe możliwości w kreowaniu zachowania się obiektów. Skrypty to też węzły, mogą wysyłać/odbierać zdarzenia, można je łączyć z pozostałymi węzłami itp. W przeciwieństwie jednak do pozostałych węzłów ich działanie zależy wyłącznie od użytkownika, a dokładnie od programu, który zleciliśmy do wykonania temu węzłowi. Programy lub, jak kto woli, skrypty możemy pisać w języku: *Java, JavaScript, ...*

W naszym przykładzie nie użyliśmy wszystkich możliwości VRML-a. Ciekawą cechą tego języka jest możliwość tworzenia nowych węzłów za pomocą już istniejących lub, jak kto woli, budowy **prototypów**. Mechanizm ten pozwala na enkapsulację, parametryzację obiektów, atrybutów, zachowań. Te nowo stworzone węzły można następnie udostępnić innym użytkownikom i w ten sposób rozszerzyć możliwości języka o nowe elementy. Użytkownik nie musi wiedzieć, jak działa prototyp, wystarczy mu tylko wiedza, jakie są jego parametry (jak go wywoływać).

VRML ma zdefiniowane trzy typy węzłów pozwalających sterować oświetleniem oglądanej sceny. Mamy między innymi możliwość wyboru koloru światła, sterowania jego natężeniem w zależności od odległości od źródła. Należy jednak podkreślić, że dostępne modele źródeł światła są jedynie przybliżeniem prawdziwych źródeł światła.

Nie wszystkie obiekty można zbudować za pomocą brył, dlatego VRML został wyposażony w węzły, które umożliwiają tworzenie terenów: łańcuchów górskich, powierzchni planet, dna mórz itp. Mamy również możliwość nakładania tekstur na obiekty. Czyli na przykład możemy zbudować ogrodzenie domu, nakładając na nie słoje drewna.

Jak zacząć?

Literaturę do nauki tego języka stanowi książka (po polsku), ale tylko do VRML w wersji 1.0. W niniejszym artykule oparłem się na wersji 97, do której nie znalazłem literatury w języku polskim. Pozostają więc anglojęzyczne pozycje bądź Internet. W 1996 roku powstała wersja 2.0 języka; w grudniu 1997 roku, po niewielkich retuszach opisu, otrzymała nazwę VRML 97. Twórcy tego języka uznali, że jedną z cech jakie powinien spełniać jest zdolność działania na wolnych łączach (14,4 kBps). Pliki VRML to pliki tekstowe. Są one łatwe do modyfikacji (wystarczy najprostszy edytor). Niestety rozmiary tych plików są znaczne, co może powodować, że transfer dużych plików może trwać relatywnie długo. Dlatego została powołana specjalna grupa robocza, której zadaniem jest opracowanie metody kompresowania formatu binarnego VRML, który umożliwi przyśpieszenie transportu plików VRML poprzez sieć. Stan i efekty tych prac można znaleźć na stronie: *http://www.vrml.org/WorkingGroups/vrml-cbf/cbfwg.html*.

Dokumentację do wersji 97 można znaleźć pod adresem: *http://vag.vrml.org/Specifications/VRML97/*. Warto ją wydrukować, mimo iż zajmuje ona około 200 stron. Początkujący powinni zajrzeć na stronę: *http://sim.di.uminho.pt/vrml/*. Zawiera ona opis poszczególnych węzłów. Ponadto zawarty na tej stronie skrypt w języku *JavaScript* umożliwia bezpośrednie generowanie kodu w języku VRML. Użytkownik może więc nie tylko teoretycznie, ale i praktycznie, zaznajomić się z danym węzłem. Strona *http://www.sdsc.edu/siggraph96vrml/* zawiera materiały z konferencji SIGGRAPH 96, na której przedstawiono VRML wersja 2.0. Pod adresem: *http://www.sdsc.edu/vrml/* znajduje się prawdziwa kopalnia wiedzy na temat języka VRML. Znajdują się tam m. in. informacje na temat: programów do oglądania plików napisanych w VRML, książek mu poświęconych, biblioteki gotowych obiektów i wiele wiele innych. Godne polecenia są również: *http://vrml.sgi.com/* oraz *http://www.vrml.org*. Wszelakie problemy można wyjaśnić na forum listy dyskusyjnej *news:comp.lang.vrml*. VRML są poświęcone również polskojęzyczne strony, np: *http://www.pwr.wroc.pl/~pankiewicz/vrml2.html* oraz *http://s1.efp.poznan.pl/~s3_0169/* .

Podziękowania

Serdecznie dziękuję prof. ***Jackowi Mościńskiemu*** *za udzieloną mi pomoc przy pisaniu niniejszego artykułu.*

Stanisław Polak jest pracownikiem Katedry Informatyki, Akademii Górniczo Hutniczej w Krakowie.
e-mail: polak@icsr.agh.edu.pl
WWW: http://galaxy.uci.agh.edu.pl/~polak/

Niniejszy artykuł jest próbą wskazania kilku zasad nowego podejścia do jakości, opartego na koncepcji jakości totalnej (TQM - *total quality management*), która wyznaje zasadę, że w każdej działalności najważniejszy jest człowiek, potrafiący stworzyć produkt wysokiej jakości zawsze tam, gdzie tej jakości od niego się oczekuje.

Zarządzanie jakością

Tomasz Byzia

Kiedy przeglądam ogłoszenia o kursach zawiązanych z doskonaleniem procesów produkcji oprogramowania, jako pozycję obowiązkową w ofercie firm konsultingowych, znajduję kurs metod kontroli jakości. Wobec rosnącego zapotrzebowania na narzędzia i metody pozwalające wytwarzać produkty o jakości wyższej niż produkty konkurencji, ten nurt projakościowy w działalności szkoleniowej wydaje się bardzo optymistyczny. Z perspektywy czasu widać jednak, że tradycyjne, tzn. bierne podejście do jakości produktów (oceniające „to co wyszło" w kategoriach udało/nie udało się) już nie wystarcza. Silna konkurencja i dynamika rynku wymagają wbudowywania jakości w produkt już od samego początku jego cyklu życia. Nikt nie ma czasu poprawiać tego, co nie zostało od razu zrobione dobrze.

Rzadko można spotkać wśród bogatej oferty kursów takie, które mówią o zapewnieniu jakości lub zarządzaniu jakością, nie jako zestawie narzędzi i metod, ale pewnej „systemowej" świadomości pracowników, dla których produkcja wysokiej jakości jest celem, zaszczytem i źródłem satysfakcji.

Co to jest jakość?

W ostatnich latach jesteśmy atakowani zewsząd informacjami o produktach wysokiej jakości. Półki sklepowe są wypełnione po brzegi proszkami, płynami do mycia naczyń i mydełkami najwyższej jakości. Dlaczego producenci reklam zadają sobie tyle trudu, aby podkreślić wysoką jakość swoich produktów? Podstawową przyczyną jest to, że słowo „jakość" działa jak magnes na każdego klienta. Z jakością spotykamy się wszędzie. Właściciele samochodów codziennie oceniają jakość dróg, sygnalizacji świetlnej, jakość serwisu, benzyny czy szmatki do wycierania szyb. Z jakością mamy do czynienia w urzędach, narzekamy na jakość usług medycznych i telekomunikacyjnych itd. Jakość jawi nam się jako zjawisko powszechne i dane nam intuicyjnie. Zauważmy, że nikt nie definiuje pojęcia jakości, a każdy się nim posługuje do oceny przedmiotów, które zamierza kupić, do ich klasyfikowania do różnych klas jakości oraz porównywania ze sobą. Znając niedogodności obcowania z bylejakością, dążymy do pozyskiwania produktów tylko wysokiej jakości.

Sądy jakościowe, wydawane przez różne osoby, mogą być oczywiście bardzo odmienne. Każdy z nas bez wyjątku ma jakiś „stosunek do spraw jakości" i każdy w zależności od swoich doświadczeń życiowych inaczej patrzy na rzeczywistość, a więc to, które produkty uzna za wysokiej jakości, jest czysto subiektywne. Z subiektywizmem sądów jakościowych wiąże się także ich zmienność. Wszyscy znamy takie sytuacje, kiedy wspaniały zakup okazuje się niczym szczególnym po przyniesieniu go do domu. Zmienność sądów jakościowych jest także tym, na czym bazują specjaliści od reklamy. Początkowy opór klienta „zwalcza się" ... liczbą powtórzeń!

Już te krótkie rozważania prowadzą nas do następujących wniosków: skoro jakość jest powszechna, subiektywna, kontekstowa, zmienna i intuicyjna, oznacza to, że definicji jakości jest tyle, ilu ludzi na ziemi. Jakość rodzi się w relacji do przedmiotu, o którym wydaje się sąd jakościowy. Zależy ona więc od podmiotu i przedmiotu sądu, kontekstu, czasu, miejsca itd.

Przyjrzyjmy się kilku definicjom jakości, które potwierdzą nasze obserwacje:

„Jakość jest to pewien stopień doskonałości."
Platon 427-347 p.n.e.

„Jakość jest jedną z dziesięciu kategorii, które umożliwiają podział wszystkich pojęć na grupy logiczne (czas, miejsce, ilość, substancja ...)"
Arystoteles, 384-322 p.n.e.

„Jakość to istotne cechy przedmiotu wyróżniające go spośród innych i stanowiące o jego swoistości pod danym względem."
Encyklopedia Popularna PWN

„Jakość to zgodność z wymaganiami."
Crosby

„Jakość to przydatność użytkowa."
Juran

„Jakość jest to stopień, w jakim użytkownik wierzy, że produkt lub usługa spełnia jego potrzeby i oczekiwania."
Gitlow

„Jakość jest tym, czego brak oznacza straty dla wszystkich."
Taguchi

„Ogół cech i właściwości produktu decydujących o jego zdolności do zaspokojenia stwierdzonych lub przewidywanych potrzeb."
ISO 8402 (9000)

Starałem się wybrać tylko takie definicje, które są potwierdzone niekwestionowanym autorytetem osób je wypowiadających.

Mimo to każda definicja mówi o jakości w inny sposób. Zauważmy, że definicji tych nie daje się jednoznacznie zrównać semantycznie. Każda jest inna, zwracając uwagę na inny aspekt jakości.

W praktyce wielokrotnie spotkałem sytuacje, w których próbowano budować systemy zapewnienia jakości, poddawano produkty najwymyślniejszym torturom testowym, realizowano plany poprawy jakości. Najczęściej jednak nie definiowano tego, co to znaczy wysoka jakość, przez domniemanie utożsamiając ją najczęściej z niezawodnością oprogramowania, tzn. minimalną liczbą błędów. W świetle dotychczasowych rozważań wszelka działalność projakościowa nie ma sensu w wypadku braku definicji jakości. Każdy z budujących system jakości będzie rozumiał go trochę inaczej, nosząc w sobie swoją „prywatną" definicję. Przypomina to budowanie wieży Babel. Każdy z budujących mówi innym językiem.

Jak zatem stworzyć w firmie skuteczny system jakości? Pierwszym krokiem do celu jest sformułowanie polityki jakości.

Polityka jakości

Pojęcie strategii jakości często jest definiowane jako ogół zamierzeń i kierunków działań firmy dotyczących jakości. Wyrażenie jej w sposób formalny przez najwyższe kierownictwo formułuje politykę jakości firmy. Ale to jeszcze za mało. Kierownictwo musi się autentycznie zaangażować w jej wdrożenie, realizację, przekonanie średniej kadry kierowniczej, a w końcu szeregowych pracowników. Zarządzanie jakością jest niczym innym, jak ogółem działań zmierzających do wdrożenia polityki jakości w firmie.

Jakość naszych produktów jest głównym celem firmy. Wysoką jakość rozumiemy jako pełną satysfakcję naszych klientów zewnętrznych i wewnętrznych z dostarczanych im produktów i usług. Osiągnięcie jakości i jej ciągłe doskonalenie jest sprawą każdego pracownika.

Prezes ...

Polityka jakości jest realizowana przez wszystkich pracowników firmy pod nadzorem kierownictwa w systemie jakości. System jakości obejmuje strukturę organizacyjną, podział odpowiedzialności za jakość i konkretne działania jej służące, procedury działania i zasoby niezbędne do realizacji postawionych zadań. Szczególną rolę w systemie jakości ma, wyznaczony przez kierownictwo firmy, pełnomocnik ds. jakości. Jako osoba postawiona wysoko w hierarchii zarządzania firmy, na przykład w randze wicedyrektora i wyposażona w duże pełnomocnictwa i kompetencje, jest ona odpowiedzialna za stworzenie i działanie systemu jakości.

Wzorcowy system jakości jest doskonale opisany w normach serii ISO 9000. Jest to zestaw minimum, który jest konieczny do otrzymania certyfikatu zgodności z normą. Czy jednak wystarcza do wyprodukowania produktu o wysokiej jakości? Czy producent mydełek z sadzy (!), który zdobył certyfikat ISO 9000 na tę produkcję, może liczyć na sukces?

Zarządzanie przez jakość

Ujmując rzecz historycznie, pierwsza była kontrola jakości. Sprowadza się ona do sprawdzania, mierzenia lub testowania jednej lub kilku charakterystyk produktu i odnoszenia wyników do wyspecyfikowanych wymagań w celu potwierdzenia zgodności. Zadanie to wykonywane zwykle przez wyspecjalizowany personel nie wchodzi w zakres obowiązków pracowników produkcyjnych. Produkty niezgodne ze specyfikacjami są odrzucane lub przekazywane do poprawienia. Proces produkcji oprogramowania w sposób naturalny zaadaptował to podejście do swojej praktyki. Testowanie oprogramowania jest dzisiaj jedną z ważniejszych (niestety często jedyną) techniką oceny jego jakości.

Wymogi długich serii produktów oraz pracochłonność przeprowadzania czasochłonnych testów spowodowały rozwój statystycznych metod kontroli jakości. Przebieg kontroli jakości ustala się na podstawie danych statystycznych i rachunku prawdopodobieństwa. Istotą procesu statystycznej kontroli jakości jest jego ciągłość.

Powyższe podejścia stosują binarne kryterium jakości: produkt przechodzi przez kontrolę lub jest odrzucany. Co zrobić, gdy kontrola pokazuje, że stale znaczny procent wyrobów się „marnuje"? Należy sterować jakością, tzn. przeprowadzając tradycyjną kontrolę produktu, włączać do systemu jakości pracowników produkcyjnych w celu stworzenia sprzężeń zwrotnych pomiędzy wynikami kontroli a linią produkcyjną. Na podstawie wyników kontroli proces produkcyjny jest modyfikowany w celu otrzymania produktów zgodnych ze specyfikacjami.

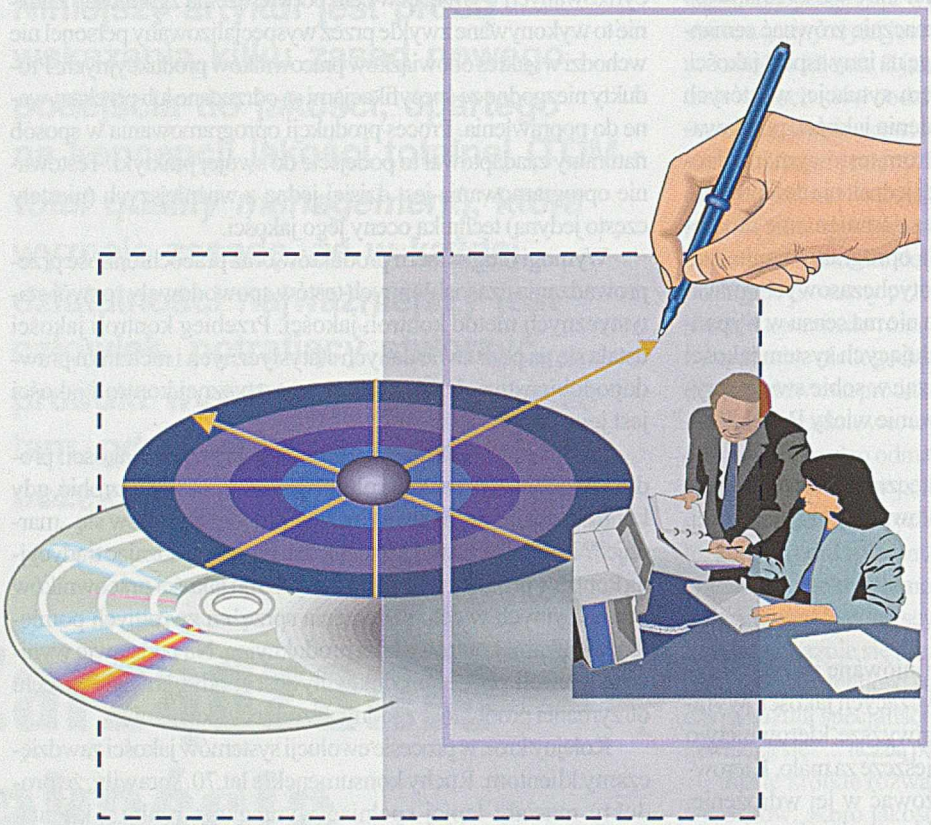
Kolejny krok w procesie ewolucji systemów jakości zawdzięczamy klientom. Ruchy konsumenckie lat 70. sprawiły, że produkty musiały lepiej spełniać wymagania rynku - klienta. Zapewnienie jakości było naturalnym rozwinięciem poprzednich praktyk. Jakość zaczęto wbudowywać w produkt od początku przez prowadzenie systematycznych i zaplanowanych działań prowadzących do wytwarzania produktów zgodnych ze specyfikacją. W celu ciągłego zapewnienia jakości dokonywano regularnych inspekcji, przeglądów, audytów i zewnętrznych ocen. System zapewnienia jakości był formalnie opisany i stosowany, a jego skuteczność stale monitorowana. Rozbudowywano działy marketingu i analizy wymagań, odpowiedzialne za dostarczanie wiarygodnych i uzgodnionych z przyszłym użytkownikiem specyfikacji wymagań.

Najnowszą koncepcją, która nie neguje pozostałych, lecz uzupełnia je o globalizację działań projakościowych, jest *zarządzanie przez jakość*. Jest to *skoncentrowane na jakości zarządzanie przedsiębiorstwem, przy współudziale wszystkich jego członków, w którym długofalowe korzyści przedsiębiorstwa oraz korzyści społeczeństwa są osiągane poprzez spełnienie oczekiwań klientów*. R. Kolman w swoim *Poradniku o jakości dla praktyków* w taki sposób wyjaśnia jego istotę: „Jest to system wielostronnego oddziaływania na jakość produktu przy racjonalnym wykorzystaniu zasobów ludzkich i materiałowych w procesach wytwórczych z ukierunkowaniem na osiągnięcie zadowolenia klientów".

Zarządzanie przez jakość zawiera w sobie wszystkie poprzednie nurty, historycznie wcześniejsze. Nie jest nową metodą, lecz filozofią opartą na pełnym i twórczym współuczestnictwie pracowników w tworzeniu produktów.

W podejściu tradycyjnym opartym na kontroli jakości:

- zarządzanie jakością jest oddzielną sferą działalności wyodrębnioną z organizacji;
- za jakość odpowiadają wydzielone komórki organizacji;
- główny nacisk jest położony na wykrywanie wad;
- decyzje operacyjne są podejmowane tylko przez kadrę kierowniczą;



Rys. G. Klechniowska

- głównym czynnikiem motywującym jest płaca.

W zarządzaniu przez jakość:

- jakość jest głównym celem przedsiębiorstwa;
- jakość jest sprawą każdego;
- jakość jest wielowymiarowa i obejmuje systemy, procesy, procedury, ludzi itd.;
- jakość polega na zapobieganiu wadom, a nie na ich wykrywaniu;
- jakość można i trzeba doskonalić.

Zasady zarządzania jakością

Koncepcja *Zarządzania przez jakość* nie jest nowa, lecz stosunkowo mało popularna. Jak zatem zabrać się do jej wdrażania w firmie, co stanowi o jej istotnych elementach, które z nich formułują konkretne zadania zgodne z jej podstawową filozofią? Czy sformułowana wcześniej polityka jakości nie zamieni się w kolejny slogan bez pokrycia?

Poniższe zasady zarządzania jakością pochodzą z prac rozwojowych nad aktualizacją norm serii ISO 9000. Ich wdrożenie i zastosowanie w praktyce zarządzania firmą stanowi fundament, na którym można budować konkretne rozwiązania systemów jakości oraz motywację pracowników do dalszego ich doskonalenia.

Ukierunkowanie na klienta

Organizacja zależy od swoich klientów, dlatego powinna dążyć do poznania i zrozumienia ich bieżących i przyszłych potrzeb, realizować ich wymagania i starać się przekraczać oczekiwania.

Odkryciem koncepcji TQM było zatarcie różnicy między klientem firmy i pracownikiem. Tych pierwszych nazywa się klientami zewnętrznymi, tych drugich wewnętrznymi. W TQM klientem jest po prostu ten (osoba lub organizacja), komu przekazuje się wyniki swej pracy. Różnymi metodami pobudza się troskę o każdego klienta: jego wymagania, oczekiwania i potrzeby. Przecież zarówno projektant, jak i użytkownik, chcą na przykład czytać dokumentację wysokiej jakości, która pomoże szybko rozwiązać problemy i pozwoli „cieszyć się życiem".

Przywództwo

Przywódcy ustanawiają jedność celu, kierunku i wewnętrznego środowiska organizacji.

Mówi się, że na polu walki żołnierzom nie jest potrzebny kierownik, ale przywódca. Nie potrzebują wyjaśnień i instrukcji, jak pewne rzeczy robić, na to był czas podczas szkolenia. Teraz potrzebny im jest ktoś, kto po prostu będzie z nimi, pomagając im znaleźć odwagę i sens w tym, co muszą robić.

Przywódcy muszą być otwarci na wymianę myśli i budowanie jasnych, długofalowych wizji organizacji. Ich główną rolą jest identyfikacja wartości, które pracownicy uznają za swoje i budowanie na tych wartościach kultury korporacyjnej firmy. Przywódca nie mówi, co pracownik musi zrobić, przywódca sprawia, że „rzeczy się dzieją".

Zaangażowanie ludzi

W zapewnienie jakości są zaangażowani wszyscy pracownicy na wszystkich szczeblach organizacji.

To ludzie są twórcami jakości. Żadne narzędzia, metody i systemy nie zastąpią ich osobistego zaangażowania. Przywódcy, budując na wartościach wspólnych dla organizacji i pracowników, kreują pełne i autentyczne zaangażowanie w osiąganie celów organizacji. Jest to zaangażowanie, które dostarcza satysfakcji z pracy i zwiększa motywację. Istotnym elementem tego procesu jest szkolenie całej kadry firmy. Tworzy to atmosferę współodpowiedzialności i wzajemnego zaufania. Jeśli firmie zależy, abym się rozwijał, to i ja włączę się w działania zmierzające do rozwoju „Mojej Wspaniałej Firmy".

Podejście procesowe

Pożądane rezultaty są osiągane skuteczniej, gdy odpowiednie zasoby i działania widzi się jako elementy dynamicznego procesu.

Jakość rodzi się nie w ogólnej relacji klient-producent, ale w wielu mniejszych relacjach między poszczególnymi pracownikami. To analityk systemowy tworzy specyfikację wymagań, którą potem czyta projektant i na tej podstawie projektuje system. Nie ma żadnej obiektywnej, zewnętrznej „instancji", która może się wypowiadać o jakości specyfikacji wymagań. Tym, który ją ostatecznie weryfikuje, jest zawsze projektant, gdyż to on stworzy „arcydzieło" z dobrego surowca lub będzie się męczył, budując na piasku.

Opisana przezemnie sytuacja to klasyczny łańcuch jakości, którego ogniwami są pracownicy, a łącznikami relacje między nimi, wynikające z procesu wytwórczego - cyklu życia produktu (projektu). Myślenie procesowe oznacza skoncentrowanie się na tych relacjach i doskonalenie ich tak, aby „rodziły" jakość zamiast problemów.

Myślenie procesowe oznacza także rozbudowany system miary produktywności na wejściu, wyjściu i wewnątrz procesu oraz system akcji korygujących. Ten ostatni bazuje na osobistym zaangażowaniu pracowników, które sprawia, że pracownicy sami „donoszą" o wszystkich mankamentach, niedociągnięciach i wadach produktu i systemu produkcji. Doskonalenie procesu staje się wtedy łatwiejsze i skuteczniejsze.

Podejście systemowe

Identyfikacja, zrozumienie i zarządzanie systemem wzajemnie powiązanych procesów przyczynia się do zwiększenia skuteczności i wydajności organizacji.

Istotną innowacją, którą koncepcja TQM wniosła do tradycyjnego spojrzenia na system jakości, było spostrzeżenie, że jakość produktu rodzi się nie tylko w procesie produkcyjnym, ale w całym jego otoczeniu. W dziale marketingu, sprzedaży, serwisie, usługach, administracji firmy, księgowości, dyrekcji itd. Wszędzie tam, gdzie coś się może nie udać lub coś można ulepszyć, jest miejsce na działania projakościowe.

TQM widzi kompleksowość działań obejmującą wszystkie etapy powstawania produktu oraz złożone procesy funkcjonujące w złożonych relacjach. Doskonalenie oznacza równoległe doskonalenie wszystkich powiązanych ze sobą procesów.

Ciągłe doskonalenie

Ciągłe doskonalenie jest stałym celem organizacji.

Nie od razu Kraków zbudowano. To przysłowie świetnie oddaje ducha TQM w dziedzinie doskonalenia jakości. Szkoda czasu na kosztowne analizy i plany nienagannych systemów zapiętych „na ostatni guzik". Stwórzmy zamiast tego, samoregulujący i samodoskonalący się system oparty na zaangażowaniu pracowników. Róbmy to, co możemy, aby było najlepiej i doskonalmy to. Mówi się, że firmy zarządzane przez jakość mają obsesję na punkcie doskonalenia. Rozbudowane mechanizmy raportowania błędów, dostrzeżonych niedociągnięć, wad i mankamentów w produkcie, procesie produkcyjnym i zasobach ludzkich, systematyczne przeglądy procesów i systemu jakości (audyty), systemy premiowania inicjatyw i „postawy czujności" pracowników, w dłuższej perspektywie dają lepsze efekty niż kosztowne i spektakularne „przewroty" organizacyjne.

Decyzje oparte na faktach

Skuteczne decyzje i działania są oparte na logicznej i intuicyjnej analizie danych i informacji.

W sytuacji ciągłej pogoni za uciekającym rynkiem i użytkownikiem często podejmujemy szybkie decyzje, oparte tylko na doświadczeniu i intuicji kadry kierowniczej i często ... źle na tym wychodzimy. Polega to zwykle na tym, że trudno w krótkim czasie zebrać wszystkie informacje niezbędne do wypracowania decyzji o najniższym stopniu ryzyka. A co by było, gdyby te informacje gromadzić w sposób ciągły? System jakości jest odpowiedzialny nie tylko za zapewnienie jakości, ale i za stałe monitorowanie procesów w firmie, tzn. za gromadzenie faktów, analizę oraz dostarczanie informacji do wypracowania decyzji. Ważne jest nie to, co my myślimy o procesie, ale fakty - udokumentowane konkrety.

Partnerstwo dla jakości

Partnerskie powiązania między organizacją i jej dostawcami oraz klientami zwiększają zdolność wspólnego tworzenia wartości.

Tworzenie coraz większych systemów i produktów powoduje, że związki producentów z klientami stają się coraz bliższe. Ich wzajemne „uzależnienie" może przetrwać lata. W takiej sytuacji lepsze rozpoznanie i przystosowanie do potrzeb klienta, współpraca i jej doskonalenie, tworzą międzyorganizacyjny efekt synergiczny. Producent i klient we wzajemnym klimacie zaufania i bezpieczeństwa mogą wbudowywać w produkt nie tylko wymagania użytkownika, ale także jego oczekiwania. Nie od dziś wiadomo, że na rynku wygrywa ten producent, który zgadnie czego oczekuje, a nie czego chce przyszły użytkownik.

❖ ❖ ❖

Zdaję sobie sprawę, że przedstawione przeze mnie zasady mogą być odbierane w różny sposób. Część czytelników może uznać je za zbędne teoretyzowanie, całkowicie oderwane od rzeczywistości. Inni będą starali się znaleźć coś dla siebie, zgadzając się z pewnymi rzeczami z innymi nie. Jest to dla mnie naturalne, gdyż ocena jakości tego artykułu jest subiektywną sprawą każdego czytelnika.

Moją intencją jest jednak to, aby nikt nie pozostał obojętny wobec zaprezentowanych tu idei. Można przecież wytwarzać doskonałe produkty, posiadając lub nie certyfikat ISO 9000. To, co się liczy naprawdę, to autentyczne zaangażowanie w poszukiwanie wszelkich rozwiązań, przynoszących poprawę jakości produktów, czy w sferze narzędzi, metod, procesów, czy też relacji międzyludzkich. Ja wierzę, że taka postawa leży w sercu TQM - zarządzania przez jakość.

Tomasz Byzia jest pracownikiem warszawskiej firmy konsultingowej InfoViDE. Zajmuje się systemami zapewnienia jakości oraz doskonaleniem procesów produkcji oprogramowania. E-mail: tbyzia@infovide.pl

POLSKIE TOWARZYSTWO INFORMATYCZNE

BIULETYN

NUMER 8 (157) ROK XVII WRZESIEŃ 1998

W czasie gdy oddajemy do druku kolejny numer Biuletynu, trwają ostatnie przygotowania do XV Kongresu IFIP (International Federation for Information Processing). Hasło tegorocznego kongresu brzmi „Globalne społeczenstwo informacyjne w drodze do następnego tysiąclecia". Kongres odbędzie się w terminie od 31 sierpnia do 4 września w dwóch pięknych, połączonych Dunajem i bogatą historią, miastach: Wiedniu i Budapeszcie. W trakcie siedmiu kongresowych konferencji wygłoszonych zostanie 350 referatów, a w przeddzień i w dzień po Kongresie odbędzie się seria imprez dodatkowych, w tym specjalna prezentacja Europejskiego Komputerowego Prawa Jazdy. Tutorial na temat „Formal Specification of Computer Systems - Selected Methods and Supporting Software Tools" poprowadzi prof. Jan Madey. Polska jest reprezentowana w IFIP przez Polską Akademię Nauk, a pośrednio także przez PTI. Warto bowiem przypomnieć, że nasze Towarzystwo jest zrzeszone w afiliowanej przy IFIP-ie Radzie CEPIS (Council of European Professional Informatics Societies). W trakcie Kongresu CEPIS będzie uroczyście obchodzić dziesięciolecie swojego istnienia.

Oba Jubileusze stanowią doskonałą okazję, by w bieżącym numerze Biuletynu zamieścić krótką prezentację obchodzących je organizacji. W uzupełnieniu zamieszczamy sprawozdania z ostatnich posiedzeń Zarządu Głównego PTI.

International Federation for Information Processing

IFIP

IFIP powstał w 1960 roku pod auspicjami UNESCO. Główne cele jego działalności dotyczą promowania informatyki w nauce i technice, głównie poprzez pielęgnowanie współpracy miedzynarodowej, stymulowanie badań, rozwoju i zastosowań technik przetwarzania informacji w nauce i wszelkiej innej działalności ludzkiej, popieranie rozpowszechniania i wymiany informacji oraz wspomaganie inicjatyw edukacyjnych w dziedzinie przetwarzania informacji. IFIP liczy 59 członków, z czego 44 członków stałych a 11 afiliowanych organizacji miedzynarodowych, reprezentujacych wszystkie regiony swiata. Władze i sekretariat IFIP mają swoją siedzibę w Laxenburgu (Austria). Sztandarowym wydarzeniem jest odbywający się co dwa lata Światowy Kongres Komputerowy. Jego tegoroczna piętnasta edycja została zorganizowana w Wiedniu i Budapeszcie. Ponadto corocznie IFIP zaangażowany jest w organizacje ponad 65 miedzynarodowych sympozjów, z których referaty są publikowane w ponad trzydziestu książkach. Podstawowe prace IFIP-u są prowadzone przez 12 Komitetów Technicznych obejmujących ponad 70 Grup Roboczych. Pełne informacje o działalności IFIP można znaleźć pod adresem: *http://www.ifip.or.at/*.

Council of European Professional Informatics Societies

CEPIS został zarejestrowany w Holandii w 1988 roku. Reprezentuje głosy około 150 000 zawodowych informatyków – członków 23 towarzystw z 20 państw. Członkostwo w CEPIS-ie oparte jest na członkostwie w Radzie Europy. Stowarzyszenia międzynarodowe lub paneuropejskie mogą być członkami afiliowanymi.

Polska i Węgry były pierwszymi krajami Europy Centralnej, które zasiliły szeregi CEPIS-u, a po ostatnim spotkaniu w Lejdzie (maj 1998 r.) dołączyły do nich Litwa, Słowenia i Czechy.

Podstawowy cel działania CEPIS-u stanowi dbałość o wysoki poziom nauczania i dokształcania w dziedzinie przetwarzania informacji w Europie, staranie o wysoki poziom kompetencji i etyki zawodowej informatyków, a także o wysoki poziom umiejętności użytkowników oraz kształtowanie świadomości wspólnoty europejskiej.

Jako zrzeszenie zawodowych informatyków CEPIS stawia sobie za zadanie promowanie wspólnoty celów i możliwości swobodnego przemieszczania się zawodowych informatyków w całej Europie, współpracy naukowej i technicznej w dziedzinie przetwarzania i wykorzystania informacji, doprowadzenie do wzajemnego uznawania kwalifikacji informatyków i akceptacji standardów zawodowych w różnych krajach, propagowanie postępowania zgodnego z opracowanym przez CEPIS Kodeksem Postępowania Zawodowego oraz sponsorowanie wspólnych przedsięwzięć w dziedzinie informatyki.

Jako reprezentant społeczności informatyków europejskich CEPIS prowadzi działalność mającą na celu:

- informowanie instytucji europejskich i znanych gremiów europejskich o poglądach zawodowych informatyków i wpływanie na decyzje władz i instytucji Unii Europejskiej,
- doradztwo i uczestnictwo w rozwoju legislacji ogólnoeuropejskiej w świetle dynamicznie rozwijającej się informatyki,
- koordynacje prac legislacyjnych i standaryzacyjnych związanych z zawodem informatyka.

CEPIS utrzymuje swoją stronę WWW (*http://www.cepis.org/*).

LISTA CZŁONKÓW CEPIS

E.Ł. na podstawie Programu Kongresu IFIP
http://www.ifip.or.at/, http://www.cepis.org/

L.p.	Skrót	Nazwa	Kraj
1.	AICA	Associazione Italiana per 'Informatica	Włochy
2.	ATI	Asociacion de Tecnicos de Informatica	Hiszpania
3.	BCS	The British Computer Society	Wielka Brytania
4.	CCS	Cyprus Computer Society	Cypr
5.	CSCI	Czech Society for Cybernetics and Informatics	Czechy
6.	DD	Dansk Dataforening	Dania
7.	DF	Dataforeningen i Sverige	Szwecja
8.	DND	Den Norske Dataforening	Norwegia
9.	FIPA	Finnish Information Processing Association	Finlandia
10	GCS	Greek Computer Society	Grecja
11.	GI	Gesellschaft fuer Informatik eV	Niemcy
12.	ICS	Irish Computer Society	Irlandia
13.	ISIP	Icelandic Society for Information Processing	Islandia
14.	ITG	Informationstechnische im VDE Gesellschaft im Verband Deutscher Elektrotechniker	Niemcy
15.	LIKS	Lietuvos Kompiuterininko Sajunga	Litwa
16.	NGI	Nederlands Genootschap voor Informatica	Holandia
17.	NJSzT	John v Neumann Computer Society	Węgry
18.	OCG	Osterreichische Computer Gesellschaft	Austria
19.	PTI	Polskie Towarzystwo Informatyczne (PIPS:The Polish Information Processing Society)	Polska
20.	SDI	Slovensko Drustvo Informatika	Słowenia
21.	SI	Societe Suisse des Informaticiens	Szwajcaria
22.	VRI	Vereniging van Register Informatici	Holandia
23.	ECDL-F	European Computer Driving Licence Foundation (Europejskie Komputerowe Prawo Jazdy)	Irlandia

Sprawozdanie z posiedzenia Zarządu Głównego z dnia 2 kwietnia 1998 r.

1. Kol. Andrzej Marciniak (prezes Oddziału Wielkopolskiego) poinformował o piśmie „Pro Dialog", współwydawanym przez ten właśnie Oddział. Pismo wychodzi dwa razy w roku, w nakładzie od 600 do 1000 egz., jest w nim publikowane sprawozdanie z pracy Oddziału.
2. Sekretarz Generalny przypomniał, że członkowie PTI, którzy chcą otrzymywać nieodpłatnie pismo „Informatyka", muszą wyrazić pisemną zgodę na udostępnienie ich danych osobowych. Zgoda może być wyrażona za pośrednictwem poczty elektronicznej. Do tej pory złożyło ją około 100 osób.
3. Dyskutowano nad założeniami budżetu na 1998 r. i nad współpracą w tym zakresie z poszczególnymi oddziałami. Zwrócono uwagę na trudną sytuację Oddziału Mazowieckiego.
4. Przyjęto 5 nowych członków zwyczajnych PTI.
5. Przyjęto dwóch nowych członków wspierających: firma Océ-Poland z Warszawy (kategoria A) oraz firma International Business Systems z Wrocławia (kategoria B).
6. Rozpatrzono listę 126 osób, przewidzianych do skreślenia z listy członków za niepłacenie składek. Ustalono, że zostanie do nich raz jeszcze wysłany blankiet wpłaty. W razie niezapłacenia Zarząd Główny podejmie decyzję o ich skreśleniu.
7. Przedyskutowano sprawę ustalania przynależności członków PTI do oddziałów i przekazywania informacji o opłacanych składkach. Kol. Sekretarz Generalny ma zaproponować odpowiednią procedurę.
8. Wysłuchano informacji o konferencjach w Świnoujściu, Szczyrku, Mrągowie i Kazimierzu nad Wisłą, a także o II Kongresie Informatyki (30 listopada – 2 grudnia 1998 r.)
9. Wysłuchano sprawozdania o realizacji programu CRIT-2, przedyskutowano możliwości zakupów ze środków przeznaczonych na dalszą realizację programu.
10. Kol. Marek Miłosz poinformował o rozwoju akcji ECDL (Europejskie Komputerowe Prawo Jazdy). Wydano około 500 kart umiejętności (EKUK), uczestnicy zdali około 700 egzaminów, w tym około 20 osób zdało wszystkie egzaminy modułowe i otrzymało (lub otrzyma w najbliższym czasie) Prawo Jazdy. Pozostała jeszcze jedna wpłata do Fundacji ECDL. Akcja dobrze rozwija się w Lublinie, Katowicach i Poznaniu, gorzej w Warszawie. Istnieje potrzeba zwiększenia liczby egzaminatorów w Krakowie.
11. Zarząd Główny w swej uchwale wyraził szczególne uznanie dla Marka Miłosza za kierowanie biurem ECDL i postanowił przyznać mu dyplom uznania i specjalną nagrodę.
12. Kol. Zygmunt Mazur (Wrocław) poinformował o przygotowaniach do XI Konkursu Prac Magisterskich. Zarząd Główny zaakceptował wysokość nagród: pierwsza – 1300 zł, druga – 1000 zł, trzecia – 800 zł. Trzy wyróżnienia po 600 zł. Przewodniczącym jury ponownie będzie prof. Czesław Daniłowicz.
13. Z okazji 50-lecia polskiej informatyki Zarząd Główny postanowił zwolnić z opłacania wpisowego osoby, wstępujące do PTI w okresie od 1 czerwca do 31 grudnia 1998 r.

Sprawozdanie z posiedzenia Zarządu Głównego z dnia 2 lipca 1998 r.

1. Prezes PTI zapoznał członków Zarządu z listem p. Lesława Wawrzonka, redaktora naczelnego „Informatyki", podsumowującego dotychczasową współpracę. Tegoroczny jedenasty numer pisma ma być poświęcony II Kongresowi Informatyki.
2. Prezes PTI przedstawił stan przygotowań do II Kongresu. Członkowie PTI bedą prowadzili kilka sesji, poświęconych różnym aspektom informatyki, m.in. związkom informatyki z nauką, kulturą i administracją.
3. W maju 1999 r. Odbędzie się kolejny Zjazd PTI. Na następnym posiedzeniu zostaną przyjęte uchwały, określające m.in. zasady wyboru delegatów.
4. Zarząd Główny postanowił zaproponować kol. Zdzisława Szyjewskiego, prezesa PTI, na członka Rady Informatyki przy Ministrze Spraw Wewnętrznych i Administracji.
5. Kolega Andrzej Marciniak przedstawił propozycję utworzenia Sekcji Studenckiej PTI. Sekcja ta gromadziłaby studentów i pozwoliłaby przywrócić tradycje wymiany doswiadczeń m.in. uczestników studenckiego ruchu naukowego (coroczne seminaria „Infosem"). Zarząd Główny przyjął te informacje do wiadomości. Sekcja zostanie formalnie powołana po przedstawieniu konkretnych form działania. Chętni do współpracy powinni się skontaktować z Oddziałem Wielkopolskim.
6. Zarząd Główny wysłuchał informacji o pracach mających na celu reaktywowanie Oddziału Małopolskiego.
7. Przyjęto jednego nowego członka.
8. Kol. Marek Miłosz poinformował, że PTI w całości uregulowało swoją składkę w Fundacji ECDL, co pozwala ubiegać się w Fundacji o środki na popularyzację akcji.
9. Zarząd Główny wysłuchał informacji o Szkole Górskiej w Szczyrku.

J. Deminet

Redaktor: EWA ŁUKASIK
e-mail: lukasik@put.poznan.pl, tel. (0-61) 878 23 73
Instytut Informatyki, Politechnika Poznańska,
ul. Piotrowo 3a, 60-965 Poznań

Polskie Towarzystwo Informatyczne, Zarząd Główny
tel. (22) 624 60 61 w.328, tel./fax (22) 652 32 59
URL: http://www.pol.pl/pti
ul. Żelazna 87, 00-879 Warszawa

Set your business free

Freedom to Grow

IFS Applications - informatyczne systemy wspierające zarządzanie przedsiębiorstwem – – jest rozwiązaniem skalowalnym, co pozwala na jego rozwój równocześnie z rozwojem przedsiębiorstwa. Dzieki temu łatwo i szybko wybijesz się ponad konkurencję.

Freedom to Change

IFS Applications to rozwiązanie elastyczne, oparte o bazę danych Oracle. Z łatwością dostosowuje się do zmian wewnątrz i na zewnątrz przedsiębiorstwa, niezależnie od jego lokalizacji, waluty i języka.

Freedom of Mind

Wszystkie moduły IFS mają łatwy w obsłudze graficzny interfejs, który w prosty sposób może być dostosowany do wymagań każdego użytkownika.

Od wielu lat tworzymy informatyczne rozwiązania wspierające zarządzanie przedsiębiorstwem. Pracując nad IFS Applications opieramy się na bardzo prostych zasadach. Wierzymy, że przedsiębiorstwa, tak jak i ludzie, chcą rozwijać się bez ograniczeń. Chcą zmieniać się i rosnąć bez uzależniania się od nietypowej technologii informatycznej. Chcą odnosić sukcesy. Niezależnie czy wybierzecie Państwo jedno rozwiązanie z rodziny IFS Applications, czy cały ich zestaw, błyskawicznie zauważycie realne efekty ich stosowania.
Konkurencja również!

INDUSTRIAL & FINANCIAL SYSTEMS

IFS

Warszawa
Tel. (48 22) 608 46 00
Fax (48 22) 608 46 01

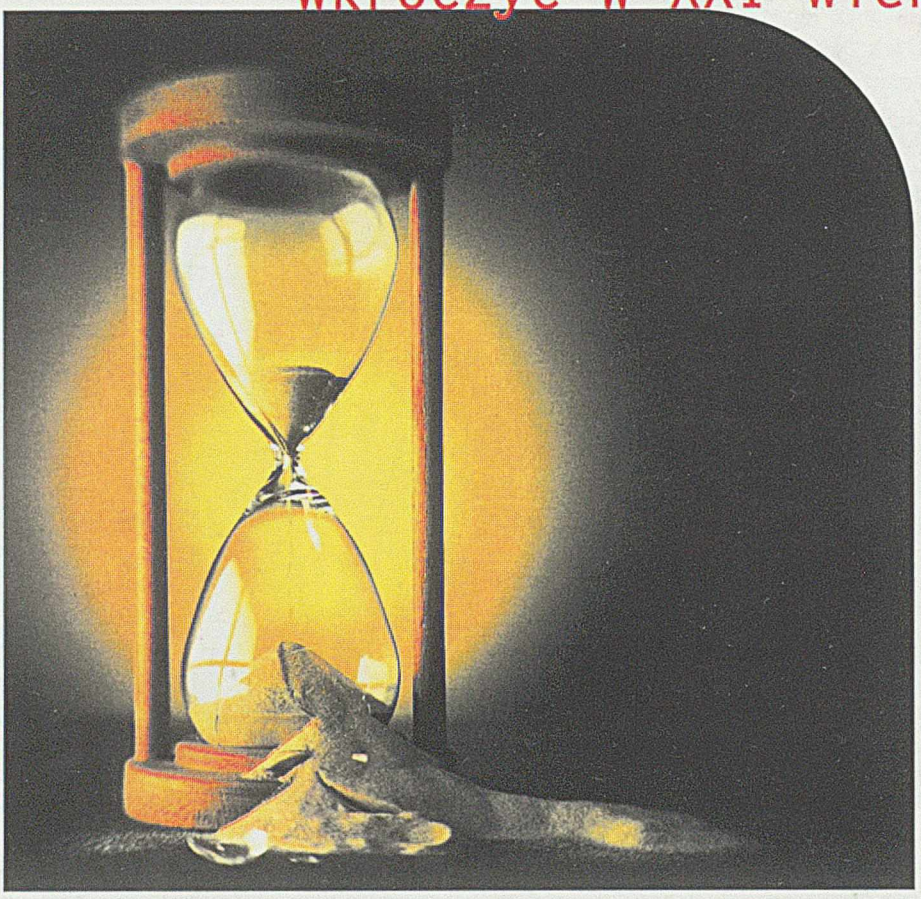
Kraków
Tel. (48 12) 422 50 15
Fax (48 12) 421 45 29

Gdańsk
Tel. (48 58) 345 29 64
Fax (48 58) 345 29 67

Poznań
Tel. (48 61) 851 92 55
Fax (48 61) 851 96 50

http://www.ifsab.com info@ifs.com.pl

Czy twój system jest gotowy wkroczyć w XXI wiek?



Wraz z nadejściem roku 2000 użytkownicy wielu wykorzystywanych obecnie programów będą musieli sprostać nowym problemom. Dwie cyfry oznaczające rok będą wówczas cofały przedsiębiorstwo do roku 1900, zamiast umożliwić mu wkroczenie w następne tysiąclecie. Problem ten pojawił się już w przypadku długoterminowych planów i kontraktów. A czas ucieka.

System R/3® firmy SAP® umożliwia rozwiązanie tego i innych problemów, które mogą pojawić się w przyszłości. Dostępne są w nim na przykład funkcje przeliczania i obsługi wielu walut (związane z planowanym wprowadzeniem w całej Europie wspólnej waluty – Euro), a także aplikacje Internetowe, dzięki którym możliwe jest przeprowadzanie transakcji elektronicznych z wykorzystaniem międzynarodowej sieci komputerowej. Twórcy systemu R/3 zawsze spoglądają w przyszłość, oferując jeszcze więcej.

Już po krótkim etapie wdrożenia standardowy system R/3 wspomagający zarządzanie umożliwia automatyzację najważniejszych procesów realizowanych we wszystkich działach przedsiębiorstwa i powiązanie ich w sieć wzajemnych zależności. Dzięki takiemu połączeniu działów rachunkowości, produkcji, sprzedaży, zarządzania kadrami oraz innych obszarów przedsiębiorstwa uzyskuje się lepszy i pełniejszy przepływ informacji, co ma ogromny wpływ na szybkość podejmowania decyzji i ich trafność. Przedsiębiorstwo zaczyna funkcjonować w taki sposób, jakiego zawsze oczekiwało kierownictwo.

Dzięki modułowej budowie systemu R/3 każdy klient otrzymuje rozwiązanie idealnie dostosowane do swoich potrzeb. W dowolnym momencie system może być rozszerzany o kolejne aplikacje, dzięki czemu staje się najlepszym rozwiązaniem dla przedsiębiorstw o dowolnej wielkości, działających w każdym sektorze gospodarki.

Nasz adres:
SAP Polska Sp. z o.o. Mokotów Business Park
02-672 Warszawa, ul. Domaniewska 41
tel. (+48 22) 606 06 06; fax (+48 22) 606 06 07

SAP
A Better Return On Information.