E-GOSPODARKA

Poradnik przedsiębiorcy

Warszawa 2003

Autor
Adam Wawszczyk

Redakcja i korekta
Agnieszka Tokaj-Krzewska

Projekt okładki
Jakub Osiński, Jacek Pacholec

Projekt serii
Tadeusz Korobkow

ISBN 83-88802-63-1

Wydanie I

Nakład 1000 egzemplarzy

Druk i oprawa
Instytut Technologii Eksploatacji
26-600 Radom, ul. K. Pułaskiego 6/10, tel. centr. 364-42-41, fax 3644765

SPIS TREŚCI

Wstęp
Gospodarka elektroniczna – wprowadzenie, rys historyczny i polskie perspektywy

Gospodarka elektroniczna rozumiana jest jako realizacja procesów gospodarczych z wykorzystaniem środków elektronicznej wymiany danych. Rozwijające się technologie teleinformatyczne sprawiły, że zmienia się forma procesów zachodzących wewnątrz przedsiębiorstw, pomiędzy nimi (tzw. B2B), w kontaktach z klientami indywidualnymi (B2C), a nawet między samymi klientami (C2C). Podstawowe procesy, jak obsługa zamówień, płatność, promocja oraz dostawa mogą być realizowane na drodze elektronicznej. Przedmiotem transakcji handlowych stają się produkty i usługi cyfrowe nie mające postaci materialnej. Kluczowym elementem takich nowych form działalności gospodarczej są technologie informatyczne.

W historii istniał zawsze ścisły związek między gospodarką a formami jej finansowania i środkami technicznymi stosowanymi do obrotów pieniężnych[1]. Gdy pojawił się pieniądz kredytowy (banknot), zrezygnowano z waluty kruszcowej i pokrycia w złocie. Współczesnym obliczem tych zależności są nowoczesne metody rozliczeń między bankami i ich klientami, realizowane przez rozmaite dostępne technologie. Te zmiany wyrażają się w tym, co właśnie określamy jako gospodarka elektroniczna.

Powstanie systemu ekonomicznego opartego na gospodarce elektronicznej nie jest problemem technicznym, ale zagadnieniem dotyczącym organizacji, zarządzania, stworzenia odpowiedniego środowiska gospodarczego. Nie jest to kwestia mody związanej z pojawieniem się nowych technik i wykorzystywaniem technologii teleinformatycznych, jest to kwestia zrozumienia, że są to tylko narzędzia, które pojawiły się wskutek przeobrażeń w funkcjonowaniu gospodarki.

Do tych zmian w gospodarce doszło w chwili wprowadzenia masowej produkcji, skrócenia cyklu życia produktów i pojawienia się popytu na dobra wyższego rzędu. Przyczyniło się to do destabilizacji otoczenia przedsiębiorstw i konieczności przystosowania się do zmian. Aby to zrobić, firmy musiały naruszyć

[1] Z. Stempnakowski, *Problemy z wprowadzaniem gospodarki elektronicznej*, referat IV Forum Teleinformatyki w Legionowie, Uniwersytet Szczeciński, 2002.

swoje utarte rozwiązania i kanony organizacyjne. Nastawienie sił głównie na produkcję powodowało słabe efekty sprzedaży. Należało zrezygnować z utrzymywania izolowanych pionów operacyjnych w przedsiębiorstwach.

W latach trzydziestych zaczęto wprowadzać do zarządzania metody reklamy i marketingu. Powstała specjalizacja związana z badaniem rynku. W latach sześćdziesiątych marketing stał się wiodącym obszarem działalności firm, które jednocześnie koncentrowały się na metodach zapewniających wysoką jakość. W Japonii rozpoczęto produkowanie towarów, np. samochodów, zgodnie z konkretnymi, indywidualnymi zamówieniami klientów. Poszczególne zamówienia trafiały na stanowisko montażu, skąd wysyłano na papierze zapotrzebowanie na części do dostawców. Ci ostatni produkowali zamówione części dopiero w chwili otrzymania zlecenia. W ten sposób drastycznie redukowano zbędne zapasy, a także koszta ich wytworzenia i magazynowania oraz czas dostawy (Just–In–Time).

Procedury w handlu międzynarodowym również były niewydolne i należało je zmieniać. W 1963 r. powstała Grupa Robocza Nr 4 EKG ONZ do standaryzacji większości dokumentów handlu zagranicznego i metody ich wystawiania. W jej ramach wypracowano m.in. znany dokument celny SAD. Informacje o tym dokumencie można umieścić w formie kodów zapisywanych w określonych segmentach, które są rozłożone w ustalony sposób na jednej kartce papieru. Taka organizacja informacji umożliwia mechaniczny odczyt dokumentów.

Obok tych zmian następowały także przemiany techniczne związane głównie z gwałtownym rozwojem komputerów i ich zastosowań. Wymiana informacji między różnymi systemami informatycznymi firm jest możliwa tylko po uzgodnieniu odpowiednich standardów, które w technikach EDI[2] zaczęły się nadmiernie mnożyć. Powiązania podmiotów w gospodarce są jednak zbyt ścisłe, by można było pozwolić na taki zróżnicowany system standardów. Różne branże muszą mieć możliwość wymiany dokumentów elektronicznych. W cytowanej wyżej Grupie Roboczej ONZ zdawano sobie z tego sprawę i przystąpiono do ujednolicania standardów na potrzeby teletransmisji między systemami komputerowymi poszczególnych partnerów handlowych.

[2] Electronic Data Interchange (EDI) – elektroniczna wymiana danych – standard elektronicznej wymiany dokumentów handlowych, takich jak faktury i zlecenia zakupu. Standard ten opracowało Stowaryszenie ds. Normalizacji Wymiany Danych (DISA).

Obecnie wszystkie inne większe standardy wymiany zapowiedziały i realizują migrację w kierunku standardu EDIFACT[3]. Prawie w każdym kraju są organizacje mające na celu integrację działań w obszarze EDI i standardu EDIFACT[4].

Działająca w Polsce organizacja Centrum EDI Polska (CEDIP) zrzesza przedstawicieli różnych branż gospodarki. Celem jej działalności jest wypracowywanie, przy współpracy z innymi jednostkami krajowymi i zagranicznymi, zaleceń dla instytucji gospodarczych i administracyjnych w dziedzinie EC/EDI ułatwiających wdrażanie i upowszechnianie w Polsce EC/EDI oraz wprowadzanie standardu UN/EDIFACT. We współczesnych czasach międzynarodowy system finansowy jest oparty na elektronicznej automatyzacji, a jednym z typowych tego przejawów jest elektroniczny pieniądz. Daje on możliwość globalizacji gospodarki i będzie generował zanikanie gospodarczych granic. Dlatego technika EDI, pozwalająca na automatyzację procedur, musiała dotrzeć do Polski. Wszędzie tam, gdzie należy wykonywać masowo te same rutynowe czynności, można zastosować odpowiednie algorytmy, o jasnych kryteriach decyzyjnych, a przekaz dokumentów lub transfer środków finansowych można zautomatyzować. Analiza zjawisk związanych ze stosowaniem elektronicznej wymiany danych prowadziła do wniosku, iż stosowanie EDI wymusza procesy optymalizacji organizacji i funkcjonowania przedsiębiorstwa, przyczyniając się tym samym pośrednio do wzrostu efektywności gospodarowania[5].

---

[3] Ang.: electronic data interchange for administration, commerce and transport – standard elektronicznej wymiany danych (EDI) dla rozwiązań w administracji, handlu i transporcie.

[4] W Polsce czyni to Centrum EDI Polska. Ustalono polską normę związaną z tym standardem, spolonizowano zasady składni oraz promuje się wdrażanie dokumentu elektronicznego w Polsce.

[5] Optymalizacji transakcji w e-gospodarce służy też wprowadzenie różnych form pieniądza elektronicznego. Są to na przykład powszechnie używane karty debetu i kredytu. Gdy konsument płaci kartą za usługę czy towar, pieniądz płynie z jego konta na konto sprzedawcy w formie elektronicznych komunikatów, a banki automatycznie pobierają prowizję. Nowe systemy płatności stosują inteligentne karty. Można wydawać z nich pieniądze wszędzie tam, gdzie są zainstalowane odpowiednie czytniki i gdzie nie wymaga się potwierdzenia przez bank. Teoretycznie można nawet w ten sposób posługiwać się fikcyjnym pieniądzem, realizowanym w formie zapisów komputerowych zainteresowanych partnerów gospodarczych. Ten wirtualny pieniądz mógłby nie mieć nawet żadnego odpowiednika w oficjalnych, bankowych zasobach, a byłby tylko formą wzajemnego rozliczania się. Jest to osobny problem dla rządów i instytucji, mających ustawowy obowiązek nadzorowania przepływów pieniężnych. Może bowiem powstać świat wzajemnie konkurencyjnych walut elektronicznych, z których jedne wypychają drugie.
Szereg takich rewolucyjnych zmian doprowadzić może do zniknięcia granic narodowych w gospodarce elektronicznej. Cyfrowa gospodarka światowa i elektronizacja w finansach międzynarodowych powstaje i będzie się rozwijać. Odpowiednio do tego będą musiały zmieniać się i standaryzować uregulowania międzynarodowe, a także krajowe.

Rozkwit EDI związany ze zjawiskiem globalizacji gospodarki, a także pomysł wykorzystania do jej celów Internetu nadały elektronicznej wymianie danych charakter filozofii prowadzenia działalności gospodarczej i zmusiły do podjęcia prób kompleksowego uregulowania związanych z nią kwestii. Zagadnienie to zaczyna być palącym problemem. Dobrym przykładem upowszechniania się EDI w krajach wysoko rozwiniętych jest sytuacja w USA. EDI jest tam szeroko stosowane nie tylko w gospodarce, ale również w administracji, przy czynnym poparciu najwyższych władz USA. EDI stosuje się w wymianie danych między i wewnątrz instytucji bankowych, w administracji państwowej, ale także w zarządzaniu wymianą informacji w dużych przedsiębiorstwach posiadających oddziały.

Światowa gospodarka jest w fazie globalizacji, dotykającej szczególnie elektronicznego handlu, usług i produkcji opartej na zaawansowanych technologiach. Systemy informatyczne, dzięki którym te przemiany są możliwe, można zakwalifikować do grupy systemów strategicznych, przełomowych w osiąganiu przyszłych sukcesów gospodarczych. Nieuchronnie gospodarka elektroniczna wyeliminuje gospodarkę posługującą się papierowymi dokumentami. Jest to spowodowane głównie względami ekonomicznymi, a od tych w zdrowej gospodarce rynkowej nie ma odwrotu.

1. Podstawy prawne e-gospodarki na świecie i w Polsce

- Inicjatywa Społeczeństwa Informacyjnego,
- E-biznes w dokumentach organizacji miedzynarodowych,
- Podpis elektroniczny w prawie polskim.

1.1. Unormowania międzynarodowe

1.1.1. Prawne aspekty elektronicznego obrotu towarowego w UE[6]

FAST

Pierwsze kroki na rzecz budowy społeczeństwa informacyjnego w Europie Zachodniej zapoczątkowano już w 1979 roku, kiedy rozpoczęto pięcioletni program eksperymentalny pod nazwą Forecasting and Assessment in the Field of Science and Technology (FAST).

Jego głównym zadaniem było wyznaczenie podstawowych założeń, priorytetów oraz celów długoterminowej wspólnotowej polityki badań i rozwoju. Wśród wniosków i propozycji, jakie opracowano w trakcie realizacji programu FAST, naczelne miejsce zajęła konkluzja, iż „rozwój społeczeństwa informacyjnego, przyczyniając się do wzmocnienia przyszłej politycznej, społecznej oraz ekonomicznej kondycji i roli Europy Zachodniej, musi przebiegać w dwóch, ściśle związanych czy też wręcz wzajemnie przenikających się wymiarach: technologiczno-przemysłowym oraz społecznym (tzw. dual challenge)".

Z dzisiejszej perspektywy spostrzeżenie to można uznać za kamień węgielny polityki wspólnotowej na rzecz budowy społeczeństwa informacyjnego w Europie.

eEurope

Najbardziej dojrzałą i kompleksową okazała się jednak inicjatywa unijna dotycząca budowania społeczeństwa informacyjnego w Europie, z grudnia 1999 roku. Określona została nazwą eEurope i została przedstawiona na szczycie Rady Europejskiej w Helsinkach. Jest to dokument ramowy wyznaczający do realizacji w relatywnie krótkim okresie (lata 2000–2005) cele służące umożliwieniu każdemu obywatelowi UE współuczestniczenie w two-

[6] W. Czyżowicz, *Prawo celne w gospodarce elektronicznej,* KNoP SGH, Warszawa 2002.

rzeniu społeczeństwa informacyjnego oraz korzystanie z wynikających z tego profitów. Proponowane projekty dotyczą bardzo wielu dziedzin życia – począwszy od edukacji informatycznej i ochrony zdrowia, kończąc na rozwiązaniach służących rozwojowi handlu elektronicznego czy wprowadzeniu tzw. smart cards.

Jako zadania wyznacza się utworzenie kilku typów baz danych, np. z aktami legislacyjnymi i administracyjnymi, z których obywatele będą mogli czerpać wiarygodne i aktualne informacje. Dodatkowo postuluje się korzystanie z interaktywnych technik komunikowania w celu np. konsultacji czy opiniowania nowych projektów regulacji wielu aspektów życia społecznego i gospodarczego oraz politycznego[7].

Action Plan

W marcu 2000 roku w Lizbonie został przedstawiony pierwszy raport z postępów w implementacji inicjatywy, zaś w czerwcu miał zostać przyjęty przez Radę UE eEurope Action Plan, w którym miały zostać wyznaczone konkretne środki, jakie państwa członkowskie podejmą dla realizacji inicjatywy. Bezpośrednio sprawom gospodarki elektronicznej poświęcony został rozdział II tego dokumentu pt. „Nowe metody pracy i handlu elektronicznego". Jednym z głównych zadań, jakie postawiono w tym programie, jest: „przyspieszenie handlu elektronicznego: szybkie zastosowanie ram prawnych, pozwalających na rozszerzenie drogą elektroniczną zamówień publicznych".

Społeczeństwo Informacyjne

Tak więc, jak widać, stosunkowo niewiele problemów odnosiło się do handlu elektronicznego i jego prawnych aspektów. Tym niemniej, nie czekając na ten dokument, różne instytucje Unii Europejskiej, zwłaszcza jej Komisji, wcześniej podejmowały działania na rzecz realizacji idei zawartych w „*Inicjatywie Społeczeństwa Informacyjnego*". Szczególnie aktywną w tej sferze okazała się Dyrekcja Generalna III – Przemysł w Komisji Europejskiej. To z jej inicjatywy pojawiły się projekty dyrektyw odnoszących się do handlu elektronicznego. Do najistotniejszych z nich należy zaliczyć inicjatywę zawartą w Komunikacie Komisji Europejskiej z 1997 r. „*Propozycję Dyrektywy w sprawie niektórych prawnych aspektów handlu elektronicznego*", która została przyjęta w 1998 r.

Inicjatywa europejska w dziedzinie handlu elektronicznego

Z kolei podjęta w 1997 r. w UE „*Inicjatywa europejska w dziedzinie handlu elektronicznego*" wskazała na cztery główne priorytetowe wytyczne, dotyczące handlu elektronicznego. Odnosiły się one do:

[7] Sam projekt eEurope umieszczony został w Internecie wraz z prośbą o przesyłanie pocztą elektroniczną wszelkich uwag i komentarzy na jego temat.

- liberalizacji rynku telekomunikacyjnego;
- ustanowienia ram prawnych i administracyjnych, jasnych i możliwych do przewidzenia;
- rozwoju R&D (badań i wdrożeń);
- stworzenia otwartego i konkurencyjnego środowiska gospodarczego sprzyjającego rozwojowi handlu elektronicznego.

Komisja Europejska wskazała, że: „w ciągu dwóch ostatnich lat wykonano poważną pracę w dziedzinie prawnej i administracyjnej w celu popierania, na szczeblu europejskim i światowym, jasnych i dających się przewidzieć ram prawnych, dotyczących istotnych aspektów handlu elektronicznego, a także praw autorskich, ochrony danych, zabezpieczenia i uwierzytelnienia oraz piractwa informatycznego. (...) Propozycja ta (dyrektywa w sprawie niektórych aspektów prawnych) poświęcona zasadniczym przeszkodom napotykanym przez przedsiębiorstwa, które zaangażowały się w handel elektroniczny ponad granicami, stanowi poważny krok naprzód w celu ustanowienia jasnych i możliwych do przewidzenia ram, przyczyniających się do inwestowania i większej konkurencyjności (...)

Handel elektroniczny i podatki pośrednie

Równie pierwszoplanową sprawą jest zniesienie niepewności w dziedzinie opłat, które, jak wiadomo, stanowią poważną przeszkodę w rozwoju handlu elektronicznego. W przewidywaniu tego, komunikat zatytułowany „*Handel elektroniczny i podatki pośrednie*", zatwierdzony przez Radę ECOFIN, dał podstawy do międzynarodowego porozumienia (układu) na temat wielkich tendencji skarbowych, który mógłby być zawarty w czasie konferencji OECD".

Na bazie wskazanych analiz i kierunków proponowanych rozwiązań w dniu 18 listopada 1998 r. Komisja Europejska przyjęła propozycję Dyrektywy Parlamentu Europejskiego i Rady w sprawie niektórych aspektów prawnych handlu elektronicznego na Rynku Wewnętrznym.

Usługi Społeczeństwa Informacyjnego

Dyrektywa formułuje m.in. definicję usługi w ramach Społeczeństwa Informacyjnego, która jest rozumiana jako

„... wszelkie usługi, zwykle świadczone za wynagrodzeniem, na odległość poprzez wyposażenie elektroniczne, przy pomocy wyposażenia elektronicznego dla przetwarzania (w tym kompresji cyfrowej) i przechowywania danych i na indywidualne zamówienie otrzymującego usługę (...)".

Jak więc widać na definicję tę składa się kilka elementów:
- są to wszelkie usługi realizowane, w zasadzie, za wynagrodzeniem;
- są one realizowane na odległość;

- są one realizowane za pomocą sprzętu elektronicznego;
- są one realizowane na indywidualne zamówienie otrzymującego usługę.

Definicja Usług Społeczeństwa Informacyjnego

Choć nie można wysnuć stąd jednoznacznej definicji odbiorcy usługi, to można zakładać, że dotyczy to zarówno osób fizycznych, jak i prawnych oraz podmiotów gospodarczych nie posiadających osobowości prawnej. Sprawa ta bez żadnych wątpliwości wyjaśniona zostaje w punkcie (18) wstępu do tej Dyrektywy. Stwierdza się w nim to, że: „Usługi Społeczeństwa Informatycznego obejmują szeroki wachlarz działalności gospodarczej, która, w szczególności, może składać się ze sprzedaży towarów w trybie on-line; jednakże działalność polegająca na dostarczaniu towarów jako takich lub prowadzenie działalności usługowej off-line nie są włączone w tę kategorię, ale usługi Społeczeństwa Informacyjnego nie są ograniczone wyłącznie do usług zmierzających do zawierania kontraktów on-line, ale również, jeśli tylko przedstawiają one sobą działalność gospodarczą, obejmują sobą także usługi, które nie są wynagradzane przez tych, którzy je otrzymują, jak na przykład usługi oferujące informację w trybie on-line lub przekaz informacji handlowych, albo dostarczające narzędzia pozwalające wyszukiwać, zdobywać dostęp i pobierać dane; usługi Społeczeństwa Informatycznego obejmują również usługi polegające na transmisji informacji przez sieci komunikacyjne, zapewnianiu dostępu do sieci komunikacyjnej lub przechowywaniu informacji dostarczonych przez otrzymujących usługi; (...)

prowadzenie działalności w rozpowszechnianiu telewizyjnym, a także rozpowszechnianie radiowe nie są usługami Społeczeństwa Informacyjnego, ponieważ nie są dostarczane na indywidualne zamówienie;

odmiennie od powyższego, usługi które są transmitowane między dwoma punktami, takie jak obraz na żądanie lub wysyłanie informacji handlowych pocztą elektroniczną są usługami Społeczeństwa Informacyjnego; użycie poczty elektronicznej lub jej ekwiwalentu w indywidualnym komunikowaniu się na przykład osób fizycznych działających poza ramami swojej profesji, handlu czy biznesu, włączając ich użycie dla zawarcia kontraktu między takimi osobami nie są usługą Społeczeństwa Informacyjnego; stosunki umowne między pracodawcą i jego pracownikiem nie są usługą Społeczeństwa Informacyjnego; działalność, która ze swojej natury nie może być realizowana na odległość i przy pomocy środków elektronicznych, taka jak statutowa kontrola kont firmy czy porada medyczna wymagająca fizycznego zbadania pacjenta nie są usługami Społeczeństwa Informacyjnego".

Ten obszerny cytat pokazuje bardzo wyraźnie, że w ramach Społeczeństwa Informacyjnego część usług zawiera w sobie katego-

rię „towar", jednakże związaną jedynie ze sprzedażą, ale fizycznym dostarczeniem go tradycyjną drogą („off-line"). Stanowisko to, wyłączające z omawianej Dyrektywy z 8 czerwca 2000 r., regulacje handlu tradycyjnego, a dokładniej realizowanego przy pomocy tradycyjnych, innych niż elektroniczne, środków transportowych jest powtarzane jeszcze parokrotnie w omawianej dyrektywie (np. w Art. 2 pkt (h) podpkt (ii). Dyrektywa ta nie zawiera regulacji w sprawach celnych. I nie ma w tym nic dziwnego, ponieważ Dyrektywa jest skierowana do krajów członkowskich UE i ściśle wiąże się z jednolitym rynkiem europejskim, na którym obrót towarowy dokonywany jest bez barier celnych.

Postanowienia usług

Oczywiście jej twórcy zdają sobie sprawę z globalnego charakteru Internetu. Stąd też niejednokrotnie podkreślają, że Dyrektywa nie dotyczy usług dostarczanych przez providerów ustanowionych w krajach trzecich i że nie ma ona zaszkodzić dyskusjom prowadzonym w tej sprawie na forum innych organizacji międzynarodowych, takich jak WTO czy OECD (pkt 58 Wstępu). Co więcej, w kolejnych punktach wprowadzenia (wstępu) do tej Dyrektywy wskazuje się na konieczność prowadzenia konsultacji między UE i większością regionów pozaeuropejskich w celu tworzenia zgodnych (kompatybilnych) praw i procedur (pkt 60). Najbardziej bezpośrednio wskazuje się na to w punkcie 62, kiedy stwierdza się tak: „Współpraca z krajami trzecimi powinna być zacieśniona na polu handlu elektronicznego, w szczególności odnosi się to do krajów aplikujących (o członkostwo w UE – CW), krajów rozwijających się i innych partnerów handlowych Unii Europejskiej".

Z tego sformułowania nie wynika nic ponadto, że Unia będzie starać się o to, by ewentualnie regulacje, jakie sama stosuje w odniesieniu do handlu elektronicznego, ale realizowanego w ramach jednolitego rynku, przynajmniej częściowo, stały się standardami międzynarodowymi. W tym celu chce wykorzystać wymianę poglądów nie tylko z krajami aplikującymi o członkostwo (a więc i z Polską), ale i do ich prezentacji na międzynarodowych forach zajmujących się regulacjami handlu międzynarodowego, przede wszystkim WTO i OECD.

A ma po temu poważne powody, zwłaszcza po kolejnej nowelizacji Kodeksu celnego Unii Europejskiej.

Kodeks celny

W dniu 16 listopada tegoż roku – Parlament Europejski i Rada Europejska przyjęły Rozporządzenie Nr 2700/2000 uzupełniające i zmieniające unijny Kodeks celny.

Zmiany i uzupełnienia Kodeksu celnego Unii Europejskiej nie były czymś nieoczekiwanym. Wręcz przeciwnie. Już w momen-

cie tworzenia KC UE zakładano, że po pierwszym okresie jego stosowania zostaną poddane analizie i ocenie przyjęte w nim i w KCW UE regulacje. Ocena ta miała być dokonana nie tylko przez administracje celne krajów członkowskich Unii Europejskiej i Komitet Kodeksu Celnego (organ techniczno-doradczy Komisji Europejskiej), ale i przez społeczność gospodarczą UE.

Prace nad zmianami i uzupełnieniami trwały praktycznie permanentnie. Było to związane nie tylko z poszerzaniem Unii Europejskiej o nowe kraje członkowskie czy poszerzaniem obszaru celnego tego ugrupowania, ale i wymogami wynikającymi z rozwoju handlu międzynarodowego, jego rosnącej dynamiki i nowych technik informatycznych. Potrzeba z jednej strony wprowadzenia maksymalnych uproszczeń i ułatwień dla zwiększenia szybkości obrotu towarowego, a więc i konkurencyjności unijnych przedsiębiorstw na rynku światowym, z drugiej strony zaś konieczność wprowadzania nowych technik i skutecznych metod kontroli oraz zwalczania przemytu i przestępczości celnej były punktami wyjściowymi dla zaproponowanych zmian.

Elektroniczny przekaz danych

Wśród zaproponowanych nowych metod przewidziano daleko idące uproszczenia wynikające z zastosowania metod elektronicznego przekazu danych, przy czym zrezygnowano, z dotychczas istniejącego, bezwzględnego wymogu dostarczania wraz ze zgłoszeniem celnym wszystkich pozostałych dokumentów do urzędu celnego. Mają być one dostępne dla administracji celnej. Zawarte to zostało w zmianie dotychczasowego Art. 77 KC UE przez dodanie do niego punktu 2 przewidującego taką właśnie sytuację.

1.2. Różne ujęcia e-biznesu w dokumentach głównych organizacji międzynarodowych

E-biznes w dokumentach międzynarodowych

Jeśli UE skupiła swoją uwagę na rozstrzyganiu problematyki handlu elektronicznego w ramach Jednolitego Rynku Europejskiego, to inne organizacje międzynarodowe zajmujące się sprawami handlu podjęły to zagadnienie w kontekście obrotów dokonywanych między poszczególnymi państwami. Do najważniejszych z nich, o powszechnym charakterze, należą takie, jak Organizacja Narodów Zjednoczonych (**ONZ**), Organizacje Współpracy Gospodarczej i Rozwoju (Organization of Economic Co-operation and Development – **OECD**), Światowa Organizacja Handlu (World Trade Organization – **WTO**), Światowa Organizacja Celna (World Customos Organization – **WCO**) czy pozarządowa Międzynarodowa Izba Handlowa (International Chamber of Commers – **ICC**). W nich właśnie powstają i są proponowane krajom

członkowskim uniwersalne regulacje prawne albo ich projekty czy modelowe propozycje aktów prawnych, odnoszące się do nowych zjawisk w sferze międzynarodowych obrotów towarowych. Każda z nich ma swoje specyficzne pole regulacji. Mimo że wszystkie są organizacjami międzyrządowymi, to specjalizują się w innych obszarach handlu międzynarodowego. WCO to organizacja skupiająca swoją uwagę na przygotowywaniu i międzynarodowym wdrażaniu technicznych standardów w sferze celnej. WTO i OECD natomiast skupiają swoją uwagę na polityce handlowej oraz podatkowej związanych z handlem międzynarodowym, w tym i handlem elektronicznym. ONZ natomiast zajmuje się tymi zagadnieniami na najbardziej ogólnym poziomie.

1.2.1. ONZ – UNCITRAL

ONZ, a zwłaszcza jej Komisja ds. Prawa Handlu Międzynarodowego (United Nations Commission on International Trade Law – UNCITRAL) zajmuje się przygotowaniami najbardziej uniwersalnych praw związanych z normami i standardami regulującymi międzynarodowy obrót towarowy. To właśnie w tej Komisji, powołanej przez Zgromadzenie Ogólne ONZ, w grudniu 1996 r., powstał najbardziej uniwersalny dokument prawny zatytułowany „Model prawny UNCITRAL dla handlu elektronicznego z przewodnikiem realizacyjnym", który został przyjęty jako Rezolucja Zgromadzenia Ogólnego ONZ.

Model prawny UNCITRAL

Jest to obszerny dokument służący jako punkt odniesienia dla wielu szczegółowych regulacji przyjmowanych tak w organizacjach międzynarodowych, jak i na poziomie narodowym. Już we wstępie tego ważnego aktu wskazuje się na jego znaczenie dla rozwoju handlu międzynarodowego i doskonalenia narodowego ustawodawstwa. Podkreśla się dążenie do: „... dalszej harmonizacji i unifikacji prawa handlu międzynarodowego (...) oraz ze względu na rosnącą liczbę transakcji w handlu międzynarodowym dokonywanych przy pomocy środków elektronicznej wymiany danych i innych środków komunikacji, popularnie (commonly), określanych jako „handel elektroniczny", który wprowadza w użycie alternatywne do bazujących na papierze metody komunikowania się i przechowywania informacji, (...)".

To w tym akcie, bodajże najszerzej ze wszystkich podobnych dokumentów organizacji międzynarodowych, podchodzi się do handlu elektronicznego jako do zjawiska ogarniającego ogromną gamę zagadnień ze sfery międzynarodowego obrotu towarowego. W zakresie jego regulacji znajduje się „... każdy rodzaj informacji w formie danych elektronicznych (data message) używanych w kontekście działań handlowych".

Definicja handlu elektronicznego

Wspomniany dokument pełen jest szczegółowych definicji kategorii, jakimi się posługuje lub do jakich się odnosi. Jego część pierwsza to w istocie słowniczek pojęć. Choć Artykuł 1 poświęcony jest zakresowi stosowania, niemal każde słowo użyte w nim jest szczegółowo definiowane w przypisie. I tak właśnie definiowany jest termin „handlowy", przez który rozumie się „... szeroką interpretację tego, co wiąże się ze sprawami powstającymi z każdego stosunku o naturze handlowej, zarówno kontraktowego, jak i nie kontraktowego. Stosunki o naturze handlowej włączają, lecz nie są do tego ograniczone, następujące transakcje: każdą transakcję handlową związaną z dostarczeniem lub wymianą towarów lub usług; porozumienia o dystrybucji; handlowe przedstawicielstwo lub działalność agencyjną; faktoring; leasing; roboty budowlane; konsulting; prace inżynieryjne; licencjonowanie; inwestowanie; finansowanie; prowadzenie działalności bankowej; ubezpieczenia; porozumienie o eksploatacji lub koncesje; joint venture i inne formy współpracy przemysłowej lub biznesowej; przewóz towarów lub pasażerów drogą powietrzną, morską, kolejową lub drogową".

To modelowe prawo dotyczące handlu elektronicznego wskazuje na konieczność zrównania tradycyjnych dokumentów papierowych i własnoręcznego podpisu, pod określonymi przez narodowe ustawodawstwo warunkami, z dokumentami i podpisem elektronicznym (Art. 6 i 7). To samo odnosi się do konieczności przedstawienia odpowiednim władzom oryginału jakiegoś dokumentu, który może być przygotowany i przechowywany w formie elektronicznej (Art. 8).

1.2.2. OECD

OECD

W OECD kilkakrotnie podejmowano próby zdefiniowania pojęcia handlu elektronicznego. W rezultacie prac różnych grup roboczych przyjęto w zasadzie dwie definicje. Pierwsza z nich, ustalona w 1997 r. stwierdza, że handel elektroniczny: „to wszelkie formy transakcji związanych z komercyjnym wykorzystaniem, z uwzględnieniem indywidualnych, jak też instytucjonalnych podmiotów, które bazują na cyfrowym przetwarzaniu i transmisji danych".

W nowszej, z 1998 r., definicji handlu elektronicznego został on określony jako: „biznes prowadzony w sieciach komputerowych takich jak Internet, z uwzględnieniem pokrewnej infrastruktury".

W obydwu przypadkach sprawa handlu elektronicznego ogranicza się wyłącznie do operacji przeprowadzanych w drodze elektronicznej – od kontraktu po realizację dostawy produktu czy usługi.

Jest to całkowicie inne podejście do zjawisk handlu międzynarodowego niż zostało zaprezentowane w dokumencie ONZ.

WTO

1.2.3. WTO

Także WTO jako organizacja wyspecjalizowana w sprawach handlu zagranicznego i polityki handlowej podjęła zagadnienie handlu elektronicznego.

We wrześniu 1998 r. Rada Generalna tej organizacji, na mocy decyzji drugiej sesji Konferencji Ministerialnej o przyjęciu „*Deklaracji w sprawie globalnego handlu elektronicznego*", zrealizowała zawarte w niej postanowienie o stworzeniu roboczego programu mającego kompleksowo przeanalizować zagadnienia związane z handlem elektronicznym.

Deklaracja w sprawie globalnego handlu elektronicznego

Zgodnie z tym, niewielkim objętościowo, dokumentem zatytułowanym „*Roboczy program działań w sprawie handlu elektronicznego*" Rada Generalna winna poddać analizie szeroki krąg zagadnień dotyczący handlu elektronicznego realizowanego na arenie międzynarodowej.

Równocześnie w „*Roboczym programie działań w sprawie handlu elektronicznego*" przyjęto – jak podkreślono – wyłącznie na potrzeby tego projektu – następującą definicję handlu elektronicznego: „termin »handel elektroniczny« jest rozumiany jako środki produkcji, dystrybucji, marketingu, sprzedaży lub dostawy towarów i usług środkami elektronicznymi".

Jak widać jest to jeszcze inna – w porównaniu z poprzednio przedstawionymi – definicja omawianej podstawowej kategorii niniejszych rozważań, jaką jest „handel elektroniczny".

1.2.4. WCO a handel elektroniczny

WCO

Podstawowym, wyjściowym dokumentem dla działań WCO (World Customs Organization – Światowa Organizacja Celna) w zakresie handlu elektronicznego i wykorzystania nowoczesnych technik elektronicznych w procedurach celnych związanych ze współczesnym handlem międzynarodowym okazał się dokument opracowany przez Stały Komitet Techniczny, a dokładniej podkomitet ds. automatycznego przetwarzania danych i jego Grupę Doradczą ds. EDI (Permanent Technical Committe, ADP Sub–Committee, the EDI Advisory Group) zatytułowany „*Handel elektroniczny a cło*". Jego podstawowym celem było rozpoczęcie szerokiej dyskusji wśród członkowskich administracji celnych państw człon-

kowskich WCO na temat tego „... gdzie, kiedy i jak te nowe i rozwijające się formy technologii telekomunikacyjnych i komputerowych mogą być wykorzystane dla wspierania operacji celnych".

Dokument definiuje pojęcie handlu elektronicznego traktując tę kategorię jako: „...użycie innych form technologii informatycznej (I.T.), które wspierają ruch danych między niezależnymi systemami komputerowymi partnerów handlowych. Terminem powszechnie używanym na określenie tego zjawiska jest „handel elektroniczny".

Co to jest handel elektroniczny?

W innym miejscu autorzy dokumentu w rozdziale zatytułowanym „Co to jest handel elektroniczny?" odpowiadają na to pytanie następująco: „Termin „handel elektroniczny" wszedł w użycie stosunkowo niedawno i w dominującym znaczeniu sugeruje, iż jest to nowy sposób prowadzenia biznesu. Wiele organizacji, łącznie z Administracjami Celnymi, już wykorzystuje w swoim działaniu sporo elementów otoczenia związanego z „handlem elektronicznym". Informacje rutynowo wymieniane są między partnerami biznesowymi przy użyciu EDI, poczty elektronicznej, faksów, etc. Najbardziej syntetycznie można stwierdzić, że „handel elektroniczny" oznacza elektroniczne organizowanie działalności biznesowej. Może to być definiowane bardziej formalnie jako „sposób prowadzenia działalności gospodarczej przy użyciu technologii telekomunikacyjnej i komputerowej dla wymiany danych między niezależnymi systemami informacji komputerowej w zakresie zawierania transakcji biznesowych"

1.2.5. Stanowisko Międzynarodowej Izby Handlowej (ICC)

ICC

Międzynarodowa Izba Handlowa (International Chamber of Commerce – ICC), z siedzibą w Paryżu, to jedna z najbardziej powszechnych i wpływowych, pozarządowych, organizacji kręgów gospodarczych współczesnego świata. Nic więc dziwnego, że i ta organizacja zwróciła uwagę na sprawy handlu elektronicznego i opracowała własne stanowisko w tej kwestii. Zostało ono sformułowane – przy współpracy kilkudziesięciu międzynarodowych i narodowych organizacji biznesowych – i przedstawione Konferencji Ministerialnej OECD (Organizacji Współpracy Gospodarczej i Rozwoju) przeprowadzonej w Ottawie w Kanadzie w październiku 1998 r. Ten bardzo obszerny i szczegółowy dokument podjął najważniejsze problemy handlu i gospodarki elektronicznej z punktu widzenia nie tylko kręgów biznesowych. Zawarte w nim zostały propozycje podjęcia przez biznes i rządy poszczególnych państw wspólnych akcji mających na celu pełne wykorzystanie nowoczesnych technologii informatycznych na potrzeby stabilnego rozwoju społeczeństw narodowych i całej ludzkości. Został on zatytułowany: „*Globalny Plan Działań na Rzecz*

Globalny Plan Działań na Rzecz Handlu Elektronicznego

Handlu Elektronicznego". Dokument ten zawiera pakiet podstawowych zasad będących bazą wyjściową dla podjęcia działań, jakie powinny być wdrożone w zakresie polityki państwowej wobec handlu elektronicznego.

Oto część z nich:

- Handel elektroniczny ze swej natury jest globowym. Polityka rządowa odnosząca się do niego powinna być międzynarodowo skoordynowana i zgodna z zasadą tworzenia ułatwień we wzajemnych operacjach międzynarodowych w stosowaniu uzgodnionych standardów.
- Transakcje prowadzone przy użyciu handlu elektronicznego powinny otrzymać neutralne traktowanie podatkowe w porównaniu z transakcjami prowadzonymi środkami nie elektronicznymi. Opodatkowanie handlu elektronicznego powinno być zgodne z ustanowionymi praktykami międzynarodowymi [...]".

Jeśli chodzi o samą problematykę gospodarki elektronicznej czy handlu elektronicznego, nie została ona w omawianym dokumencie podjęta wprost. Jednakże przyjęto szereg ustaleń wynikających z wcześniej powstałych definicji w WTO, ONZ czy OECD. Równocześnie wysunięto ideę wykorzystania globalnej infrastruktury informacyjnej i na jej bazie stworzenia wysokiego poziomu zaufania Globalnego Społeczeństwa Informacyjnego (Global Information Society – GIS) nawiązującego do idei Unii Europejskiej „e-Europe". Pochodną od GIS była koncepcja „*Stworzenia podstawowych zasad dla rynku cyfrowego*" (Establishing groundrules for the digital marketplace).

Globalne Społeczeństwo Informacyjne

Stanowisko ICC zostało wyrażone jednoznacznie w następującym stwierdzeniu: „Żądanie dla ustanowienia wolnej strefy taryfowej dla transmisji elektronicznych bazuje na długiej tradycji redukcji lub eliminacji barier (takich, jak cła i obciążenia celne) w handlu międzynarodowym. Obniżanie barier handlowych, łącznie z taryfami celnymi, jest jednym z najbardziej obowiązkowych środków, jest nadzieją tak dla handlu międzynarodowego, jak i globowego handlu elektronicznego".

W szczegółowych propozycjach działań wskazuje się na to, że kręgi gospodarcze współpracują z agendami rządowymi nad wprowadzeniem systemu umożliwiającego w największym stopniu wolny od barier, także taryf celnych, handel międzynarodowy.

Tak więc, jak widzimy, również międzynarodowa społeczność podmiotów gospodarczych wyraża swoje zainteresowanie gospodarką elektroniczną (e-biznesem), a zwłaszcza handlem elektronicznym (e-commerce).

Nie tylko stawia diagnozę istniejącego stanu, ale i proponuje konkretne przedsięwzięcia, w których chciałaby współuczestniczyć.

Odnoszą się one zarówno do zagadnień legislacyjnych, jak i problemów wynikających z infrastruktury, jaka stoi do dyspozycji administracji celnych poszczególnych państw.

1.3. Unormowania krajowe[8]

1.3.1. Polskie ujęcie zagadnienia e-biznesu

Prawo bankowe

Problematyka e-biznesu pojawiła się, na zasadzie „pierwszej jaskółki", w ustawodawstwie polskim już w połowie lat 90. Art. 7 Prawa bankowego (ustawa z dnia 29 sierpnia 1997 r. – Dz.U. Nr 140, poz. 939 z późn. zm.). Przewiduje, że „oświadczenia woli – składane w związku z dokonywaniem czynności bankowych, mogą być wyrażone za pomocą elektronicznych nośników informacji. Związane z czynnościami bankowymi dokumenty mogą być sporządzane za pomocą elektronicznych nośników informacji, jeżeli dokumenty te zostaną w sposób należyty utrwalone i zabezpieczone. Jeżeli ustawa zastrzega dla czynności prawnej formę pisemną, uznaje się, że czynność dokonana w (powyższej) formie spełnia wymagania formy pisemnej". Nie można przy tym zapominać, że zasadą naszego prawa jest dowolna forma dokonywania czynności prawnych (a więc zawierania umów), a gdy ustawodawca wymaga formy pisemnej – zasadą jest forma pisemna dla celów dowodowych (art. 74 i 75 kodeksu cywilnego), a nie forma pisemna pod rygorem nieważności.

W rezultacie, podstawowe znaczenie w dyspozycji cytowanego przepisu Prawa bankowego ma wymóg należytego utrwalenia i zabezpieczenia dokumentów elektronicznych. Wymóg ten – oznaczający włączenie do materii prawnej wielu aspektów tech-

[8] Niektóre akty prawne mające wpływ na funkcjonowanie gospodarki elektronicznej w Polsce: ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. Nr 140, poz. 939 z późniejszymi zmianami) (zgodnie z art. 7 tej ustawy oświadczenia woli składane w związku z dokonywaniem czynności bankowych mogą być wyrażane za pomocą elektronicznych nośników informacji. Ustawa dopuszcza także sporządzanie dokumentów związanych z czynnościami bankowymi za pomocą elektronicznych nośników informacji), ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. Nr 88, poz. 553 z późniejszymi zmianami) (wprowadza przepis (art. 115 § 14) stanowiący, że dokumentem jest każdy przedmiot lub zapis na komputerowym nośniku informacji, z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne), ustawa z dnia 19 listopada 1999 r. – Prawo działalności gospodarczej (Dz.U. Nr 101, poz. 1178) (przepisy (art. 12) wprowadzają obowiązek podawania przez przedsiębiorcę w ofercie sprzedaży za pośrednictwem m.in. sieci informatycznych, co najmniej danych dotyczących: oznaczenia przedsiębiorcy, numeru, pod którym jest on wpisany do rejestru przedsiębiorców wraz z oznaczeniem sądu rejestrowego oraz siedziby i adresu przedsiębiorcy), ustawa z dnia 2 marca 2000 r. – o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz.U. Nr 22, poz. 271) (regulacje dotyczące m.in. umów zawieranych na odległość, do których należy również umowa zawierana drogą elektroniczną (Rozdział 2 ustawy)), szczegóły i teksty ustaw: www.sejm.gov.pl/, www.kondrat.pl/e-handel/, www.kti.ae.poznan.pl/.

nicznych, w tym należących do sfery kryptografii – stanowi sam w sobie jeden z podstawowych problemów tzw. podpisu elektronicznego, a wraz z nim całej gospodarki elektronicznej.

Z punktu widzenia perspektyw rozwoju handlu elektronicznego w naszym kraju i związanych z nim zagadnień najistotniejsze jest rozstrzygnięcie dwóch podstawowych problemów prawnych:

- jak wprowadzić regulacje prawne e-biznesu kompleksowo regulujące to zagadnienie i
- jak rozstrzygnąć problem związany z tzw. podpisem elektronicznym.

Zespół ds. gospodarki elektronicznej

Zagadnienie problematyki gospodarki elektronicznej i handlu elektronicznego zostało podjęte w pracach specjalnego zespołu powołanego Zarządzeniem nr 27 z dnia 17 maja 1999 r. przez Prezesa Rady Ministrów. Zadaniem powołanego Zespołu miało być przygotowanie założeń regulacji prawnych w odniesieniu do transakcji realizowanych drogą elektroniczną.

Zespół dokonał analizy funkcjonujących w Polsce regulacji prawnych związanych z szeroko pojętą problematyką gospodarki elektronicznej, dokonał ich porównania z regulacjami zawartymi w prawie Unii Europejskiej, a także z wytycznymi i zaleceniami międzynarodowych organizacji, których członkiem jest Polska. W rezultacie swych prac Zespół ten przygotował raport końcowy. Został on zawarty w „Sprawozdaniu Międzyresortowego Zespołu do spraw handlu metodami elektronicznymi przyjętym 11 lipca 2000 roku przez Radę Ministrów RP".

Definicja e-commerce

W dokumencie tym podjęto również próbę definicyjnego ujęcia e-commerce. Jego autorzy stwierdzają: „Najpopularniejsze jest odnoszenie pojęcia electronic commerce (e-commerce) do handlu elektronicznego. Jednakże ze względu na obejmowanie swoim zakresem poza handlem, także działalności wytwórczej i usługowej prawidłowe jest ogólniejsze tłumaczenie tego pojęcia jako gospodarki elektronicznej".

Równocześnie jednak rozwijając to pojęcie i bardziej go precyzując dochodzą do następujących wniosków:

„W transakcjach zawieranych w obrocie elektronicznym można wyodrębnić dwie kategorie: pierwsza kategoria dotyczy elektronicznego zamawiania towarów materialnych, które następnie są dostarczane „fizycznie" tradycyjnymi kanałami (poczta, usługi kurierskie), druga kategoria odnosi się do zamawiania online „niematerialnych towarów lub usług" (np. oprogramowanie software, zestawy materiałów, usługi informacyjne), przy czym także płatność i doręczenie odbywa się drogą elektroniczną".

Rozróżnienie to, jak widać, nawiązuje do stanowiska, jakie zostało przyjęte w tej sprawie, przede wszystkim, w Światowej Organizacji Celnej.

Międzyresortowy Zespół do spraw Handlu Metodami Elektronicznymi

Należy stwierdzić, że w Polsce zrobiono już wiele na drodze ukształtowania nowego środowiska prawnego dla rozwoju gospodarki elektronicznej i handlu elektronicznego. Także w rezultacie działalności wspomnianego Międzyresortowego Zespołu do spraw Handlu Metodami Elektronicznymi.

Tradycyjne przepisy i regulacje prawne okazały się mało przydatnymi w rozwiązywaniu problemów współczesnej gospodarki, w tym i handlu w epoce rewolucji elektronicznej.

Zjawisko gospodarki elektronicznej i handlu elektronicznego stało się przedmiotem podejmowania prób nowych regulacji prawnych, w tym i w zakresie prawa oraz procedur celnych.

Z punktu widzenia prawnego i praktycznego do najistotniejszych osiągnięć rozwiązań prawnych należy rozróżnienie handlu elektronicznego, czy nawet szerzej gospodarki elektronicznej, w jego podwójnym znaczeniu.

- Pierwsze podejście, szersze – wskazuje na handel elektroniczny jako zjawisko polegające na łańcuchu działalności gospodarczej realizowanej przy pomocy elektronicznej, w tym i za pomocą Internetu, od momentu zawierania transakcji, przez jej realizację zarówno na drodze elektronicznej, jak z wykorzystaniem tradycyjnych środków transportu (lądowego, powietrznego czy wodnego, w tym linii przesyłowych energii elektrycznej czy rurociągów) aż po zapłatę należności, także celnych i podatkowych.
- Drugie podejście, węższe – określa mianem handlu elektronicznego tylko taki łańcuch działalności gospodarczej, jaki wiąże się z realizacją wyłącznie za pomocą sieci elektronicznych, w tym Internetu, od momentu złożenia oferty i zawarcia kontraktu, po jego realizację i dokonanie płatności za dostarczony drogą elektroniczną towar lub usługę.

Podpis elektroniczny

Wprowadzono też ustawę o podpisie elektronicznym[9]. Podpis elektroniczny – rozumiany jako dopuszczenie jego ekwiwalentności w stosunku do właściwego podpisu w zakresie czynności cywilnoprawnych, oczywiście pod warunkiem spełnienia określonych wymogów – można w tej sytuacji uznać za istotny, lecz w istocie najprostszy do rozwiązania element problematyki prawnej gospodarki elektronicznej. Mamy zresztą przykłady – i to niekoniecznie nowe – ustawowego uznania ekwiwalentności podpisu, jak uznanie ekwiwalentności podpisu zarządu spółki akcyjnej na akcji oraz faksimile tego podpisu w kodeksie handlowym.

[9] Ustawa z dnia 20 sierpnia 1997 roku o Krajowym Rejestrze Sądowym (Dz.U. 01.17.209).

Podpis elektroniczny poza sferą prawa cywilnego

Podpis elektroniczny w wąskim znaczeniu dotyczy wyłącznie sfery stosunków cywilnoprawnych, jednakże z uwagi na to, że stanowi jedno z narzędzi funkcjonowania gospodarki elektronicznej musi być rozpatrywany w szeregu innych płaszczyzn prawnych, takich jak:

- prawo podatkowe i celne, tzn. w Polsce przepisy ordynacji podatkowej i odsyłającego do tej ordynacji kodeksu celnego, przy czym nie można nie zaznaczyć, że przepisy te są u nas bardziej sformalizowane niż w wielu innych krajach;
- akty organów administracji publicznej (decyzje, postanowienia, zaświadczenia itp.), w których zakresie podstawowe znaczenie mają ogólne przepisy procedury administracyjnej zawarte w kodeksie postępowania administracyjnego, które znają wyjątki od tradycyjnej dla administracji zasady pisemności; pewne doświadczenia praktyczne występują już w sprawach składek ubezpieczenia społecznego;
- akty postępowania sądowego (wyroki, postanowienia, zarządzenia, pisma procesowe itp.), przy czym w tym zakresie spotykamy próby wprowadzenia elektronizacji w funkcjonujących już przepisach o zastawie rejestrowym i rejestrze zastawów, który wszedł w życie 1 stycznia 2001 r. oraz w przepisach o Krajowym Rejestrze Sądowym;
- czynności wynikające z prawa pocztowego.

W rezultacie lista ustaw spoza sfery prawa cywilnego, których dotyczyć może nowa regulacja prawna związana z wymogami gospodarki elektronicznej, może objąć ponad dwadzieścia pozycji, nie licząc bardzo istotnych ustaw dotyczących notariatu – instytucji najbardziej odpornej na zmiany wynikające z tej gospodarki[10].

1.3.2. Kwestie instytucjonalne

Nie wychodząc jeszcze poza materię podpisu elektronicznego, trzeba też zaznaczyć potrzebę dokonania dogłębnej analizy instytucjonalnej. Podpis elektroniczny – w skali ogólnej, a nie tylko ograniczonej do poszczególnych banków czy też współpracujących ze sobą banków, wymaga instytucji certyfikujących i autoryzujących.

Instytucje certyfikujace

W tym ostatnim zakresie istnieje potrzeba stworzenia odpowiedniego organu regulacyjnego – w tym rozumieniu regulacji, jakie powstało w USA i przeniosło się do Europy, którego pewnym od-

[10] Pomijamy przy tym obrót prawny nie dotyczący wprost gospodarki, lecz bardzo ważny dla obywatela – w szczególności nie związane wprost z czynnościami cywilnoprawnymi akty organów administracji publicznej.

powiednikiem są u nas zadania Urzędu Regulacji Energetyki, a w przyszłości również Urzędu Regulacji Telekomunikacji. Wzory zachodnie – to wzory niezależnych agencji, wyłączonych ze struktur ministerialnych, wyposażonych także w uprawnienia stanowienia powszechnie obowiązujących przepisów prawa.

Nie można nie zauważyć, że bardzo rygorystyczna pod względem systemu źródeł prawa Konstytucja RP z 1997 r., w powiązaniu z przepisami ustawy z 4 września 1997 r. – o działach administracji rządowej, wymagając formy rozporządzenia Rady Ministrów, Prezesa Rady Ministrów albo właściwego ministra, uniemożliwiają praktycznie wykonywanie przez organ regulacyjny zadań normodawczych.

Instytucja autoryzacyjna

Należy jednak mieć na uwadze, że krajowa instytucja autoryzacyjna wcale nie musi być organem publicznym – szczególnym rodzajem organu administracji publicznej. Jak wynika z doświadczeń banków ze wzajemnym honorowaniem kart kredytowych, możliwe jest szerokie funkcjonowanie mechanizmów samoregulacji – na zasadzie porozumienia zainteresowanych podmiotów oraz „akredytora". Ze względu na rangę i zakres materii, potrzeba wówczas nadzoru publicznego nad działalnością takiego niepublicznego „akredytora": nadzoru państwowego typu obecnego nadzoru bankowego czy ubezpieczeniowego, ale też może nadzoru stworzonego w tym celu w drodze ustawy samorządu gospodarczego.

Wydaje się, że najbardziej zainteresowane omawianą problematyką sektory: telekomunikacyjny i bankowy są w stanie wypracować takie instytucje i mechanizmy samoregulacji, a także wypracować wspólne stanowisko w przedmiocie koniecznej instytucji nadzorczej.

Podsumowanie

Problematyka handlu elektronicznego zajmuje coraz więcej miejsca w regulacjach prawnych zarówno tych na poziomie krajowym, jak i ponadnarodowym. Kwestia zapewnienia bezpieczeństwa obrotu gospodarczego, realizowanego z wykorzystaniem technologii informatycznej, stanowi coraz ważniejszy aspekt wszystkich unormowań. Prace legislacyjne idą przy tym w dwóch różnych kierunkach – mechanicznego przeniesienia znanych i sprawdzonych w rzeczywstym świecie reguł na grunt wirtualny lub maksymalnego sankcjonowania wszelkich zachowań charakterystycznych e-gospodarki. W polskim systemie prawa kwestia obrotu elektronicznego dopiero się pojawia. Uchwalona została już ustawa o podpisie elektronicznym, a także ustawa o świadczeniu usług drogą elektroniczną. Są to pierwsze jaskółki zmian w tej dziedzinie.

2. Perspektywy rozwoju gospodarki elektronicznej

- Co to jest nowa gospodarka?
- Jak duży jest potencjał rynków elektronicznych?
- Jakie są perspektywy rozwoju e-gospodarki?
- Co czeka Polskę w tej dziedzinie?

2.1. Nowa gospodarka – kluczowe zagadnienia[11]

Rewolucja związana z wprowadzeniem nowoczesnych technologii informatycznych w sferze zarządzania przedsiębiorstwem daje się porównać z rewolucją przemysłową w sferze środków produkcji. Pojęcie nowej gospodarki (e-gospodarki, gospodarki elektronicznej) nierozerwalnie wiąże się z pojęciem Internetu. Zmienił on nieodwołalnie oblicze współczesnego biznesu, a trzeba się liczyć z tym, że jesteśmy dopiero na początku tych zmian. Globalizacja rynku nabiera niespotykanego dotąd rozmachu. Przy wyborze partnera czynnik geograficzny ma już znikome znaczenie. Produkty i usługi są dostępne niezależnie od fizycznego usytuowania sprzedających i kupujących. Dobierają się oni za pośrednictwem globalnych aukcji internetowych i tzw. business marketplaces – takich, jak na przykład Convisint[12].

Podaż i popyt

Podaż i popyt. W „starej" gospodarce zmiany popytu i podaży są ograniczone różnymi czynnikami. Stosowane metody analizy określają popyt jedynie w sposób przybliżony, głównie na podstawie badań statystycznych, co w powiązaniu z bezwładnością cykli produkcyjnych i masowym, nie zindywidualizowanym marketingiem – generuje znaczne opóźnienie, z jakim przedsiębiorstwa reagują na zmieniającą się sytuację rynkową. W nowej gospodarce informacja zwrotna pozyskiwana jest wprost od klientów drogą elektroniczną (systemy CRM) może być natychmiast wykorzystana w zarządzaniu przedsiębiorstwem. Sterowane elektronicznie cykle produkcyjne mogą niemal natychmiast adaptować się do zmiennych oczekiwań klientów. Elektroniczny obieg i wymiana dokumentów usprawniają zarządzanie produkcją i rewolucjonizują logistykę, przyczyniając się do zwiększenia ela-

[11] J. Francik, K. Trybicka-Francik: *Studia Informatica 2001*, Volume 22 Number 2 (44), Politechnika Śląska, Instytut Informatyki.

[12] Jest to wspólne przedsięwzięcie przodujących firm motoryzacyjnych (GM, Daimler Chrysler, Ford, Nissan i Renault), którego celem jest minimalizacja kosztów i czasu wyszukiwania kontrahentów w globalnym łańcuchu dostaw.

styczności przedsiębiorstwa na niespotykaną dotąd skalę. Marketing jest kierowany już nie do określonych grup klientów, ale do konkretnych klientów; następuje indywidualizacja podaży. Możliwa się staje – w skali globalnej – produkcja na zamówienie; klienci mają możliwość składania precyzyjnych zamówień, firma zaś może błyskawicznie na nie reagować. Z drugiej strony, klienci zyskują też większe możliwości porównywania konkurencyjnych produktów. W związku z tym walka konkurencyjna rozgrywa się o każdego klienta, a nie – jak dotąd – o całe sektory rynku.

Minimalizacja kosztów

Minimalizacja kosztów, maksymalizacja dochodu. Korporacja Oracle w ciągu pierwszego roku korzystania z pakietu E-Business Suite, który zresztą sama wyprodukowała, zaoszczędziła miliard dolarów. W ciągu drugiego roku korzystania z pakietu zaoszczędziła dwa miliardy dolarów. Oszczędności wynikają z automatyzacji dostaw, planowania produkcji, usprawnienia i zautomatyzowania obsługi łańcucha dostawców itd. Oszczędności mają ogromny wpływ na dochód: szacuje się, że pięcioprocentowa redukcja kosztów ma przeciętnie taki sam wpływ na zysk, jak trzydziestoprocentowy wzrost sprzedaży. Ale e-gospodarka oznacza także nowe źródła przychodów: pojawiły się one wraz z rozwojem technik internetowych. Do najbardziej oczywistych należą przychody z e-handlu. Do tego dochodzą wszelkiego rodzaju usługi internetowe, płatne serwisy, hosting itp. Obecnie wartość firm przestaje być zależna tylko od kapitału. Jedną z „nowych" przesłanek jest liczba internautów odwiedzających firmową witrynę www. W USA stosowany jest prosty przelicznik: jeden klient internetowy to około 1000 $.

Infrastruktura telekomunikacyjna

Uzależnienie od infrastruktury telekomunikacyjnej. Przedsiębiorstwo, które nie posiada odpowiedniej infrastruktury (sprzęt, oprogramowanie, dostęp do sieci, wiedza – tzw. know how) wypada z gry na globalnym, elektronicznym rynku. Wniosek z dotychczasowych rozważań jest jeden: Internet to już nie tylko czynnik przewagi konkurencyjnej. Internet to po prostu warunek przetrwania na rynku. Przedsiębiorstwo, które nie jest przygotowane do gry na elektronicznym rynku, nie rozumie jego specyfiki, nie reaguje błyskawicznie na zmieniające się czynniki – jest skazane na zagładę. Wkrótce wystarczającym powodem do upadłości może być brak obecności w internetowych aukcjach. Prowadzić to będzie do niemożności nawiązania kontaktów biznesowych z partnerami i kontrahentami. Już w tej chwili na przykład dostawcy podzespołów motoryzacyjnych nie mają większych szans nawiązania współpracy z czołowymi graczami tego rynku, jeżeli nie są zdolne ogłosić swojej oferty za pomocą wspomnianego już wortalu www.covisint.com. Przedsiębiorstwa, które mimo to nawiążą kontakty han-

dlowe, mogą je szybko stracić ze względu na niemożność dostosowania się do schematu elektronicznego obiegu dokumentów. Wreszcie przyczyną przegranej gry konkurencyjnej może być niewykorzystanie szans, jakie nowa gospodarka daje w takich dziedzinach, jak analiza popytu i podaży, sterowanie produkcją i logistyką, automatyzacja dostaw itp.

Zagrożenia technologiczne

Zagrożenia technologiczne. Zagrożenia technologiczne, które związane są z pojawieniem się gospodarki elektronicznej, nie są nowe. Wynikają z faktu korzystania ze znanej infrastruktury, fizycznej i programowej sieci. Zmienia się natomiast ciężar spoczywający na systemach ochrony, ponieważ zwiększa się wartość informacji krążących w sieci.

Infrastruktura systemów e-biznesu

Infrastruktura systemów e-biznesu. Jak łatwo zauważyć, można wyróżnić tu kilka elementów. Pierwszym z nich jest wewnętrzna sieć przedsiębiorstwa, gdzie mamy do czynienia z takimi działami, jak administracja, księgowość, marketing, logistyka itp. Są to te obszary, które powinny pozostać niewiadomą dla ciekawskich oczu konkurencji. Do tej pory najłatwiejszym sposobem ochrony tych zasobów było odcięcie sieci lokalnej od zewnętrznego systemu, jakim w tym przypadku jest Internet. W nowej sytuacji jest to niemożliwe. Idea e-biznesu oparta jest na pełnej integracji. Istotne jest, by konsument na bieżąco miał dostęp do oferty firmy, mógł zgłaszać swoje zapotrzebowanie i był jak najlepiej i efektywniej obsłużony. To pociąga za sobą konieczność wyeliminowania jak największej liczby węzłów pośrednich. A zatem, na przykład, informacja o zamówieniu ze strony klienta powinna się niezwłocznie pojawić w działach księgowości, logistyki, marketingu itd., a zamówiony towar zejść ze stanów magazynowych, co oczywiście powinno mieć swoje odzwierciedlenie w informacjach przeznaczonych dla klienta. Obejmuje on serwer bazodanowy wraz z bazą danych o produktach oraz serwer WWW będący oknem na świat – to za jego pośrednictwem firma i jej oferta są widoczne w Internecie. Elementem scalającym w jedną całość sieć wewnętrzną firmy, bazę danych i serwis WWW jest serwer transakcji. W tym miejscu należy zwrócić szczególną uwagę na znaczenie serwera WWW.

Okno na świat może się stać równocześnie furtką dla intruzów.

Bezpieczeństwo WWW

Dlaczego należy zająć się bezpieczeństwem WWW?

Ponieważ serwery WWW są atrakcyjnymi celami dla wszelkiego rodzaju napastników. Udany atak jest wydarzeniem publicznym, mogącym zniszczyć wizerunek firmy. Wiele serwerów WWW związanych jest z możliwością dokonywania operacji finansowych. Integracja systemów firmy, związana z ideą e-biznesu, sprawia, że są składnicami ważnych i poufnych informacji. Internet za pośred-

nictwem serwisów WWW wykorzystywany jest do wymiany poufnych informacji wewnątrz firmy (pomiędzy pracownikami), jak również do komunikacji z odbiorcami zewnętrznymi. Zastrzeżone informacje firmy są atrakcyjnym celem zarówno dla wrogów, jak i konkurentów. Ze względu na to, że serwery WWW są wykorzystywane tak przez pracowników firmy, jak i przez osoby spoza niej, stanowią one faktyczny pomost między światem zewnętrznym a siecią wewnętrzną firmy. Jest to niewątpliwie następstwem ogromnych możliwości, jakie niosą ze sobą technologie WWW. Niestety, ich elastyczność to również zagrożenia. Oto niektóre z ich źródeł:

Zagrożenia

- rozszerzalność serwerów: możliwość podłączenia baz danych, systemów oprogramowania starszej generacji,
- rozszerzalność przeglądarek: technologie i narzędzia, takie jak ActiveX, Java, Java–Script, VBscript czy aplikacje pomocnicze, pozwalają na wzbogacenie możliwości przeglądarek o funkcje niedostępne w standardzie HTML,
- możliwość przerwania usługi: atak metodą blokady usługi,
- złożoność usług pomocniczych: korzystanie z usług zewnętrznych, takich jak DNS czy trasowanie, które narażone są na błędy, awarie i ataki,
- pośpiech w tworzeniu oprogramowania (czas to pieniądz).

Istniejące technologie nie są doskonałe. Należy zaakceptować ich ograniczenia i konieczne środki bezpieczeństwa.

Sposoby zabezpieczenia stron WWW

Na bezpieczeństwo WWW składają się trzy zagadnienia:

- zabezpieczenie serwera WWW i zgromadzonych na nim danych. Proces ten można podzielić na etapy: zabezpieczenie samego komputera z wykorzystaniem tradycyjnych mechanizmów bezpieczeństwa (na przykład system uprawnień dla użytkowników) oraz zminimalizowanie liczby usług dostępnych przez komputer, na którym serwer WWW jest uruchomiony; należy się również upewnić, że dostęp do serwera w celach administracyjnych zrealizowany jest z użyciem narzędzi gwarantujących bezpieczeństwo;
- zabezpieczenie informacji przekazywanych pomiędzy serwerem i użytkownikiem. Jest wiele sposobów zabezpieczania transmisji przed podsłuchem: fizyczna ochrona sieci przed podsłuchem, ukrycie istotnych informacji wśród innych błahych i najczęściej stosowane: szyfrowanie;
- zabezpieczenie komputera użytkownika. To, wbrew pozorom, najtrudniejsze zagadnienie.

Błędy w systemach zabezpieczeń przeglądarek są faktem, wirusy, które pozostają uśpione aż do momentu, gdy użytkownik wpisze hasło udostępniające zawartość elektronicznego portfela, to również nie fikcja.

Bezpieczeństwo WWW, a co za tym idzie i e-biznesu, nie jest problemem typu „wszystko albo nic". To kompromis pomiędzy dopuszczalnym ryzykiem i zastosowanymi środkami bezpieczeństwa.

Wbrew pozorom okazuje się, że zapewnienie bezpieczeństwa w WWW jest coraz łatwiejsze i niewątpliwie dzieje się tak za sprawą handlu w Internecie. By osiągnąć sukces, należy również pamiętać, że bezpieczeństwo to nie produkt, który się kupuje, instaluje i pozostawia samemu sobie, to proces, który musi być integralną częścią polityki przedsiębiorstwa.

2.2. Wielkość rynku elektronicznego

2.2.1. Struktura dostępu do Internetu

Starając się porównać różne rynki światowe, należy pamiętać, że Internet jest zupełnie nowym medium przekazu dóbr. Cała infrastruktura światowego Internetu ma około 5 lat, co rok zostajemy zaskakiwani nowościami technicznymi z dziedziny rozwiązań internetowych. Internet w Stanach Zjednoczonych ma najdłuższą historię. Rynek ten jest bardzo podatny na nowości, co wpływa na przewodnictwo tego kraju pod względem wykorzystania e-biznesu.

Rynek elektroniczny w USA

Ameryka Północna/Stany Zjednoczone
Dynamika przyrostu nowych użytkowników w Stanach Zjednoczonych w ostatnim okresie nie jest zbyt imponująca. Jednak pamiętajmy, że Stany Zjednoczone okres „przyłączania użytkowników" mają już za sobą – teraz następuje znaczne zwiększanie dynamiki rozwoju e-commerce (patrz podrozdział e-commerce).

Warto zwrócić tutaj uwagę na liczbę użytkowników Internetu w stosunku do wszystkich mieszkańców tego kraju.Jako „aktywnego" użytkownika zdefiniowano osobę przebywającą w Internecie raz w tygodniu przez godzinę. Prognozy wskazują, że do roku 2002 42% mieszkańców (powyżej 14 roku życia) będzie korzystało w Internetu.

Jako przyczyny dominacji Stanów Zjednoczonych (jeśli chodzi o rozwój, infrastrukturę oraz e-commerce) można wyszczególnić:
- masowość dostępu do Internetu,
- dominacja Stanów Zjednoczonych pod względem ekonomicznym na świecie, przekłada się to również na płaszczyznę Internetu,
- coraz młodsze osoby korzystają z Internetu,
- rosnąca akceptacja dla zakupów on-line,
- dominacja języka angielskiego na świecie,
- tanie koszty podłączenia do sieci.

Dodatkowym aspektem jest liczba komputerów w USA. Poniżej przedstawione zostało zestawienie niektórych państw europejskich i Stanów Zjednoczonych, dotyczące liczby komputerów oraz liczby hostów, czyli komputerów podłączonych do sieci Internet (dane te pochodzą z roku 1998).

Europa

Rynek elektroniczny w Europie

Rynek europejski znacznie różni się od amerykańskiego głównie dynamiką wzrostu. Między rokiem 1998 a 2002 wzrost liczby użytkowników wyniesie około 280% (rynek amerykański odnotuje wzrost około 100% dla osób powyżej 18 roku życia).

Zróżnicowanie rynku

Badania przeprowadzone przez Arthur Andersen Consulting wskazują na podział Europy na trzy kategorie:

- kraje skandynawskie – rozwój Internetu już się niemalże ustabilizował i jest porównywalny z rynkiem amerykańskim. E-commerce zajmuje w tych krajach dość silną pozycję,
- Niemcy, Szwajcaria, Holandia, Wielka Brytania – kraje wciąż rozwijające swoją infrastrukturę, jednak będą z pewnością walczyć o dominację w Europie,
- południowa Europa (Włochy, Hiszpania, Portugalia, ale również Belgia, Irlandia) – są to kraje o stosunkowo małym rynku.

Osobnym przypadkiem jest Francja ze swoim systemem e-commerce Minitel. System ten skupia większość biznesu we Francji. Liczba użytkowników szacowana jest na około 35 milionów. Poniżej przedstawiona została liczba użytkowników sieci w Europie.

Jako „aktywnego" użytkownika zdefiniowano osobę przebywającą w Internecie raz w tygodniu przez godzinę. Firma konkurencyjna w stosunku do eMarketer– IDC przewiduje podobny rozwój Internetu w Europie (w roku 1998 szacowana liczba użytkowników to 16,8 mln, w roku 2002 przewidywana to 82 mln).

Coraz większe zainteresowanie Internetem występuje u osób niepełnoletnich (do 18 roku życia). Jest to ważny aspekt rozwoju Internetu i z pewnością nie możemy pomijać go w badaniach.

Bariery rozwoju Internetu

Ważnym aspektem są bariery występujące w rozwoju Internetu w Europie. Do najważniejszych zaliczyć można (głównie w porównaniu z USA):

- większe ograniczenia prawne i podatkowe (niż w Stanach Zjednoczonych),
- mniejsza podatność na nowości technologiczne,
- bariera językowa (w Europie 28% osób zna język angielski – łącznie z Europą Środkową),
- koszty podłączenia.

Data Monitor przeprowadził badania odnośnie do kosztów podłączenia do Internetu. Wyniki zdecydowanie przemawiają na korzyść

Stanów Zjednoczonych. Porównując Wielką Brytanię z innymi krajami widzimy, że miesięczne koszty są trzykrotnie większe niż w krajach skandynawskich i pięciokrotnie większe niż w USA.

Do czynników przyczyniających się do rozwoju Internetu w Europie można zaliczyć m.in.
- zwiększająca się liczba osób mających dostęp do Internetu,
- zmniejszające się koszty podłączenia,
- konkurencja pomiędzy Dostawcami Internetu (ISP),
- wielojęzyczne portale internetowe,
- mocno rozwinięty rynek telefonów komórkowych (Internet i telefonia komórkowa coraz bardziej się zbliżają ku sobie),
- coraz większa świadomość istnienia e-biznesu (głównie na przykładzie USA),
- zwiększająca się akceptacja dla Internetu i zakupów.

Polska

Rynek elektroniczny w Polsce

Mimo że jesteśmy w czołówce krajów Europy Środkowej, to wciąż wiele nam brakuje do sytuacji panującej w krajach rozwijających swój Internet (np. Niemcy).

Według HomeNet (www.home.pl) 100 największych dostawców Internetu w Polsce utrzymuje ponad 26.000 domen (na 10.03.2000). Liczba użytkowników jest różna i waha się od 0,95 mln (Global Reach) do 2,5 mln użytkowników. Serwis Informacyjny www.e-biznes.pl ocenia, że na koniec roku 1999 w Polsce było około 2 milionów aktywnych użytkowników Internetu.

Do barier rozwoju można głównie zaliczyć:
- dominacja TP S.A. w zakresie podłączeń stałych i komutowanych,
- niewielka liczba dostawców Internetu (w porównaniu z USA),
- słaba jakość usług oferowanych przez dostawców Internetu,
- zbyt wyraźna czołówka portali internetowych (ONET, WP),
- brak wiary w potrzebę istnienia Internetu w firmie,
- brak zaufania do zakupów internetowych, – zbyt wolne „wyjście" na świat z Polski (wolne łącze).

Czynniki rozwoju

Pomimo barier w najbliższym czasie możemy się spodziewać gwałtownego rozwoju Internetu w Polsce – z pewnością będzie on porównywalny (jeśli nie szybszy) niż obecnie notowany w Europie. Do głównych czynników przyczyniających się do rozwoju zaliczyć można:
- łączenie dużych firm internetowych (np. Internet Partners),
- pomimo dominacji, TP S.A. przeznacza duże kwoty na rozwój Internetu,
- tanie połączenia z Internetem (łącze komutowane) – bez potrzeby wykupywania kont,

- zapowiadane wejścia dużych koncernów tworzących portale,
- rosnąca akceptacja w stosunku do Internetu wśród kadry kierowniczej,
- specjalizacja serwisów na różnych płaszczyznach (np. praca, giełda, motoryzacja),

2.2.2. Rynek reklamy internetowej

Reklama internetowa

W ciągu kilku ostatnich lat nastąpił prawdziwy rozwój reklamy w Internecie. Rozwój zarówno jakościowy, jak i ilościowy. Jeszcze kilka lat temu oglądaliśmy statyczne bannery – dziś są one już w zdecydowanej większości animowane i znacznie bardziej efektowne.

Jednym z powodów coraz większej atrakcyjności bannerów jest większa przepustowość łącza, pozwalająca na załadowanie większej reklamy w krótszym czasie (dla porównania na początku lat 90. bannery – wtedy niekoniecznie o charakterze komercyjnym – miały wielkość około 3–4 Kb, dziś zazwyczaj jest to powyżej 10 Kb).

Obok bannerów do najczęstszych form reklamy należą (dokładne omówienie znajduje się w rozdziale Firma w Internecie- start): e-mail, listy dyskusyjne, serwisy specjalistyczne, konkursy, bezpłatne usługi internetowe.

USA

Stany Zjednoczone

Wyraźnie widać (według prognoz eMarketer), że wzrost znaczenia reklamy Internetowej dopiero jest przed nami. Do roku 2002 amerykańskie firmy przeznaczą około 9 mld dolarów – dla porównania na reklamę w TV w roku 1998 przeznaczono prawie 48 mld dolarów). Reklama internetowa odznacza się największą dynamiką wzrostu – w latach 1996/97 wynosiła ona 271%. W przypadku tradycyjnych metod reklamy wzrost nie przekraczał 15%.

Jeśli przyjrzymy się statystykom, widzimy, że udział Stanów Zjednoczonych w reklamie internetowej maleje – będzie to głównie spowodowane dynamicznym rozwojem e-biznesu w Europie.

Ważnym aspektem– jeśli chodzi o kierunkowość reklamy– jest cel i miejsce korzystania z Internetu. Z badań przeprowadzonych przez eStats (1998) wynika, że w Stanach Zjednoczonych około 70 procent osób (mających dostęp do sieci) korzysta z Internetu w domu, 57% w pracy. Osoby te najczęściej korzystają z Internetu w celach (wg Forrester Research):

- wysyłanie e-maili 89%,
- www 84%,
- wyszukiwarki 77%.

Ponadto sporo czasu poświęcamy na sprawdzanie informacji, wyników sportowych, pogody. Przyszłościowym rozwiązaniem (prace i testy trwają) są serwisy wyszukiwawcze, które tematycznie związują reklamę z poszukiwanym przez nas hasłem, np. będąc w USA i szukając informacji o Polsce pokazywałaby się reklama biur podróży oferujących wycieczki do Polski.

Europa

Europa

W Europie wydatki na reklamę internetową są bardzo niskie. Dynamiczny rozwój jest przewidywany za kilka lat. Ciekawym zjawiskiem są eBanki (oferujące możliwość realizowania wszelkich transakcji z wykorzystaniem Internetu). W Europie ta technologia jest zdecydowanie bardziej rozwinięta (nawet w Polsce mamy interaktywne banki, np. BPH Sezam) niż w USA.

Obecnie w porównaniu z całkowitymi nakładami na reklamę, na Internet przeznaczane jest 0,16%. Nakłady te w ciągu najbliższych 5 lat wzrosną blisko 30-krotnie (według Forrester Research). Najwięcej w Europie na reklamę przeznaczają Niemcy – około 39 mln dolarów w 1998 roku. Nie jest to liczba imponująca, ale należy jeszcze raz podkreślić, że Europa dopiero buduje swoje oblicze internetowe. Liderzy technologii internetowej w Europie – państwa skandynawskie przeznaczają dość spore kwoty na reklamę. Według itAfferer w roku 1998 wydatki wyglądać będą następująco (różnią się one nieco od wyników badań udostępnionych przez eStats).

Polska

Polska

Wydatki na reklamę w roku 2000 w Polsce to około 15 mln zł (4,5 mln $). Nie jest to wynik imponujący – nie zapominajmy jednak, że Polska jest dopiero w okresie wzrostu znaczenia komercyjnego wykorzystania Internetu. Jeśli chodzi o reklamę internetową w Polsce znaczące z pewnością będzie najbliższe kilka lat. Według raportu firmy Andersen Consulting (z czerwca 1999) dotyczącego stanu i uwarunkowań handlu elektronicznego w Polsce, jest on jeszcze w powijakach. Według szacunków, całkowity obrót uzyskany przez Internet w Polsce wyniósł ok. 40 mln$.

2.3. Przyszłość rynku elektronicznego w Polsce

2.3.1. Zagadnienia ogólne

Rozwój komercyjnej strony Internetu przebiega w Polsce łagodniej i wolniej niż w USA czy w Europie Zachodniej. Tam początkowy etap wprowadzania technologii internetowych do biznesowej codzienności charakteryzował się inwestorską euforią, czę-

sto pozbawioną racjonalnych podstaw. Inwestowano ogromne pieniądze w rozwój przedsiębiorstw internetowych we wszystkich sektorach gospodarki. Następujący później proces racjonalnej weryfikacji i oceny dalszych perspektyw wiązał się z nagłym – i dla wielu uczestników tej gry nieoczekiwanym – końcem internetowej hossy. W Polsce uniknęliśmy najbardziej drastycznych aspektów wzlotu i upadku dot-comów. Niewykluczone, że wyuczeni na błędach innych, unikniemy ich w przyszłości.

B2B

B2B Rynek B2B (business to business) jest w Polsce na wczesnym etapie rozwoju. Wkrótce jednak sytuacja ta może się zmienić, gdyż jego rozwój jest pochodną rozwoju tego rynku w krajach Europy Zachodniej. Według raportu Gartner Group[13] wartość rynku internetowego w Europie Zachodniej będzie wzrastać o 87% rocznie, przekraczając w roku 2004 bilion dolarów – co stanowić będzie 15% produktu krajowego brutto PKB. W tym samym raporcie czytamy też, że w ramach przeprowadzonej ankiety ponad 75% respondentów zgodziło się, że Internet w sposób fundamentalny i nieodwracalny zmienia sposób prowadzenia interesów. Ciekawe, że opinię tę podziela także – uważany za konserwatywny – sektor produkcyjny. Z kolei z danych firmy AMR Research wynika, że penetracja rynku B2B, to jest odsetek transakcji wykonywanych elektronicznie w stosunku do ogółu realizowanych transakcji, wzrośnie z 1% w 1999 roku do 29% w roku 2004.

W porównaniu z krajami Europy Zachodniej przewidywany rozwój rynku B2B w Polsce przejawia zbliżoną dynamikę. Można nawet zauważyć silniejszą niż na Zachodzie tendencję wzrostową, szczególnie w najbliższych latach (w latach 2000–2001 wzrost nawet dziesięciokrotny!). Szacuje się, że firmy e-biznesowe (typu B2B) to jedyny segment rynku internetowego, który już dziś jest w zasadzie dochodowy. Najszybciej rosną przychody firm związanych z portalami i wortalami biznesowymi oraz z e-integracją. Brakuje natomiast dostawców związanych z bezpieczeństwem danych i transakcji w Internecie – jest to rynek mający bardzo dobre perspektywy w najbliższych latach.

B2C

B2C Dynamika wzrostu rynku B2C (business to customer) odznacza się nieco mniejszą tendencją wzrostową niż w przypadku rynku B2B. Niektóre prognozy mówią nawet o zaledwie 20–30% rocznym wzroście w perspektywie 2–3 lat w Polsce, co zresztą po-

[13] http://www4.gartner.com/Init

krywałoby się z przewidywaniami dotyczącymi liczby internautów. Z drugiej strony w raporcie firmy Global eMarketing czytamy, że stopa wzrostu sprzedaży elektronicznej w ubiegłym roku wyniosła aż 400%. Jaka jest więc realna sytuacja rynku B2C? W tym samym raporcie odnajdujemy też informację o 90 milionach PLN deficytu. Łączna wartość sprzedaży wyniosła w tym czasie około 110 milionów złotych, z tym że zaledwie jedna piąta tej kwoty przypada na polskie e-sklepy. Prawie połowa przebadanych sklepów wykazała obroty poniżej 10 tys. złotych, a liczba transakcji nie przekroczyła 20 miesięcznie – są to wyniki, które dystansuje każdy wiejski sklepik.

Global eMarketing

Powyższe dane sugerują, że gotowość polskich konsumentów do zakupów wyprzedza to, co oferują im w tej chwili krajowe sklepy internetowe. W połączeniu z dającym się obserwować w polskim handlu szybkim wzrostem obrotów mogłoby to sugerować znakomite perspektywy dla handlu elektronicznego. Oczywiście, pod warunkiem, że sklepy internetowe sprostają wymogom konkurencyjnym narzuconym przez sklepy zagraniczne. Zanim jednak damy się wciągnąć optymistycznym prognozom, należy wziąć pod uwagę czynniki ograniczające rozwój tego sektora. Pierwszym z nich jest penetracja rynku: obecna liczba internautów w Polsce (5 milionów) to zaledwie około 11% społeczeństwa – w porównaniu z 25% na Zachodzie. Z tej liczby tylko jedna trzecia (31,5%) to osoby, które choć raz coś kupiły w Internecie. Jeszcze groźniejsze, bo nie zawsze rokujące poprawę w przewidywalnej przyszłości, są bariery rynku B2C wynikające z czynników socjalnych. Istotnym powodem, dla którego wiele osób nie decyduje się na zakupy w Internecie, jest brak możliwości obejrzenia, dotknięcia czy przymierzenia kupowanego towaru. Jest to poważnym utrudnieniem na przykład w branży odzieżowej. Świadczy o tym niedawne bankructwo potentata – firmy boo.com. Dla wielu osób internetowe zakupy nie są atrakcyjne, gdyż osoby te po prostu lubią robić zakupy w zwykłym sklepie (najlepsi klienci to tacy, którzy lubią kupować i lubią być w sklepie). W ostatnim czasie obserwuje się też dążenie do przywrócenia kontaktów międzyludzkich. Odhumanizowany handel elektroniczny traci na atrakcyjności. W Japonii, gdzie niezwykle dynamicznie rozwija się technologia imode – tamtejszy odpowiednik WAP – w ponad połowie przypadków klienci załatwiają płatność przez telefon komórkowy, po czym odbierają zakupy osobiście, w sklepie. Z analizy struktury sprzedaży elektronicznej wynika, że do najchętniej kupowanych towarów należą książki, płyty CD, oprogramowanie, a nieco rzadziej również sprzęt komputerowy i zabawki. Większość zakupów to przedmioty, co do których kupujący dokładnie wie, czego się spodziewać (na przykład konkretne tytuły książek) i w niewielkim stopniu potrzebuje ich oglądania przed zakupem. Przebojem na rynku elektronicznym

WAP

są i będą także usługi turystyczne. Tych z kolei w ogóle nie da się obejrzeć z bliska – nawet w biurze podróży. Istnieje jedna jeszcze grupa produktów, których potencjalni klienci mogą nie chcieć oglądać przed zakupem – są to codzienne, „nudne" sprawunki, jak żywność, pieluszki czy proszki do prania. Tu jednak pojawia się problem natury logistycznej: wirtualny proszek nadaje się tylko do wirtualnego prania, a rzeczywisty towar musi być jeszcze dostarczony do klienta. Wysoki koszt skompletowania zakupów i wysyłki, kłopoty z punktualnością (korki), czy choćby prozaiczny problem – co zrobić z zakupami, gdy klienta nie ma w domu – wszystko to skutecznie utrudnia działania sprzedawców w tej dziedzinie.

Do innych często wymienianych powodów niedokonywania lub rzadkiego dokonywania zakupów w Internecie należy niski poziom zaufania do zabezpieczeń transakcji elektronicznych. Problem ten zostanie przedyskutowany w następnym punkcie. Podsumowując, perspektywy rynku B2C nie są aż tak obiecujące, jak B2B. Mimo to i w tym sektorze – mimo istotnych barier rozwojowych – należy się spodziewać rozwoju, szczególnie w Polsce, gdzie rynek ten jest dopiero na etapie raczkowania. Należy się jednak spodziewać konsolidacji istniejących firm (w drodze fuzji, przejęć lub upadków), co wydaje się warunkiem niezbędnym do uzyskania rentowności przez pozostałe przedsiębiorstwa.

Szansę utrzymania się mają przede wszystkim firmy największe. Strategią dla małych firm może być współpraca ze znanymi adresami URL.

2.3.2. E-gospodarka w e-Polsce

Wielokrotnie zwracano uwagę na konieczność wdrożenia technologii informatycznych w Polsce. Jakie jednak są perspektywy i bariery dla gospodarki elektronicznej w polskiej rzeczywistości. Dotychczasowe wyniki polskich firm internetowych mogłyby napawać sporym optymizmem, gdyby nie fakt, że istniejąca w naszym kraju infrastruktura techniczna, prawna, administracyjna i polityczna nie dorasta już do wymogów chwili bieżącej, a w przyszłości może być istotnym czynnikiem blokującym rozwój Internetu w Polsce. Tę smutną tezę uzasadnimy analizując czynniki o krytycznym znaczeniu dla rozwoju nowej gospodarki.

Infrastruktura informatyczna

Infrastruktura informatyczna jest w Polsce niewystarczająca i droga. Usługi typu dialup nie nadają się do zastosowań profesjonalnych. Oferowane przez TP SA usługi SDI oraz Neostrada nie są wystarczająco dostępne, by móc zaspokoić zapotrzebowanie. Są one w praktyce ograniczone do centrów dużych aglomeracji, a i tam, jak dotąd, większość wniosków o podłączenie jest odrzucanych z „braku możliwości technicznych". Komórkowa technologia GPRS jest powolna i droga, zaś UMTS pozostaje w odległej jeszcze perspektywie.

Wykształcone społeczeństwo

Wykształcone społeczeństwo. Niestety, zajmujemy w tej dziedzinie jedno z ostatnich miejsc w europejskich rankingach. Coroczne cięcia budżetowe w zakresie oświaty i nauki nie wróżą nic dobrego.

Profesjonalna administracja

Profesjonalna administracja. Gospodarka elektroniczna staje się efektywna tylko wtedy, gdy obejmuje wszystkie obszary aktywności społecznej. Stopień zinformatyzowania administracji państwowej jest wciąż nikły; istniejące doświadczenia (Zakład Ubezpieczeń Społecznych) nie napawają optymizmem.

Elektroniczny system transakcji

Elektroniczny system transakcji (e-podpis, e-dokument, e-pieniądz) wymaga uregulowań prawnych, przede wszystkim w zakresie podpisów i certyfikatów. Uregulowania takie być może wkrótce się pojawią, na razie obowiązuje jedynie ustawa o podpisie elektronicznym. Komisja Europejska sformułowała trzy tezy „e-Europy" – określają one sektory o kluczowym znaczeniu przy wdrażaniu technologii informatycznych. Przyjrzymy się ich perspektywom w Polsce.

Demonopolizacja sektora telekomunikacyjnego

Demonopolizacja sektora telekomunikacyjnego. Mimo deklaracji monopol jednej firmy jest w Polsce ciągle podtrzymywany formalnie i nieformalnie. Powoduje to między innymi wywindowanie cen dostępu do Internetu do jednych z najwyższych w Europie, co stanowi niezrozumiałe kuriozum w kraju o stosunkowo niewielkim dochodzie na głowę ludności. Formalnie utrzymywany jest monopol na połączenia międzynarodowe. Raczkująca konkurencja w telekomunikacji, jak również operatorzy komórkowi, borykają się z licznymi zakazami, zezwoleniami i fiskalizmem regulacyjnym (wystarczy wspomnieć o aferze z przyznawaniem koncesji na UMTS).

Edukacja internetowa

Edukacja internetowa w Polsce niemal nie funkcjonuje. Wykonuje się głównie ruchy pozorowane – inwestycji jest za mało, te, które są, oparte są na technologii dial-up. Koszty łączności z Internetem zawężają wykorzystanie wyposażonych znacznym kosztem pracowni szkolnych. Edukacja internetowa w zasadzie mija się z celem, jeżeli się narzuca – z konieczności – drastyczne ograniczenia na czas połączenia. Niebagatelnym problemem jest też brak dobrych materiałów dydaktycznych.

Przedsiębiorczość

Przedsiębiorczość (szczególnie małych i średnich przedsiębiorstw). Z pozoru w tym sektorze sprawy układają się najlepiej – Polakom przedsiębiorczości nie brakuje, począwszy od 1995 roku Polska zyskała sobie opinię najbardziej dynamicznie rozwijającej się gospodarki naszej części Europy – wyprzedzając Czechy i Węgry.

Ograniczanie wolności gospodarczej

Jednak sytuacja prawna i polityczna nie jest sprzyjająca dla przedsiębiorców. W Polsce następuje szybki powrót do etatyzmu. Wyraża się on w ograniczaniu wolności gospodarczej – poprzez lawinowy wzrost liczby potrzebnych koncesji i ograniczeń, niepokojąco narastającą liczbę obciążeń fiskalnych i formalnych, biurokrację niejednokrotnie przeradzającą się w korupcję, wreszcie poprzez nierówne traktowanie podmiotów gospodarczych – na przykład uprzywilejowanie sektorów deficytowych.

Istotnym mankamentem jest brak spójnej wizji gospodarki elektronicznej w Polsce. Zagadnienia informatyczne wychodzą na światło dzienne głównie za sprawą kolejnych skandali: komputeryzacji ZUS czy sprawy światłowodu jamalskiego. Niepokojącym symptomem jest, że w tej ostatniej sprawie polityków nie zaprzątał problem, w jaki sposób stworzoną infrastrukturę światłowodową udostępnić podmiotom polskim, ale raczej – jak zablokować do niej dostęp dla podmiotów zagranicznych.

Perspektywy

Rozwój Internetu na rynku polskim przebiega zgodnie z rozwojem w krajach Europy Zachodniej i USA, z pewnym opóźnieniem i w odpowiednio mniejszej skali. Z jednej strony dowodzi to, iż – jak dotąd – sytuacja w gospodarce polskiej w tym sektorze jest stosunkowo zdrowa. Z drugiej jednak strony rozwój ten może zostać gwałtownie – i z opłakanym skutkiem – zatrzymany, jeśli nie podejmiemy dalszych wyzwań i nie będziemy intensywnie pracować nad usunięciem barier, które już teraz coraz bardziej doskwierają przedsiębiorstwom na internetowym rynku. Internet to wyścig. Szybcy gracze pozostawiają wolnych daleko w tyle. Bez zrozumienia tej prawdy grozi nam odsunięcie do gospodarczego trzeciego świata. Z drugiej strony właściwe rozegranie szans, jakie daje globalna konkurencja na elektronicznym rynku, może być kluczem do nadrobienia strat, jakie gospodarka polska ma w stosunku do przodujących w tym wyścigu państw.

Podsumowanie

Dynamika rozwoju e-gospodarki uzależniona jest w ogromnej mierze od „przechodzenia" firm z działalności tradycyjnej do elektronicznej wymiany handlowej. Takie zmiany powinny być zawsze wpisane w strategię firmy.

Strategiczne planowanie jest pierwszym krokiem, który należy wykonać przed wprowadzeniem handlu elektronicznego. Wiele organizacji ma tendencję do popadania w gorączkę towarzyszącą e-commerce. Często nie zastanawiają się one nad strategicznymi możliwościami, które mogłyby być dla nich dostępne. Rynek internetowy wymaga przeprowadzenia wnikliwych kalkulacji, produkty powinny być jasno określone, powinien być przygotowany długookresowy plan strategiczny na najwyższym poziomie organizacji. Do planów strategicznych powinna być dołączona prognoza rozwoju bezpośrednich konkurentów. Na tym etapie ważne jest także, aby zdać sobie sprawę z tego, że handel elektroniczny może mieć duży wpływ na procesy biznesowe oraz na personel wspomagający te procesy.

3. Zasady działania handlu elektronicznego

- Zakładanie sklepu internetowego,
- Rodzaje katalogów stosowanych w e-handlu,
- Sposoby realizacji zamówień,
- Platformy komercyjne.

Cechy sklepu elektronicznego

Pierwszy kontakt większości ludzi z e-biznesem to sklep elektroniczny, rozumiany jako witryna oglądana na ekranie komputera. Jak każdy inny biznes, charakteryzują go pewne cechy i zalety, jakie każdy dobry sklep mieć powinien.

Po pierwsze, musi dobrze wyglądać – gdyż inaczej nie przyciągnie uwagi oglądającego, a okazja zrobienia interesu będzie stracona. Jest to jednak dopiero początek. Następnie należy w pewien sposób „uwieść" potencjalnego klienta. W witrynie sklepu elektronicznego powinno być coś, co przyciągnie jego uwagę, lub, co lepsze, wyzwoli u niego pragnienie dokonania zakupu. Musi wreszcie istnieć bardzo prosty sposób sfinalizowania ewentualnej transakcji. W końcu najlepiej sprzedaje się to, co jest łatwe do kupienia.

Pod wieloma względami sklep elektroniczny nie różni się od „zwykłego" sklepu, a zatem powinna istnieć prosta możliwość przetłumaczenia wszystkich zmyślnych sposobów handlowania i dobrych zwyczajów handlu tradycyjnego na obraz oglądany na ekranie monitora.

Aby tego jednak dokonać, trzeba najpierw pomyśleć o towarach, jakie zamierzamy sprzedawać i o sposobie ich prezentowania. Różne rodzaje e-biznesu wymagają różnych sposobów podejścia. Nabywca dokonujący zakupów na rzecz ogromnej sieci supermarketów, dla których pracuje wielu dostawców, nie zainteresuje się pięknym obrazkiem świeżych owoców. Pragnie raczej móc porównywać koszty i harmonogramy dostaw wszystkich dostawców. Z drugiej strony detaliczni sprzedawcy odzieży on-line muszą przekonać kupującego, że oferują mu coś naprawdę pożądanego.

Klasyfikacja sklepów elektronicznych

Istnieją różne sposoby klasyfikacji sklepów elektronicznych:
- pod względem modelu działalności handlowej (jeden–jeden, jeden–wielu, wielu–wielu),
- od względem rodzaju rynku (rynek nabywcy, rynek sprzedawcy),
- pod względem skali (duża czy mała),
- pod względem rodzaju klienta (np. hurtowy czy detaliczny).

Celem jest wybór prawidłowego rozwiązania w zależności od skali e-biznesu, bazy nabywczej i modelu rynku.

3.1. Katalogi sklepów internetowych

Katalog sklepów internetowych

Katalog stanowi elektroniczny odpowiednik półek sklepowych, towarów, działów itd. Jest on reprezentacją on-line tego, „co jest na sprzedaż" (lub bardziej prawidłowo tego, czym się handluje). Niektórzy sprzedawcy stosują katalog do symulacji rzeczywistego sklepu (z „działami", w których sprzedaje się określone towary i „półkami" je zawierającymi). Inni tworzą natomiast strukturę swej witryny w oparciu o katalog drukowany, podobny do tego, jaki otrzymuje się na zamówienie drogą pocztową. W dalszej części rozdziału przeanalizujemy poszczególne typy katalogów i zasady ich funkcjonowania, ukazując ich zalety i wady.

Katalogi są różne – od zbioru stron internetowych i prostego skryptu pozwalającego na zbieranie zamówień na towary, poprzez średniej klasy katalogi ze wstępnie zdefiniowaną strukturą kategorii i podkategorii produktów, aż do katalogów wielkich korporacji, możliwych do zmodyfikowania pod kątem określonego klienta. Zwykle są one zintegrowane (back-end integration) z systemami ewidencji zapasów i składania zamówień. Układ katalogów jest związany z rodzajem prowadzonego e-biznesu. Niższej klasy witryna oferuje jedynie kilka specjalistycznych produktów i usług. Dane są wprowadzane ręcznie i przechowywane na kilku dyskach. Prowadzenie bardziej złożonego katalogu (a więc wprowadzanie danych, formatowanie i zapewnienie jakości danych) wymaga już zatrudnienia specjalisty. Innym, dobrze znanym przykładem katalogu wyższej klasy, jest Amazon.com sprzedający między innymi książki on-line lub jego polski odpowiednik MERLIN[14].

Nie jest praktyczne tworzenie sklepu sprzedającego dużo produktów, gdyż odpowiednie strony je opisujące muszą być tworzone ręcznie.

[14] W przypadku małej firmy łatwo zorganizować proste środowisko interaktywne za pomocą kilku stron HTML i formularza zamówień generującego wiadomość e-mailową dla kupca. W tym celu można połączyć kilka skryptów napisanych w języku Perl czy Visual Basic lub w podobnym i zbudować w ten sposób prosty model „karty zakupów" używanej przy kupowaniu towarów w sklepie. Tego typu rozwiązania opisano dokładniej w dostępnych podręcznikach dotyczących HTML i Perl i nie będziemy się nimi zajmować. Trzeba jednak zdawać sobie sprawę, że podlegają one ograniczeniom.

Wprowadzanie zmian towaru jest skomplikowane. Dla pewnych rodzajów produktów, modele i ceny zmieniają się nieustannie i dlatego potrzebny jest automatyczny system aktualizacji katalogu.Tak samo, jak w przypadku witryny internetowej o wielu stronicach HTML, głównym problemem stają się koszty stałe jej utrzymania.Nie istnieje prosty sposób integracji z systemami już funkcjonującymi, włączając płatności, logistykę i kontrolę zapasów. Klient powinien, w idealnym przypadku, móc zawsze sprawdzić, jakie produkty są na składzie, przed dokonaniem zamówienia.

Pomimo wymienionych ograniczeń, podany sposób podejścia jest szeroko stosowany, gdyż założenie i prowadzenie sklepu elektronicznego jest wówczas łatwe i szybkie. Poznawanie takich języków, jak Perl (będący z pewnością domeną fanatyków komputerowych) nie jest już konieczne, gdyż pojawiły się tanie i łatwe w użyciu produkty w rodzaju Multiactive EC Builder. Dają one taki sam efekt końcowy przy znacznie mniejszym wysiłku. Istnieją na rynku komercyjne produkty e-biznesowe, za pomocą których można zorganizować i prowadzić sklep elektroniczny nawet, jeśli nie ma się założonych stron internetowych.

Język programowania

Obecnie wszystko wskazuje na to, iż małe katalogi zostaną prawdopodobnie w niedalekiej przyszłości powiązane z podstawowym oprogramowaniem serwera sieciowego (np. jak to zrobił Microsoft). Daje to bowiem możliwość łatwego zorganizowania niewielkiego sklepu on-line używając „gotowych" narzędzi. Podstawowym zajęciem sprzedawcy jest w tym przypadku zarządzanie swą własną witryną WWW, a głównym wydatkiem jest konieczność utrzymywania stałego połączenia z Internetem.

Alternatywnie, pewna liczba firm oferuje miejsce w katalogach rezydujących na ich serwerach, przy wykorzystaniu których potencjalny handlowiec może utworzyć sklep elektroniczny nie prowadząc własnych stron internetowych. Przykład takiego rozwiązania stanowi katalog prowadzony przez ICAT (firma będąca obecnie własnością Intela) pod adresem www.icat.com, gdzie rezyduje wiele „wirtualnych" katalogów przeznaczanych dla handlowców. W modelu tym strona katalogowa gospodarza (hosta) zawiera zbiór katalogów „wirtualnych" będących w gestii wielu firm handlowych. Firmy te mogą używać witryn on-line obsługiwanych przez przeglądarki internetowe, celem tworzenia oraz aktualizacji własnych katalogów wirtualnych. Narzędzia takie są zwykle łatwe w obsłudze, lecz wymagają ręcznego aktualizowania. Dlatego nie ma możliwości integracji z innymi systemami sprzedawcy, takimi jak kontrola zapasów.

ICAT

Klienci mają dostęp do tego katalogu także przez Internet, przy czym dla nich każda z firm widziana jest jako oddzielna – nie będą więc w stanie stwierdzić, iż dana firma dzieli swą infrastrukturę z pozostały-

Host

mi. W szczególności dotyczy to sytuacji, w której właściciel serwera (host) oferuje handlowcom nazwy domen związane z nazwą danej firmy handlowej, a nie firmy oferującej dostęp do serwera.

Oferując taką kompleksową usługę, firmy załatwiają ponadto wiele problemów, z którymi handlowiec musiałby się sam uporać:

- posiadanie i obsługa własnego serwera sieciowego wraz z odpowiednim sprzętem komputerowym,
- utrzymywanie stałego połączenia z Internetem,
- utrzymywanie składników i procesów związanych z bezpieczeństwem: ochrona typu firewall, monitorowanie systemu itd.,
- zapewnienie serwerów rezerwowych w przypadku awarii,
- utrzymywanie kopii zapasowych i archiwizacja danych.

Katalog rezydentny

Metoda katalogu rezydentnego nie tylko uwalnia przedsiębiorcę od potrzeby utrzymywania własnych stron internetowych, co powoduje wymienione powyżej problemy, pozwala również dzielić między sobą pewne systemy, takie jak bramy obsługujące płatności. Na przykład Wirtualna Polska zapewnia dostęp do systemu obsługi kart kredytowych (dla firm mających już konta handlowe) oraz wysyłanie pocztą elektroniczną danych o każdej transakcji na ich adresy e-mailowe.

Narzędzia umożliwiające customizację pozwalają handlowcom uwzględniać potrzeby klienta w sensownym stopniu i umożliwiają wykorzystanie istniejącej struktury oprogramowania katalogowego.

Omawiane podejście jest szczególnie wygodne dla firm handlowych prowadzących już „konwencjonalny" biznes i pragnących bez dużego ryzyka włączyć się do handlu elektronicznego, pozwala im utworzyć prezentujący się profesjonalnie sklep internetowy, oferujący skromną gamę produktów, bez potrzeby dużych inwestycji we własny sprzęt komputerowy i wiedzę informatyczną[15].

[15] Katalogi wyższej klasy są zazwyczaj budowane wokół „przemysłowej siły" relacyjnych systemów zarządzania bazami danych (RDBMS), takich jak Oracle lub Microsoft SQLserver. Ma to wiele zalet. Systemy RDBMS są w dużym stopniu skalowalne, zarówno jeśli chodzi o wielką liczbę danych, jakie są zdolne przetwarzać, jak i pod względem jednoczesnego przetwarzania dużej liczby wczytywanych plików. W tym ostatnim przypadku systemy RDBMS skalują się stosunkowo łatwo przy całkiem skromnym oprogramowaniu, jak również przy systemach wieloprocesorowych o bardzo dobrej jakości.
Systemy RDBMS mają własne programy narzędziowe do takich rutynowych operacji, jak tworzenie kopii zapasowych i archiwizacja danych. Są elastyczne i odporne na fałszowanie danych, uszkodzenie dysku itd. Zwykle są też wyposażone w elastyczne narzędzia do generowania sprawozdań. Podsumowując, są one wyposażone w podstawowe, choć niezbyt wyrafinowane narzędzia, nie będące głównym przedmiotem zainteresowania sprzedawców posługujących się katalogami.
Systemy RDBMS oferują też standardowe interfejsy do integracji z innymi aplikacjami biznesowymi, np. używając SQL, LDAP, COBRA oraz innych protokołów i technik integracyjnych.

Specyfika katalogów wyższej klasy

Opisane wyżej rodzaje katalogów mają wiele zalet, lecz nie spełniają wszystkich oczekiwań. W szczególności istnieją pewne specyficzne wymagania odnośnie do katalogów wyższej klasy:

- bardzo duża liczba przechowywanych produktów,
- strony internetowe w wysokim stopniu dostosowane do potrzeb klienta i dające wyraźny obraz reprezentowanej marki,
- integracja z innymi procesami w firmie, takimi jak kontrola zapasów.

3.2. Katalogi nabywców i sprzedawców

Katalogi nabywców

Katalogi dla nabywców i sprzedawców są różne – ten pierwszy jest katalogiem wirtualnym, za pomocą którego nabywca może zobaczyć konkurujące ze sobą produkty od różnych dostawców, ten drugi jest zbiorem informacji o tym, co dostawca ma do sprzedania.

Technologia użyta do utworzenia katalogu powinna pasować do jednej ze struktur (tzn. być zoptymalizowana pod kątem jednego sprzedawcy i wielu nabywców lub vice versa).

Przykładem katalogu nabywcy jest Buynet firmy BT, nastawiony na firmy kupujące od wielu dostawców. Tego rodzaju firmą jest łańcuch supermarketów zaopatrywanych przez licznych małych dostawców. Nabywcy zatrudniani przez taką firmę wolą dokonywać wyboru na podstawie jednego dużego katalogu („nadzbioru"), zawierającego wszystkie dobra oferowane przez wielu dostawców, zamiast uciążliwego przeszukiwania licznych katalogów pojedynczych dostawców. Wszyscy sprzedający trzymają szczegółowe dane o swoich własnych produktach w „katalogu nadzbioru", który nabywca może oglądać. Sprzedawcy mają natomiast dostęp tylko do ich własnych części katalogu, a z kolei każdy z kupujących może obejrzeć całą zawartość katalogu, włącznie z podobnymi produktami, jakie może oferować więcej niż jeden sprzedawca.

3.3. Handel detaliczny i hurtowy

Handel detaliczny i hurtowy

Inny sposób podziału katalogów polega na rozróżnieniu między katalogiem typu firma–firma (business–to–business, B2B), a katalogiem firma–klient (business–to–consumer, B2C). W katalogach ukierunkowanych na konsumenta bardziej zwraca się uwagę na prezentację, gdyż celem jest zachęcenie klienta do kupna przeważnie na podstawie wyglądu towaru. Katalogi biznesowe konstruuje się pod kątem szybkiego dostępu do poszukiwanego produktu. Korzystają z nich najczęściej nabywcy zawodowi, dokonujący zakupu takich samych produktów wielokrotnie, a poszukiwanie odbywa się raczej za pomocą kodów przypisanych produktom, a nie długich opisów tekstowych. Zdjęcia poszczególnych towarów nie

mają przy tym znaczenia (chyba, że przy okazji „specjalnych" zakupów dokonywanych tylko sporadycznie). Podobne różnice istnieją w „realnym" świecie, gdzie nie oczekuje się takiej samej fachowości ze strony kupującego silniki samochodowe i klienta butiku przy głównej ulicy.

3.4. Rynki

Modele rynku

W niniejszym podrozdziale omawiane będą modele rynku typu „jeden–wielu" (tzn. różnymi typami katalogów detalicznych w handlu firma–kupujący) oraz modelem „wielu–jeden" (tzn. katalogami nabywcy). Są jeszcze transakcje typu „wielu–wielu". W realnym świecie jest to określone mianem rynkowej koncepcji handlu: rynek, na którym działa wielu handlowców zawierających transakcje z dużą liczbą konsumentów.

Maklerstwo ubezpieczeniowe

W świecie e-biznesu handel „wielu–wielu" łączy się zwykle z działalnością maklerów i pośredników. Przykładem może być maklerstwo ubezpieczeniowe, gdzie wielu klientów ma dostęp do stron maklerów, a ich wymagania odnośnie ubezpieczeń są konfrontowane z usługami oferowanymi przez liczne towarzystwa ubezpieczeniowe. Duża liczba stron internetowych oferuje obecnie ubezpieczenia on-line, lecz wiele z nich nie jest w istocie rynkami on-line. Dla przykładu, zbiera się dane o klientach i przekazuje e-mailem do „fizycznego" maklera ubezpieczeniowego lub jedynie konfrontuje zamówienia z kilkoma standardowymi polisami, wpisanymi statycznie w system. Taki system pozwala klientom na zakup ubezpieczenia domu poprzez Internet w trybie on-line. Działa on w następujący sposób. Klienci chcący ubezpieczyć dom najpierw wypełniają formularz podstawowy, celem dokonania selekcji wstępnej, po czym ewentualnie kierowani są do bardziej wyspecjalizowanego serwisu manualnego, gdy nie mieszczą się w „głównym potoku" klientów ubezpieczeniowych (np. gdy wartość ich domu leży powyżej pewnego progu; gdy zamieszkują w rejonie zagrożonym powodzią lub osuwaniem się gruntu itp.). Klienci należący do głównej kategorii wypełniają następnie drugi formularz internetowy, zbierający informacje o posiadanych dobrach, rodzaju poszukiwanego ubezpieczenia oraz ich dane osobowe. Firmy ubezpieczeniowe mogą wprowadzić dane o swych polisach, zapisane za pomocą takich samych parametrów jak dane wprowadzane przez klientów (np. przedziały wartości domu), włączając ceny związane z poszczególnymi polisami.

System ofertowy

Maklering ubezpieczeniowy działa w „systemie ofertowym", dokonującym konfrontacji wymagań klienta z polisami ubezpieczeniowymi i podającym klientowi zbiór ofert alternatywnych (uszeregowanych w kolejności cen). Klient może teraz dokonać wyboru on-line i zapłacić natychmiast kartą kredytową. Dane przesyła się do firmy ubezpieczeniowej, która wysyła (papierowe) polisy bezpośrednio pod adres klienta.

Firma maklerska przeprowadza operację płatności klienta i pobiera prowizję od każdej transakcji przed dostarczeniem wartości salda firmie ubezpieczeniowej.

3.5. Pośrednictwo

Pośrednictwo

Pośrednictwo rynkowe jest ściśle powiązane z rynkiem otwartym. Funkcja pośrednika polega przykładowo na działaniu w imieniu kupującego, celem wyszukania najkorzystniejszej transakcji. Wszyscy znamy przeglądarki internetowe, należące do najprostszych produktów tego rodzaju: przeglądarka „buszuje" po Internecie w poszukiwaniu informacji najbardziej dostosowanej do wymagań konsumenta. Ta sama zasada może zostać wykorzystana w przypadku sklepów elektronicznych, kiedy serwis pośredniczący może w zasadzie przeszukiwać witryny wielu handlowców w poszukiwaniu określonych towarów, znajdując też towary o najniższej cenie. W rezultacie nie mamy tu do czynienia z rynkiem otwartym, gdyż usługa pośrednika jest w naszym przykładzie wykonywana w imieniu nabywcy.

Podany przykład maklera ubezpieczeniowego jest nieco inny, bo chodzi tu o prawdziwy rynek otwarty, na którym oferty kupna i sprzedaży są konfrontowane ze sobą.

XML

Obecnie podejście oparte na pośrednictwie rynkowym stosowane jest w sposób ograniczony, gdyż nie ma dotąd norm dla katalogów on-line, a używane katalogi są oczywiście dostosowane do użytkownika – człowieka i nie oferują informacji wyjściowej z możliwością odczytu automatycznego. Technologią, z którą wiąże się obecnie nadzieję na rozwiązanie tego problemu, jest język XML[16].

Jedną z powszechnie dostrzeganych zalet biznesu prowadzonego za pomocą Internetu jest trend do zmniejszania liczby pośredników – wyeliminowanie zbędnych łączy w ciągu od surowca do końcowego nabywcy, tj. profesjonalnych pośredników. Internet umożliwia wytwórcy budowanie globalnego kanału sprzedaży bezpośrednio do końcowych użytkowników, bez potrzeby tworzenia fizycznych skle-

[16] XML jest językiem oznakowań mającym wiele wspólnego z językiem HTML, znanym szeroko jako język służący do tworzenia stron internetowych. W języku HTML znaczniki określają jedynie strukturę strony, tzn. pokazują, która część strony powinna być traktowana jako nagłówek, która jako tablica, która jako przypis itd. Język XML dopuszcza także znaczniki wewnątrz samej zawartości strony. Przykładowo, dana strona katalogu może mieć znaczniki XML identyfikujące nazwę produktu, inne znaczniki identyfikujące jego cenę, a jeszcze inne oznaczające liczbę sztuk znajdujących się na składzie. Przez uzgodnienie norm dla znaczników XML w środowisku sprzedawców katalogów, można tworzyć strony katalogowe odczytywane tak przez ludzi, jak też automatycznie. Ich szerokie upowszechnienie pozwoli przeglądarkom „rozumieć" sens zawartości katalogu w większym stopniu niż obecnie. Nabywcy będą mogli wówczas wynajdywać produkty (i dostawców) znacznie łatwiej niż obecnie. Gdy tylko przeglądarki zapewnią bardziej sensowne poszukiwanie produktów, staną się same „witryną", poprzez którą nabywca będzie poszukiwał odpowiedniego dostawcy. Opisana wersja katalogu interaktywnego nie jest jednak pozbawiona wad.

pów i sieci handlu detalicznego. Otwierają się też możliwości nowego rodzaju pośrednictwa, opartego głównie na użyciu technologii „agentów interfejsu". Agent softwarowy ma wiele możliwości: ma pewną autonomię; może się uczyć; potrafi też współdziałać z innymi jednostkami, takimi jak inni agenci (interfejsu) lub użytkownicy (ludzie). Niektóre wczesne systemy wykazujące właściwości typowe dla agenta, to znane wyszukiwarki internetowe, poszukujące określonej informacji w imieniu użytkownika.

Agent interfejsu

Roboty handlowe

Następnym krokiem (prowadzącym do królestwa e-biznesu) jest powstanie asystentów handlowych i tzw. „robotów handlowych" (znanych też pod nazwą shopping bots). Na przykład maszyna handlowa Inktom jest „zatrudniana" przez wiele sklepów internetowych. Z perspektywy użytkownika, na stronie internetowej pojawią się lista kategorii towarów (elektryczne, odzieżowe, sportowe, fotograficzne itd.) oraz proste pole poszukiwawcze, w które użytkownik wprowadza ciąg poszukiwawczy dotyczący określonego *produktu.* Jeśli użytkownik jest np. zainteresowany kupnem kamery cyfrowej, wybierze zapewne kategorię „fotograficzne" i wprowadzi słowa „kamera cyfrowa" będące jego ciągiem poszukiwawczym. W odpowiedzi robot przeszuka strony internetowe detalistów, będące prawdopodobnym źródłem produktów zadanej kategorii (w praktyce „robot[17]" zapisze uprzednio zawartość tych stron w pamięci podręcznej i będzie przeszukiwał tylko własną bazę danych, tak jak robi to większość przeglądarek internetowych). Wyniki przedstawione klientowi to lista produktów pasujących do opisu wraz z nazwami producentów, ceny, dostępność oraz łącza (linki) do innych stron zawierających być może bardziej szczegółowy opis produktu i wyniki badań konsumenckich. Lista może być ułożona w kolejności cen lub innych cech produktów. Gdy konsument wybierze jeden z oferowanych produktów, może on „kliknąć" w podświetlany wyraz „buy" („kupić"), po czym zostanie przeniesiony na stronę wprowadzania danych jego karty kredytowej celem przeprowadzenia transakcji.

W czasie oczekiwania istnieje ryzyko proliferacji DTD (Document Type Definitions), czyli błędu występującego przy powtarzalnych i identycznych procesach biznesowych polegającego na przypadkowym wyborze nazw znaczników bez zagwarantowania jednoznaczności. Taka niekontrolowana proliferacja znacznie utrudnia integrację danych wewnątrz programów aplikacyjnych. Takie firmy, jak Ariba i CommerceOne wypuszczają już konkurencyjne formaty DTD. Niektórzy sprzedawcy przewidują włączanie tych formatów do aplikacji mogących odwzorowywać (mapping) nazwy znaczników XML do nazw pól aplikacji. Dostarczają też narzędzi ułatwiających integrację z aplikacjami komercyjnymi. Oba te rozwiązania są drogie i dlatego zapewne nie przyjmą się na rynku małych i średnich przedsiębiorstw.

[17] Program działający na zasadzie wyszukiwarki internetowej, przeszukujący w „imieniu klienta" dostępne zasoby internetowe w poszukiwaniu wybranego przez użytkownika artykułu lub usługi.

Scenariusz transakcji

Ten scenariusz transakcji obejmuje strony, na których jest zakotwiczony tylko „robot" i jego pamięć podręczna. Jest on uzależniony od aktualnej sieci sprzedaży detalicznej dostarczającej danych o poszukiwanych produktach. Robot handlowy może być więc rozpatrywany jako agent działający w imieniu kupującego, któremu umożliwia „chodzenie po sklepach" i uzyskanie najlepszej ceny dla poszukiwanego produktu. Obecna tendencja wydaje się prowadzić do połączenia pracy robotów handlowych z bogatymi pod względem informacji witrynami internetowymi. W realnym świecie nabywca często kupuje specjalistyczne magazyny i publikacje konsumenckie oraz odwiedza sklepy porównując produkty i ceny. W świecie Internetu ten sam konsument uzyskuje całą informację z pojedynczej witryny sklepu elektronicznego.

Usługi interaktywne

W przyszłości korzystanie z agentów zapewniających wyższy poziom usług interaktywnych stanie się zapewne codzienną praktyką. Będziemy w szczególności świadkami usług, w których pojedynczego robota handlowego zastąpią agenci. Na rynku zawierane będą transakcje z udziałem wielu agentów, każdy z nich będzie miał inne zadanie: jeden będzie reprezentował nabywcę, drugi sprzedawcę, a trzeci maklera. Każdy z nich będzie tak zaprogramowany, by działał w danym zakresie optymalnie w interesie swego ludzkiego partnera. Agent sprzedawcy może dążyć do maksymalizacji zysku, podczas gdy agent kupującego będzie raczej dążył do minimalizacji ceny, a agent maklera do zmaksymalizowania jego dochodu.

Agenci usługowi

Inny przykład stanowi wykorzystanie agentów w biurach podróży (gdzie pozycja agenta, choć w żywym wydaniu, jest już od dawna dobrze ugruntowana!). Dostarczyciele różnych usług podróżnych (rezerwacja lotów, hoteli itp.) mogą je oferować społeczności internetowej za pośrednictwem „agentów usługowych". Nabywca usług podróżnych nie będzie się kontaktować z nimi bezpośrednio, lecz będzie korzystał z usług „agenta–maklera", działającego jak zwykły agent biura podróży[18]. Makler elektroniczny będzie otrzymywał od klienta wszystkie dane, dokonując następnie ich podziału na poszczególne elementy (takie jak loty, hotele, wypożyczenie samochodu itp.). Poprzez interaktywną wymianę informacji z agentami usługowymi gromadzi dane o cenach oraz dostępności wszystkich elementów bądź indywidualnie, bądź w pakietach.

Niektórzy agenci usługowi mogą być wyspecjalizowani w dziedzinie rezerwacji biletów lotniczych, a inni mogą oferować rozmaite usługi turystyczne. Makler będzie wówczas w stanie zaoferować swemu klientowi zbiór opcji cenowych, po czym sfinalizuje całą transakcję elektronicznie. „Możliwości informacyjne" czynią

[18] Polskie przykłady: www.traper.poznan.pl/ , www.arida.pl/ , www.exodus.com.pl/ , www.round-tour.com.pl/ , lub: www.pzm.pl/biuro_podrozy.asp/, turystyka.wp.pl/biuro-podrozy/

tego rodzaju serwis elektroniczny niezwykle przydatnym. Witryna może przykładowo zawierać wideoklipy pokazujące cel podróży, wirtualną wizytację hoteli lub dokładne mapy szlaków podróży[19].

3.6. Zamówienia

Sposoby składania zamówień

Kiedy kupujemy w zwykłym sklepie, realizacja zamówienia odbywa się często natychmiast i opuszczamy sklep z towarem w ręku.

W przypadku sklepu elektronicznego sprawa nie przedstawia się tak prosto i zwykle mamy do czynienia z pewnym sposobem integracji procesów „sklepowych" z jakimś zewnętrznym specjalistą realizującym zamówienia, takim jak poczta, Federal Express itp. „Dobra miękkie" oznacza takie artykuły, jak programy komputerowe (software), dokumenty elektroniczne, muzyka i obrazy w zapisie cyfrowym, które mogą być wystawiane na sprzedaż i są dostarczane elektronicznie poprzez Internet.

Podczas gdy oferowanie za darmo kopii plików poprzez Internet jest proste, to już sprzedaż takich samych produktów, które zostają skopiowane po dokonaniu zakupu jest nieco bardziej skomplikowane. Dzieje się tak z następujących powodów:

- jak być pewnym, iż dokonano zapłaty zanim udzielono pozwolenia na skopiowanie;
- jak postępować w przypadku błędnego kopiowania spowodowanego np. kłopotami z pracą;
- jak zabezpieczyć skopiowany produkt przed jego powtórnym kopiowaniem przez nabywców;
- jak postępować z niezadowolonymi klientami i zwrotami towarów.

Problemy z zamówieniami

Podamy teraz przykłady radzenia sobie z wymienionymi kłopotami.

- *Darmowe przenoszenie zaszyfrowanych plików.* W tym przypadku stosowane jest proste urządzenie kopiujące, lecz plik jest zaszyfrowany i nie może zostać wykorzystany przez klienta nie rozporządzającego odpowiednim kluczem. Nabycie danego produktu jest po prostu równoznaczne z zakupem klucza służącego do odszyfrowania otrzymanego pliku. Zamówienie może być przy tym realizowane ręcznie, a klucz wysyłany pocztą elektroniczną. Metoda zapewnia dostęp do pliku tylko tym, którzy

[19] Technika wykorzystywania agentów jest jeszcze w początkowym etapie rozwoju i musi dopiero zdobyć uznanie szerokich kręgów społeczności biznesowej. Choć istnieje już wiele dobrych agencji turystycznych on-line, sprzedają obecnie tylko oferty w pakietach lub wymagają od klienta rozbicia swego zapotrzebowania na poszczególne elementy i oddzielnego ich wprowadzania do komputera. Opisany w przykładzie system pracuje tylko w formie demonstracyjnej, lecz biorąc pod uwagę niezwykle szybkie tempo wprowadzania nowych produktów w „czasie internetowym" można liczyć na jego komercyjną wersję w najbliższym czasie.

kupili klucz oraz chroni klienta przed wadliwym kopiowaniem: może on swobodnie kopiować plik dowolną liczbę razy, a dostarczanie klucza jest całkiem niezależnym procesem. Rozwiązuje to pierwsze dwa z wymienionych problemów. Słabością metody jest fakt, iż ten sam klucz dostarczany jest wszystkim klientom, co powoduje ryzyko jego nielegalnego rozpowszechniania (np. na stronach internetowych „hakerów") wśród potencjalnych klientów danej firmy. Metoda jest jednak prosta i pozwala stosować prawie każdy sposób szyfrowania, przy którym klient jest w stanie odkodować plik bez użycia specjalnej aplikacji.

Wersje demonstracyjne

- *Wersje demonstracyjne z hasłami.* Wzbogacenie metody pierwszej może polegać na dystrybucji pewnych dóbr (w szczególności oprogramowania) na zasadzie „wypróbuj, zanim kupisz". Dany program może mieć ograniczony czas użytkowania lub być pozbawiony pewnych możliwości – jest jednak dawany na próbę za darmo. Aby jednak dokonać aktywacji pełnej wersji programu trzeba wprowadzić klucz „otwierający" całkowicie możliwości funkcjonalne programu. Podobnie jak w wersji pierwszej, klucz można zamawiać poprzez sieć, a otrzymywać poprzez e-mail. Sam produkt nie jest w tym przypadku zaszyfrowany, lecz zawiera wewnątrz zabezpieczenie usuwane za pomocą klucza. Podstawową zaletą tego rozwiązania jest możliwość wypróbowania produktu przed dokonaniem zapłaty, co redukuje problem zwrotów. Nadal istnieje niestety ryzyko bezprawnego rozsyłania kluczy. Rozwiązanie to nie ma zastosowania do produktów o charakterze czystej informacji, gdzie sama koncepcja „wypróbuj, zanim kupisz" nie ma sensu.

Platformy dystrybucji „dóbr miękkich"

- *Wyspecjalizowane platformy dystrybucji* „dóbr miękkich". Zamiast zezwolić na przenoszenie produktów, a potem stosować oddzielne środki zabezpieczające ich zawartość, można zastosować bardziej wyspecjalizowaną platformę komercyjną monitorującą wszystkie kroki procesu postępowania każdego użytkownika (włączając w to etap płatności) i kontrolującą proces kopiowania produktu na podstawie czynności, jakich ten klient dokona. Systemy te wymagają zwykle rejestracji oraz logowania się użytkowników tak, aby platforma mogła śledzić działania każdego z nich. Przekazywanie produktu odbywa się za pośrednictwem odpowiedniej aplikacji. Takim systemem jest Array firmy BT. Choć system ten umożliwia znaczny stopień kontroli, nadal nie zapobiega w pełni tworzeniu nielegalnych kopii produktu ani ich rozpowszechnianiu (co jest jednak znacznie trudniejsze od prostego sporządzania nielegalnych kopii kluczy). W celu uniknięcia wadliwego kopiowania (np. wskutek trudności telekomunikacyjnych) systemy pozwalają zazwyczaj użytkownikowi na szereg prób kopiowania w zadanym czasie (np. 24 godziny).

Intertrust

- *Infrastruktury* zapewniające bezpieczne dostawy Intertrust. W celu zapewnienia pełnej kontroli produktów potencjalnie możliwych do skopiowania przez nabywcę trzeba uruchomić infrastrukturę, której pewne elementy znajdują się po stronie klienta. System Intertrust obejmuje klienta mogącego integrować się z różnymi przeglądarkami dokumentów oraz typowymi aplikacjami typu Microsoft Word. Produkty dostarczane klientowi składają się z dwu części: zaszyfrowanej części informacyjnej, którą może odszyfrować tylko wyspecjalizowany klient, oraz zbioru reguł (też zaszyfrowanych) podających sposób wykorzystywania produktu. Klient komunikuje się z serwerem sieciowym, nie tylko w celu skopiowania pliku, lecz w innych momentach cyklu życia tego produktu. Sam produkt nie może być oglądany, chyba że pod kontrolą wyspecjalizowanego klienta, a i to jedynie zgodnie z regułami ukrytymi w tym samym produkcie. Na tym poziomie wyrafinowania można ustanowić wiele elastycznych opcji, np. : treść kasowana po pewnym czasie (może być oglądana przez zadany okres, a następnie staje się niewidoczna do czasu zapłaty); opłatę trzeba wnosić za każde oglądanie produktu; płaci się raz po załadowaniu, a potem za każdą zrobioną kopię itd. Opisana metoda załatwia wszystkie podstawowe problemy związane z dystrybucją „dóbr miękkich" (chyba, że będziemy mieli do czynienia ze szczególnie zdeterminowanym hakerem), lecz wszystko ma swoją cenę. Konsument musi się więc pogodzić z obecnością specjalnego klienta w swoim komputerze, który będzie komunikować każdą czynność użytkownika serwerowi użytkowanej sieci.

3.7. Platformy komercyjne

Platformy komercyjne

Sprzedawcy platform coraz częściej dostarczają rozwiązań komercyjnych, oferując nie tylko produkt katalogowy, lecz całą gamę narzędzi dla tworzenia sklepu elektronicznego, włączając system dokonywania płatności, przetwarzanie dokumentów oraz integrację zaplecza. Przykładem jest tu Commerce Server firmy Microsoft, stosowany też przez innych sprzedawców jako podstawa tworzenia witryn handlowych i aplikacji. Microsoft Commerce Server jest nie tylko rodzajem witryny komercyjnej: zapewnia też szereg narzędzi do kreowania i rozszerzania możliwości handlu elektronicznego. Dalej przedstawiono jego główne elementy[20].

- Otwarta architektura systemu płatności. Jest to architektura softwarowa zaproponowana przez Microsoft, pozwalająca na rozwi-

[20] W związku z potencjalnym zarzutem kryptoreklamy opisano wyłącznie zagraniczne rozwiązania do tworzenia sklepów internetowych; większość polskich platform bazuje na „importowanym" jądrze takiego systemu. Opis jednej z wielu z polskich platform do tworzenia sklepu internetowego zawiera Aneks 2.

janie przez osoby trzecie elementów umożliwiających prowadzenie dowolnego systemu przetwarzania płatności. Architektura ta nie tylko pozwala uwzględniać różne metody płatności, lecz ponadto bezpieczne protokoły płatności włączając SSL i SET. Protokół SET jest standardem popieranym przez wiele wiodących firm, takich jak Visa i Mastercard. Stanowi on dlatego ważną inicjatywę w dziedzinie zapewnienia bezpieczeństwa finansowego. SET jest protokołem trójstronnym, zarządzającym interfejsami klienta, handlowca i instytucji finansowej za pośrednictwem pojedynczego pliku. Wiele niezależnych firm oferujących oprogramowanie płatnicze dostarcza programy SET oparte na systemach Microsoft Wallet i Site Server oraz API Enterprise Edition.

SET

- *Microsoft Wallet.* Jest to system oparty na technologii ActiveX lub Netscape, dokonuje hermetyzacji i zapamiętuje informację o kliencie (taką jak nazwisko, adres, numer karty kredytowej) tak, aby użytkownik nie musiał wpisywać jej za każdym razem od nowa, ułatwiając tym samym proces kupowania. Wallet przesyła też w sposób bezpieczny tę informację do serwera. Przesłana informacja wygląda jak standardowa poczta HTTP i może ją odczytywać każdy serwer, nie tylko Site Server Commerce. Jest ona dostępna za darmo w sieci WWW oraz powiązana z aplikacjami i systemami operacyjnymi Internet Explorer, Windows 9X i Windows NT i pochodnymi, a stosowana już przez Site Server Commerce i inne systemy, jak Intershop i Mercantec.

Microsoft Wallet

- *Potok zamówień.* Potoki są rozwiązaniem stosowanym przez Microsoft do modelowania procesów biznesowych, takich jak zamawianie produktów. Potok stanowi strukturę zawierającą pewną liczbę etapów, przy czym każdy etap reprezentuje oddzielną operację na obiekcie biznesowym (jak np. formularz zamówienia). Na każdym etapie jeden lub większa liczba wyspecjalizowanych składników działa na obiekt, przesyłając go dalej do następnego etapu potoku. W systemie Site Server Commerce 2.0 potoki były z góry zadane, lecz już w wersji 3.0 umożliwiono klientom tworzenie swoich własnych potoków. Site Server Commerce generuje potok zamówień podzielony na 14 wstępnie zdefiniowanych etapów:
  1. Informacja o produkcie,
  2. Informacja handlowca,
  3. Informacja sprzedawcy,
  4. Zainicjowanie zamówienia,
  5. Sprawdzenie zamówienia,
  6. Cena jednostkowa,
  7. Korekcja ceny jednostkowej,
  8. Korekcja ceny zamówienia,
  9. Suma częściowa,
  10. Koszty transportu,
  11. Opłata manipulacyjna,
  12. Podatek,

Potok zamówień

13. Suma całkowita,
14. Korekcja inwentaryzacji.

Site Server Commerce

- Architektura potokowa jest bardzo elastyczna. W systemie Site Server Commerce potok zamówień jest już wstępnie skonfigurowany, jak podano. Handlowcy mogą jednak w razie potrzeby dodawać lub usuwać dowolne etapy. Na przykład, gdy pragną uwzględnić dodatkowo wiadomość o prezencie dodawanym do pewnego zakupu, mogą dodać do potoku etap sprawdzania, czy była wiadomość o prezencie, a jeśli tak, skontrolować wysyłaną wiadomość i dodać odpowiednią opłatę. O elastyczności systemu decydują elementy przetwarzające informację na każdym etapie. System Site Server Commerce składa się z zestawu domyślnych elementów. Jest w nim jednak ponad 50 elementów dodatkowych dotyczących wielu etapów. Na przykład, zamiast etapu dotyczącego spedycji, gdzie oblicza się opłatę za transport jako procent całkowitej sumy zamówienia, można dołączyć znacznie bardziej skomplikowaną procedurę oferującą kilka metod transportu (np. lądowy lub lotniczy) i obliczającą dokładnie koszty transportu dla wybranej opcji i danej wagi towarów. Ponadto wszystkie interfejsy używane do realizacji danej procedury są dokumentowane i handlowcy mogą bez trudu tworzyć własne procedury, celem dalszego dostosowania swego zestawu zamówień do potrzeb klienta. Architektura formularza zamówienia: formularz stanowi przykład obiektu biznesowego, na który działają procedury potoku. W systemie Site Server Commerce formularz jest po prostu obiektem zawierającym pary wartości kluczowych. Wartości te mogą z kolei wskazywać na listy zawierające więcej par wartości kluczowych.

Store Builder Wizard

- *Store Builder Wizard*. Jest to narzędzie opracowane dla uproszczonych i zarządzanych on-line sklepów elektronicznych.

Podsumowanie

Gdy porównujemy sklepy w realnym świecie, jasno widzimy pomiędzy nimi różnice. Niektóre, jak banki, nie mają żadnych towarów na wystawach, lecz widzimy tam ogromnie dużo firm reprezentowanych jedynie przez swoje logo. Inne sklepy mają atrakcyjne wystawy, a ceny wypisywane są na dyskretnych metkach (jeśli w ogóle są). Czasem piętrzą się stosy towarów i można tam kupić taniej niż gdzie indziej. Każdy styl przemawia do innej cechy naszego „ja" – czasem przyciąga nas jakość, czasem chęć posiadania, a czasem oszczędność. Subtelności związane z zaspokajaniem wymagań klientów sklepów tradycyjnych trzeba było przenieść w dziedzinę sklepów internetowych. Temu służą właśnie katalogi, platformy cyfrowe itp.

4. Rozliczenia w e-gospodarce

- Sposoby dokonywania płatności,
- Rozliczenia finansowe w e-gospodarce,
- Karty kredytowe i debetowe,
- Czeki elektroniczne,
- Transfer funduszy,
- SWIFT.

Biznes istnieje tylko po to, aby możliwe było zwiększanie udziału jednostek gospodarujących w podziale dochodu. Może to oznaczać wymianę wiedzy, bonów lub usług, lecz zwykle walutą biznesu jest gotówka. Biorąc pod uwagę płynność i szybką ewolucję rynku wirtualnego, transfer rzeczywistego pieniądza nie jest sprawą łatwą. Sprzedawcy chcą być pewni, iż zostanie im zapłacone; nabywcy nie chcą dawać więcej niż się należy (ani podawać tajnych danych na temat swych kont bankowych), a obie strony poszukują bezpiecznego, niezawodnego i prostego w obsłudze mechanizmu zabezpieczającego spełnienie ich wzajemnych zobowiązań.

Transfer pieniądza

Postęp technologiczny w dziedzinie elektronicznych systemów płatniczych był w ciągu ostatnich kilku lat powolny, lecz stały. Najważniejszą przyczyną tego pozornego braku pośpiechu w tej tak ważnej dla e-biznesu dziedzinie była koncentracja wysiłku w celu zintegrowania rozmaitych elementów tworzących handel elektroniczny i umożliwienie dokonywania zakupów on-line, a nie opracowywanie systemów płatności. Mimo wielkiego rozgłosu regulowanie płatności w systemie on-line ciągle nie jest tak rozpowszechnione, jak przewidywano, brak jest zaufania do tego sposobu płacenia, co jest jednym z głównych powodów, dla których użytkownicy nie dokonują zakupów on-line.

Rozmaitość terminologii związanej z biznesem elektronicznym wykazuje z pewnością wszelkie symptomy zapędów dyktatorskich (głównie ze strony środowiska technicznego). Zanim więc rozpoczniemy wyjaśnianie tajników pieniądza elektronicznego, podamy kilka podstawowych definicji:

- *Fakturowanie.* Pierwszy krok procesu płatności związany zwykle z fakturami elektronicznymi nadsyłanymi pocztą elektroniczną lub innym systemem zapewniającym otrzymywanie rachunku on-line.

Fakturowanie

- *Rozliczanie.* Następnym krokiem jest przesyłanie, uzgadnianie oraz, w pewnych przypadkach, potwierdzanie zlecenia zapłaty zgodnego z fakturą, przed uregulowaniem rachunku.

Rozliczanie

- *Regulowanie rachunków.* Proces zapisu księgowego po stronie „winien" i po stronie „ma" uczestników zaangażowanych

Regulowanie rachunków

w procesie przelewu środków. Regulowanie rachunków może być dokonywane „brutto" lub „netto". W systemie brutto każda transakcja jest regulowana indywidualnie. W systemie netto, strony wymieniające płatności będą wzajemne zobowiązania kompensować tak, aby dostarczać identyczne pozycje (np. EURO lub USD) w ustalonym czasie, np. na koniec dnia. W tym punkcie tylko jedna suma netto z każdej pozycji jest wymieniana. Na przykład, gdy jestem Ci winien 10 euro plus 3 dolary, a Ty mi jesteś winien 6 euro i 11 dolarów, rozliczymy się prawdopodobnie w systemie netto, gdzie ja Ci dam 4 euro (10 minus 6), a Ty dasz mi 8 dolarów (11 minus 3).

Inkasowanie należności

- *Inkasowanie należności.* Ostatni etap procesu płatności, gdy na jedno konto księgowana jest wpłata, a na drugie wypłata. Inkasowanie należności jest zakończone, gdy autoryzacja należności ze strony dostarczyciela usług finansowych (np. banku) zostanie potwierdzona. Inkasowanie nie jest tak proste, gdy weźmiemy pod uwagę, iż np. okresowe obciążanie za pomocą kart kredytowych nie jest dozwolone przez przepisy obowiązujące w Wielkiej Brytanii. Ten właśnie problem oraz przepisy Cardholder Not Present przewidujące możliwość zwrotów należności, stwarzają potrzebę ustanowienia instrumentów zarządzania długami.

4.1. Płatności

Formy płatności

Stosunek do różnych mechanizmów płatności ulega ciągłym zmianom. Najważniejsze formy płatności za towary i usługi to:

- gotówka,
- czeki,
- bezpośrednie obciążenie rachunku,
- karta kredytowa,
- karta debetowa
- rachunek kredytowy,
- inne formy, takie jak „barter", które nie są poważnie traktowane w handlu międzynarodowym, lecz mają potencjalny odpowiednik w e-biznesie.

Preferencje w stosunku do tego lub innego sposobu płatności zmieniają się w zależności od tego, czy jest to transakcja biznes–biznes (B2B) (gdzie rachunek kredytowy jest najbardziej rozpowszechniony), czy transakcja biznes–konsument (B2C) (gdzie faworyzowane są karty kredytowe) bądź transakcja osoba–osoba (C2C) (kiedy to najpopularniejszą formą jest czek lub gotówka). Wewnątrz samej społeczności biznesowej istnieją także różnice, przy czym w małym biznesie używa się zwykle kart kredytowych. W niektórych gałęziach przemysłu istnieje szczególna niechęć do kredytu, podczas gdy w innych jest on „normą".

W prognozach rozwoju e-gospodarki przewiduje się, iż w roku 2007 (przy założeniu 10% udziału w rynku transakcji drobnych (agenci wiadomości, automaty, sprzedaż biletów itd.)) nastąpi spadek procentowy udziału transakcji gotówkowych do 63%. Zauważa się ponadto, iż niektóre części świata i kultury są w swym podejściu do poszczególnych form płatności bardziej konserwatywne niż inne.

Przy rozpatrywaniu możliwej ewolucji w dziedzinie płatności on-line należy brać pod uwagę głównych graczy dokonujących płatności w „tradycyjnych" systemach. Globalni dostarczyciele usług płatniczych, to Visa i Mastercard. Te nieliczne firmy są obecnie głównymi graczami na globalnym rynku usług płatniczych. Na przykład, Barclayard działa już w 247 krajach, obsługuje więcej niż 13 milionów handlowców i ponad 650 milionów kart kredytowych. Podstawowym wyzwaniem jest tu dostateczny system zabezpieczeń wersji on-line ich tradycyjnych form działalności. Jest to dzisiaj najważniejsza siła promująca nowoczesne systemy płatnicze on-line[21] .

4.2. Karta kredytowa i debetowa

Karty kredytowe i debetowe

Przyglądając się elektronicznym systemom płatności zaczniemy po kolei od „tradycyjnych" sposobów płacenia, a następnie będziemy rozważać, jak ewoluują w kierunku uwzględniania potrzeb e-biznesu.

Karty kredytowe i debetowe będą tu rozpatrywane łącznie, gdyż przetwarzane są w ten sam sposób. Na nich skupiała się głównie uwaga w czasie tworzenia wczesnych systemów płatniczych on-line.

Załóżmy, że konsument pragnie nabyć towar od handlowca i zapłacić zań kartą kredytową. Aby transakcja mogła dojść do skutku, konsument musi najpierw otworzyć konto z kartą kredytową w banku, który oferuje taką usługę dla klientów indywidualnych. Sprzedawca także powinien mieć konto, w tym przypadku w ban-

[21] Narodowe zrzeszenia płatnicze, takie jak APACS oraz LIINK. Organizacje te powstały w celu zaspokojenia specyficznych potrzeb banków, będących ich członkami w dziedzinie oznaczania marką, zachowania norm oraz przetwarzania informacji. Zrzeszenia płatnicze w Wielkiej Brytanii i w Europie mają swą odrębną specyfikę, jeśli chodzi o ich rolę i obowiązki.
Dochodzą jeszcze przedsiębiorstwa dominujące w dziedzinach powiązanych z omawianym zagadnieniem, lecz nie będące w stanie szybko przenosić swej działalności w dziedzinę systemów płatniczych. Najbardziej znaczącą wśród nich jest Microsoft. Będąc właścicielem standardów w dziedzinie oprogramowania klienta, firma jest potencjalnie w stanie wejść w zagadnienia transakcji elektronicznych po stronie klienta (np. utworzyć elektroniczny portfel wbudowany w przyszłą wersję systemu operacyjnego Windows).

ku przygotowanym do przetwarzania kart kredytowych. Bank ten zaopatruje również handlowca w środki rejestracji transakcji (np. elektroniczny punkt sprzedaży lub urządzenie obsługiwane manualnie wyposażone w czytnik kart). Dodatkową stroną transakcji jest operator usług płatniczych (tzn. firma obsługująca karty kredytowe, jak Visa lub Mastercard).

Rozliczanie transakcji

Rozliczanie transakcji za pomocą kart kredytowych wraz z inkasowaniem należności jest procesem trójstopniowym i obejmuje:

- autoryzację, gdzie bank emitujący kartę potwierdza (lub odmawia potwierdzenia) transakcję proponowaną w punkcie sprzedaży,
- inkasowanie należności, gdzie bank obsługujący handlowca zbiera dane dotyczące transakcji od handlowca i dostarcza do kompanii obsługującej kartę kredytową, a ta z kolei przekazuje je do banku emitującego karty. Bank na tej podstawie księguje transakcję na konto posiadacza karty,
- regulowanie rachunków, gdzie instytucja obsługująca karty kredytowe pobiera należność od banku emisyjnego i wpłaca je na konto firmy handlowej.

W przypadku typowej transakcji posiadacz karty może udać się do sklepu i oferować kartę kredytową w zamian za określone towary. Handlowiec zapisuje dane z karty kredytowej i dane dotyczące transakcji, przepuszczając ją zwykle przez czytnik terminalu.

Dane te są przesyłane za pośrednictwem instytucji obsługującej kartę kredytową do banku, który wystawił kartę. Bank potwierdza lub odmawia potwierdzenia transakcji, w zależności od stanu konta posiadacza karty. Potwierdzenie lub odmowa jest przekazywana elektronicznie do sklepu za pośrednictwem banku przyjmującego kartę kredytową. Sieć łącząca punkt handlowy z bankiem jest zwykle siecią PSTN lub staromodną, lecz niezawodną siecią informatyczną X.25 (np. BT Cardway Service)[22] .

Ostatnim etapem transakcji jest regulowanie rachunków, kiedy kompania obsługująca karty kredytowe inkasuje należności z konta banku emitującego kartę, po czym dokonuje ich transferu na konto handlowca w jego banku.

Po uregulowaniu rachunków bank emitujący kartę umieszcza transakcję jako pozycję miesięcznego wyciągu posiadacza karty, a gdy

[22] Regulowanie rachunków odbywa się zazwyczaj wieczorem, gdy placówka handlowa przesyła wszystkie dane o transakcjach dokonanych za pomocą kart kredytowych elektronicznie (polecenie wypłaty) do swego banku. Bank ten z kolei kredytuje konto handlowca sumą transakcji i ten znajduje się już poza pętlą. Bank obsługujący handlowca też pragnie pobrać prowizję za przeprowadzoną transakcję i wysyła w tym celu dane dotyczące transakcji elektronicznie do kompanii obsługującej karty kredytowe, a ona rozsyła te dane po kolei do odpowiednich banków emitujących karty.

ten zapłaci bankowi emitującemu kartę, cykl staje się kompletny. Łącze od handlowca do jego banku jest już zwykle typu elektronicznego (poprzez bezpieczną sieć prywatną), tak jak w przypadku łącza międzybankowego.

Problemy rozwoju e-biznesu

Rozwój e-biznesu koncentruje się obecnie wokół dwu problemów:
- doprowadzenie do tego, aby transakcja między posiadaczem karty i handlowcem odbywała się poprzez Internet,
- automatyzacja funkcji handlowca w procesie przetwarzania karty, danych dotyczących transakcji i połączenie go za pośrednictwem interfejsu z prywatną siecią bankową.

Osiągnięcie tego celu napotyka na kilka wyzwań.

- Posiadacze kart uważają Internet za niebezpieczny i nie chcą wysyłać danych z karty w sposób jawny poprzez sieć publiczną,
- Posiadacz karty i handlowiec chcą mieć pewność, że ten drugi jest tym, za kogo się podaje,
- Nawet mając pewność, że handlowiec jest „autentyczny", posiadacze kart są ostrożni w podawaniu danych ze swoich kart komuś, z kim nie mają osobistego kontaktu,
- Banki są ostrożne w przyjmowaniu odpowiedzialności za transakcje zawierane pod nieobecność posiadacza karty (CNP – Cardholder Not Present).
- Handlowcy muszą się liczyć ze zwrotami pieniędzy klientom.

Istnieją pewne praktyczne strategie prowadzenia płatności kartą kredytową poprzez Internet. Przedstawimy je tutaj w kolejności od najmniej do najbardziej złożonej.

Przyjmiemy, że pewna firma ma zamiar sprzedawać towary, akceptując składanie zamówień i płacenie kartą kredytową za pośrednictwem Internetu.

(sposób 1) ***Niezabezpieczone dane kart kredytowych***

W omawianym przypadku, gdy klienci wybiorą towary do zakupu, jest im przedstawiony formularz w postaci strony WWW, na którą muszą wprowadzić dane dotyczące swoich kart kredytowych. Po wypełnieniu formularza należy kliknąć słowo „submit" (przedłożyć), co powoduje wysłanie danych klienta poprzez Internet do serwera sprzedawcy, w postaci nadającej się do przetwarzania przez aplikację CGI (Common Gateway Interface)[23].

[23] Aplikacja CGI przetwarza tę informację do postaci możliwej do ręcznego przetwarzania przez handlowca. Można tego dokonywać na różne sposoby: aplikacja CGI może wysyłać sprzedawcy dane o transakcji e-mailem; może po prostu przechować je w bazie danych, do której sprzedawca ma dostęp poprzez formularz WWW; może też wydrukować te dane w firmie celem ich ręcznego przetwarzania. Po wyselekcjonowaniu danych dotyczących płatności handlowiec wpisuje je na formularz w terminalu POS, skąd zostaną wysłane poprzez zwykłą sieć bankową do jego banku, który wysyła zwrotnie potwierdzenie ważności karty. Omawiane podejście ma pewne zalety: jest proste w realizacji; szczególnie gdy jest dodatkiem do istniejącej działalności handlowej. Detalista, mający już konto handlowe może w prosty sposób założyć witrynę do przyjmowania zamó-

(sposób 2) ***Stosowanie klucza szyfrującego po stronie serwera***

Jak wynika z rozważań przeprowadzonych w rozdziale dotyczącym zaufania i bezpieczeństwa, tajność w Internecie osiąga się zwykle przez wprowadzenie zaszyfrowanego kanału, stosując przykładowo standardową warstwę zabezpieczenia łączy używaną powszechnie w serwerach sieciowych i przeglądarkach. Początkowa interakcja między przeglądarką i serwerem zachodzi z użyciem kryptografii z kluczem publicznym, w której jeden klucz (klucz publiczny) jest używany do szyfrowania wiadomości, a inny klucz (klucz prywatny) służy do jej odszyfrowywania. W najprostszym opisywanym tutaj przypadku jeden klucz prywatny jest przechowywany w serwerze, a pasujące do niego klucze publiczne są dostępne dla klientów. Podejście to daje dwie korzyści: po pierwsze transfer danych z karty kredytowej klienta dokonywany jest poprzez zaszyfrowane łącze, usuwając tym samym podstawową wadę opcji I. Po drugie, pod warunkiem że handlowiec przydziela klucze publiczne, uwierzytelnione uprzednio przez godną zaufania stronę trzecią, konsumenci mogą być pewni, że udostępniają dane ze swych kart tylko temu, kto jest tym, za kogo się podaje.

Taki poziom bezpieczeństwa może zostać zagwarantowany jako opcja dla większości serwerów sieci WWW. Certyfikat po stronie serwera można zakupić od godnej zaufania strony trzeciej, takiej jak np. VeriSign w OSA i TrustWise, za równowartość kilkuset dolarów.

Opisywane podejście nic jednak nie daje w dziedzinie automatyzacji procesu po stronie handlowca i nadal nie zabezpiecza danych z karty płatniczej przed nieuprawnionym wykorzystaniem przez nieuczciwego handlowca, mimo iż dane te nie są w omawianym systemie dostępne w Internecie.

---

wień internetowych równolegle z zamówieniami przyjmowanymi metodą tradycyjną. Infrastruktura handlowca może zostać jeszcze bardziej uproszczona, gdy usługi w sieci WWW i aplikacje CGI są dostarczane przez „internetowe biuro handlowe" należące do strony trzeciej, zajmujące się wysyłaniem zamówień e-mailem lub faxem. Najważniejszymi wadami tego systemu, jeśli chodzi o bezpieczeństwo, są: brak zabezpieczeń dostępu do Internetu na drodze między konsumentem a handlowcem, przy czym ten ostatni (a niekiedy i biuro usługowe) przechowuje dane karty kredytowej klienta. Dane te mogą zostać nielegalnie wykorzystane przez nieuczciwą firmę. Z punktu widzenia handlowca, choć otrzymuje on potwierdzenie z banku, że karta kredytowa klienta jest ważna, transakcja jest nadal zawierana bez obecności posiadacza karty (CNP) i handlowiec ten ponosi ryzyko, w przypadku gdy karta (bądź tylko jej dane) została ukradziona innej osobie. Dalszą wadą omawianej opcji jest brak automatyzacji działań po stronie handlowca.

(sposób 3) ***Stosowanie zautomatyzowanej bramy płatniczej (card gateway)***

Handlowcy sprzedający dużo towarów mogą bardzo skorzystać na automatyzacji procesu, podczas którego dane z kart kredytowych są pobierane z aplikacji serwera WWW i wprowadzane do sieci banku obsługującego sprzedawcę. Innymi słowy, ręczny proces pobierania danych zastąpiono tu bramą płatniczą.

Przykładami bram płatniczych są Commedia Soft–EFT oraz Servebase Computers Ltd. PC–EFT. Soft–EFT jest zbiorem programów przetwarzania płatności poprzez komputer PC, stosowanym dla kart Visa, MasterCard, Switch, American Express, JCB, Diners Club i Style. Programy te zaprojektowano w celu łatwej integracji z aplikacjami używanymi przez handlowców.

„Sieć bankowa" może w rzeczywistości składać się z pewnej liczby fizycznie istniejących sieci: większość banków obsługujących handlowców ma np. dostęp do sieci PSTN, ISDN i X.25. Wiadomości przekazywane przez tę sieć mają format zdefiniowany przez APACS (Association for Payment Clearing Services), znany jako APACS 30 i APACS 50[24] .

APACS

Najważniejszym problemem, jakiego ta opcja nie rozwiązuje, jest sprawa przechowywania danych z kart kredytowych konsumentów.

Istnieją w zasadzie dwa różne modele bram płatniczych dla kart kredytowych. Jeden, w którym klient pyta o pewne produkty, załatwia sprawę z handlowcem i podaje mu dane dotyczące płatności, które sprzedawca przekazuje celem zainkasowania należności. W najprostszym przypadku handlowiec zatrzymuje u siebie na pewien czas dane z karty kredytowej (celem ewentualnego zwrotu).

W drugim modelu klient zamawia towar u dostawcy, który kieruje nabywcę do centrum rozliczeniowego (Clear Commerce, Open Market). Dane z kart kredytowych nie są tutaj w ogóle podawane

[24] APACS 30 definiuje metodę stosowaną w elektronicznym potwierdzaniu transakcji dokonywanych za pomocą kart kredytowych, podczas gdy APACS 50 definiuje transfer danych składających się na samą transakcję. Banki, obsługujące firmy handlowe, określają dolną granicę wartości dokonywanych transakcji, poniżej której sprzedający może dokonywać autoryzacji bez udziału banku, skanując „czarną listę" kart ukradzionych; transakcje o wartościach przekraczających podany limit są załatwiane poprzez bank za pomocą protokołu APACS 30. Ten proces związany jest tylko z autoryzacją i nie dotyczy transferu środków pieniężnych. Sposób działania systemu jest opisywany jako „w przeważającej mierze off-line".
Standard APACS 50 definiuje drugi zbiór protokołów, za pomocą których bank obsługujący handlowca łączy się z bramą płatniczą celem wczytania transakcji oraz zaktualizowania „czarnej listy". Informacja zebrana przez bank służy tym razem do transferu środków finansowych, co następuje w ciągu kilku dni.

sprzedawcy – kliknięcie opcji „kupuję" powoduje skierowanie danych pod adres logiczny URL (Unique Resource Locator), a po uaktywnieniu łącza następuje ich przekazanie (nabywca, handlowiec, towary, cena).

(sposób 4) ***Zastosowanie standardów SET***

Najlepsza metoda dokonywania płatności to taka, która gwarantuje tajność informacji, zapewniając do niej dostęp tylko osobom jej potrzebującym. Daje też każdej z zaangażowanych stron zaufanie odnośnie tożsamości wszystkich innych stron. Ponadto wszystkie zainteresowane osoby powinny mieć możność autoryzowania transakcji (tzn. ich podpisywania). Wszystkie te problemy ujęto w standardach SET (Secure Electronic Transactions).

Cała transakcja może być prowadzona poprzez sieć publiczną Internet do punktu, gdzie dane o tej transakcji zostają zaszyfrowane (tzn. do bramy płatniczej) tak, iż ma sens jej bliższe powiązanie z bankiem obsługującym handlowca.

Ryzyko

Ryzyko w transakcjach kartą kredytową. Najważniejsze rodzaje nadużyć przy transakcjach kartami kredytowymi obejmują:

- nieuprawnione używanie zgubionych lub skradzionych kart (około 50% wszystkich nadużyć związanych z kartami kredytowymi),
- używanie kart w sposób przestępczy (np. wykorzystywanie fałszywej tożsamości),
- podrabianie lub dokonywanie zmian na kartach,
- nieuprawnione posługiwanie się numerem posiadacza karty kredytowej,
- przestępcze działanie konsumenta.

Gdy posiadacz karty nie płaci swych zobowiązań, bank wydający kartę zmuszony jest płacić bankowi obsługującemu sprzedawcę.

Handlowiec ponosi odpowiedzialność za wszystkie koszty związane z fałszerstwami kart kredytowych. Aby tego uniknąć, musi uczynić przynajmniej jedną z trzech rzeczy:

- otrzymać autoryzację,
- podpis właściciela karty lub
- elektroniczny odcisk karty.

Sposoby redukujące ryzyko

Inne trendy technologiczne redukujące ryzyko w transakcjach kartą kredytową:

- Systemy oparte na sieciach neuronowych. Pozwalają bankom emitującym karty śledzić rodzaj wydatków właścicieli kart i wykrywanie wszelkich nietypowych zachowań klientów, a stąd i potencjalnych nadużyć. Na przykład, gdy właściciel

karty, dokonujący zazwyczaj niewielkich zakupów spożywczych, zaczyna w pewnym momencie kupować drogi sprzęt elektroniczny, system może powiadomić bank o potencjalnym przestępstwie.

- Służba weryfikacji adresów AVS (Adress Verification Service) pozwala firmom realizującym zamówienia przez telefon sprawdzać on-line adresy billingowe właścicieli kart kredytowych. Ten program ma na celu ograniczenie nieuprawnionego wykorzystywania numeru karty kredytowej właściciela. Używając AVS, firmy realizujące zamówienia przez telefon mogą porównać adres wysyłkowy dostarczony przez konsumenta z adresem billingowym znajdującym się w banku wydającym karty. Jeśli oba adresy są różne, pojawia się podejrzenie przestępstwa.

AVS

- Usługi rozliczeniowe wydawców kart płatniczych (ICS) System ICS pozwala bankom na porównywanie szczegółów dokonanej transakcji z bazą danych o nieważnych adresach i numerach ubezpieczeniowych (Social Security Number). Baza danych ICS zawiera takie informacje, jak numery ubezpieczeniowe, nazwiska i daty urodzenia osób posługujących się kartami kredytowymi.

ICS

4.3. Elektroniczny pieniądz

Elektroniczny pieniądz

Niezależnie od nadmiaru wyrafinowanych instrumentów płatniczych wymyślonych przez instytucje finansowe, stosowanie gotówki jest jednak ciągle jeszcze popularne. Ma to miejsce szczególnie w przypadku transakcji drobnych, lecz istnieją dziedziny biznesu, gdzie jest to powszechnie przyjęte. Koszty obrotu gotówkowego są jednak wysokie: IBM szacuje, że roczny koszt przeprowadzania transakcji gotówkowych na całym świecie sięga 30 miliardów euro, a jak wynika z badań przeprowadzonych przez Boston Consulting Group, koszty ponoszone przez detalistów i konsumentów w Wielkiej Brytanii wynoszą 4,5 miliarda funtów rocznie. Mówienie o „pieniądzu elektronicznym" może się komuś wydawać pomyleniem pojęć, lecz całkowicie realne jest utworzenie środka płatniczego mającego wszystkie cechy gotówki (chyba tylko z wyjątkiem takich wrażeń dotykowych, jak szelest banknotów czy brzęk monet!) i przesyłanego elektronicznie.

Karta pieniężna

Wiele systemów (z których najbardziej znanym jest Mondex) pozwala konsumentowi na dokonywanie płatności elektronicznych za pośrednictwem tak zwanej „karty pieniężnej". Wygląda ona tak samo, jak karta kredytowa, lecz różni się od niej pod kilkoma względami. Po pierwsze, inaczej niż karta kredytowa przechowuje ona pewną wartość pieniężną (a nie tylko dane dotyczące konta bankowego); po drugie, w momencie dokonania

transakcji pewna suma pieniędzy zostaje zdjęta z karty, jak pieniądz wyjęty z fizycznie istniejącego zwykłego portfela. Dlatego użytkownicy kart pieniężnych nie muszą posiadać konta w banku, a handlowcy nie potrzebują sprawdzać tożsamości posiadacza karty przy zakupach. Typowym rynkiem dla kart pieniężnych jest rynek transakcji o małych wartościach, zbyt małych, aby opłacało się korzystać z kart kredytowych bądź debetowych. Rynek ten ma więc dużo wspólnego z mikropłatnościami. Karta pieniężna może więc być uważana za przedpłatowy system mikropłatnościowy, w którym pieniądze przechowuje klient.

Karty ogólnego użytku

Niektóre karty pieniężne są nazywane kartami „celowymi" w tym sensie, iż mogą służyć do obsługiwania tylko jednego rodzaju płatności. Typowym przykładem są karty telefoniczne. Karty „ogólnego użytku" można stosować przy zakupach dóbr i usług u różnych sprzedawców. Niektóre z nich są jednorazowego użytku: są ładowane wstępnie do określonej kwoty pieniężnej, zmniejszającej się wraz z każdą transakcją, aż do wyczerpania się zadanej kwoty, po czym karta nie nadaje się już do użytku. Inne karty są jednak odnawialne i można je ładować wkładając do odpowiedniego urządzenia, takiego jak wyspecjalizowany bankomat bądź specjalny terminal podłączony do sieci telefonicznej. Jednym z celów e-biznesu jest umożliwić klientowi ładowanie swych kart pieniężnych za pośrednictwem komputera PC dołączonego do Internetu.

Ekonomiczna opłacalność kart opisanego typu nie została do dzisiaj dowiedziona. Jedną z głównych przeszkód jest obawa, że dla osiągnięcia pewnej masy krytycznej niezbędne są ogromne inwestycje w dziedzinie bankomatów, kas elektronicznych i innych urządzeń niezbędnych do obsługi opisywanego systemu[25].

[25] W Swindon zaoferowano odnawialne karty, ważne w większości miejscowych sklepów oraz przy płaceniu za telefony i autobusy. W praktyce używało tych kart 8000 osób. Spośród 1000 handlowców pracujących w Swindon, 750 zobowiązało się do akceptowania kart.
Za pośrednictwem franszyzy Mondex zainicjował 23 wdrożenia swego systemu w różnych krajach świata. W samym tylko Hongkongu do roku 1999 rozprowadzono 180 tysięcy kart, akceptowanych przez 300 banków, 700 bankomatów, 7000 firm (w tym 220 supermarketów), autobusy, baseny pływackie i inne instytucje.
Karta Mondex ma nie tylko zakodowane dane; zawiera bowiem komputer jednomodułowy z własnym systemem operacyjnym o nazwie MULTOS. Ten system operacyjny dopuszcza stosowanie wielu aplikacji napisanych przez różne firmy (i zapisanych na karcie w bezpieczny sposób). Co więcej, aplikacje te nie muszą być zapisywane przy produkcji karty: mogą być ładowane lub usuwane z karty, np. poprzez włożenie karty do odpowiedniego terminala. Obecnie istnieją dwa typy kart Mondex/MULTOS; jedna firmy Hitachi, a druga firmy Siemens. Tym, co różni kartę Mondex od innych jest fakt, iż ma ona wszystkie właściwości fizycznej gotówki: np. jedna osoba może przesyłać „gotówkę" innej osobie za pośrednictwem „portfela", do którego można włożyć obie karty. Tego typu transakcja może odbywać się bez pośrednictwa osób trzecich (tzn. banku).

4.4. Konta kredytowe

Konta kredytowe

Do tej pory rozpatrywaliśmy sytuacje, w których natychmiast po dokonaniu zakupu dokonuje się płatności (choć sama należność wypłacana z konta karty kredytowej może pozostawać przez pewien czas nie uregulowana). Często „konwencjonalne" transakcje nie są regulowane w momencie składania zamówienia: dobra zostają zakupione i sprzedawca rejestruje dane na koncie kredytowym. Po pewnym czasie (lub co pewien określony czas) sprzedawca przedstawia nabywcy fakturę, którą trzeba uregulować w określonym terminie. Jest to zwyczajny sposób postępowania w wypadku transakcji biznes–biznes (B2B) i niektórych transakcji biznes–konsument (B2C): jak np. rachunki telefoniczne i rachunki przedsiębiorstw użyteczności publicznej.

Część tego procesu dotycząca płatności nie różni się od przedstawionych uprzednio (tzn. fakturę można uregulować za pomocą karty kredytowej, stałego zlecenia przelewu lub gotówką). Gdy jednak chcemy płacić nasze rachunki on-line, warto otrzymywać je także on-line. Dlatego najważniejszą sprawą do rozpatrzenia jest dostarczanie faktur przez Internet. Proces ten nazywa się przedstawianiem rachunku i tego ostatniego terminu będziemy dalej używać.

Przedstawianie rachunku

Przedstawianie rachunku elektronicznie nie tylko pozwala na bezpośrednie zastępowanie rachunków papierowych, ale oferuje nowe możliwości, takie jak sprawdzanie dowolnych rachunków w dowolnym czasie, a nie tylko ich otrzymywanie po upływie pewnego ustalonego terminu. Wynikają stąd następujące zagadnienia:

- przedstawianie informacji billingowej on-line;
- integracja z systemem przetwarzania w celu umożliwienia dodatkowych opcji billingowych takich, jak oglądanie rachunków w czasie rzeczywistym;
- spełnienie wymagań prawnych łącznie z prawem podatkowym;
- łączenie rachunku z następującą po niej płatnością elektroniczną.

Proces billingu

Konwencjonalny proces billingu obejmuje czynności:

- zbieranie informacji o zdarzeniach związanych z billingiem. Mogą nimi być np. liczba sekund spędzonych na wykorzystywaniu pewnego serwisu on-line, czy też zakup dóbr. Informacje te należy zbierać w czasie rzeczywistym i muszą one być dostarczane w standardowych formatach;
- wyznaczanie ceny i obciążanie kosztami. Dokonuje się tego na podstawie portfela produktów i usług, gdzie podane są ceny każdego składnika i pakietu (np. bezpłatne korzystanie z serwera WWW pod warunkiem jednoczesnego zakupu usługi regulowania rachunków);
- obniżanie cen. Rabaty przyznawane pewnym klientom (zwykle na podstawie ich wielkości i siły nabywczej);
- agregacja i zbieranie danych. Sporządzanie rachunku danego klienta przeprowadzane jest na podstawie wszystkich zaku-

pionych przez niego towarów i usług oraz rabatów przyznanych temu klientowi i na towary. W przypadku indywidualnego klienta jest to operacja prosta, lecz może być bardzo skomplikowana w odniesieniu do dużego przedsiębiorstwa;
- drukowanie rachunku. Jest zwykle procesem wsadowym uruchamianym w odpowiednim czasie celem wygenerowania rachunku.

Rachunek elektroniczny

W e-biznesie ten ostatni etap należy zmodyfikować, aby wytworzyć rachunek elektroniczny. W najprostszym przypadku można zmodyfikować go otrzymując inny proces wsadowy, generujący e-mail, zawierający informację o billingu. Przejmując jednak proces billingu na wcześniejszym etapie, uzyskamy możliwość oferowania serwisu billingowego on-line, co stanowi już znaczne zbliżenie do ideału, jakim jest proces przebiegający w czasie rzeczywistym.

Internet otwiera nie tylko możliwość oglądania swoich rachunków w trybie on-line, lecz zarazem szansę utworzenia powszechnie dostępnej izby rozrachunkowej dla rachunków lub usługowego biura billingowego.

W tym wypadku klient będzie miał pojedyncze konto, na które wpływają rachunki z wielu źródeł (takich, jak instytucje użyteczności publicznej, firmy obsługujące karty kredytowe, karty sklepowe itd.). Biuro to stanowi punkt odniesienia dla wszystkiego, co klient posiada. Daje również możliwość wglądu we wszystkie dotychczas otrzymane rachunki, umożliwiając tym samym wyszukiwanie ewentualnych anomalii.

W tym przykładzie usługi opłacane są przez wielkie firmy. Ich motywacja jest jasna (i warta przedstawienia); jako klienci dokonujący wielkich zakupów, oszczędzają pieniądze na elektronicznym handlu, a ich dostawcy są motywowani tym, że mogą dostać się na listę kwalifikowanych dostawców największych korporacji jedynie wtedy, gdy będą obecni on-line. Dlatego sprzedawcy używają swej siły nabywczej jako dźwigni stymulującej rozwój e-biznesu.

Biuro obejmuje oddzielne konto dla każdego konsumenta. Rachunki z różnych źródeł (takich jak instytucje użyteczności publicznej, sklepy itp.) dostarczane są do biura[26]. Instytucjom generującym rachunki daje to oszczędności na kosztach druku i wysyłki pocztą (są firmy, gdzie idą one w miliony). Do tego dochodzą jeszcze zyski pośrednie płynące z lepszego zorganizowania wierzycieli.

[26] Konsument może przeglądać je bez pośpiechu i w dowolnym miejscu. Wystarczy kliknąć w pole z napisem „pay", aby rachunek został zapłacony. Pojedynczą „skrzynkę pocztową" na rachunki można tak przerobić na życzenie klienta, aby przykładowo krótka wiadomość typu SMS mogła być wysłana do klienta zaraz po nadejściu nowego rachunku. Klienci mogą tym sposobem porównywać napływające rachunki z zestawieniem rachunków dotychczas otrzymanych (billingiem).

4.5. Płacenie rachunków

Płacenie rachunków

Przedstawienie rachunku jest dopiero pierwszym etapem całego procesu. Usługi elektronicznego opłacania rachunków są oferowane przez wiele banków i innych instytucji, gotowych (za darmo) płacić po uprzedniej autoryzacji wyznaczone rachunki w imieniu konsumenta. Takie płatności mogą być dokonywane elektronicznie lub drukowanym czekiem papierowym. W wypadku gdy beneficjent nie akceptuje płatności elektronicznych, instytucja świadcząca usługi płatnicze drukuje i wysyła czek w imieniu konsumenta. Ten rodzaj systemu płatniczego nie różni się wiele od ręcznego wypisywania czeku przez klienta: jedyna różnica polega na dostarczaniu czeku beneficjentowi za pośrednictwem scentralizowanego systemu komputerowego.

Usługi płatnicze banków

Niektóre banki świadczą usługi płatnicze swoim klientom lub kontaktują się z zewnętrznym elektronicznym serwisem płatniczym, aby zapewnić tę usługę klientom banku. Konsumenci mogą się dodatkowo niezależnie kontaktować z elektronicznym serwisem płatniczym; w tym przypadku, między bankiem a serwisem nie istnieje żaden kontrakt. Klient, komunikując się z systemem płatniczym, posługuje się komputerem domowym wyposażonym w modem i odpowiednie oprogramowanie. Wiadomości transmitowane są za pośrednictwem prywatnej sieci telekomunikacyjnej (a nie przez Internet).

Operatorzy elektronicznych systemów płatniczych zalecają, aby konsument dokonywał płatności na trzy do czterech dni przed upływem obowiązującego terminu, gdyż może zaistnieć konieczność uregulowania należności drogą pocztową zamiast elektronicznej i musi być czas na dokonanie rozrachunku.

4.6. Czeki elektroniczne

Czeki elektroniczne

Czek papierowy jest popularnym instrumentem płatniczym używanym przez pojedyncze osoby, firmy i rządy, przy regulowaniu należności za towary i usługi.

MICR

Informacja podawana na czekach papierowych obejmuje nazwy płatnika i beneficjenta, kwotę czeku i nazwę banku płatnika. Pole widniejące na dole czeku (Magnetic lnk Character Recognition (MICR)) zawiera bankowy kod porządkowy (identyfikujący bank płatnika), numer konta płatnika i numer identyfikacyjny samego czeku. Pole MICR umożliwia obróbkę czeku za pomocą szybkich urządzeń przetwarzających. Na wstępie tego procesu kwota czeku zostaje zakodowana na dole czeku za pomocą atramentu magnetycznego.

Większość indywidualnych klientów usługi biura billingowego uzna za miłą alternatywę dokumentu papierowego, który zdaje się ginąć, ilekroć jest najbardziej potrzebny. Perspektywa posiadania konfigurowalnej poczty elektronicznej lub zawiadomień otrzymywanych poprzez SMS stwarza wielu klientom nadzieję uniknięcia dodatkowych opłat za zbyt późne regulowanie rachunków.

Czeki „na siebie”

Istnieją różne sposoby rozliczania czeków. Gdy czeki deponowane są w tym samym banku, na który zostały wystawione, odpowiednie transakcje reguluje się na miejscu i takie czeki są nazywane czekami „na siebie” (on–us).

Przez ostatnie kilka lat niektóre z największych zrzeszeń izb rozrachunkowych w USA, przemysł bankowy OSA i Bank Centralny USA (US Federal Reserve) aktywnie pracowały nad rozwojem nowej technologii, mającej na celu skrócenie czasu rozliczania i regulowania czeków, polepszając w ten sposób efektywność całego systemu płatniczego.

Ta nowa technologia obróbki czeków znana jest pod nazwą Electronic Cheque Presentment (ECP). ECP jest procesem, w którym informacja zawarta w polu MICR czeku jest przesyłana elektronicznie do banku płacącego czek. Część dużych banków komercyjnych należy do utworzonej w roku 1990 organizacji o nazwie Electronic Cheque Clearing House Organization (ECCHO). ECCHO opracowuje przepisy i projektuje formaty elektronicznego przetwarzania czeków dla banków będących jej członkami.

Banki należące do ECCHO mogą więc wymieniać między sobą dane z czeków elektronicznie, zanim czeki papierowe zostaną fizycznie przedstawione do wypłaty.

„Ścinanie” czeku

Technologia ECP może obejmować „ścinanie” czeku i zostać wsparta techniką zobrazowywania czeku. „Ścinanie” jest procesem, w którym fizycznie istniejące czeki papierowe zostają zatrzymane w pewnym punkcie procesu obróbki i tylko informacja zapisana na czekach zostaje wysłana dalej do banku płacącego za czek. ECCHO opracowuje zbiór narodowych przepisów ścinania czeków. Zobrazowywanie czeków jest to proces, w którym tworzy się obrazy obu stron czeku i zapisuje w sposób elektroniczny, aby wykorzystać w razie potrzeby.

Choć ścinanie i zobrazowywanie czeków jest coraz częściej stosowane, nie jest jasne, ile czeków będzie przetwarzane tym sposobem w dającej się przewidzieć przyszłości.

Niechęć niektórych banków do inwestowania w rozwój technologii i preferowanie przez konsumentów czeków zwrotnych może w istotny sposób ograniczać ścinanie i zobrazowywanie czeków. Jeden z urzędników banku Federal Reserve przewiduje, że ścinanie czeków nie będzie powszechnie stosowane do czasu, aż konsumenci zaakceptują fakt, iż ich czeki nie będą im fizycznie wydawane. Ponadto, zgodnie z obecnie obowiązującymi przepisami, banki depozytowe muszą fizycznie przedstawiać czeki bankom je płacącym, aby otrzymać ich rozliczenie.

4.7. Agregacja płatności

Gdy mamy do czynienia z transakcjami elektronicznymi, spotykamy się z rozmaitą skalą płatności: takie towary, jak np. książki są regularnie kupowane przez Internet (np. poprzez Amazon.com), a typowy pojedynczy klient kupuje zwykle jedną książkę dokonując jednostkowej transakcji z użyciem karty kredytowej. Koszt przetwarzania danych z karty kredytowej dla takiej transakcji jest jednak dosyć wysoki i może się nie opłacać w przypadku zakupu towarów o małej wartości, takich jak raporty konsumenckie lub płyty CD. Istnieją specjalne metody realizacji tych niewielkich płatności (zwanych „mikropłatnościami"), polegające na łączeniu ich w większe transakcje. Przy cenach poniżej równowartości 1 USD mówi się nawet o obszarze „nanopłatności". Płatności tego rodzaju mogą stanowić np. opłaty za korzystanie z pojedynczych informacyjnych stron internetowych – podających np. bieżące ceny akcji.

Mikropłatności

Agregacja (łączenie) płatności może zachodzić po stronie serwera lub po stronie klienta. Obecnie pracujące systemy działają zwykle z wykorzystaniem serwera, gdyż po stronie klienta zabezpieczenie informacji dotyczącej płatności jest trudne. Przykładowo, działanie prostych systemów agregacji płatności po stronie klienta może zostać zawieszone po prostu przez usunięcie danego pliku. Zwykłym sposobem rozwiązania problemu jest więc przechowywanie konta użytkownika na serwerze i zapisywanie tam każdej transakcji dokonywanej przez tego użytkownika. Systemy z agregacją po stronie klienta, choć trudniejsze do implementacji, mają pewne zalety: są dogodniejsze przy aplikacjach używanych przez bardzo wielką liczbę użytkowników (ponieważ cała informacja o kontach bardzo dużej liczby konsumentów nie musi być gromadzona w sposób scentralizowany). Oferują one takie opcje, jak „portfele elektroniczne" noszone przez konsumenta, a co jeszcze ważniejsze – nadają się do systemów płatniczych powszechnego użytku nie powiązanych z określoną aplikacją biznesową. Przykładowo, to samo urządzenie może zapisywać koszty korzystania z wielu różnych usług internetowych.

Łączenie płatności

Portfele elektroniczne

Możemy wybierać między systemami z agregacją po stronie serwera lub po stronie klienta, taki też istnieje wybór między przedpłatą i zapłatą po otrzymaniu towaru lub usługi. Innymi słowy, gdy oferujemy klientom wiele tanich produktów, za które będą oni kumulować mikropłatności, możemy żądać od nich zapłaty za pewną minimalną liczbę transakcji, zanim zaczną kupować (a następnie rejestrować wykorzystany już „kredyt"). Możemy również rejestrować wartość każdej transakcji i czekać, aż klient osiągnie pewien próg, zanim obciążymy jego konto.

Przykład systemu przedpłatowego można znaleźć na stronie WWW firmy Scottish Register Office (www.origins.net). Sys-

System przedpłatowy

tem ten umożliwia klientom w trybie on-line poszukiwanie świadectw urodzin, ślubów i zgonów, a następnie ich zamawianie. Przed uzyskaniem pozwolenia na poszukiwanie konkretnego dokumentu klienci muszą się zarejestrować oraz dokonać płatności kartą kredytową. W czasie pisania książki minimalna opłata wynosiła 6 funtów. Dokonując tej zapłaty on-line klienci otrzymują kredyt odpowiadający przeszukaniu 30 stron wyświetlanych na ekranie. Mogą wówczas rozpocząć poszukiwanie, np. wszystkich osób o imieniu i nazwisku Hamish Robert Brown, których urodzenia zarejestrowano w grudniu 1851 roku. Lista takich osób może zajmować jedną lub więcej stron ekranu i za każdym razem, gdy wchodzimy na stronę, system zmniejsza liczbę stron kredytowanych. Gdy klient przeszuka wszystkie 30 stron i licznik wyzerowano, trzeba od nowa wprowadzić dane z karty kredytowej dokonując tym samym następnej płatności[27].

Agregacja różnych kategorii małych płatności wymaga nie tylko różnych technologii, lecz w przypadku e-biznesu potrzeba także różnych strategii. Obejmują one:

Przedpłatę:
- Konsument jest obciążany przed zakupem. Jego konto jest obciążane przy każdym zakupie;
- Mniejsze ryzyko dla handlowca (karta kredytowa może być obciążona zanim towar zostanie zakupiony);
- Potencjalni klienci mogą zostać zniechęceni wstępnymi kosztami. Osoby kupujące kredyty, a potem dokonujące mało zakupów mogą być niezadowoleni z takiej usługi.

Zapłatę z dołu:
- Ceny zakupów są dodawane, aż do przekroczenia pewnego progu (i/lub limitu czasowego), kiedy to następuje zapłata.

Kłopoty z kartą kredytową mogą się pojawić, gdy nadejdzie termin płatności (np. nieważna karta). Dane z karty kredytowej muszą być przechowywane (co stawia handlowcowi dodatkowe wymagania odnośnie bezpieczeństwa). Niektóre regulacje prawne interpretują to jako oferowanie kredytu, co sprawia, że handlowiec podlega przepisom dotyczącym udzielania kredytów konsumpcyjnych.

[27] Przykładem systemu z zapłatą po otrzymaniu towaru lub usługi jest BT Array. Klienci muszą wprowadzić dane z karty kredytowej przy rejestracji do systemu. Mogą wówczas dokonywać zakupów, a ich konto w systemie będzie obciążane (choć jeszcze bez dokonywania żadnej transakcji finansowej). Gdy suma (którą są winni) przekroczy pewien próg (zwykle 30 funtów), ich karta kredytowa zostanie obciążona do wyzerowania długu. W praktyce dokonuje się takiej samej płatności kartą kredytową po przekroczeniu pewnego limitu czasowego.

4.8. Transfer środków finansowych

Transfer środków finansowych

Na początku tego rozdziału powiedzieliśmy, że będziemy się koncentrować na powiązaniach istniejących pomiędzy posiadaczem karty a handlowcem oraz między handlowcem a jego bankiem. Pomijaliśmy przy tym interakcje pomiędzy samymi instytucjami finansowymi, takimi jak bank wydający kartę i bank obsługujący handlowca.

Te „zakulisowe" interakcje są domeną elektronicznego transferu funduszy EFT. Trzy najważniejsze systemy transferowe to: globalny system SWIFT oraz Fedwire i CHIPS.

Serwis transferowy

Serwis transferowy Banku Rezerwy Federalnej Fedwire, używany pierwotnie do regulowania płatności na terenie USA, jest systemem pracującym w czasie rzeczywistym, w którym Bank Rezerwy Federalnej gwarantuje zapłatę odbiorcy funduszy. CHIPS, organizacja dokonująca rozliczeń multilateralnych sektora prywatnego, zajmuje się głównie rozliczeniami transakcji wymiany międzynarodowej zdenominowanymi w dolarach.

W roku 1996 średnia wartość transakcji dziennych dokonywanych za pomocą serwisu transferowego Fedwire sięgała 989 miliardów dolarów, a średnia suma na jedną transakcję wynosiła 3 miliony dolarów. Średnia wartość transakcji dziennych przy wykorzystaniu serwisu CHIPS była równa 1,3 biliona dolarów, a średnia suma na jedną transakcję wynosiła 6,2 miliona dolarów.

4.8.1. SWIFT

SWIFT

Firma Society for Worldwide Interbank Financial Telecommunication (SWIFT), z siedzibą w Belgii, funkcjonuje na zasadach spółdzielni, w skład której wchodzi ponad 2800 banków z całego świata, włączając w to 150 banków z USA. Założono ją we wczesnych latach 70. Kieruje ona siecią przetwarzania i przesyłania komunikatów finansowych pomiędzy instytucjami członkowskimi i innymi użytkownikami w 137 krajach. W czasie pisania książki obsługiwała ona ponad 6000 instytucji finansowych w 178 krajach.

W roku 1998 ogólnoświatowa sieć SWIFT przesłała ponad 900 milionów komunikatów, których średnia wartość dzienna przekraczała 2 miliardy dolarów USA.

Dzisiaj, poza 2800 bankami członkowskimi, użytkownikami systemu SWIFT są zarówno członkowie stowarzyszeni i tacy uczestnicy, jak brokerzy, dyrektorzy działów inwestycji, depozyty papierów wartościowych, organizacje rozrachunkowe i giełdy.

Komunikaty systemu

Komunikaty systemu SWIFT przesyłają informacje lub instrukcje między instytucjami finansowymi: komunikaty są formatowane i zawierają informację o nadawcy, celu, przeznaczeniu, warunkach i odbiorcy. System SWIFT jest najczęściej używany do obsługi ko-

munikatów o płatnościach, poprzez które jedna instytucja przesyła drugiej instytucji instrukcje dotyczące dokonywania danej płatności. Inne komunikaty mają na celu potwierdzanie szczegółów kontraktów zawieranych pomiędzy dwoma użytkownikami, w ramach międzynarodowej wymiany handlowej lub w dziedzinie lokat międzybankowych.

W dziedzinie papierów wartościowych komunikaty SWIFT mogą zawierać polecenia kupna lub sprzedaży bądź przenosić instrukcje dotyczące spedycji lub rozliczeń[28].

Jakość usług systemu SWIFT

Jakość usług systemu SWIFT

SWIFT jest systemem pracującym prawie w czasie rzeczywistym. Choć jest on oparty na architekturze typu zapamiętaj i wyślij, komunikaty i pliki są przetwarzane natychmiast.

Gdy zatem nadawca i odbiorca są połączeni ze sobą on-line, przesłanie komunikatu trwa zazwyczaj mniej niż 20 s, nawet w międzynarodowej wymianie komunikatów.

SWIFT udziela gwarancji finansowych przy dostarczaniu wszystkich komunikatów wysłanych poprzez jego sieć. SWIFT odpowiada za bezpośrednie szkody materialne wynikłe na skutek uwierzytelnionych płatności lub transferów, jakie nie doszły do skutku.

Jest także zapewniony pełny monitoring, a system jest dostępny 24 godziny na dobę, przez 7 dni w tygodniu.

Aplikacje i usługi systemu SWIFT

Aplikacje i usługi systemu SWIFT

Podstawowy serwis komunikatów zapamiętaj i wyślij ma markę FIN, ma również wiele rozszerzeń takich, jak FINcopy (dostarczający kopie komunikatów stronom trzecim, aby wspomagać pewne

[28] Sieć SWIFT oparta jest na protokole komutacji pakietów X.25 wykonywanym na liniach dzierżawionych i komutowanych. Klienci (np. banki oraz instytucje finansowe) podłączają się do tej sieci poprzez lokalne „punkty dostępu" (tzn. punkty obecności), do których są dołączeni poprzez linie dzierżawione lub, w pewnych krajach, poprzez publiczne sieci teleinformatyczne, takie jak Transpac, Accunet i Sprintnet. Klienci muszą przy tym korzystać z interfejsów dopuszczonych przez SWIFT, umieszczanych między ich własnymi systemami a siecią. Interfejsy te są dostarczane bądź bezpośrednio przez SWIFT, bądź przez inne firmy.
System przetwarzania instrukcji jest siecią serwerów wybierających drogę komunikatów i monitorujących przepływ tych informacji w sieci. Systemy komputerowe są zdublowane w dwu centrach operacyjnych (jedno w USA, a drugie w Holandii) celem uzyskania ich większej elastyczności.
Centra operacyjne zawierają trzy typy układów przetwarzających:

- Procesory regionalne będące „zewnętrzną warstwą" przetwarzania. Sterują one przepływem informacji od i do punktów dostępu, monitorując komunikaty przychodzące i wychodzące z systemu, sprawdzając przy tym ich składnię oraz integralność. Przekazują komunikaty do „wewnętrznej warstwy" tak zwanych procesorów segmentowych.
- Procesory segmentowe stanowią rdzeń infrastruktury typu zapamiętaj i wyślij. Ponadto generują kopie komunikatów (celem monitoringu) oraz wysyłają nadawcy potwierdzenie po odebraniu każdego komunikatu.

transakcje finansowe, takie jak clearing, rozliczanie i regulowanie rachunków) oraz FINInform (umożliwiający kopiowanie komunikatów dla stron trzecich w ramach tej samej instytucji finansowej).

Serwis transferu dużych plików umożliwia pracę w trybie zapamiętaj i wyślij dla niestrukturalnych plików zawierających dowolną ilość danych. Jest on oparty na standardach przesyłania komunikatów X.400.

Inne rodzaje usług, typowe dla sektora finansowego, to m.in. dobieranie (matching – automatyczne legalizowanie i uzgadnianie kontraktów) oraz rozliczenia bilateralne (netting).

W finansach stosuje się pojęcie przetwarzania kompletnego STP (Straight Through Procecssing), oznaczającego zdolność do całkowitego zautomatyzowania procesu bez interwencji ręcznych. Komunikaty strukturalne w systemie SWIFT są podatne na automatyczny rozbiór i przetwarzanie. SWIFT realizuje to oferując usługę pod nazwą serwis analizy ruchu, pozwalający rozróżnić „czyste" komunikaty od takich, które mogą spowodować kłopoty dla zautomatyzowanego terminala.

Standard bezpieczeństwa ISO 15022

Standard bezpieczeństwa

Podstawowym obowiązującym obecnie standardem międzynarodowym dotyczącym dokumentów jest standard bezpieczeństwa ISO, a mianowicie ISO 15022 „Zabezpieczenia – Schemat dla dokumentów (słownik pola danych)". Zastępuje on dwa poprzednie standardy międzynarodowe dla dokumentów elektronicznych wymienianych między firmami działającymi w sektorze zabezpieczeń: ISO 7775 – „Schemat dla typów dokumentów" oraz ISO 11521 –

- Procesory sterujące systemu zarządzają całym systemem, monitorują jego działanie, administrują siecią i wspomagają zadania eksploatacyjne. Sieć SWIFT tak zaprojektowano, by sprostała wielu zagrożeniom, takim jak złośliwe lub oszukańcze użycie sieci, ataki na zasoby fizyczne lub klęski żywiołowe. Dalej podamy przykładowe zabezpieczenia.
- Sieć prywatna: SWIFT jest oparta na sieci prywatnej (a nie na publicznej, jak Internet), co zmniejsza podatność na ataki przypadkowych hakerów internetowych.
- Sprawdzanie poprawności komunikatów: komunikaty są sprawdzane na zgodność z regułami składni i formatami: obecność niezbędnych pól, ciągów odpowiednich znaczników, rozkazów itd.
- Sprawdzanie kolejności komunikatorów: wszystkie komunikaty systemu SWIFT mają przypisywane jednoznacznie kolejne liczby przy wchodzeniu oraz wychodzeniu z systemu. Liczby te są sprawdzane w momencie nadawania i odbioru, komunikaty odebrane w niewłaściwej kolejności są odrzucane, a odpowiadające im połączenie z terminalem przerywane.
- Integralność komunikatu: gdy komunikat trafia na wejście sieci SWIFT, generowany jest „kod uwierzytelniający komunikatu" zgodny z jego zawartością. Proces ten przypomina tworzenie „skrótu komunikatu". Pozwala on upewnić się, że komunikat jest bezpieczny pod względem przypadkowych (lub umyślnych) zmian, jakie mogą zostać dokonane w czasie jego przesyłania.
- Silne uwierzytelnienie z logowaniem: jest oparte na inteligentnych kartach i wymianie elektronicznych kluczy uwierzytelniających.
- Szyfrowanie danych: dane są szyfrowane w sieci od jednego do drugiego punktu dostępu, a opcjonalnie także do interfejsu użytkownika. Dlatego komunikaty są chronione przed wglądem ze strony pracowników systemu SWIFT tak podczas przesyłania, jak w czasie przechowywania w systemie.

„Schemat dla typów dokumentów wymienianych pomiędzy depozytariuszami".

Standard ISO 15022 zawiera zbiór reguł składniowych i reguł tworzenia dokumentów, słownik pól danych oraz katalog dla obecnych i przyszłych dokumentów.

Zawartość słownika pól danych i katalogu dokumentów pozostają poza standardem, lecz są sprawdzane przez biuro rejestrowe. ISO mianował SWIFT jako biuro rejestrowe dla normy ISO 15022.

SWIFT doprowadził zbiór swoich dokumentów do stanu zgodności z normą ISO 15022 i rejestruje szczegółowe pola danych w biurze rejestrowym.

EDIF ACT

Istnieje jeszcze inny standard dokumentów, jest on kontrolowany przez EDIF ACT (Electronic Data Interchange for Administration, Commerce and TrancsSport). Serwis SWIFT będzie przesyłał standardowe komunikaty płatnicze dla EDIFACT. Komunikaty SWIFT podzielono na dziesięć głównych kategorii[29]:

1. Informacja ogólna,
2. Transfery klientów,
3. Transfery instytucji finansowych,
4. Handel finansowy,
5. Inkaso i listy gotówkowe,
6. Handel finansowy (papiery wartościowe),
7. Handel metalami szlachetnymi i ich reasekuracje,
8. Kredyty i gwarancje dokumentowe,
9. Czeki podróżne,
10. Zarządzanie gotówką i status klienta.

4.9. Bezpieczeństwo i ochrona

Bezpieczeństwo i ochrona

Nowe technologie elektroniczne stosowane obecnie lub znajdujące się w fazie przygotowań, takie jak internetowe transakcje finansowe, pieniądz elektroniczny czy karty gotówkowe obiecują konsumentowi szeroki wybór sposobów dokonywania płatności.

Technologie te niosą jednocześnie nowe ryzyko nadużyć i nielegalnej działalności. Środowiska prawnicze zainteresowane wzmocnieniem prawa wyrażają zaniepokojenie, wskazując na możliwość wykorzystania tych nowych produktów i usług w celach nielegalnych, takich jak pranie brudnych pieniędzy. Niektóre formy działań przestępczych dotyczących transakcji prowadzonych za pośrednictwem Internetu już ujawniono. Ciągle trwają prace mające na celu uczynienie elektronicznych produktów i usług bardziej bezpiecznymi oraz mniej podatnymi na nielegalne wykorzystanie.

[29] Najpopularniejsze standardy stosowane w USA, które powoli znajdują swoje zastosowania w naszym kraju opisane są w Aneksie 1.

Klienci mają teraz poprzez Internet dostęp do kartowych systemów płatniczych, bankowości elektronicznej i innych usług finansowych w stopniu, jaki nigdy nie był dotąd możliwy. Wymienione usługi oferują klientowi wiele nowych, dogodnych metod dokonywania transakcji finansowych. Ze względu jednak na samą naturę Internetu – będącego w zasadzie nie zabezpieczonym środkiem przesyłania informacji – klienci, handlowcy i inni dostarczyciele usług są coraz bardziej zainteresowani sprawami bezpieczeństwa i ochrony prowadzonych przez nich transakcji. Dla przykładu, jeśli intruz z powodzeniem zaatakuje system kart kredytowych, klienci zostają narażeni na utratę dostępu do swych kont, a w najgorszym razie cały system kart kredytowych upadnie.

Firewall

Firewall i inne metody filtrowania informacji przychodzącej z Internetu do komputera mogą po części zwiększyć bezpieczeństwo transakcji internetowych. Firewall jest metodą zabezpieczenia się przed intruzami poprzez ograniczenie informacji przychodzących do sieci wewnętrznych handlowców oraz instytucji finansowych. Szyfrowanie jest innym środkiem zwiększenia bezpieczeństwa transakcji internetowych. Ani Firewall, ani szyfrowanie nie dają jednak gwarancji bezpieczeństwa tych transakcji. O ile transakcje finansowe prowadzone poprzez Internet będą coraz mniej wrażliwe na ataki ze strony intruzów lub przejęcie przez nieuprawnione strony trzecie, klienci będą się skłaniać ku zwiększaniu użycia Internetu w działalności finansowej, a każdy większy udany atak będzie zmniejszać publiczne zaufanie do handlu elektronicznego w ogóle.

Przestępstwa internetowe

Niezależnie od podstawowego problemu zapewnienia jego bezpieczeństwa Internet stanowi też dla kryminalistów źródło nowego rodzaju przestępstw popełnianych na niekorzyść konsumenta. Przestępstwa tego rodzaju są ryzykowne dla klientów, gdyż Internet stanowi stosunkowo łatwy i opłacalny ekonomicznie środek dostępu do milionów osób.

Instytucje stanowiące prawo wzmacniają swoje wysiłki w celu identyfikacji oraz zapobiegania takim działaniom, lecz trzeba się dopiero przekonać, czy wysiłki te nadążają za narastającym wykorzystywaniem handlu elektronicznego oraz Internetu do działalności przestępczej.

Nowe technologie, takie jak stosowanie Internetu w transakcjach finansowych oraz karty pieniężne, stwarzają w dodatku nowe możliwości prania brudnych pieniędzy.

Instytucje stanowiące prawo są szczególnie zainteresowane internetowymi i kartowymi systemami, pozwalającymi na transfery między poszczególnymi osobami. Karty pieniężne umożliwiają bowiem przestępcom łatwe przenoszenie brudnych pieniędzy z konta bankowego na kartę pieniężną, gdzie mogą być wydawane bez pozostawiania śladów.

Ponieważ jednak karty tego rodzaju są zwykle przystosowane do transakcji o małej wartości, to przy obecnie stosowanych niskich limitach przechowywanej na nich waluty (około 500 USD) nie są one zbyt ekonomicznym sposobem prania dużych pieniędzy.

4.9.1. Działania standaryzacyjne

Działalność organizacji opracowujących standardy w dziedzinie zaufania i bezpieczeństwa pracy organizacji płatniczych koncentruje się w czterech głównych dziedzinach[30]:

Protokoły płatnicze

- *Protokoły płatnicze:* definiują dwie lub większą liczbę ról przyjmowanych przez podmioty elektroniczne uczestniczące w wymianie komunikatów dotyczących transakcji tak, że płatność może mieć miejsce. Uwierzytelnianie posiadacza karty, handlowca i banków uczestniczących w transakcji jest prowadzone przez jeden lub więcej takich protokołów. To samo dotyczy tajności oraz integralności danych płatniczych. Podstawowe standardy rozwijane w tej dziedzinie, jakimi należy się zainteresować i ewentualnie wprowadzić, to SET, EMV, Mondex i Visa Cash. Standard SSL jest obecnie szeroko stosowany przy płatnościach dokonywanych za pośrednictwem Internetu głównie dlatego, że jest on wbudowany w każdą przeglądarkę. Brakuje mu jednak tej bardziej wszechstronnej struktury bezpieczeństwa, obecnej w pozostałych standardach.

Protokoły handlowe

- *Protokoły handlowe* sklepowe: o szerszym zakresie niż protokoły płatnicze (lecz te ostatnie mogą być do nich włączane), odnoszą się do zdarzeń obejmujących cały przebieg transakcji, włączając w to negocjacje warunków, fakturowanie, księgowanie, wycenę, spedycję itd. Najważniejszym i protokołami tego rodzaju są: Internet Open Trading Protocol (IOTP)[31], przyjęty już przez firmę Internet Engineering Task Force (IETF) oraz Open Buying Protocol (OBI) oparty na protokole internetowym, dostosowanym przede wszystkim do działalności typu biznes–biznes (B2B) i opisywanym jako „EDI – sieć". Jest bardzo prawdopodobne, iż rządy Niemiec i Wielkiej Brytanii przyjmą protokół IOTP dla transakcji internetowych obciążonych podatkiem od wartości dodanej.

Standardy czytników

- *Standardy czytników* i systemów operacyjnych dla kart inteligentnych: dziedzina kart inteligentnych ucierpiała z powodu nadmiaru rozwiązań stanowiących własność firm, promowanych zwykle przez wpływowych niegdyś wytwórców kart. W związku z zainteresowaniem przemysłu softwarowego i technologii informacyjnej dziedziną kart inteligentnych, zarówno Microsoft

[30] Pomimo iż są to rozwiązania głównie pochodzące z USA, wszystkie te standardy znajdują swoje zastosowanie w mniejszym lub większym stopniu w polskim e-biznesie.

[31] Protokół Otwartego Handlu za pośrednictwem Internetu – protokół OTP dla przeprowadzania transakcji za pośrednictwem Internetu.

(PC/SC) jak SUN/IBM (Opencard) promują ostatnio „otwarte" rozwiązania konstrukcyjne interfejsów dla czytników tych kart.
- Bezpieczeństwo oparte na standardzie IP: „IP Sec" jest standardem sponsorowanym przez IETF.

Działają obecnie różne konsorcja produkujące specyfikacje zarówno dla ogólnej działalności handlowej, jak i poszczególnych protokołów płatniczych. Konsorcja te są motorem rozwoju e-biznesu w sytuacji, gdy obecna proliferacja (nadmiar) rozwiązań stanowiących własność firm zmusza detalistów do inwestowania w coś, co ma krótki żywot. Niezależnie od wymienionego już protokołu SET opiszemy jeszcze trzy konsorcja o podstawowym znaczeniu:

Internet Engineering Task Force

- *Internet Engineering Task Force*: firma IETF przejęła obecnie protokół OTP[32] od jego pierwotnego właściciela konsorcjum OTP, w którym główną rolę odgrywał Mondex. Ponieważ Mondex jest jedynie protokołem płatniczym, istnieje potrzeba protokołów handlowych wyższego poziomu, określających środowisko, w którym płatności mogą być realizowane. Te protokoły wyższego poziomu obejmują takie zagadnienia, jak negocjowanie warunków, fakturowanie, księgowanie, spedycję itd. Niektórzy z głównych operatorów elektronicznych systemów płatniczych (Cybercash, Mondex, Globe ID) działali według oryginalnych specyfikacji OTP i dlatego jest bardzo prawdopodobne, iż elementy ich systemów nie dotyczące płatności zostaną przeniesione do wspólnego zbioru protokołów.

World Wide Web Consortium

- *World Wide Web Consortium:* firma W3C opracowywała protokół o nazwie Micro Payment Transfer Protocol (MPTP) od 1995 roku. Ostatnio prowadzona działalność grupy mikropłatności W3C dotyczyła protokołu płatniczego API. Ta koncepcja zakłada istnienie portfela klienta użytkownika, lecz zakładając użycie języka XML, konsekwencją może być zdefiniowanie standardowego znacznika płatniczego, jaki może być osadzony na stronach HTML publikowanych przez detalistę. Ten znacznik byłby następnie interpretowany przez klienta w celu zainicjowania płatności przy wykorzystaniu odpowiedniego mechanizmu płatniczego.

Open Financial Exchange

- *Open Financial Exchange:* standard OFX jest owocem połączonej inicjatywy firm CheckFree, Intuit oraz Microsoft z roku 1996. Format rachunku OFX jest częścią tego standardu i pozwala dużym organizacjom rozwinąć system stanowiący interfejs z partnerami i konsolidatorami rachunków. CheckFree skonstruował program partner ski E-Bill, aby zachęcić do szerszego wprowadzania billingu internetowego. Firma ta oferuje obecnie e-billing i usługi płatnicze ponad dwu milionom klien-

[32] Protokół Otwartego Handlu – protokół wyższego poziomu służący do określania środowiska, w którym mogą być realizowane płatności – OTP zawiera wszystkie działania związanie z przeprowadzeniem transakcji – od negocjacji warunków przeprowadzenie transakcji, przez fakturowanie i przelew środków aż do spedycji.

tów w USA, a także łącza elektroniczne do 1000 firm handlowych. AT&T wspólnie z CheckFree zaoferowało w połowie roku 1998 stałym klientom możliwość oglądania i płacenia swych rachunków poprzez Internet za pośrednictwem systemów elektronicznych firmy CheckFree.

Techniki płatności elektronicznych

Techniki płatności elektronicznych rozwinęły się do tego stopnia, że osiągnęły pewną dojrzałość i są coraz lepiej rozumiane. Wiele firm oferuje już rozwiązania rynkowe, oparte głównie na systemach kartowych. W sytuacji, gdy technologia umożliwia w pełni realizację płatności on-line, nieufność użytkowników pozostaje. Ogólna świadomość stanu bezpieczeństwa w Internecie oznacza, że opory przed wprowadzaniem danych ze swych kart kredytowych do komputera podłączonego do Internetu stopniowo maleją.

Postęp w integracji dostawców katalogów i organizacji płatniczych oznacza, że otwieranie witryn internetowych obsługujących płatności on-line stało się znacznie łatwiejsze dla detalistów. Przyszłe schematy organizacyjne oferujące różnorodne metody realizacji płatności zostaną prawdopodobnie wprowadzone na rynek, gdy nowe, powstające wówczas modele biznesu, będą wymagać metod płatności nie opartych na wykorzystaniu kart płatniczych.

Podsumowanie

Jeszcze nie tak dawno wydawało się, że elektroniczna gotówka wyprze metody oparte o karty kredytowe. To, że się tak nie stało wynika zapewne z dużego bezpieczeństwa posługiwania się kartami, jak i z przyzwyczajeń klientów. Różne warianty gotówki elektronicznej posiadają jednak tak wiele zalet, że w dalszej perspektywie czasowej z pewnością staną się dominującą formą płatności. W przeciwieństwie do systemów opartych o karty kredytowe pozwalają one na realizację tzw. mikropłatności – w przypadku kart koszty ich obsługi przekroczyłyby wielokrotnie wartość transakcji. Mikropłatności są idealnym sposobem opłaty, np. za oprogramowanie dostępne tylko w wersji sieciowej. Nie kupuje się wówczas licencji na jego użytkowanie, ale płaci się wyłącznie za faktyczny czas jego użytkowania. Innym obszarem zastosowania są serwisy informacyjne.

Postęp w integracji dostawców katalogów i organizacji płatniczych oznacza, że otwieranie witryn internetowych obsługujących płatności on-line staje się znacznie łatwiejsze dla detalistów. Przyszłe schematy organizacyjne, oferujące różnorodne metody realizacji płatności, zostaną prawdopodobnie wprowadzone na rynek, gdy nowe powstające wówczas modele biznesu będą wymagać metod płatności nie opartych na wykorzystaniu kart płatniczych.

5. Bezpieczeństwo transakcji internetowych

- Ogólne zasady szyfrowania,
- Stosowanie podpisów cyfrowych,
- Inteligentne karty,
- Zasady i nawyki zwiększające bezpieczeństwo.

Zaufanie i bezpieczeństwo

Zwykle decyzje o skorzystaniu z oferty sklepu podejmuje się na podstawie jego lokalizacji, wielkości, rodzaju lokalu, od tego, jak długo istnieje itd. Gdy się nam to wszystko spodoba, jesteśmy gotowi zostawić tam gotówkę w zamian za produkt. Ryzyko jest niewielkie i mamy zaufanie do tego, co robimy. Nawet, gdy coś okaże się nie tak, wiemy, gdzie wrócić i oczekujemy zawsze uczciwego potraktowania. Kiedy jednak handlujemy za pośrednictwem Internetu, sprawa nie przedstawia się tak prosto. Rozkosze zakupów on-line mogą okazać się iluzoryczne. Skąd bowiem konsument ma wiedzieć (przed ujawnieniem danych ze swojej karty kredytowej), że firma jest godna zaufania i jest tą, za jaką się podaje? Jaka jest pewność, że owa firma pozostanie tam jutro? Z drugiej strony, skąd handlowiec ma wiedzieć, czy klient nie posługuje się danymi z karty skradzionej lub podrobionej? Czy obie strony transakcji mogą mieć pewność, że ich transakcja odbywa się poufnie, bez świadków, a ponadto bez nieuprawnionej ingerencji w czasie przesyłania danych poprzez sieć? A gdy sprawy się tak źle potoczą, to jakimi dowodami dysponują obie strony przy dochodzeniu swych roszczeń?

Zaufanie i bezpieczeństwo to dwa najważniejsze elementy każdej transakcji elektronicznej, które są również podawane jako największe bariery w rozwoju e-biznesu.

Nie jest to dziwne jeśli zważyć, że obie strony transakcji nigdy się nie spotykają, nie znają swoich miejsc pobytu, a tylko pragną zrobić interes; coraz częściej opiewający na znaczne kwoty.

Ochrona informacji

Najbardziej podstawową sprawą jest zapewnienie ochrony informacji przesyłanej poprzez sieć. Dlatego tak ważną rolę odgrywa w transakcjach elektronicznych szyfrowanie – żadne późniejsze wysiłki nie pomogą, jeśli samo połączenie nie jest bezpieczne. Gdy więc dialog pomiędzy konsumentem i dostawcą zostanie już zabezpieczony, trzeba sprawdzić tożsamość obu stron, nim rozpoczną w dobrej wierze zawieranie transakcji handlowej. Każdy uczestnik transakcji pragnie ponadto mieć pewność, iż druga strona jest godna zaufania.

Innym, często spotykanym problemem jest zapobieganie „uchylaniu się od zobowiązań, czyli niezaprzeczalność (non reputiation). W przypadku e-biznesu potrzebne są środki pozwalające nam udowodnić, kiedy i komu dany towar dostarczono.

Tak więc istnieje wiele aspektów zaufania i bezpieczeństwa w sieci, poczynając od technicznych zabezpieczeń połączeń komunikacyjnych, poprzez udowadnianie swojej tożsamości przez strony transakcji, a kończąc na temacie pozyskiwania zaufania kontrahenta.

5.1. Szyfrowanie danych

Szyfrowanie danych

Tajne szyfry używane były od dawna, aby zapewnić poufność informacji przesyłanej nie zabezpieczonymi kanałami, takimi jak publiczna sieć telekomunikacyjna. Niektóre z najwcześniej znanych szyfrów sięgają czasów starożytnych Egipcjan.

W e-biznesie szyfrowanie (czym zajmuje się kryptografia) musi być silniejsze z uwagi na obecny rozwój kryptoanalizy, którą posługują się potencjalni intruzi, mający nieraz dostęp do dużych komputerów i wyspecjalizowanego oprogramowania. Opiszemy teraz podstawowe techniki stosowane w serwerach WWW i przeglądarkach internetowych, jak również ograniczenia nakładane przez rządy wielu krajów[33] .

5.2. Przed czym trzeba się bronić?

Bezpieczeństwo sieci oznacza ochronę jej prawidłowego działania i zachowanie integralności w obliczu przypadkowego uszkodzenia lub celowego ataku. Problem bezpieczeństwa ma wiele aspektów, od tajności (zdolności do zachowania tajemnicy) i integralności, aż do tzw.„3A": uwierzytelnienia (Authentication) (wiedzy o tym kto, jest kto), autoryzacji (Authority – aby każdy robił tylko to, do czego jest upoważniony) oraz audytu (uprawnionego śledzenia tego, co się stało, kto tego dokonał i kiedy).

Przedstawimy teraz najważniejsze zagrożenia, którym powinny przeciwdziałać stosowane środki bezpieczeństwa.

Bezpośredni atak

Bezpośredni atak – atakujący ma na celu zalogowanie się do aplikacji z zamiarem posługiwania się nią jak prawowity użytkownik, lecz w ukrytych zamiarach. Atak może obejmować wy-

[33] W USA zezwala się jedynie na eksport „miękkich" produktów kryptograficznych; we Francji stosowanie kryptografii było do tej pory nielegalne itd. Zastanówmy się na początek, jakie wymagania stawia się dobremu systemowi zabezpieczeń.

kradanie lub odgadywanie haseł, stosowanie systemu operacyjnego lub aplikacji w rodzaju „furtek" (niczego nie podejrzewający użytkownicy mogą ładować i używać programy zawierające „konia trojańskiego" wprowadzającego tego rodzaju „furtkę", np. program „Back Office" atakujący komputery PC) lub pokonywanie procedur uwierzytelniania użytkownika[34].

Utrata tajności

Utrata tajności – dane przechwytuje się w czasie transmisji, a potem można użyć ich w celach kryminalnych. Urządzenia służące do podsłuchu w sieci LAN (sniffers) i WAN (datascopes) są już dostępne i mogą zostać użyte do tych nielegalnych celów.

Modyfikacja danych – dane mogą być modyfikowane w czasie transmisji (np. po zakupie towaru za 1000 USD atakujący zmieni dane tak, iż wykażą kupno towaru za jedyne 10 USD).

Maskarada

Maskarada – atakujący podaje się po prostu za uprawniony serwer. Może to być strona WWW o podobnym wskaźniku zasobów URL (Uniform Resource Locator), przeznaczona do skompromitowania danej firmy lub zbierania pieniędzy pod fałszywym szyldem.

Zbieranie informacji

Zbieranie informacji – będące często wstępem do jednego z wymienionych rodzajów ataku. Wyrafinowane narzędzia skanujące mogą tu posłużyć do systematycznego przeszukiwania naszego serwera w celu znalezienia słabych punktów systemu zabezpieczeń (np. SATAN). Wiele bardzo skutecznych narzędzi hakerskich można obecnie za darmo ściągnąć z Internetu!

Istnieje zatem bardzo wiele sposobów narażenia na szwank transakcji zawieranych za pośrednictwem sieci publicznych. Na szczęście jest też równie wiele metod przeciwdziałania tym zagrożeniom, a także wiele firm produkujących urządzenia zabezpieczające oraz firm służących odpowiednim doradztwem fachowym. Podstawowym zabezpieczeniem jest efektywny sposób szyfrowania informacji wysyłanej poprzez Internet.

5.3. Standardy szyfrowania

Standardy szyfrowania

Głównym celem szyfrowania jest zapewnienie tajności danych podczas ich transmisji przez sieć publiczną, taką jak Internet.

[34] Naruszenie prawidłowego działania – uniemożliwia sieci bądź aplikacji (np. serwerowi WWW) poprawną pracę. Istnieje wiele opcji, z jakich może w tym celu skorzystać haker dokonując ataku (można w tym celu posłużyć się programem użytkowym, ang. ping, testującym wszystkie węzły sieci lub Internetu celem uzyskania dostępu do poszukiwanego serwera), aby podłączyć się do serwera (uniemożliwiając dostęp do gniazdek TCP/IP (Transmission Control Protocol/ /Internet Protocol) z użyciem TCP SYN itd.

Dlatego jednym z najbardziej efektywnych sposobów ochrony sieci jest szyfrowanie wszystkich danych przesyłanych w sieci tak, aby dla hakera nie było żadnych danych nadających się do odczytania.

Wiele dzieci w wieku szkolnym zapoznało się z szyfrowaniem – posługiwały się bowiem jakimś szyfrem w tajnej korespondencji z kolegami. Przestawianie liter (bardzo proste w tym przypadku) jest podstawowym sekretnym algorytmem. Ten sam pomysł może być zastosowany w przypadku danych cyfrowych. Na przykład, procesor Clipper skonstruowany przez siły zbrojne USA zawiera algorytm szyfrujący o nazwie Skipjack. Dowolne dwa urządzenia wyposażone w ten procesor mogą wymieniać między sobą dane[35].

DES

Ustalonym standardem kryptograficznym jest system DES. Jest to system symetryczny z kluczem prywatnym o 56 bitach. Klucz ten rozszerzono do 64 bitów dodając 8 bitów parzystości i w tej formie stosowany jest do szyfrowania danych, dzielonych na bloki mające też po 64 bity. Algorytm pobiera te 64-bitowe bloki danych i łączy je z kluczem za pomocą skomplikowanego ciągu operacji dokonywanych na poziomie pojedynczych bitów, takich jak LUB wykluczające (exclussive-OR), z jednoczesnym przesuwaniem bitów.

Opisywany algorytm pierwotnie zaprojektowano do sprzętu hardwarowego, gdzie przesuwanie bitów oraz porównywanie odbywa się automatycznie i bardzo efektywnie. Obecnie jednak te same zadania mogą być łatwo wykonywane w software. 56-bitowy algorytm DES pozostaje podstawowym środkiem kryptograficznym w wielu dziedzinach przemysłu, a szczególnie w sektorze finansowym. Technologia komputerowa pozwala jednak obecnie na szybkie przełamanie 56-bitowego algorytmu DES w bardzo krótkim czasie i dlatego istnieje wzrastające zapotrzebowanie na skuteczniejsze metody szyfrowania.

---

[35] Jedyną wadą ostatniej metody jest fakt, iż wszystkie dane zostają ujawnione, gdy tylko algorytm zostanie odkryty. Gdy ten algorytm jest wtopiony w krzemowy układ scalony, jak w przypadku systemu Clipper, przywrócenie bezpieczeństwa staje się trudne.
Klucz, będący po prostu ciągiem cyfr, zawiera zbiór reguł sterujących algorytmem szyfrującym. Problemem staje się więc raczej ochrona klucza, a nie algorytmu, dlatego sposób zarządzania kluczem (bądź kluczami) trzeba szczegółowo przeanalizować.
Istnieją dwa podstawowe sposoby zarządzania kluczem. Pierwszy jest znany jako „kryptografia z kluczem prywatnym„ i jest systemem, w którym bezpieczeństwo szyfrowania zależy od utrzymania sekretu znanego tylko dwóm komunikującym się stronom. Sekret ten stanowi klucz prywatny, używany do szyfrowania danych po stronie nadawczej i do rozszyfrowywania ich po stronie odbiorczej. Przykładami systemów z kluczem prywatnym są IDEA (International Data Encryption Algorithm) oraz DES (Data Encryption Standard). Ze względu na symetrię procesu szyfrowania i rozszyfrowywania, kryptografia z kluczem prywatnym znana jest też pod nazwą „kryptografii symetrycznej”.

Alternatywnym sposobem podejścia jest „kryptografia z kluczem publicznym".

Kryptografia z kluczem publicznym

Jest to system, gdzie każdy użytkownik posiada parę kluczy – jeden prywatny i jeden publiczny. Wiadomość zaszyfrowaną przy użyciu klucza publicznego można rozszyfrować jedynie kluczem prywatnym i vice versa, tak iż możemy otrzymywać komunikaty od każdego, kto zna nasz klucz publiczny (które rozszyfrowujemy używając naszego klucza prywatnego). Możemy także wysyłać zaszyfrowane komunikaty każdemu, którego klucz publiczny znamy. Kryptografię z kluczem publicznym nazywamy „kryptografią niesymetryczną", ze względu na różne klucze używane w procesach szyfrowania i rozszyfrowywania wiadomości.

Stosowanie systemów z kluczem publicznym może odbywać się na dwa sposoby – za ich pomocą można uzyskać: tajność – klucz publiczny szyfruje dokument w taki sposób, iż może go odczytać jedynie właściciel odpowiedniego klucza prywatnego. Podejście to jest często stosowane jako bezpieczny sposób wymiany kluczy symetrycznych oraz podpisy cyfrowe – dokumenty podpisane za pomocą prywatnego klucza osoby podpisującej mogą być sprawdzane pod względem zgodności przy użyciu odpowiedniego klucza publicznego. Stanowi to podstawę do uwierzytelniania, integralności oraz niezaprzeczalności (non–repudiation), co zostanie omówione bardziej szczegółowo dalej.

RSA

Przypuszczalnie najbardziej znanym systemem kryptografii z kluczem publicznym jest RSA. Do generowania kluczy bardzo odpornych na atak (tzn. na złamanie szyfru) stosuje się w nich bardzo duże liczby pierwsze. W systemie RSA wykorzystuje się fakt, iż mając iloczyn dwu wielkich liczb pierwszych, wyznaczenie tych liczb jest matematycznie bardzo trudne. Ze względów praktycznych, systemy z kluczem prywatnym, których działanie jest oparte na algorytmie symetrycznym są bardziej rozpowszechnione. Ponieważ stosuje się w nich ten sam klucz do szyfrowania i rozszyfrowywania, operują one blokami danych, poddając je permutacjom bitów i operacjom logicznym według schematu zależnego od wartości klucza. Systemy te są z zasady szybkie i nadają się do implementacji w technologii krzemowej. Systemy z kluczem publicznym są raczej wolne i dlatego stosuje się je tylko do celów specjalnych (np. do ochrony transmisji kluczy prywatnych i do podpisów cyfrowych).

Niezależnie od wartości samej techniki szyfrowania stwarza ona jednak liczne problemy. Najważniejszym jest zdobycie odpowiedniego sprzętu komputerowego i oprogramowania, zdolnych do wykonywania (nieraz) bardzo złożonych procesów przetwarzania, jakie stanowi szyfrowanie i rozszyfrowywanie danych. Spe-

cjalne procesory (takie jak Clipper) stworzono właśnie do tego celu, lecz z uwagi na ich militarne zastosowanie sprzedaż i eksport tych urządzeń są ściśle kontrolowane. Najbardziej znanym przykładem tego rodzaju restrykcji jest należący do rządu USA system szyfrowania DES. Sklasyfikowano go jako „amunicja" i dlatego stał się obiektem restrykcji eksportowych.

Przełamywanie szyfru

Drugim problemem związanym z szyfrowaniem jest szybkość rozwoju tej technologii – szyfry uważane za bezpieczne jeszcze kilka lat temu, są dzisiaj łamane w ciągu kilku minut przy użyciu najnowszych procesorów. Ponieważ efektywność kryptografii tak z kluczem publiczny, jak i prywatnym zależy od utrzymywania kluczy w sekrecie, muszą one być odporne na atak. Poziom odporności klucza zależy od długości (tzn. liczby bitów) klucza używanego do szyfrowania danych. Niezależnie od tego, jak dobry jest algorytm szyfrujący, może on zostać łatwo złamany, gdy tylko klucz zostanie odgadnięty; im krótszy klucz, tym łatwiej tego dokonać. W praktyce, „odgadywanie" klucza sprowadza się do próbowania wszystkich możliwych kluczy, aż znajdziemy właściwy. Jest to jak próba otwarcia zamka kombinacyjnego przez wypróbowanie wszystkich możliwych kombinacji. Takie „brutalne" podejście nie jest sensowne dla pojedynczej osoby, lecz używając potężnego komputera zdolnego podjąć miliony prób na sekundę staje się ono, jak to pokażemy, bardzo prostym zadaniem.

Trudność przełamania algorytmu szyfrującego wzrasta wraz ze wzrostem liczby bitów klucza. Czas potrzebny do złamania szyfru wynosi 2 do potęgi równej liczbie bitów klucza minus liczba prób przełamania, a wszystko podzielone przez 2.

Deep Crack

W USA skonstruowano za skromną sumę 210.000 USD urządzenie służące do przełamywania systemu DES, zwane „Deep Crack". Urządzenie to jest zdolne do przetestowania około 92 160000000 kluczy/s, co w zapisie wykładniczym oznacza 247 kluczy/s. Ta liczba robi wrażenie, a wielokrotnie przewyższa szybkość przepisywania tekstu z prędkością kierowcy wyścigowego.

Atakowany algorytm (w tym przypadku DES) charakteryzuje się raczej prostym sposobem wyznaczania klucza (key schedule), co znacznie upraszcza konstrukcję maszyny rozszyfrowującej. Stąd oczekujemy szybkiego rezultatu i nie zawiedziemy się.

Stosując bowiem podany wzór na „czas przełamywania szyfru" stwierdzimy, że 56-bitowy algorytm DES padnie ofiarą maszyny Deep Crack w ciągu 25647/2 sekund, co daje mniej niż pięć minut; a to przy założeniu, że nie mamy szczęścia do trafienia na właściwy klucz już przy pierwszej próbie.

Czy jednak powinniśmy się tym martwić? Mają może rację sceptycy, gdy mówią, że bezpieczeństwo w Internecie po prostu nie jest na miarę potrzeb biznesu? Gdy przyjąć, że przeciwnik chcąc zbudować dla naszego algorytmu urządzenie analogiczne do Deep Crack jest przygotowany na inwestycję powiedzmy 27 milionów dolarów (128 razy więcej niż podana wcześniej suma), a postęp w dziedzinie technologii spowoduje czterokrotny wzrost szybkości działania tego urządzenia, da to w sumie efektywną szybkość przełamywania szyfru 247 x 22 x 27 = 256 kluczy/s. Gdy będziemy się posługiwać jednym z najbardziej dziś wyrafinowanych systemów o kluczu 128-bitowym, Deep Crack II będzie w stanie znaleźć nasz klucz (średnio) po 212b–56/1 sekundach, co równa się 74 miliardom lat. Chyba więc lęk związany z bezpieczeństwem to bardziej sugestia, niż realne zagrożenie.

Przykład dobrze wyjaśnia jedną sprawę, a mianowicie dlaczego szeroko znana metoda, potrójny algorytm DES o dłuższym kluczu niż obecnie, będzie, jak się uważa, bezpieczna jeszcze przez kilka lat. Potrójny algorytm DES szyfruje dane źródłowe trzykrotnie za pomocą podstawowego algorytmu DES, najpierw jednym kluczem, potem drugim, a za trzecim razem znowu pierwszym kluczem. Wynik jest uważany za równoważny użyciu klucza 112-bitowego – dostatecznie długiego, aby być bezpiecznym, a przy tym na tyle krótkiego, by zachować efektywność systemu. Deep Crack II potrzebowałby ciągle około jednego miliona lat na złamanie potrójnego algorytmu DES.

Deep Crack II

Nie ma jednak powodu do samozadowolenia, gdyż moc obliczeniowa komputerów stale rośnie i jest zapotrzebowanie na klucze o coraz większej długości, zabezpieczające przed ewentualnym atakiem. Dwa czynniki ograniczają jednak długość stosowanego klucza: po pierwsze, im dłuższy klucz, tym większa moc obliczeniowa jest potrzebna do przeprowadzania operacji szyfrowania i rozszyfrowywania (a więc im dłuższy klucz, tym więcej czasu zabiera uprawnionym użytkownikom wysyłanie zabezpieczonych komunikatów), a po drugie, jak uprzednio zaznaczono, rządy (a szczególnie rząd USA) nakładają restrykcje na eksport (a niekiedy także na używanie) silnych produktów kryptograficznych. Pozostają więc ciągle w mocy pewne ograniczenia rządu USA dotyczące używania szyfru DES; 56-bitowy DES może być wprawdzie stosowany bez ograniczeń, lecz restrykcje eksportowe zezwalają tam na używanie potrójnego algorytmu DES jedynie do aplikacji służb finansowych.

Skuteczność stosowania technik kryptograficznych zależy nie tylko od prawidłowego zarządzania kluczami szyfrującymi (włączając w to ich regularną wymianę), lecz także od bezpiecznej lokalizacji systemów szyfrujących.

Skuteczność technik kryptograficznych

Ideałem jest, aby szyfrowanie odbywało się w końcowych serwerach i terminalach systemu tak, aby ani jeden fragment drogi sygnału nie pozostawał bez ochrony.

Nie jest to zawsze możliwe, a rozwiązanie kompromisowe polega na szyfrowaniu danych wewnątrz specjalnych urządzeń sieciowych (np. ruterów) bądź umieszczaniu wolno stojących urządzeń kryptograficznych w wyznaczonych miejscach.

Szyfratory ładunku

Większość wolno stojących systemów szyfrujących dostępnych na rynku jest tak zaprojektowana, by pracowały poprzez dwupunktowe synchroniczne łącza danych, jest jednak coraz więcej systemów pracujących w sieciach zorientowanych pakietowo, jak Internet. Te pakietowo zorientowane urządzenia szyfrujące nazywane są także „szyfratorami ładunku" (payload encryptors), gdyż szyfrują tylko dane użytkowników, pozostawiają nagłówki protokołu w postaci jawnej tak, iż pakiety mogą być prawidłowo rozsyłane po sieci[36].

5.4. Podpisy elektroniczne

Podpis cyfrowy

Jak już stwierdziliśmy, kryptografia z kluczem publicznym, z użyciem pary kluczy – publicznego i prywatnego – stanowi dogodną podstawę technologiczną do wprowadzenia „podpisów cyfrowych". Jeśli na przykład osoba X zaszyfruje wiadomość używając swego własnego klucza prywatnego, a osoba Y jest w stanie go rozszyfrować za pomocą klucza publicznego X, Y może być niemal pewien, że wiadomość pochodzi od X. Gdy owa wiadomość upoważnia Y do wykonania pewnej czynności (takiej jak np. pobranie pewnej sumy z konta bankowego X), fakt że wiadomość została, jak można udowodnić, wysłana przez X daje podobny poziom zaufania, jak gdyby X własnoręcznie podpisał omawiany dokument.

Opisana technika jest trochę niewygodna, gdyż „podpis" stanowi tu zaszyfrowaną wersję całego komunikatu (który może być bardzo długi). W praktyce podpis cyfrowy tworzony jest na podstawie skrótu danego komunikatu, a nie jego kompletnego tekstu.

---

[36] Ostatnio wprowadzane standardy, mające na celu stworzenie, bezpiecznych zaszyfrowanych tuneli w publicznej sieci Internet, zostały stworzone przez IPSec (grupę roboczą działająca wewnątrz Internet Engineering Task Force, zajmującą się definiowaniem zbioru specyfikacji usług dotyczących uwierzytelniania, integralności i tajności w warstwie datagramu protokołu IP). W odróżnieniu od DES, funkcjonującego zasadniczo na aplikacyjnym poziomie komunikacji, standardy IPSec są zintegrowane z poziomem IP komunikacji TCP/IP. Składają się one zasadniczo z dwu części obejmujących: szyfrowanie zawartości pakietów IP (szyfrator ładunku IP z algorytmem typu DES) oraz protokół nagłówka pakietu (MD5/SHA), zapewniający dodatkowe sprawdzanie integralności. Zarządzanie kluczem odbywa się z użyciem metod klucza publicznego RSA.

Funkcja jednokierunkowa

Skrót ten tworzy się przepuszczając cały komunikat przez „funkcję jednokierunkową" (nazywaną funkcją skrótu (hash function), o następujących właściwościach:

- jest ona „jednokierunkowa" w tym sensie, iż łatwo przekształcić oryginalny tekst na skrót, natomiast odtworzenie oryginalnego komunikatu na podstawie jego skrótu jest niemożliwe;
- skrót ma niewielką i standardową długość, niezależnie od długości oryginalnego komunikatu;
- każdy znak oryginalnego komunikatu jest istotny przy tworzeniu skrótu tak, iż zmiana pojedynczego znaku oryginału spowoduje utworzenie innego skrótu;
- funkcja skrótu jest dostatecznie skomplikowana, aby dokonanie wielokrotnych zmian oryginału celem uzyskania takiego samego skrótu było bardzo trudne.

Ta ostatnia właściwość jest niezbędna, aby uniemożliwić intruzowi dokonanie celowych zmian oryginału (jak np. dopisanie dodatkowego zera do sumy pieniężnej), a następnie innych „kompensacyjnych" zmian, by cały komunikat miał ten sam skrót, co oryginał.

SET

Algorytm stosowany powszechnie do tworzenia podpisów cyfrowych (używany np. w standardach bankowych SET) tworzy skróty o długości 20 bajtów, niezależnie od długości oryginalnego komunikatu. Algorytm ten spełnia z założenia wymóg jednokierunkowości, gdyż redukcja długiego tekstu aż do uzyskania 20-bitowego skrótu powoduje konieczność „odrzucenia" dużej części oryginalnej informacji gwarantując, że nie ma możliwości wtórnego odtworzenia oryginału na podstawie jego skrótu.

Mimo odrzucania części informacji, algorytm jest tego rodzaju, iż zmiana pojedynczego bitu oryginalnego komunikatu zmienia średnio połowę bitów jego skrótu.

Dlatego prawdopodobieństwo tego, że dowolne dwa komunikaty mają ten sam skrót, jest odwrotnością liczby 10 do potęgi 48 (jest ona większa od liczby atomów systemu słonecznego). Dlatego nie jest obliczeniowo możliwe wygenerowanie dwu różnych oryginałów mających ten sam skrót.

Gdy więc X chce podpisać komunikat wysyłany do Y, musi wykonać podane czynności:

1. X tworzy komunikat,
2. X (lub jego program) tworzy 20-bajtowy skrót swego komunikatu,
3. X szyfruje skrót używając swego klucza prywatnego – otrzymany tym sposobem obiekt stanowi podpis cyfrowy komunikatu,
4. X wysyła komunikat razem z podpisem cyfrowym do Y,
5. Po otrzymaniu komunikatu, Y generuje także jego skrót.,6. Y rozszyfrowuje podpis stosując publiczny klucz X,

7. Y porównuje rozszyfrowany podpis ze swoim lokalnie wygenerowanym skrótem.

Gdy oba teksty się pokrywają, Y może być pewien, że otrzymaną wiadomość podpisał X i że nikt inny w nią nie ingerował.

5.5. Zaufanie w transakcjach internetowych

Klucz publiczny

Gdy wchodzimy na witrynę internetową o nazwie American Express, Fold lub Barclays Bank, to chcemy być pewni, że jest to rzeczywiście witryna firmy, za którą się podaje, zanim zaangażujemy się w transakcję finansową dokonywaną za pośrednictwem tej strony. Można to zapewnić, gdy witryna ma certyfikat wydany przez „zaufaną stronę trzecią", która sprawdza autentyczność witryny i dostarcza potwierdzone kopie jej „klucza publicznego", służące do bezpiecznej komunikacji z tą witryną. Grupa VeriSign Inc. jest czołową firmą świadczącą tego typu usługi, a w Wielkiej Brytanii podobną działalność prowadzi BT (BT Trust Wise) we współpracy z VeriSign. Przyjrzymy się teraz różnym typom certyfikatów wydawanych przez wymienione zaufane strony trzecie, by zbadać, do jakiego stopnia są one godne zaufania i dla jakich rodzajów transakcji elektronicznych są przydatne[37].

[37] Opisane asymetryczne algorytmy szyfrujące tworzą podstawę infrastruktur klucza publicznego. Systemy szyfrujące z kluczem publicznym są, jak już wspomniano, szeroko stosowane do podpisywania dokumentów elektronicznych (aby uwiarygodnić źródło i zapewnić niezaprzeczalność transakcji (non-repudiation) oraz przy wymianie kluczy szyfrujących. Użytkownik generuje parę kluczy: publiczny i prywatny, przy czym ujawnia jedynie klucz publiczny. Nie musimy jednak wiedzieć, że dany klucz publiczny należy do właściwej osoby, a nie do uzurpatora. Infrastruktura klucza publicznego załatwia to za pośrednictwem zaufanej strony trzeciej, która podpisuje klucz prywatny użytkownika po tym, jak użytkownik udowodni stronie trzeciej swoją tożsamość. Ten podpisany klucz jest nazywany certyfikatem i jest wydawany przez centrum certyfikacyjne (Certificate Authorit (CA)), takie jak VeriSign38. Certyfikaty powinny być dostępne w formie opublikowanej książki tak, aby odbiorca komunikatu miał do dyspozycji wiarygodne klucze publiczne. Górna część certyfikatu zawiera zwykłe informacje (które każdy może reprodukować). Ważnym elementem jest podpis zamieszczony na końcu certyfikatu. Skrót jest tworzony na podstawie górnej części certyfikatu i zostaje zaszyfrowany za pomocą klucza prywatnego zaufanego CA, takiego jak np. VeriSign. Autentyczność certyfikatu można łatwo sprawdzić porównując skrót wygenerowany na podstawie górnej połowy certyfikatu ze skrótem otrzymanym przez rozszyfrowanie podpisu kluczem publicznym wydawcy certyfikatu. Są różne klasy certyfikatów. Każdy ma inne zastosowanie i wymaga, aby inne elementy danych były zawarte w górnej połowie certyfikatu. Podstawowy certyfikat klasy 1 wiąże nazwisko użytkownika z jego adresem e-mailowym i kluczem publicznym. Jest on stosowany przez indywidualnych użytkowników Internetu do wysyłania bezpiecznej poczty elektronicznej lub uwierzytelniania swej tożsamości wobec serwerów sieci WWW. Certyfikat klasy 2 jest wydawany przez taką organizację jak bank, do ustalania tożsamości swoich klientów. Wymaga on dodatkowych elementów danych, takich jak numery kont bankowych. Certyfikaty tej klasy są też wystawiane przez CA, lecz aplikacje użytkowników są przetwarzane przez miejscowe centrum rejestracyjne RA (Regisstration Authority), które zajmuje się zatwierdzaniem zamówień na certyfikaty (np. po otrzymaniu czeków kredytowych i pisemnych zamówień na usługi). BT TrustWise Onsite jest jednym

5.6. Karty inteligentne

Karty inteligentne

Wielu użytkowników systemów kryptograficznych z kluczem publicznym przechowuje klucze prywatne za pomocą oprogramowania (np. używając zaszyfrowanych katalogów na twardych dyskach). Jest to, jak już wspomnieliśmy, dalekie od ideału, gdyż klucz prywatny jest tu chroniony tylko za pomocą pojedynczego hasła, przy czym nie zapewnia to mobilności klucza.

Karty inteligentne stanowią dogodny i zapewniający mobilność alternatywny sposób przechowywania klucza. Bezpieczeństwo systemu jest w tym przypadku większe, gdyż dostęp do klucza prywatnego jest regulowany czymś, co użytkownik rzeczywiście posiada (karta), a jednocześnie czymś, co użytkownik zna (hasło). Podobieństwo kart inteligentnych do istniejących kart kredytowych/debetowych sprawia, że wielu użytkowników zna już podstawowe zasady używania kart oraz zarządzania nimi.

---

z brytyjskich operatorów RA. Operatorzy serwerów WWW będą dążyć do otrzymania certyfikatu klasy 3. W tym przypadku CA przeprowadza szczegółowe sprawdzenie w celu potwierdzenia tożsamości właściciela serwera i jego zdolności kredytowej. Ten certyfikat obejmuje dodatkowe dane, a mianowicie URL (Uniform Resssource Locator) I serwera, nazwę organizacji i jej klucz publiczny. Gdy serwer ma taki certyfikat, użytkownicy przeglądarki internetowej mogą sprawdzać, czy komunikują się z autentycznym serwerem, a nie z oszustem. Taki certyfikat pozwala, co ważniejsze, na wymianę kluczy szyfrujących i przeprowadzanie bezpiecznych sesji HTTP (np. w e-handlu i bankowości elektronicznej). Na przykład, gdy chcemy użyć klucza publicznego z certyfikatu, aby utworzyć szyfrowane łącze do serwera handlowca. Symetryczny klucz sesji (zwykły klucz prywatny) oraz klucz publiczny z certyfikatu stosowane są łącznie do szyfrowania w czasie sesji; infrastruktury klucza publicznego PKI (Public\Key 1nfrassstructure) stosuje się do przesyłania małych plików danych potrzebnych do wymiany kluczy, a bardziej efektywną metodę klucza prywatnego do przesyłania dużych plików. Posługiwanie się centrum certyfikacyjnym ma oczywiście jakikolwiek cel tylko wówczas, gdy stanowi ono rzeczywiście zaufaną stronę trzecią i że solidnie przeprowadza adekwatne sprawdzanie danych służących za podstawę wydania certyfikatu. Skąd zatem będziemy wiedzieć, że możemy naprawdę ufać naszej zaufanej stronie trzeciej? Czy wystawca certyfikatu, z którego usług ostatnio skorzystaliśmy, jest godnym zaufania dostarczycielem certyfikatów cyfrowych? W odpowiedzi można stwierdzić, że sam klucz publiczny centrum certyfikacyjnego jest rozprowadzany wraz z certyfikatem wydanym przez bardziej jeszcze zaufaną instytucję (zaufaną stronę czwartą). Dochodzimy więc do hierarchii zaufania, w której każda strona jest certyfikowana przez inną, stojącą wyżej w tym łańcuchu. Na samym szczycie tej hierarchii stoi autorytet RSA, który udziela certyfikatu innym stronom jedynie po dogłębnym dochodzeniu odnośnie ich uwierzytelnienia. Ważnym problemem technicznym infrastruktury kluczy publicznych jest sposób przechowywania kluczy prywatnych. Jeśli trzymać je w komputerze PC, klucz będzie służył jedynie do stwierdzenia, że komunikat przychodzi z danego komputera, a nie od osoby.

Zwykłe hasła użytkownika służą do ochrony klucza prywatnego w komputerze PC, a te stanowią tylko słabe zabezpieczenie. Znacznie lepiej przechowywać klucze prywatne na karcie inteligentnej, która przemieszcza się wraz z posiadaczem od komputera do komputera.

Kiedy małe sekrety (klucze) służą do ochrony dużych sekretów (danych), jest to w każdym razie lepsza opcja – powiemy zatem kilka słów na temat kart inteligentnych.

Obecnie istniejące bariery dla ich powszechnego wprowadzenia są związane z brakiem zgody odnośnie standardu kart inteligentnych (np. Microsoft i Netscape promują rozmaite standardy integracji kart inteligentnych ze swymi przeglądarkami WWW), a w konsekwencji z brakiem czytników kart inteligentnych w komputerach PC. Jedna z firm wyprodukowała tanią klawiaturę zastępczą do komputera PC, zawierającą czytnik kart inteligentnych. Inna firma (Aladdin) proponuje klucz sprzętowy działający analogicznie do karty inteligentnej, ale podłączany do gniazda VSB na PC.

Jeszcze inna firma produkuje czytnik kart, który można włożyć do stacji dysków. Na pytanie, czy lub które z proponowanych rozwiązań zawojuje rynek, nie ma na razie jasnej odpowiedzi.

Zarządzanie kluczem

Zarządzanie kluczem jest tylko jednym z możliwych zastosowań karty inteligentnej w e-handlu. Karty inteligentne są bowiem coraz szerzej stosowane do wspomagania wielu rodzajów aplikacji, włączając uwierzytelnianie użytkownika, systemy pieniądza elektronicznego i programy lojalnościowe. W raz z wielością zastosowań kart inteligentnych nadejdzie moment, kiedy wszystkie te funkcje zostaną zrealizowane za pomocą jednej karty. Na przykład instytucje, świadczące usługi finansowe, będą wydawać pojedynczą kartę inteligentną, mającą cechy tradycyjnej karty kredytowej/debetowej i elektronicznej portmonetki, a zapewniającą silne uwierzytelnianie bankowe i zarządzanie kluczem do wspomagania bezpiecznych płatności elektronicznych.

5.7. Kształtowanie nawyków bezpieczeństwa

Kształtowanie nawyków bezpieczeństwa

W poprzednich punktach tego rozdziału koncentrowaliśmy się na środkach zapewniających bezpieczne środowisko dla transakcji elektronicznych prowadzonych poprzez Internet. Można oczywiście podać wiele innych nawyków związanych z zachowaniem bezpieczeństwa. Większość z nich nie dotyczy jednak tylko e-biznesu.

Fizyczne bezpieczeństwo serwera (gdzie nasze serwery się znajdują i komu ufamy na tyle, aby mu powierzyć ich obsługę?). Wszelkie dyskusje na temat bezpieczeństwa w e-biznesie koncentrują się zazwyczaj na samej sieci oraz ochronie aplikacji. Jak się jednak okazuje w praktyce, większość nadużyć dokonywana jest przez personel samych firm, a nie przez „hakerów" internetowych. Najważniejsza jest lokalizacja serwerów (i kto ma do nich dostęp) oraz proces zarządzania nimi. Gdzie, przykładowo, przechowuje się kopie rezerwowe i kto jest odpowiedzialny za regularne zmiany głównego hasła naszego serwera.

Zabezpieczenie Firewall i proxy (jak powstrzymać ataki hakerów na Twoje serwery).

Instalując serwery dołączone do Internetu, ustanawia się zazwyczaj kontrolę dostępu w postaci firewalla. Jest to szczególnie uzasadnione, gdy w serwerach przechowuje się ważną informację handlową i finansową. W zasadzie ogranicza się usługi przechodzące przez firewall tylko do tych, jakie chcemy oferować naszym klientom (może on, przykładowo, blokować wszystkie protokoły za wyjątkiem HTTP i bezpiecznego HTTP).

Odmowa usługi (jak zastopować kogoś, kto zasypuje nas fałszywymi transakcjami, blokując tym samym dostęp klientom do naszych usług?). Jedna z praktyk tego rodzaju stosowana w Internecie jest znana pod nazwą „spamming" i polega na wysyłaniu z dużą częstością niepożądanej korespondencji do wielu użytkowników.

Spamming

Trzeba wówczas zablokować adres, aby postawić tamę pewnej części przychodzącego ruchu. Monitorowalność (auditability) (jak możemy udowodnić, że transakcje, które naszym zdaniem miały miejsce rzeczywiście zostały zawarte). Większość wyposażenia sieciowego rejestruje przychodzące komunikaty (kto, co i kiedy). Dane te warte są przechowywania w dostępnym miejscu[38].

5.8. Infrastruktury klucza publicznego

Infrastruktury klucza publicznego

Stosowanie par kluczy szyfrujących, publicznego/prywatnego, jest sposobem na to, aby obie strony ufały sobie wzajemnie. Do tej pory nacisk kładliśmy na sposoby dystrybucji i certyfikacji kluczy. Jedno pytanie pozostaje jak dotąd bez odpowiedzi: jak można powoływać się na certyfikat pochodzący od kogoś, komu już nie ufamy. Jak tworzy się czarne listy osób i firm niegodnych zaufania. Co można zrobić dla kogoś, kto zgubi swój prywatny klucz. Co ma zrobić firma, która zaszyfrowała swoje dane, a dostęp do nich został następnie zablokowany przez pracownika, do którego utracono zaufanie (albo który zmarł lub opuścił firmę).

---

[38] Bezpieczeństwo aplikacji (czy określone aplikacje są chronione). Większość osób zauważy otwartą/zamkniętą kłódkę lub złamany cały klucz w zamku. Aplikacje, takie jak Internet Explorer i Netscape Navigator, potrafią zainicjować bezpieczną sesję ustanawiając łącze za pomocą HTTPS, zamiast HTTP. Sygnał ten przywołuje warstwę bezpiecznych łączy (SSL) inicjującą sesję serwera z użyciem portu 443 zamiast portu 80 (dobrze znany port HTTP). SSL pracuje wówczas z protokołem kontroli transmisji (TCP) ustanawiając bezpieczną sesję.
Wymienione zagadnienia są bardzo ogólne, a ponadto ich realizacja należy głównie do operatorów sieci i usług. Inni chcą zazwyczaj wiedzieć, co w tych sprawach zrobiono, lecz mają zarazem świadomość, iż nie muszą prawdopodobnie podejmować żadnych bezpośrednich działań.

Wszystkie te, a także inne problemy dotyczą implementacji infrastruktury klucza publicznego zarządzającej kluczami firm i innych organizacji.

Centrum certyfikacyjne

Podstawowym obowiązkiem centrum certyfikacyjnego (CA) jest wydawanie certyfikatów cyfrowych. Gdy Y kupuje certyfikat osobisty (klasy l), np. od firmy BT TrustWise, wypełnia przy tym formularz on-line, zawierający pewne jego dane osobiste (włączając adres e-mailowy). Wówczas, „za kulisami" jego wyszukiwarka WWW utworzy dla niego parę kluczy: publiczny i prywatny. Klucz prywatny zostaje zapamiętany lokalnie (jako plik zabezpieczony hasłem na dysku lub na karcie inteligentnej), a klucz publiczny zostaje wysłany do centrum certyfikacyjnego TrustWise.

Obsługa TrustWise utworzy certyfikat zawierający nazwisko Y, jego adres e-mailowy, klucz publiczny oraz inne informacje. Podpisze następnie ten certyfikat za pomocą własnego klucza prywatnego. Wreszcie dostarczy gotowy certyfikat Y pocztą elektroniczną.

Aby Y mógł skorzystać z tego certyfikatu, musi dać jego kopie swym przyjaciołom i znajomym, by mogli go używać do szyfrowania komunikatów, jakie do niego wysyłają: może to zrobić, wysyłając im kopie certyfikatu pocztą elektroniczną.

Będą wówczas przechowywane w systemach e-mailowych odbiorców. Użyteczność opisanego sposobu jest jednak ograniczona: gdy Y otrzyma już certyfikat, nie jest łatwo mu go potem odebrać, jeśli np. stracimy do niego zaufanie. Sposób jest wygodny tylko wtedy, gdy Y ma niezbyt dużą liczbę przyjaciół chcących wysyłać mu bezpieczne listy e-mailowe.

Bezpieczne listy e-mailowe

W przypadku dużej firmy, zatrudniającej tysiące pracowników regularnie wysyłających sobie nawzajem poufne informacje, omawiane podejście nie wystarcza i dlatego pierwszym krokiem przy tworzeniu infrastruktry klucza publicznego jest wydanie firmowej książki e-mailowej zawierającej cyfrowe certyfikaty pracowników.

Gdy jeden z pracowników zapragnie wysłać e-mail innemu pracownikowi, odczyta najpierw z książki jego dane e-mailowe i zrobi (przypuszczalnie „za kulisami") kopię certyfikatu cyfrowego adresata. Mamy tu do czynienia z bardziej skalowalnym rozwiązaniem problemu dystrybucji certyfikatów. Ponadto książka adresowa stanowi centralny punkt, w którym można od razu na wstępie przyznać pracownikom certyfikaty i który stanowi miejsce, skąd można certyfikaty usuwać lub unieważniać. Ta ostatnia

funkcja wtedy tylko będzie działać, jeśli klienci e-mailowi sprawdzają dane z książki za każdym razem, gdy mają wysłać list: w praktyce będą usiłowali ukryć certyfikat i dlatego opisana metoda nie jest zupełnie zadowalającym rozwiązaniem problemu unieważniania certyfikatów.

Generowanie par kluczy

Powszechnym środkiem generowania par kluczy publicznych/prywatnych jest, jak już powiedziano, przeglądarka internetowa użytkownika. Dlatego klucz prywatny nie musi być nigdy przesyłany poprzez sieć, a więc użytkownik nie traci nad nim bezpośredniej kontroli. Ten sposób postępowania jest nie zawsze dogodny dla korporacyjnego użytkownika infrastruktury klucza publicznego. Tak jak firmy mogą nalegać, aby ich pracownicy oddawali do depozytu w dziale ochrony dodatkowe kopie kluczy do swych pomieszczeń i biurek, tak samo mogą wymagać, aby składali tam kopie prywatnych kluczy szyfrujących. Wymaganie to zapobiega sytuacji, gdy jakiś pracownik opuści nagle firmę (lub umrze), a ktoś inny będzie zmuszony zająć się zaszyfrowaną zawartością jego skrzynki e-mailowej. Podobnie, gdy pracownik straci swój prywatny klucz (np. wskutek awarii dysku) i straci tym sposobem dostęp do zapisanej korespondencji. Firma powinna dlatego przechowywać kopie wszystkich prywatnych kluczy w bardzo bezpiecznym miejscu: opisany proces nosi nazwę depozytu kluczy (key escrow). Niektóre rządy też rozważają stosowanie depozytu kluczy jako warunku udzielania licencji na silną technologię kryptograficzną (miałoby się prawo używać silnej kryptografii dopiero po złożeniu kopii klucza w agencji rządowej). Społeczne i konstytucyjne aspekty problemu oddawania kluczy do depozytu nie mieszczą się w tematyce tej książki. Możemy tylko zasygnalizować, iż przechowując kopie wszystkich prywatnych kluczy w jednym miejscu wystawiamy się oczywiście na ataki hakerów i szpiegów, co jest głównym argumentem przeciwników takiego rozwiązania.

Depozytu kluczy

Troska o bezpieczeństwo Internetu, o której tak głośno w mediach, w niewielkim stopniu przyczyniła się do przekonania użytkowników, że Internet jest bezpiecznym miejscem handlu.

Bezpieczeństwo jest główną barierą hamującą rozwój handlu on-line. Jeśli więc liczymy na zasadniczy postęp, a nadzieje pokładane w e-biznesie mają się zmaterializować, trzeba zająć się problemami bezpieczeństwa.

Podsumowanie

W celu przeciwstawienia się niepożądanym zjawiskom spotykanym w e-biznesie wprowadza się mechanizmy pozwalające sprawdzić, czy dana osoba jest tą, za jaką się podaje, czy pieniądz przechodzi z ręki do ręki tak jak powinien i czy towar jest dostarczany zgodnie z umową. Mechanizmy te są coraz bardziej wyrafinowane, a zatem coraz bardziej złożone i kosztowne.

Troska o bezpieczeństwo Internetu, o której tak głośno w mediach, w niewielkim stopniu przyczyniła się do przekonania użytkowników, że Internet jest bezpiecznym miejscem handlu. Bezpieczeństwo jest główną barierą hamującą rozwój handlu online. Jeśli więc liczymy na zasadniczy postęp, a nadzieje pokładane w e-biznesie mają się zmaterializować, trzeba zająć się problemami bezpieczeństwa. Główne zagadnienia związane z bezpieczeństwem to przede wszystkim:

- ***poufność – dane muszą być niewidoczne dla szpiegów,***
- ***uwierzytelnianie – komunikujące się strony muszą być pewne wzajemnej tożsamości i/lub uwierzytelnień,***
- ***integralność – komunikujące się strony muszą wiedzieć, czy i kiedy dane zostały sfałszowane,***
- ***niezaprzeczalność – trzeba móc udowodnić, że transakcja została prawnie zawarta.***

Transakcje w Internecie nie są bardziej niebezpieczne od transakcji dokonanych w zwykłych sklepach. Kiedy płacimy kartą w tradycyjnym sklepie, oprócz pieniędzy zostawiamy w nim również dane o naszej karcie. Można je często znaleźć na tzw. slipie, czyli papierowym potwierdzeniu zawartej transakcji. Jedna kopia jest dla sprzedawcy, druga dla nas. Nieuczciwy sprzedawca może z łatwością wykorzystać nasze dane. Mimo wszystko mamy zaufanie do sprzedawców i bez cienia wątpliwości używamy kart do płatności w tradycyjnych sklepach.

6. Moja firma w sieci – krok po kroku

- 10 zasad innowacyjnej organizacji,
- Strategia działania w Internecie,
- Jak wybrać dostawcę usług?
- Jak zrobić dobry banner?
- Gdzie i kiedy się reklamować?

6.1. Strategia stałego wzrostu i rozwoju przedsiębiorstwa

Pojawienie się i gwałtowny rozwój Internetu rozpoczęło proces, który błyskawicznie rewolucjonizuje funkcjonowanie każdej organizacji. Istnienie jednej sieci, łączącej wszystkie przedsiębiorstwa, organizacje, organy rządowe oraz gospodarstwa domowe, na zawsze zmienia istotę prowadzenia działalności gospodarczej. Elektroniczna współpraca z partnerami handlowymi i klientami pociąga za sobą zmiany w kulturze przedsiębiorstwa i wymaga przemyślnego opracowania strategii wejścia w gospodarkę elektroniczną, a właściwie – strategii stałego wzrostu i rozwoju przedsiębiorstwa.

Kultura przedsiębiorstwa

Gospodarka elektroniczna zmienia proces tworzenia wartości.

Przyjęcie nowego modelu prowadzenia działalności jest łatwe dla nowo powstałej firmy, z założenia przystosowanej do pracy z Internetem. Jednak dla istniejącej organizacji, posiadającej ugruntowane procesy, praktyki i zakres działania nie jest właściwe przeprowadzenie gwałtownych zmian rewolucjonizujących jej zasady działania. Obecność w sieci i wprowadzenie elektronicznych kanałów sprzedaży są dzisiaj warunkiem przetrwania, ale o sukcesie decyduje umiejętność zarządzania zmianami, podejście do innowacji i znalezienie pozycji na stale zmieniającym się rynku.

Nowe modele biznesowe

Istniejący model działania należy przeanalizować pod kątem zastosowania nowych rozwiązań biznesowych i technologicznych. Proces ten obejmuje przeprowadzenie oceny każdego elementu biznesu – klientów, produktów, rynków działania, celów strategicznych, kanałów dystrybucji, personelu, wiedzy oraz kluczowych kompetencji, procesów organizacyjnych, systemów i mierników osiągnięć, a także starannego sformułowania planu strategicznego, którego celem jest przekształcenie działalności firmy w eBusiness. Nowe technologie wyzwalają proces zmian w przedsiębiorstwie. Nowe modele biznesowe dają szerokie możliwości ich adaptacji. Mogą poszerzyć aktualnie prowadzoną działalność bądź stać się nową gałęzią biznesu. W każdym z przypadków zmiany muszą być poprzedzone analizą aktualnej sytuacji i stworzeniem odpowiednich warunków dla integracji nowych rozwiązań z szeroko pojętym wewnętrznym systemem przedsiębiorstwa.

Model eCommerce

Najlepsze prognozy rozwoju ma model eCommerce B2B (business to business). Elektroniczny handel między korporacjami będzie miał największy udział w przychodach generowanych przez Internet. B2B zastosowane zarówno w kontaktach z klientami, jak i dostawcami pozwala m.in.:

- obniżyć koszty zakupów i sprzedaży,
- obniżyć koszty obsługi klienta,
- zwiększyć wydajność w zarządzaniu łańcuchem dostaw.

Stanowi również dodatkowe źródło informacji o zachowaniu i preferencjach klientów. Rozwinięciem modelu B2B są poniekąd giełdy internetowe. Zgromadzenie kupców i sprzedawców na jednej platformie stwarza nowe możliwości:

- szybszy i tańszy dostęp do informacji i produktów,
- dynamicznie zmieniające się ceny reagujące na zmianę popytu i podaży,
- łatwiejsze wejście na rynek dla małych przedsiębiorstw,
- rozwinięcie kolejnych modeli działania – CSP (Commerce Service Provider), ASP(Application Service Provider).

Paleta możliwości zależy także od rodzaju podjętych działań. W zależności od strategii można zostać:

- organizatorem giełdy,
- uczestnikiem,
- jednym i drugim,
- niezaangażowanym.

Ostatnia opcja jest raczej krótkoterminowym działaniem. Nowe kierunki rozwoju wymagają nowego podejścia strategicznego i operacyjnego. W dobie Nowej Ekonomii, gdzie konkurencja jest silniejsza niż kiedykolwiek i gdzie modele działania zmieniają się częściej niż kiedykolwiek, przeprowadzenie zmian nie jest już opcją dla dużych przedsiębiorstw – jest wymogiem. Koncentrować powinniśmy się jednak nie tyle na budowaniu samej strategii dokonania zamian, co na stworzeniu organizacji, która stale daje początek nowym koncepcjom biznesowym oraz stwarza środowisko do ich rozwoju i wdrażania.

Kapitał intelektualny

Takie podejście wiąże się ze zmianą postrzegania podstawowych wartości firmy. Nie stanowią już o nich tradycyjne aktywa, lecz przede wszystkim kapitał intelektualny – a więc wiedza i kompetencje pracowników oraz baza klientów – podstawa do rozwijania nowych form działalności. To są czynniki niezbędne do osiągnięcia sukcesu w warunkach nowej gospodarki.

Kapitał złożony z wiedzy i klientów musi zostać poparty czynnikami powodującymi wzrost wartości:

- zmiany muszą być przeprowadzane w odpowiednim czasie, powinny tworzyć nowe trendy na rynku, a nie tylko podążać za już istniejącymi. Opóźnianie zmian powoduje, że pozycja startowa jest o wiele trudniejsza niż była kilka miesięcy wcześniej,

- podejmowane inicjatywy muszą mieć dobrze określony budżet i zdefiniowane źródło finansowania,
- istotą jest prezencja w sieci, jako wspólnej platformie działania – oferta usług i produktów oraz dodatkowa działalność internetowa (rozrywka),
- globalna obecność zintegrowanej korporacji pozwala na generowanie szeregu innowacyjnych rozwiązań powstających na bazie doświadczeń z różnych części świata.

Zdolność do przegrupowania wartości i zasad działania przedsiębiorstwa czyni je gotowym do podejmowania nowych inicjatyw poszerzających bądź zmieniających prowadzoną działalność oraz pozwala na adaptację nowych technologii do realizacji zadań.

Kreowanie kultury korporacji inspirującej innowacje

Źródłem tworzenia się idei i pomysłów na innowacje musi być samo przedsiębiorstwo. Stworzenie w firmie kultury inspirującej innowacje nie jest proste. Jednak zastosowanie 10 przedstawionych zasad może pomóc w wykreowaniu głęboko innowacyjnej organizacji. Zasady te stosują na świecie z pomyślnym skutkiem korporacje, takie jak GE Capital, Charles Schwab, Royal Dutch/Shell.

10 zasad firmy innowacyjnej

Narzuć nierealistyczne oczekiwania

⇩

Rozszerz definicję swojej działalności

⇩

Stwórz cele, nie rozwiązania

⇩

Słuchaj nowych głosów

⇩

Stwórz giełdę pomysłów

⇩

Zaoferuj mechanizmy finansowania inicjatyw

⇩

Otwórz rynek dla talentów

⇩

Zmniejsz ryzyko eksperymentu

⇩

Działaj jak komórka – przeprowadzaj podziały

⇩

Dobrze wynagradzaj pomysłodawców (naprawdę dobrze)

Zasada 1 **Zasada 1 – Narzuć nierealistyczne oczekiwania**

Oczekuje się, że rocznie będziemy zwiększać przychody o 20% bądź więcej, jednak tak wygórowane oczekiwania powodują zupełnie inny sposób myślenia na temat możliwości zrealizowania celu. To przekonania pracowników wyznaczają granice możliwości. Trzeba więc wyzwolić w nich ambicje, pokazując na realnych przykładach, że można osiągnąć nieprzeciętne efekty. Znany jest przykład Steve'a Taylor'a, założyciela Fresh Express. Co można zrobić sprzedając sałatę. Nie jesteśmy w stanie zainstalować w niej procesora, ani wysyłać jej przez Internet. Taylor stworzył rynek „sałaty w opakowaniu" – wstępnie umytej i poszatkowanej. Wartość rynku wzrosła od zera w 1980 do 1,4 mld USD rocznie w 1999 roku. Jeśli coś takiego można zrobić z warzywem, to jaką my możemy mieć wymówkę. Tylko nieliniowy proces innowacji prowadzi do długoterminowego tworzenia wartości.

Zasada 2 **Zasada 2 – Rozszerz definicję swojej działalności**

Kim jesteśmy? Jest to prawdopodobnie najbardziej fundamentalne pytanie zadawane sobie przez pracowników i zarząd. Odpowiedź na nie powinna powstać w oparciu o posiadane przez przedsiębiorstwo kluczowe kompetencje i strategiczne aktywa, a nie (jak czyni to większość firm) na bazie prowadzonej działalności. Nie mamy założeń co do prowadzenia określonej działalności. Angażujemy się w dane przedsięwzięcie jeśli stwierdzimy, że:

- jest to wyzwanie dla istniejących zasad,
- pozwoli zwiększyć satysfakcję klientów,
- będzie bardziej rozrywkowe,
- będzie konkurencyjne. Nasza kultura polega na stawianiu sobie pytania „dlaczego nie", zamiast „dlaczego tak".

Zrewidujmy obszary, które dotychczas określaliśmy jako „poza zakresem" i przedefiniujmy obraz firmy biorąc pod uwagę to, co wiemy i posiadamy, a nie to, co robimy.

Zasada 3 **Zasada 3 – Stwórz cele, nie rozwiązania**

Przedsiębiorstwa muszą okresowo „zrzucać skórę". Ale taki proces nie może dokonywać się bez określonego celu. W przeciwnym wypadku indywidualności stracą odwagę do przeprowadzania zmian. Każdy zadaje sobie pytania – czy znajdę swoje miejsce w nowej rzeczywistości, jak wiele będę musiał się nauczyć, czy moje umiejętności będą adekwatne do nowych warunków, jak dużo czasu zajmie mi adaptacja? Na te pytania nie da się odpowiedzieć z góry. Odwaga do podejmowania nowych wyzwań nie wynika z przekonania, że zamiany są dobre, tylko z oddania nowej inicjatywie, nowym celom.

Zasada 4 **Zasada 4 – Słuchaj nowych głosów**

GE zebrał młody zespół – wszyscy poniżej 30 lat. Poproszono go, aby określili, gdzie leżą nowe możliwości. Bez udziału no-

wych głosów dyskusja na temat strategii nie przyniesie rezultatów. Jeśli firma chce stać się autorem rewolucji, musi dopuścić do głosu trzy grupy pracowników:

- ludzi z „młodzieńczą inicjatywą" – oni powinni brać udział w tworzeniu własnej przyszłości,
- pracowników z odległych geograficznie oddziałów firmy – zdolność do innowacji wzrasta z każdym kilometrem oddalania się od siedziby głównej,
- nowo zatrudnionych pracowników – szczególnie takich, którzy przyszli z innych branży, z firm tłumiących innowacje.

Spotkania z udziałem takich grup są regularnie organizowane przez GE. Po jednej z takich sesji, grupa młodych managerów powróciła z dwoma inicjatywami – strony www, gdzie klienci mogą znaleźć informacje finansowe potwierdzone przez niezależnych ekspertów. Odwiedzający mogą również znaleźć odnośnik do strony eCommerce, gdzie dowiadują się o finansowych produktach GE, takich jak ubezpieczenia domów, czy samochodów.

Zasada 5 – Stwórz giełdę pomysłów **Zasada 5**

Rynek pomysłów, kapitału i talentów odróżnia Silicon Valley od większości przedsiębiorstw. Tam każdego roku zgłaszanych jest 5000 biznesplanów. Ile takich powstaje w twojej firmie? Dopóki pracownicy nie zrozumieją, że pomysły naruszające zasady są drogą do tworzenia nowych wartości, rynek pomysłów w twojej firmie pozostanie jałowy.

Zasada 6 – Zaoferuj mechanizmy finansowania inicjatyw **Zasada 6**

Nie stawiamy sztucznych przeszkód dla nowych projektów. Pytania, jakie sobie zadajemy brzmią, czy pomysł jest interesujący?, czy jest innowacyjny? czy możemy na nim zarobić? Jeśli odpowiedzi brzmią: tak, finansujemy go. W większości firm dochodzi jedynie do realizacji projektów z 95% prawdopodobieństwem sukcesu. Nie dziwi więc, że rzadko kiedy realizowane są przedsięwzięcia innowacyjne. Celem jednak nie jest uzyskanie pewności, że żadna z inwestycji nie poniesie klęski, lecz pewność, że będzie wśród nich wielki zwycięzca.

Zasada 7 – Otwórz rynek dla talentów **Zasada 7**

Kultura naszej firmy pozwala każdemu na zajęcie się nową działalnością, jeśli tylko chce. Najlepsi ludzie należą do korporacji, nie do określonych działów. Managerowie nie mogą ich powstrzymywać. Tylko jeśli talent przemieszcza się w obrębie przedsiębiorstwa, jest szansa na zdobywanie nowych rynków. Kierunki przemieszczania się wskazują tendencje rozwoju i obszary, gdzie potrzebne są większe zasoby. Jeśli pracownicy chcą opuścić firmę dla nowego przedsięwzięcia – jakie ryzyko podejmujesz oferując im możliwość zrealizowania takiego projektu we własnej firmie? Stworzenie w firmie środowiska Silicon Valley otwiera nowe perspektywy.

Zasada 8

Zasada 8 – Zmniejsz ryzyko eksperymentu

Dokonujemy setek przejęć, ale rzadko realizujemy wielkie transakcje. Duża transakcja to duże ryzyko. Eksperymenty powinny pomóc przedsiębiorstwu zgromadzić wiedzę na temat nowego rynku i jego możliwości, aby następnie w niego zainwestować. Eksperyment należy rozumieć jako portfolio zadań do zrealizowania – przyswajaj naukę, gromadź doświadczenia i nagradzaj odkrywców.

Zasada 9

Zasada 9 – Działaj jak komórka – przeprowadzaj podziały

Podział i zróżnicowanie są podstawą wzrostu. Kiedy firma zaprzestaje tych działań, innowacje giną i wzrost przedsiębiorstwa jest wolniejszy. Podział na dywizje pobudza do innowacji na wiele sposobów. Po pierwsze, uwalnia kapitał intelektualny i finansowy spod rządów określonego modelu biznesowego. Osobne działy są miejscem dla nowych pomysłów i modeli działania. Po drugie, pozwala na wyłonienie utalentowanego przedsiębiorcy. Po trzecie, małe, zorientowane biznesowo dywizje pozwalają na bliższą współpracę i kontakt z klientem. I po czwarte, niweluje możliwość niszczenia projektów przez większe oddziały, z obawy przed „kanibalizacją" źródła przychodów. Decyzja podjęta przez Hewlett-Packard o utworzeniu osobnych dywizji dla drukarek laserowych i atramentowych pozwoliła na uniknięcie debaty o „kanibalizacji". Rezultat: HP stało się wiodącym dostawcą w obu branżach.

Zasada 10

Zasada 10 – Dobrze wynagradzaj pomysłodawców (naprawdę dobrze)

Wynagradzamy pomysłodawców jak samodzielnych przedsiębiorców. Wiele korporacji mówi o wewnętrznych przedsięwzięciach i karze pracownikom podejmować ryzyko. Kiedy odniosą sukces, dostają tylko mały bonus, a gdy przegrają, są zwalniani. Udziały w przedsięwzięciu są jedną z najlepszych i najefektywniejszych form wynagradzania innowacyjnych pracowników. Nie można gromadzić bogactwa, jeśli nie chce się nim dzielić. Jeśli zapytać venture capitalists, jaki jest najważniejszy zasób w łańcuchu tworzenia wartości, otrzymamy jedną odpowiedź – ktoś z przedsiębiorczą pasją i doświadczeniem operacyjnym, kto mógłby być efektywnym CEO. Prawdopodobnie w twoim przedsiębiorstwie jest tuzin takich pracowników. Czy muszą szukać swojej szansy gdzieś indziej? Dostajesz to, za co płacisz. Jeśli nie zapłacisz za przedsiębiorczość i innowacje, nie dostaniesz ich.

Analitycy rynku twierdzą jednym głosem, że już wkrótce nie będzie pojęć typu eBusiness czy eCommerce. One po prostu znikną, bo nie będzie innego, poza tym rozwiązania; nie będzie innego Businessu. Pytanie nie brzmi czy, lecz raczej kiedy? Może się okazać, że zwlekając, twoje przedsiębiorstwo zostanie pobite nie

przez znanego konkurenta, ale przez przedsiębiorstwo, o którym jeszcze 24 miesiące temu nikt naprawdę nie słyszał. Droga do gospodarki elektronicznej dziś, a do stałej obecności i konkurencyjności na rynku prowadzi prze kilka jasnych zasad:

- stwórz w firmie środowisko sprzyjające rozwojowi i innowacjom,
- buduj na bazie powstających koncepcji efektywne strategie działania,
- dostosowuj procesy wewnętrzne do nowych warunków biznesowych,
- realizuj przedsięwzięcia z zastosowaniem nowych technologii,
- ciągle ulepszaj i optymalizuj rozwiązania, sprzyjając jednocześnie powstawaniu nowych.

6.2. Wybór strategii działania w Internecie

Decydując się na rozpoczęcie działalności w Internecie możemy wyróżnić cztery zasadnicze rozwiązania. Różnią się one przede wszystkim koszt]em działalności oraz potencjalnymi korzyściami. Dla firm można zaproponować jedno z następujących rozwiązań:

- pełen dostęp do Internetu (łącze dzierżawione, obsługa serwisu www, sprzedaż kont i usług),
- pełen dostęp z ograniczeniami (łącze dzierżawione, obsługa serwisu www),
- ograniczony dostęp (łącze dzierżawione wraz z jednorazowym serwisem),
- bierny dostęp (tylko wykupione konto u providera).

Pełen dostęp do Internetu

Wariant pierwszy (*pełen dostęp do Internetu*) jest przeznaczony głównie dla firm o większych zasobach finansowych (nastawionych jednak w dłuższym okresie czasu na zysk ze sprzedaży usług). Jest to nie tylko wizytówka firmy w Internecie (traktowana jako czysta reklama), ale system obsługi klientów połączony z dodatkową działalnością, polegającą np. na sprzedaży usług internetowych. Jako przykłady takich firm można podać dostawców Internetu (ISP– Internet Service Provider), którzy to profesjonalnie zajmują się obsługą kont internetowych. Poza Dostawcami Usług Interenetowych w ten rodzaj działalności inwestują grupy przedsiębiorstw o bardzo zróżnicowanej działalności (Castrol, PizzaHut, FoxKids, Haribo).

Pełen dostęp z ograniczeniami

Wariant drugi (*pełen dostęp z ograniczeniami*) przeznaczony dla firm, gdzie Internet odgrywa dużą rolę, jednak nie ma potrzeby zatrudniania dodatkowych osób odpowiedzialnych za funkcjonowanie sieci. Kładziemy jednak duży nacisk na nasz serwis internetowy, który to jest źródłem danych dla naszych klientów.

Jako ciekawy przykład można podać regionalnych sprzedawców samochodów, gdzie widać duże zaangażowanie w stworzenie profesjonalnej witryny internetowej.

Ograniczony dostęp

Wariant trzeci (*ograniczony dostęp*) jest to typowe rozwiązanie dla małych i średnich firm w dniu dzisiejszym. Wraz z niewielkimi miesięcznymi kosztami otrzymujemy stosunkowo dużo. Wariant ten ma jednak wadę – przejście na wyższy wariant kosztuje niemalże tyle samo, co zbudowanie nowej sieci. Samo istnienie w Internecie traktowane jest jako ciekawe uzupełnienie reklamy – jako przykłady można podać gabinety odnowy biologicznej, czy nawet niewielkie gabinety lekarskie.

Bierny dostęp

Wariant czwarty (*bierny dostęp*) – najczęściej spotykane rozwiązanie w Polsce. Firma posiada tylko kupione (a nierzadko darmowe) konto u providera i stronę internetową mniej lub bardziej oddającą charakter działalności firmy.

6.2.1. Podłączenie do Internetu

Jednym z najważniejszym aspektów działalności w Internecie jest szybkie i sprawne łącze pozwalające nam na korzystanie z sieci. Wbrew pozorom nie tylko TP S.A. świadczy usługę stałego podłączenia do sieci Internet. Możemy też skorzystać np. łącza Multinet S.A. (znanego głównie z callback'a – systemu pozwalającego na znaczne oszczędności na rachunkach telefonicznych przy korzystaniu z Internetu. Polega on na oddzwanianiu z połączeniem internetowym do klienta). Samo podłączenie nie powinno zająć więcej czasu niż miesiąc. Pamiętajmy jednak o dokumencie stwierdzającym prawo do użytkowania lokalu– jeśli dane pomieszczenie wynajmujemy, będziemy potrzebować zgody właściciela. Dla wariantu czwartego (bierny dostęp do Internetu) w zupełności wystarczy dostęp do Internetu łączem komutowanym (poprzez linię telefoniczną).

6.2.2. Specyfikacja wariantów

Kryterium podziału na poszczególne warianty były potencjalne korzyści z działalności w Internecie. Wariant I jest najbardziej kosztowny, ale z pewnością przyniesie największe korzyści finansowe (przeznaczony głównie dla większych firm). Wariant IV przeznaczony jest dla przedsiębiorstw, które działalność w Internecie uważają tylko za uzupełnienie dotychczasowej działalności i nie nastawiają się one na wymierne korzyści z działalności internetowej.

Koszty instalacji i abonamentu[39]

Koszty instalacji i abonamentu

Wariant I (11900 zł)
Sprzęt niezbędny do funkcjonowania:
Serwer internetowy – 5000 zł
Router – 5000 zł
Zestawienie łącza – 1900 zł

Wariant II (11900 zł)
Sprzęt niezbędny do funkcjonowania:
Serwer internetowy – 5000 zł
Router – 5000 zł
Zestawienie łącza – 1900 zł

Wariant III (1400 zł)
Sprzęt niezbędny do funkcjonowania:
Modem na ł. dzierż. – 1000 zł
Zestawienie łącza – 400 zł

Wariant IV (150 zł)
Sprzęt niezbędny do funkcjonowania:
Modem na ł. komut. – 150 zł
Zestawienie łącza – 0 zł

Miesięczne koszty utrzymania łącza

Wariant I (3500 zł)
Łącze 1.500 zł
Pracownicy 2.000 zł (administrator i projektant www)

Wariant II (2500 zł)
Łącze 1.500 zł
Pracownicy 1.000 zł (administrator)

Wariant III (700 zł)
Łącze 700 zł
Pracownicy 0 zł

Wariant IV (200 zł)
Łącze 200 zł (średnia za użytkowanie linii telefonicznej)
Pracownicy 0 zł

[39] Połowa 2002 r.

6.2.3. Personel

Personel

W przypadku wariantu I (gdzie zajmujemy się komercyjną działalnością – sprzedażą kont i projektowaniem stron www) potrzebujemy zatrudnić osoby odpowiedzialne za funkcjonowanie tej komórki w firmie. Dla sprawnego działania potrzebujemy administratora sieci (może również administrować zdalnie całą siecią) oraz projektanta stron www. Dla wariantu IV nie potrzebujemy zatrudniać dodatkowych osób.

6.2.4. Wybór dostawcy Internetu

Wybór dostawcy Internetu

Wybór dostawcy Internetu jest sprawą najważniejszą dla firmy ponieważ jest to decyzja długoterminowa.

Podobnie istotny jak zakup odpowiedniego sprzętu oraz oprogramowania pozwalającego na korzystanie z Internetu. Podział został przeprowadzony na podstawie wariantów przedstawionych powyżej

Opcja I i II – ***Pełen dostęp do Internetu i Pełen dostęp z ograniczeniami***
Warianty te są bardzo zbliżone do siebie (różnią się tylko sposobem wykorzystania, parametry i wymagania są jednakowe). Głównym problemem, na który wskazuje praktyka, jest czas podłączenia łącza stałego przez TP SA. Według zapewnień proces ten (położenie kabla, dostarczenie odpowiedniego modemu) nie powinien trwać dłużej niż 4 tygodnie – jednak z różnych powodów trwa nawet do 7–8 tygodni. Jest to z pewnością barierą dla firm, które dopiero wynajmują pomieszczenie i muszą czekać kilka tygodni na podłączenie. Przy podłączaniu do sieci Internet łączem stałym należy również pamiętać o pozwoleniu właściciela lokalu na położenie kabla.

Jeśli chodzi o kartę graficzną oraz CD–ROM, to można powiedzieć, że nie mają one znaczenia w przypadku prędkości działania całego serwera i mogą to być podstawowe karty zgodne z systemem Linux (na którym oparty będzie serwer). Karta sieciowa odgrywa ważną rolę, jednak powinniśmy zakupić do wszystkich komputerów jednakowe karty sieciowe (np. 3Com–zapewniających wysoki poziom). Wykluczy to problemy z przesyłem danych pomiędzy komputerami. Wystarczającym typem monitora będzie 14" (nawet monochromatyczny), ponieważ na serwerze będzie wykonywanych niewiele prac – wszystko można kierować zdalnie.

Niezbędnym wyposażeniem będzie router (odpowiadający za połączenie z siecią Internet) oraz modem (dostarczany przez TP SA).

TP SA zastrzega sobie, że w niektórych przypadkach może odmówić położenia kabla (np. zły stan techniczny budynku, czy też brak zgody właściciela na zestawienie łącza). Dodatkowym warunkiem jest zbudowanie w firmie sieci lokalnej (LAN). Ponadto należy skonfigurować router (umożliwiający komunikacje ze światem), jak i serwer.

Opcja III – *Ograniczony dostęp*
Obecnie TP SA oferuje usługę SDI (Szybki Dostęp do Internetu– oparty na technologii HiS) o zbliżonych parametrach (koszt instalacji 999 zł, miesięczny abonament 160 zł, transfer 115 kB/s) jednak z wykorzystaniem istniejącej lini telefonicznej. Skupmy się jednak na łączu dzierżawionym. Tutaj mamy już wybór dostawcy Internetu – jesteśmy jednak ograniczeni odległością od providera (do około 8 km). Nie musimy w tym przypadku stawiać serwera – wystarczy istniejąca sieć lokalna i modem dostarczony przez providera.

Kable od providera do biura kładzie TP SA – wiąże się to z dodatkowymi kosztami oraz z odpowiednim okresem czasu na przygotowanie łącza (TP SA zapewnia, ze czas ten nie będzie dłuższy niż 4 tygodnie). Dodatkowym warunkiem jest zbudowanie sieci lokalnej, co wiąże się z poniesieniem dodatkowych kosztów związanych z zakupem karty sieciowej.

Opcja IV – *Bierny dostęp*
Tutaj mamy najbardziej podstawowe połączenie z Internetem, nie wymaga ono zakupu dodatkowego sprzętu (poza modemem). Jeśli chodzi o warunki techniczne, jedynym jest posiadanie linii telefonicznej oraz modemu.

6.3. Witryna

6.3.1. Co to jest witryna internetowa?

Co to jest witryna internetowa?

Witryna internetowa jest podstawowym źródłem o firmie w Internecie. Jest to swego rodzaju wizytówka, czy też katalog reklamowy. Zawierać może ona, obok elementów statycznych, różne animacje, widok z kamery, filmy, muzykę, animacje. To wszystko tworzy wizerunek firmy w Internecie.

Witryny jednorazowe

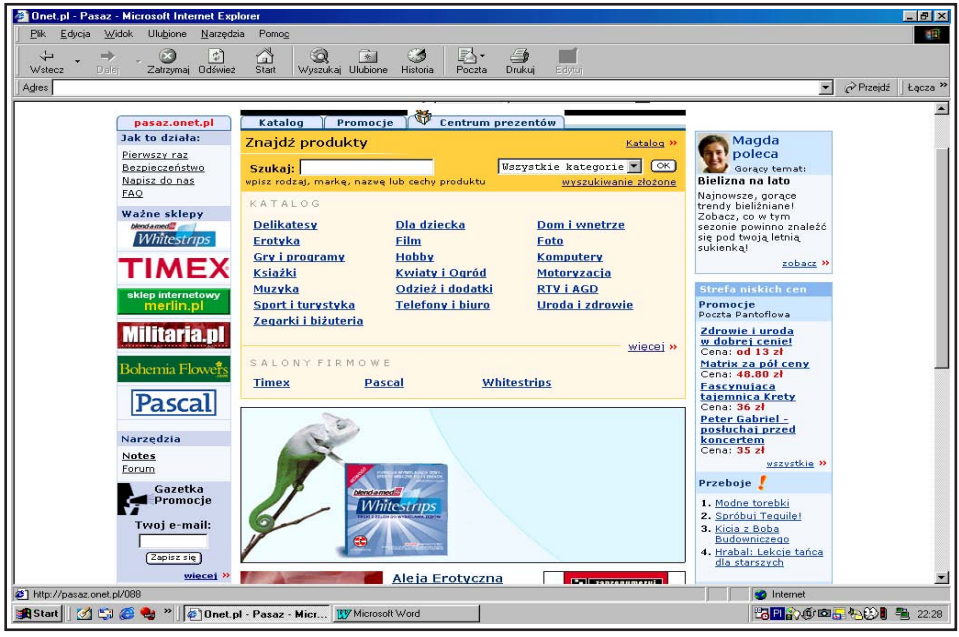
Zasadniczo możemy wyróżnić trzy rodzaje witryn. Pierwszy typ to witryny tworzone jednorazowo. Są one niemalże skopiowaniem naszej zwykłej broszury reklamowej. Zamieszczone są tam najczęściej informacje, takie jak: adres firmy, kontakt (również e-mail), dziedzina działalności, katalog produktów, czy np. ważniejsi klienci. Witryna stworzona raz funkcjonuje w niezmienionej postaci przez

cały okres trwania umowy z dostawcą. Ten rodzaj witryny najczęściej wybierają firmy, gdzie brak jest wykwalifikowanej kadry odpowiedzialnej za funkcjonowanie Internetu w przedsiębiorstwie. Niestety, w Polsce wciąż zbyt dużo istnieje witryn tego typu – nawet można powiedzieć więcej, możemy znaleźć tam nieaktualne informacje, co niestety nie ułatwia kontaku z firmą.

Witryna aktualizowana

Innym rodzajem jest witryna aktualizowana w miarę potrzeby (np. zmiany oferowanych produktów, promocje). Jest to o tyle dobre rozwiązanie, że klient ma pewne zaufanie w stosunku do naszej firmy. Wie, że zawsze może znaleźć aktualne informacje. Wie, że gdy napisze do nas e-mail, to z pewnością odpiszemy.

Rys. 1. Przykład witryny handlowej



Witryna ciągłej aktualizacji

Kolejnym rodzajem są witryny o ciągłej aktualizacji. Jest to dość kosztowny wydatek, ale dla części firm wręcz konieczny (firmy komputerowe, sklepy internetowe, strony dostawców, serwisy informacyjne). Często na takich stronach możemy znaleźć szereg dodatkowych informacji nie tylko na temat samej firmy, ale np. o nowych produktach na świecie w danej dziedzinie.

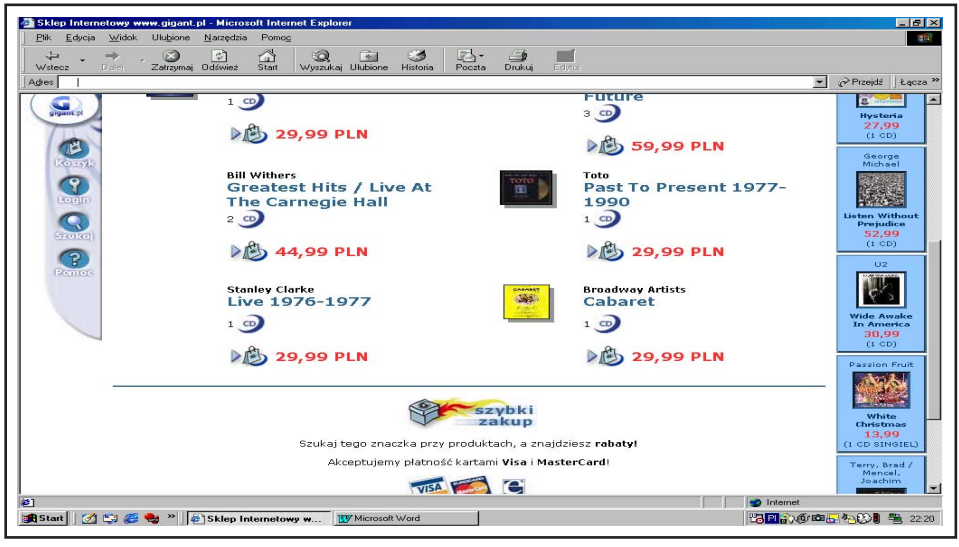
Na stronach takich nierzadko możemy brać udział w konkursie, pobrać pliki (różnego typu).

Po wyborze rodzaju strony (aktualizacji) przechodzimy do etapu II – budowanie witryny. Najczęściej jednak sami nie mamy o tym

pojęcia, w jaki sposób możemy to zrobić, zatrudniamy więc również naszego providera do stworzenia witryny. Powinniśmy się zdecydować, jaka strona nas interesuje.

Jeśli jesteśmy np. firmą produkującą kalendarze ścienne, w zupełności wystarczy nam strona aktualizowana w miarę potrzeby z informacjami, takimi jak: adres (zwykły i internetowy), prosty katalog produktów (kilka naszych najlepszych produkcji) wraz z ładnie zeskanowanymi zdjęciami.

Rys. 2. Przykład sklepu internetowego



Natomiast, jeśli jesteśmy firmą komputerową, powinniśmy witrynę przygotować w ten sposób, aby zawierała ona np. najnowsze sterowniki do sprzedawanego przez nas sprzętu, aktualny cennik, warunki rabatów etc. Taka inicjatywa wymaga ciągłej aktualizacji z naszej strony.

Ponosimy dodatkowe koszty, ale przez to jesteśmy znacznie lepiej postrzegani przez klientów. Ponadto możemy również na stronie umieszczać różnego rodzaju krótkie zapytania (badające preferencje), konkursy, a nawet gry. Jeśli nasza witryna cieszy się sporą oglądalnością (ponad 10.000 wyświetleń miesięcznie) możemy wprowadzić na stronie zapytania dotyczące preferencji klientów. Pytania mogą być w różnej formie i nie muszą odnosić się tylko do naszej działalności. Jeśli wypełnionych zostanie około 1000 ankiet miesięcznie, z powodzeniem możemy je traktować jako badania marketingowe i wyniki tychże badań powiązać z przyszłą działalnością firmy.

Używanie słów kluczowych w znacznikach TITLE

Sposoby „zaistnienia" w wyszukiwarkach

Znacznik ten jest wyświetlany jako tytuł danej strony. W jednym zdaniu powinniśmy starać się zamieścić dane szczegółowe o naszej firmie, np. „BODY – Centrum zdrowia". Tutaj możemy zamieścić znacznie więcej informacji na temat naszej firmy. To, co wpiszemy w to pole, zostanie wyświetlone w wyszukiwarce, dlatego starajmy się, aby te informacje były jak najbardziej zgodne z tym, co jest umieszczone na naszej stronie. Przykładowo: „Fitness Club „BODY" w centrum Warszawy. Oferujemy siłownię, saunę, indywidualne ćwiczenia, pomoc profesjonalnych trenerów".

Znacznik META name = ="description"

Znacznik META name = = "keywords"

Tutaj powinniśmy zamieścić jak najwięcej pojedynczych słów opisujących to, co oferujemy, z czym się kojarzy nasza działalność.

W celu zwiększenia „liczby trafień" powinniśmy używać zarówno liczby pojedynczej, jak i mnogiej (np. „siłownia, siłownie").

Przykładem dobrze dobranych słów kluczowych może być: „siłownia, siłownie, bieg, biegi, zdrowie, sauna, aerobic, callanetics, step ..." itd. Powinniśmy również zwrócić uwagę na obecność polskich liter, niestety niektóre wyszukiwarki ich nie rozpoznają, więc powinniśmy umieszczać również bez takich, np. „siłownia, silownia".

6.3.2. Sposoby „zaistnienia" w katalogach

Sposoby „zaistnienia" w katalogach

Przykładowa droga do wyszukania przepisu na pizzę wegetariańską została pokazana powyżej. Jest jednak kilka rzeczy, o których powinniśmy pamiętać:

- pamiętajmy, że dana kategoria w każdym z serwisów może mieć nieco inne znaczenie. Dlatego przed umieszczeniem upewnijmy się, czy nasza witryna będzie pasowała do danej kategorii,
- jeśli nie możemy znaleźć odpowiedniej kategorii, nie bójmy się stworzyć nowej (oczywiście, jeśli tylko mamy taką możliwość),
- jeśli w danej kategorii znajdziemy dużo firm o podobnym profilu, to znaczy, że jesteśmy we właściwym miejscu,
- jeśli natomiast w danej kategorii znajduje się zbyt dużo firm, nie starajmy się znaleźć innej, gdzie jest znacznie mniej firm, ale o opisie mniej odpowiadającym działalności Twojej firmy,
- niektóre serwisy umieszczają strony według alfabetu, dobrze jest więc dobrać tak nazwę witryny, żeby znalazła się na początku. Tak więc nasza firma „Body Center" ma dość dużą szansę bycia na początku.

6.3.3. Kiedy się zarejestrować?

Trzymajmy się zasady, że rejestrujemy się dopiero wtedy, gdy nasza strona jest w 100% gotowa. Gdy zrobimy to wcześniej odwiedzający naszą witrynę może uznać ją za mało atrakcyjną i już do niej nie powrócić.

Kiedy zmienić treść w katalogu/znaczniku?

Kiedy zmienić treść w katalogu/ znaczniku?

Powinniśmy to uczynić tylko wtedy, gdy zawartość naszej strony odbiega od opisu.

6.3.4. Nieetyczne sposoby zwiększania liczby odwiedzających

Nieetyczne sposoby zwiększania liczby odwiedzających

Wymienione zostaną tylko w celu pokazania możliwości zwiększenia liczby odwiedzających. Może to jednak odnieść przeciwny skutek do zamierzonego, tzn. osoba odwiedzająca naszą witrynę może już więcej do niej nie powrócić.

- Umieszczanie w znacznikach słów, które cieszą się dużą popularnością, ale które nie są spójne z naszą działalnością. Przykładami takich słów są: „software, download, sex".
- Częste zmiany znacznika TITLE. Roboty odwiedzające serwer będą widziały wtedy naszą witrynę jako zupełnie nową stronę, zwiększając tym samym liczbę wyświetleń naszej firmy.
- Używanie w znacznikach META nazw konkurencyjnych firm. Przykładowo, jeśli jesteśmy dealerem Fiata, to umieszczenie słów kluczowych, takich jak Opel, BMW, czy podobne, zwiększy liczbę odwiedzających, ale będą oni tylko wprowadzani w błąd.
- Możemy stosować sztuczki, takie jak umieszczanie np. znaku „!", czy liczby na początku tytuły naszej strony („!Body Center"), jednak upewnijmy się, czy taki znak umieści nas na początku, nie zaś na końcu.

Dobrze jest jeśli poinformujemy również uczestników grup dyskusyjnych o istnieniu nowej witryny. Tutaj jednak należy znacznie bardziej uważać. Decydując się na wysłanie e-mail'a, czy news'a do grupy, powinniśmy pamiętać o kilku zasadach.

SPAM

Uważajmy na SPAM – nie wysyłajmy informacji do zbyt dużej liczby odbiorców. Jeśli nasz list zostanie uznany za SPAM (czyli komercyjny list skierowany do dużej liczby odbiorców, gdzie temat raczej nie jest związany z grupą odbiorców – bez uprzedniej zgody odbiorców), możemy mieć nawet zablokowane konto.

Jeśli jednak chcemy wysłać list do grupy dyskusyjnej, to powinniśmy pamiętać o związku naszej firmy z odbiorcą. Przykładowo, jeśli jesteśmy producentem książek fantastycznych, to skierujmy naszą ofertę do takich właśnie odbiorców. Przed wysłaniem listu zachęcającego do odwiedzenia naszej strony dobrze jest kilkakrotnie zabrać głos na danej liście. Zwiększy to liczbę odwiedzających. Nie zapomnijmy o umieszczeniu sygnatury pod listem.

6.3.5. Łatwy sposób rejestracji

Łatwy sposób rejestracji

Ręczna rejestracja naszej witryny w około 200 światowych serwisach byłaby zadaniem dość czasochłonnym. Oczywiście możemy się ograniczyć tylko do 5 czy 10 serwisów. Jednak, gdy chcemy zaistnieć we wszystkich ważniejszych serwisach na świecie powinniśmy wydać kilkadziesiąt dolarów na „pełną" rejestrację. Poniżej przedstawiona została oferta kilku firm z kraju i zagranicy.

- **49.90 zł**

Jest to godna uwagi polska oferta „Start" (www.start.com.pl), obejmująca ponad 150 serwisów, w tym również polskie wyszukiwarki.

- **$49.95**

Taka cena jest za rejestrację w 250 serwisach. Tyle kosztuje rejestracja shareware'wego programu „The Spider". Nie jest to więc jednorazowa operacja, ale obejmująca nieograniczoną liczbą uaktualnień naszej strony.

- **$60**

Taką cenę oferuje serwis Submit–it! za rejestrację dwóch adresów w 400 wyszukiwarkach i katalogach.

- **$99.90**

Program „The Spider", jednak wersja profesjonalna obejmująca ponad 400 serwisów.

Podsumowując, należy podkreślić, że koszty ponoszone na rejestrację naszej witryny są raczej jednorazowe (zakładając w miarę stabilną działalność naszej firmy), nie należy więc zwlekać. Pamiętajmy również, że prawidłowe podanie słów kluczowych znacznie zwiększy szansę wyszukania danej informacji przez klienta. Dlatego też zastanówmy się, czy dane słowa uwzględniają całą naszą działalność, czy może tylko część.

6.4. Przygotowanie reklamy – na przykładzie bannerów

Przygotowanie reklamy

Coraz więcej mówi się o Internecie jako nowym środku przekazu informacji. Nakłady firm na Internet wciąż rosną w bardzo szybkim tempie (w Europie w ciągu dwóch lat jest przewidywany wzrost o około 100% liczby użytkowników Internetu). Na reklamę w roku 2000 w USA przeznaczone zostanie około 2,5 mld dolarów. Tworzy to ogromny rynek dla agencji reklamowych i wymusza powstanie profesjonalnej reklamy w Internecie. Spotykamy różne formy reklamy, jednak najpopularniejszą wciąż są bannery.

Rys. 3. Przykłady bannerów

Początkiem reklamy internetowej były proste bannery (rysunki prezentowane na stronach www reklamujące inną witrynę). Internet kilka lat temu ograniczał wielkość takich reklam. Przeciętną spotykaną wielkością było około 5 kB – dodatkowo bannery te były statyczne, co znacznie zmniejszało atrakcyjność takowych. Obecnie powszechnie stosowane są reklamy animowane (wielkość to już około 10 kB). Do najważniejszych wad zaliczyć można brak „interaktywności" z użytkownikiem. Reklamy najczęściej przedstawiają kilka słów kluczowych, bez możliwości wpływania na

wynik kliknięcia. Jest to szczególnie uciążliwe, jeśli banner ma do pokazania większą gamę produktów, jak ma to miejsce np. w dużych sklepach internetowych.

6.4.1. Sztuka przygotowania skutecznego bannera

Skuteczny banner

Aby nasz banner był skuteczny, kierujmy się kilkoma zasadami przy tworzeniu reklamy.

Animacja może zwiększyć ilość odpowiedzi o około 30–40%[40].

Kolorystyka banerów

Nasza animacja powinna współgrać z ogólnym wizerunkiem reklamy. Nie powinna być również zbyt skomplikowana, co znacznie wydłuży czas ładowania. Jako przykład wzorowo wykonanej reklamy połączonej z animacją można podać banner firmy ICon. Początkowo ilość odpowiedzi wynosiła 19%. Później ustabilizowała się na poziomie 15%. Powinniśmy unikać używania nieokreślonych, zlewających się kolorów, jak na przykład beżowy na tle szarego. Badania przeprowadzone przez Internet Profiles Corp. i DoubleClick wykazały, że kolor np. zielony i żółty przewyższają ilością „odpowiedzi" czarny i biały. Standardowo używany jest rozmiar zbliżony do 480x60. Większe reklamy odznaczają się większą ilością odpowiedzi. Jednak nie przesadzajmy, duże reklamy załadowują się znacznie dłużej. Najlepszymi miejscami na umieszczenie reklamy są nagłówek i stopka strony. Natomiast, jeśli chodzi o wybranie odpowiedniej strony na umieszczenie bannera, to pamiętać należy o powiązaniu działalności naszej firmy z treścią umieszczoną na stronie, np. zajmując się produkcją zeszytów dobrym miejscem na umieszczenie reklamy będą strony poświęcone edukacji.

Hasło powinno być powiązane z działalnością komputerową.

Hasło reklamowe

Przykładowo hasło „bezpłatne oprogramowanie do ściągnięcia" będzie miało większy odzew aniżeli „bezpłatna oferta przesyłana do domu". Częstotliwość występowania i żywotność reklamy – nie powinniśmy umieszczać reklamy zbyt długo. Powszednieje i nie powoduje takiego odzewu. Lepiej umieszczać reklamy rzadziej, ale różne. Niektóre reklamy powodują złe odczucia, takie powinniśmy natychmiast zmieniać. Nie umieszczajmy zbyt dużo danych na naszej reklamie. Powoduje to chaos i nieczytelność. Jako wyjątek potwierdzający regułę można przytoczyć bannery firm dostarczających Internet do firm. Wtedy to najczęściej zobaczymy na reklamie bardzo dużo treści opatrzonej niewielką ilością grafiki.

[40] Źródło: ZD Net.

Jeśli, pomimo tych wszystkich rad, wyniki naszej pracy nie zadowalają nas, możemy zgłosić się do jednej z wielu Agencji Reklamowych. Koszt przygotowania reklamy animowanej będzie się wahał od 50 do ok. 300 zł.

6.4.2. Banner interaktywny

Banner interaktywny

Bannery interaktywne są kombinacją kodu HTML, grafiki, Javy, CGI czy ShockWave'a. Powstanie tego typu reklam było tylko kwestią czasu, na interaktywnych bannerach nie tylko klikamy, ale mamy możliwość skorzystania między innymi z:

- listy wyboru (np. lista dostępnych produktów wybierana bezpośrednio z bannera),
- map (kliknięcie na różnych regionach bannera powoduje przeniesienie na inną stronę),
- wypełnianie formularzy,
- głosowania,
- przeszukiwanie serwisu,
- czy nawet grania w proste gry (np. kilkanie w ruszający się element).

Rezultatem wykorzystania tych elementów jest kilkukrotne zwiększenie zainteresowania naszą reklamą (na zwykłych bannerach liczba kilknięć wynosi około 4%).

Ten rodzaj reklamy ma też jednak wady. Przede wszystkim reklama ładuje się dłużej, co może zniechęcić część osób do kliknięcia na niej. Ponadto bannery interaktywne korzystają z Javy czy Shockwave'a – pamiętajmy, że część potencjalnych klientów nie ma zainstalowanych odpowiednich komponentów, co uniemożliwi im zobaczenie naszej reklamy. Zwrócić uwagę należy również na fakt, że „optycznie" reklamy zwykłe i interaktywne się nie różnią– aby klient zwrócił na to uwagę należałoby go o tym powiadomić (np. „Wybierz produkt z listy i kliknij!"), niestety – zwiększa to objętość naszej reklamy. Ponadto kolejną wadą jest konieczność umieszczenia odpowiedniego kodu HTML na stronie, gdzie ma być wyświetlana reklama. W Polsce wciąż jest niewiele tego typu stron, gdzie można skorzystać z takiej oferty.

6.4.3. Gdzie można się reklamować?

Gdzie się reklamować?

W Polsce jest niewiele stron oferujących zamieszczanie interakcyjnych bannerów. Również najważniejsze portale internetowe tego jeszcze nie oferują. Na świecie jednymi z najważniejszych są; Yahoo, Infoseek czy OTH. Ponadto są jeszcze inni, lecz mniej znani polskiemu czytelnikowi stron, którzy oferują produkcje bannerów interaktywnych.

6.4.4. Koszty przygotowania oraz utrzymania

Koszty przygotowania

W Stanach Zjednoczonych rozsądną ceną za przygotowanie takiego bannera jest cena około $50. Oczywiście, można znaleźć też tańsze oferty, jednak bannery przedstawiane przez te firmy nie są najlepsze. Koszt utrzymania danej reklamy jest większy od umieszczenia zwykłej reklamy. Dzieje się tak w głównej mierze dlatego, że koszt przygotowania oprogramowania na serwerze jest dość wysoki. Pamiętajmy, że dla każdej reklamy przygotowany kod będzie inny.

6.4.5. Banner statyczny czy interakcyjny?

Banner statyczny czy interakcyjny?

Obecnie zauważamy z pewnością potrzebę istnienia bannerów interakcyjnych. Są one znacznie bardziej atrakcyjne dla klientów. Pozwalają przekazać znacznie więcej treści niż tradycyjne reklamy. Jednak wciąż jest niewiele miejsc, gdzie można taką reklamę umieścić. Trudno zatem jest porównać oferty na rynku polskim, ponieważ brakuje konkurencji. Miejmy nadzieję, że ta sytuacja ulegnie zmianie w najbliższym czasie.

Wszyscy już przyzwyczailiśmy się do reklamy w Internecie. Mimo że wzbudza ona obecnie mniejsze zainteresowanie niż jeszcze rok temu (wtedy to odsetek osób nie zwracających uwagi na reklamę wynosił 39% – obecnie jest to już 49%, źródło: eMarketer), można powiedzieć, że zastosowanie bannerów interaktywnych przyjęło się na stałe w Internecie. Teraz już będziemy tylko czekać na reklamy wykorzystujące dźwięki (z technicznego punktu widzenia nie jest to trudne, jednak głównym problemem wydaje się być akceptacja).

6.4.6 Zamieszczenie płatnej reklamy

Zamieszczenie płatnej reklamy

Reklama płatna powinna być brana pod uwagę w przypadku, gdy Internet staje się poważną inwestycją (głównie Wariant I i II). Do głównych pojęć przydatnych przy analizie efektywności reklamy internetowej zaliczamy: CPM – (costs per mille) wskaźnik określający, ile kosztować będzie nas wyświetlenie 1000 banner ów reklamowych na danej witrynie. Wyświetlenie zostaje „zaliczone", gdy przeglądarka internetowa (np. Internet Explorer) wyśle rządanie do serwera wyświetlanie bannera. Warto zaznaczyć, że kupno bannerów odbywa się raczej w pakietach po 1000 wyświetleń (lub większych). Jeśli chcemy, aby nasza reklama została pokazana 30.000 razy i wskaźnik CPM wynosi $15, to koszt całej reklamy wyniesie $450 (30x$15). Wskaźnik CPM jest różny dla różnych stron. Zależy on głównie od odbiorcy danej

strony (w ten sposób ukierunkowana reklama jest znacznie skuteczniejsza). Na przykład prowadząc serwis motoryzacyjny możemy się skupić na pozyskiwaniu klientów z branży motoryzacyjnej przy znacznie większym CPM (czasami nawet do $60). CTR – (click through rate) wskaźnik określający, ile osób zobaczyło i kliknęło na naszej reklamie (pokazuje, jakie zainteresowanie wzbudza nasza reklama). I tak, gdy 'click rate' wynosi 5% oznaczo, to że 5% osób, które widziały naszą reklamę kliknęło na nią i zostało przeniesionych na strony naszej firmy.

Aby reklama płatna przyniosła spodziewane efekty, powinniśmy przygotować strategię.

Punkty, na których powinniśmy się skupić to m.in.:
- zasięg – ile osób ma zobaczyć naszą reklamę (tym samym możemy w przybliżeniu obliczyć koszty reklamy),
- częstotliwość występowania – określający, czy będziemy skupiać się tylko na jednej reklamie, czy też będziemy często przygotowywać nowe,
- czas – oznaczający, jak długo chcemy, aby reklama była wyświetlana (ściśle powiązany z zasięgiem).

Skuteczne miejsca, gdzie możemy zamieszczać własną reklamę, to:
- główne portale krajowe (www.wp.pl, www.onet.pl, www.interia.pl),
- serwisy specjalistyczne (np. prowadząc firmę o specjalizacji motoryzacyjnej powinniśmy umieszczać reklamę właśnie na serwisach specjalistycznych, często takowy jest włączony do głównych portali).

6.4.7. Zamieszczenie bezpłatnej reklamy

Zamieszczenie bezpłatnej reklamy

Różnica pomiędzy wielką korporacją międzynarodową a niewielką firmą produkująca np. długopisy w Internecie zaciera się. Dzieję się tak m.in. dlatego, że koszty przeznaczane na promocję w sieci są niewielkie – małe firmy stać na robienie profesjonalnych stron.

Sposobem na jeszcze większe obniżenie kosztów promocji są serwisy oferujące umieszczanie bannerów za darmo.

Nie płacimy nic, a nasze reklamy umieszczane są w wielu miejscach na świecie (choć niekoniecznie – możemy ograniczać się np. tylko do stron polskich). Ogólna zasada jest taka, że aby ktoś umieścił naszą reklamę za darmo, to i my musimy umieścić banner na swojej stronie.

Opis działania takich serwisów oraz główne zasady przedstawione zostały poniżej.

- Musimy zgodzić się na umieszczenie odpowiedniego kodu HTML na swojej stronie, tak aby możliwe było umieszczanie bannerów. Kodu tego nie możemy najczęściej zmieniać bez zgody danego serwisu.
- Wyświetlany banner na naszej stronie będzie reklamą innego członka serwisu.
- Nie będziemy mogli reklamować pornografii, przemocy i innych działań niezgodnych z prawem.
- Powinniśmy umieszczać bannery na widocznym miejscu (tak, aby zwiększać liczbę „trafień", a tym samym zwiększać nasz kredyt).

6.4.8. Kredyt

Kredyt

Kredyt jest to liczba określająca ilość wyświetleń naszej strony. Najczęściej jest tak, że nasz kredyt zwiększa się o jeden, gdy naszą stronę (wraz z reklamą umieszczoną przez serwis) odwiedzą dwie osoby. Tak więc, czym więcej załadowań ma nasza witryna, tym więcej razy nasza reklama będzie wyświetlana na innych stronach. Trzeba zaznaczyć, że prosta metoda zwiększania liczby odwiedzających poprzez kliknięcie na przycisku „reload" lub „odśwież" najczęściej nie powoduje zwiększenia kredytu.

6.4.9. Stworzenie własnego bannera

Własny banner

To, jakimi cechami powinien charakteryzować się nasz banner, zostało przedstawione powyżej. Na stronach www. serwisów znajdziemy wskazówki, jakimi programami możemy się posługiwać, aby stworzyć własną reklamę. Jeśli takich programów nie posiadamy, to będziemy mogli je „ściągnąć" z miejsca wskazanego przez serwis. Pamiętać należy, że każdy serwis ma inną wymaganą wielkość bannera (np. Smartclick 400x50, a LinkExchange 400x40). Możemy zlecić stworzenie takiej reklamy firmie zajmującej się na co dzień przygotowaniem bannerów, jednak wtedy nie będzie to już całkowicie darmowa promocja naszego przedsiębiorstwa.

NetOn's Banner Exchange
Jest to chyba jeden z najbardziej rozwiniętych serwisów. Możemy wybierać, na jakiego typu stronach mają być wyświetlane nasze strony. Możemy ograniczać zakres tylko do jakiegoś kontynentu, a nawet państwa, adres: http://www.net-on.net/

Link Exchange
Serwis ten ma już ponad 200.000 członków, jest więc chyba największym. adres: http://www.linkexchange.com/
Smartlinks
adres: http://www.smartlinks.net.pl/
Bannermania
adres: http://www.bannermania.nom.pl/

Oczywiście takich serwisów jest znacznie więcej, przytoczone zostały jednak te, które są najciekawsze.

Idea darmowych reklam jest idealnym rozwiązaniem m.in. dla stron niewielkich firm, a nawet stron prywatnych.

Trudno powiedzieć, czy odnosi ona takie skutki, jak reklama komercyjna na najczęściej odwiedzanych witrynach, ale z pewnością jest doskonałym uzupełnieniem i co najważniejsze – całkowicie darmowym.

6.5. Promocja

Promocja

Obok stworzenia profejsonalnej Strony Firmowej i reklamy powinniśmy zająć się promocją. Ma ona na celu częste przyciąganie klientów na nasze strony. Z czasem umożliwi nam to zamieszczanie płatnych reklam komercyjnych przynoszących zyski. Do głównych metod promocji na stronach www należą: konkursy, bezpłatne usługi internetowe, specjalistyczny Serwis Informacyjny, lista dyskusyjna.

6.5.1. Konkursy

Konkursy

Uruchamiając nową stronę z powodzeniem można organizować konkursy. Przyniosą one nam jednak wymierne korzyści tylko wtedy, gdy nasza strona cieszy się sporym zainteresowaniem (czyli np. po przeprowadzeniu reklamy – reklama mogłaby być przeprowadzona równocześnie z konkursem, co zwiększy efektywność bannera reklamowego). Wzorowym przykładem zastosowania konkursów może być nowy portal Interia, który to wraz z uruchomieniem zorganizował konkursy tematyczne (biznes, motoryzacja, turystyka etc.). Z pewnością wpłynęło to pozytywnie na pozyskanie stałych czytelników. Możemy również szukać sponsorów do naszego konkursu (warunkiem jest tu jednak spore zainteresowanie naszą stroną). Jako przykład posłużyć może konkurs organizowany przez Onet.pl i BOŚ (konkurs gry giełdowej– http://gra.onet.pl). Mając ograniczone środki finansowe do puli nagród, możemy włączyć np. utrzymanie kont komercyjnych.

Konto e-mailowe na serwerze

Ciekawym rozwiązaniem jest zakładanie kont e-mailowych na serwerze (dotyczy to jednak tylko Wariantu I i II). Zakładając darmowe konto użytkownik zgadza się na „doklejanie" do każdego listu wiadomości o naszej stronie. Przykładowo, będąc dealerem samochodów BMW i posiadając domenę bmw.pl możemy każdemu chętnemu założyć konto e-mailowe (cały proces może odbywać się automatycznie). Na dole każdego listu dołączamy tylko małą adnotację w postaci:

>...TREŚĆ WIADOMOŚCI...

_ _

Wiadomosc zostala wyslana z wykorzystaniem
stron dealera samochodow Syrena.
http://www.samochody–syrena.pl

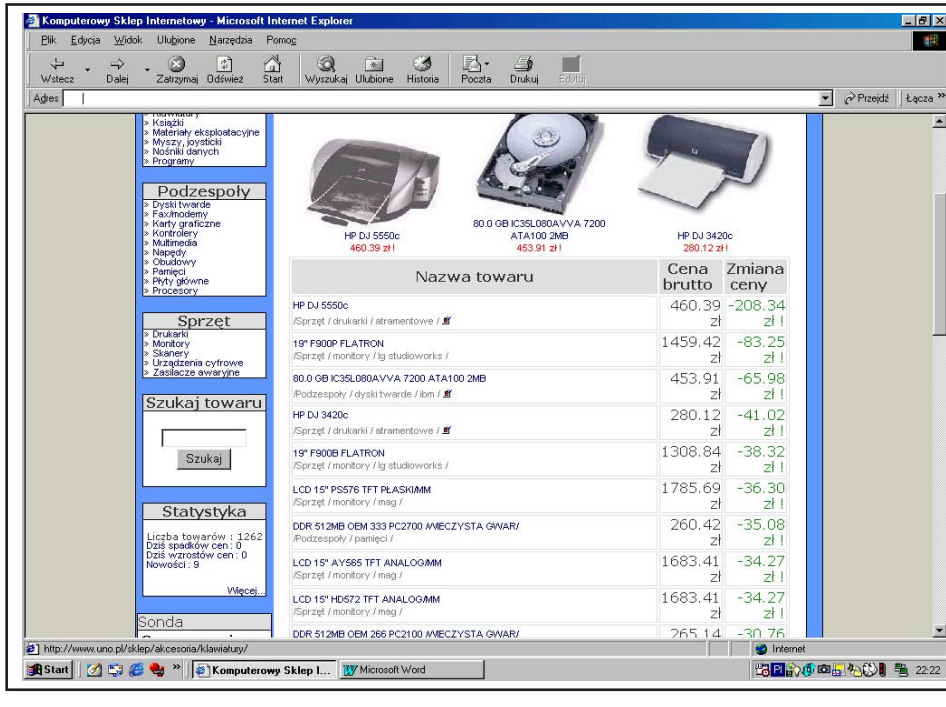
_ _

Zakładając, że przeciętnie otrzymujemy i wysyłamy około 13 e-maili dziennie (źródło: eMarketer) okazuje się, że koszt tej formy promocji będzie naprawdę niewielki.

Fikcyjne serwery wirtualne

Do innej formy bezpłatnej usługi jest założenie „fikcyjnych" serwerów wirtualnych (nie mamy założonego nowego komercyjnego konta, to nowe jest tylko przekierowaniem na dotychczas istniejące). Przykładem może być serwis of.pl. Bezpłatnie możemy założyć „serwer wirtualny" np. http://www.wakacje.of.pl, który będzie faktycznie istniał np. na bezpłatnym serwerze (koszty utrzymania prawdziwego serwera wirtualnego jest dość wysoki i waha się w granicach 50–100 zł miesięcznie). Każdy założony w ten sposób adres będzie reklamą naszej firmy.

Rys. 4. Przykład specjalistycznego serwisu sklepowego zawierającego serwis informacyjny o produkcie



Zakładając specjalistyczny Serwis Informacyjny zakładamy jego częstą (najlepiej codzienną) aktualizację. Taki Serwis ma dużo zalet, m.in.:

- cały czas powiększa nam się grono użytkowników, ponieważ posiadamy stałą grupę czytelników (dzięki częstej aktualizaji) i wciąż zdobywamy nowych,
- wprowadzając „listę subskrybcyjną„ możemy zbierać adresy e-mail naszych Czytelników (umożliwi to w przyszłości wysyłanie powiadomień o zmianach na stronie, reklam, informacji o promocjach czy nowych produktów),
- stworzenie specjalistycznego Serwisu pozwoli zgromadzić grupę użytkowników Internetu zainteresowanych tylko daną dziedziną – umożliwi nam to zwiększenie wskaźnika CPM (jeśli decydowalibyśmy się na umieszczanie na własnej stronie bannerów reklamowych innych firm).

Jeśli spojrzymy na główne portale internetowe w Polsce (i na świecie), to zobaczymy, że niemalże w każdym znajdziemy następujące:

- biznes,
- motoryzacja,
- film,
- muzyka,
- informacje/polityka,
- pogoda,
- sport,
- rozrywka.

Zbudowanie i utrzymanie Serwisu Informacyjnego nie jest z pewnością tanie – jednak przynosi zyski dzięki skierowaniu specjalistycznych informacji do odbiorcy.

6.5.2. Lista dyskusyjna

Lista dyskusyjna

Jest z pewnością doskonałym uzupełnieniem powyższych form promocji. Lista dyskusyjna pozwala zapisanym uczestnikom wymieniać informacje z różnych dziedzin. Temat listy dyskusyjnej definiujemy z góry (np. motoryzacja). Do zalet tej formy promocji należy głównie duży ruch generowany przez uczestników (pamiętajmy, że każdy e-mail jest reklamą naszej firmy). Jeden temat (najczęściej wzbudzający spore kontrowersje – np. czy zakazać pornografii w Internecie) może być poruszamy przez setki uczestników nawet przez kilka tygodni. Lista dyskusyjna jest też znakomitym sposobem na kolekcjonowanie adresów e-mailowych, które to pozwalają przesyłać uczestnikom komercyjne reklamy firm zainteresowanych dotarciem do tegoż grona.

Podsumowanie

Podjęcie działalności w Internecie wymaga przygotowania odpowiedniej strategii postepowania. Kluczowymi elementami sukcesu są: wybór właściwego dostawcy usług, wybór łącza, opracowanie reklamy i, ogólnie – minimalizacja kosztów przy maksymalizacji jakości i indywidualizacji produktu. W warunkach polskich dwa pierwsze elementy nabieraja szczególnego znaczenia ze względu na ograniczoną podaż i bardzo wysokie koszty instalacji. Nawet w tak skromnych warunkach można jednak dokonać optymalnego wyboru stosując strategię wariantową.

Aneks 1

Standardy zabezpieczeń transakcji w USA

Fedwire

System transferów funduszy Fedwire jest jednym z dwu najważniejszych elektronicznych systemów płatniczych obsługujących duże transakcje dolarowe w Stanach Zjednoczonych.

W roku 1996 średnia wartość transakcji dziennych dokonywanych za pomocą serwisu transferowego Fedwire sięgała 989 miliardów dolarów, a średnia suma na jedną transakcję wynosiła 3 miliony dolarów. System Fedwire umożliwia instytucjom będącym depozytariuszami transferować fundusze w swoim własnym imieniu lub w imieniu swoich klientów; większość płatności realizowanych poprzez system Fedwire to transakcje krajowe. Departament Skarbu USA i inne agencje federalne też wykorzystują Fedwire do wypłacania oraz inkasowania funduszy.

Fedwire jest systemem dokonywania rozliczeń na dużą skalę, pracującym w czasie rzeczywistym RTGS (Real–Time Gross Settlement (RTGS). Składa się z dwu elementów: szybkiej sieci telekomunikacyjnej (FED–NET), obejmującej swym zasięgiem całe USA, łączącej wszystkie banki rezerwy federalnej i ich oddziały z instytucjami depozytowymi oraz zbioru komputerów przetwarzających i rejestrujących poszczególne transfery funduszy klientów indywidualnych, w miarę ich dokonywania.

Centrum komputerowe systemu Fedwire EROC (East Rutheford Operation Center) kieruje głównym systemem komputerowym z rezerwą dynamiczną (typu hot –standby), która jest w stanie przejąć pracę niemal natychmiast w przypadku katastrofalnego uszkodzenia systemu głównego. Istnieje też dodatkowe centrum rezerwowe (Bank Rezerwy Federalnej w Richmond) zdolne podjąć pracę w ciągu 60 do 90 minut od całkowitej awarii systemu głównego. Jest ponadto trzecie centrum zapasowe w przypadku, gdyby pierwsze dwa uległy awarii. Ochrona przed katastrofą jest w tym systemie sprawą najważniejszą.

Wiele środków bezpieczeństwa zapewnia integralność i tajność informacji oraz ciągłość systemu. Środki te obejmują kontrolę dostępu, uwierzytelnienie i weryfikację; szyfrowanie danych; kontrolę proceduralną procesów dokonywania zmian w aplikacjach, bankach danych i wprowadzania danych; bezpieczeństwo fizyczne oraz wymagania odnośnie personelu. Wymienione środki kontroli systemu Fedwire mają na celu zapobieganie fałszerstwom, niszczeniu lub ujawnianiu danych przez personel Rezerwy Federalnej bądź przez hakerów zewnętrznych. Na przykład, aby uniemożliwić przejmowanie i fałszowanie danych, komunikaty Fedwire przesyłane między instytucjami obsługującymi depozytariuszy a Rezerwą Federalną są szyfrowane i poddawane uwierzytelnieniu.

Takie środki kontroli dostępu, jak indywidualne kody identyfikacji użytkowników i hasła są podstawowymi sposobami zapobiegania niedozwolonym transferom. Dla przy-

kładu, każdy pracownik instytucji depozytowej musi używać ważnych kodów identyfikacji użytkownika oraz hasła, by zalogować się do systemu Fedwire i wysłać komunikat. Ten komunikat musi pochodzić od instytucji, w której dany urzędnik pracuje.

Bardzo istotną cechą systemu Fedwire jest to, że oferuje on odbiorcy natychmiastową „ostateczność" (tzn. ostateczny i nieodwołalny kredyt). Bank Rezerwy Federalnej „gwarantuje" dokonanie płatności na rzecz instytucji depozytowej, w przypadku obsługi tej transakcji przez Fedwire, przyjmuje również na siebie każde ryzyko kredytowe, o ile w Banku Rezerwy Federalnej na koncie banku wysyłającego zapłatę nie ma dostatecznych środków finansowych.

Międzybankowy system płatniczy izby rozrachunkowej (CHIPS)

CHIPS (Clearing House Interbank Payments System) jest drugim elektronicznym systemem płatniczym dla obsługi dużych kwot w USA. Stanowi własność prywatną i funkcjonuje w ramach Stowarzyszenia Izb Rozrachunkowych w Nowym Jorku NYCHA (New York Clearing House Asociation). Rozpoczął on działalność w roku 1970 jako elektroniczny ekwiwalent czeków papierowych w międzynarodowych płatnościach dolarowych, podczas gdy płatności dokonywane za pośrednictwem systemu Fedwire dotyczą głównie transakcji krajowych, płatności w dolarach USA związane z transakcjami zagranicznymi przechodzą głównie poprzez system CHIPS.

Mimo iż transfery dokonywane poprzez CHIPS są nieodwołalne, są one ostateczne tylko po zakończeniu rozliczenia dziennego. CHIPS rozlicza swe transakcje na zasadach multilateralnych. Jeśli więc bank otrzymujący transfer CHIPS udostępnia fundusze swym klientom zanim rozliczenie dzienne zostanie zakończone, naraża się tym samym na ryzyko strat, gdy CHIPS nie dokona rozliczenia. Podczas 27 lat działalności systemu CHIPS nigdy się to jednak nie zdarzyło (to odróżnia system CHIPS od Fedwire oferującego natychmiastową ostateczność rozliczenia – Rezerwa Federalna „gwarantuje" płatność i przyjmuje na siebie każde ryzyko kredytowe.) Przebieg transakcji CHIPS poznamy na przykładzie handlowca europejskiego, który pragnie zapłacić 2 miliony dolarów pewnemu dostawcy z USA za dostawę dóbr konsumpcyjnych. Handlowiec zleca swemu bankowi, aby obciążył jego konto sumą w euro, stanowiącą równowartość 2 milionów USD i aby dokonał płatności w dolarach dostawcy amerykańskiemu na jego konto w USA. Transakcja między tymi dwoma bankami nie zostanie rozliczona, zanim CHIPS nie dokona rozliczenia dziennego.

Z technicznego punktu widzenia bank w USA będzie wystawiony na ryzyko, jeśli wypłaci klientowi sumę 2 milionów USD w dniu przeprowadzenia transakcji.

W typowym dniu uczestnicy CHIPS mogą w sposób ciągły wymieniać płatności między sobą, a system CHIPS będzie obliczać na bieżąco stan konta każdego z nich vis-a-vis wszystkich innych uczestników. Proces ten nazywany jest „rozliczaniem multilateralnym".

Uczestnicy procesu biorą udział w rozliczeniach systemu CHIPS wysyłając i otrzymując płatności Fedwire niezbędne do realizacji rozliczenia. Uczestnicy nie dokonujący rozliczeń muszą wyznaczyć uczestnika rozliczającego, aby dokonać rozliczenia w ich imieniu, a ten musi wyrazić zgodę na przyjęcie roli rozliczającego.

Po tym, jak wszyscy rozliczający się uczestnicy będący na debecie dokonają wypłaty środków pieniężnych, a uczestnicy będący w stanie kredytu otrzymają transfery funduszy Fedwire od NYCHA, konto rozrachunkowe CHIPS w Nowojorskim Banku Rezerwy Federalnej (FRBNY) osiągnie stan bilansowy zerowy. W tym właśnie momencie transakcja dokonana poprzez CHIPS między uczestnikami zostaje rozliczona, a rozliczenie staje się ostateczne.

CHIPS utrzymuje centrum rezerwowe w stanie rezerwy dynamicznej. Pozwala mu to podjąć proces płatniczy w ciągu pięciu minut od chwili ewentualnej awarii głównego centrum przetwarzania. Gdy baza danych systemu CHIPS ulegnie awarii, CHIPS ma możliwość komputerowej odbudowy tej bazy danych. Każdy uczestnik jest w stanie automatycznie powtórzyć komunikat o płatności wysłany już uprzednio, jeśli CHIPS zasygnalizuje utratę tego komunikatu, wysyłając odpowiednie zawiadomienie.

Zgodnie z dokumentem NYCHA, system CHIPS testuje kwartalnie swoje plany akcji pod kątem rozmaitych symulowanych zdarzeń w ramach obowiązkowych ćwiczeń obejmujących wszystkich uczestników.

Aneks 2

Platforma Supersam B2B

Platforma Supersam B2B jest to oprogramowanie sklepu internetowego klasy **B2B**. Bazuje na platformie Akopia Interchange TM, rozpowszechnianej na zasadach Open Source. Integralnymi częściami systemu jest baza danych POSTGRES **SQL** oraz Apache Web Server. Dzięki szerokim możliwościom, otwartej architekturze i dużej elastyczności system SUPERSAM jest trafnym wyborem.

Cechy podstawowe

- inteligentne sprzedawanie,
- mechanizmy uczenia się upodobań klientów,
- łatwy dostęp do podzielonych na grupy oraz szczegółowo opisanych artykułów,
- podpowiadanie klientowi ofert uzupełniających i komplementarnych; oferowanie sprzedaży wiązanej i promocyjnej,
- szybki proces kupowania; dostępne listy zakupowe,
- wbudowana wyszukiwarka,
- kreowanie nowych kanałów dystrybucji dzięki programom partnerskim,
- system rabatów oparty o indywidualne profile klienta, umowy handlowe, upusty ilościowe oraz promocje,
- zaawansowana obsługa klienta, włącznie z listem elektronicznym oraz personalizowaną stroną przedstawiającą historię transakcji,
- możliwość integracji z systemami ERP,
- możliwość kreowania sieci dystrybucji.

Zarządzanie produktami

- maksymalizowanie zysków dzięki możliwości kreowania polityki cen w oparciu o atrybuty produktu,
- łatwa aktualizacja zawartości witryny dzięki łatwemu aktualizowaniu opisów produktów i możliwości wgrywania zdjęć,
- prezentowanie klientom dostępności towarów oraz czasów realizacji w oparciu o systemy magazynowe.

Zarządzanie witryną

- łatwe dodawanie nowych stron do witryny z wykorzystaniem szablonów,
- prezentowanie klientom oczekiwanych przez nich produktów, dynamiczne generowanie zawartości, indywidualnie dla każdego klienta,
- łatwa edycja zawartości i wyglądu witryny poprzez administratora opartego o przeglądarkę internetową.

Monitorowanie transakcji

- ewidencjonowanie listy zamówień,
- możliwość implementowania schematu obiegu dokumentów oraz praw dostępu do funkcji programu,

- oferowanie klientowi całości informacji w momencie składania zamówienia,
- możliwość akceptacji różnych form płatności włącznie z kartami płatniczymi, czekami, przelewem, zaliczeniem pocztowym,
- powiadamianie listem elektronicznym o składanych zamówieniach,
- automatyczne naliczanie prowizji e-partnerom.

Obsługa klientów
- umożliwienie klientom samodzielnego modyfikowania własnych danych,
- podniesienie satysfakcji klientów dzięki obsłudze 24 h na dobę z możliwością śledzenia stanu realizacji zamówień,
- redukcja kosztów obsługi klienta dzięki udostępnieniu on-line archiwalnych danych związanych z obsługą klienta,
- redukcja czasu zwrotu towaru dzięki autoryzacji zwrotów on-line.

Raportowanie
- wszechstronne analizy zamówień,
- możliwość eksportowania raportów w celu zewnętrznej analizy,
- możliwość definiowania raportów,
- raporty odwiedzalności sklepu.

Administracja techniczna witryną
- pełna kontrola nad zarządzaną witryną dzięki panelowi kontrolnemu zabezpieczonemu systemem haseł,
- możliwość definiowania użytkowników z dowolnie określonymi prawami dostępu
- możliwość bezpośredniej edycji danych,
- dowolna skalowalność systemu możliwość pracy w oparciu o bazę danych ORACLE.

Aneks 3

Centrum Certyfikacji Unizeto Certum

1. Podpis elektroniczny wg Unizeto

Centrum Certyfikacji Unizeto Certum jest strukturą wydzieloną w ramach Unizeto Sp. z o.o. Jednostka macierzysta została utworzona w 1965 roku, jako jeden z Zakładów Elektronicznych Technik Obliczeniowych. Szczecińskie ZETO, podobnie jak inne przedsiębiorstwa tej grupy, w pierwszym okresie działalności zajmowało się przede wszystkim świadczeniem usług obliczeniowych dla podmiotów mających potrzebę wykonywania dużej liczby operacji liczbowych, nie dysponujących ku temu odpowiednim sprzętem. Wraz z rozwojem technologii informatycznych, upowszechnieniem dostępu do komputerów i wzrostem ich mocy obliczeniowej zmieniał się profil działalności firmy.

Na początku lat dziewięćdziesiątych przedsiębiorstwo zostało sprywatyzowane i przyjęło nazwę Unizeto.
Unizeto jest aktywnym na terenie całej Polski integratorem bezpiecznych rozwiązań teleinformatycznych, dostawcą oprogramowania i sprzętu komputerowego oraz wykonawcą instalacji (sieci komputerowe, instalacje inteligentnego budynku). Firma świadczy również usługi serwisowe i szkoleniowe. W 2001 r. Unizeto utworzyło Ogólnopolską Sieć Ośrodków Szkoleniowych w zakresie podpisu i dokumentu elektronicznego – UCATC.

Centrum Certyfikacji Unizeto Certum powstało w roku 1998. Pierwsza dedykowana, ogólnopolska infrastruktura klucza publicznego, dla Zakładu Ubezpieczeń Społecznych została uruchomiona na początku 1999 roku. W czerwcu 2002 r. Unizeto rozpoczęło wdrożenie największej w Polsce wydzielonej infrastruktury dla PZU Życie SA (docelowo 5.000.000 użytkowników).

W dniu wejścia w życie ustawy o podpisie elektronicznym Centrum Certyfikacji Unizeto Certum: zarządza około 210.000 certyfikatami klucza publicznego, odnotowuje średnio 120 000 odsłon w ciągu doby (w serwisie www), obsługuje ponad 150 000 klientów indywidualnych i firm komercyjnych, poprzez swych konsultantów i operatorów udziela porad i konsultacji oraz obsługuje proces certyfikacji dla kilkuset klientów dziennie.

1.1. Charakterystyka PKI Centrum Certyfikacji Unizeto Certum[41]

Infrastruktura Klucza Publicznego, którą posługuje się CC Unizeto Certum jest rozwiązaniem autorskim, stworzonym we współpracy z kadrą naukową Politechniki Szczecińskiej oraz niezależnymi ekspertami z zakresu kryptografii.

[41] W marcu 2003 należące do TP Internet centrum certyfikacji Signet zostało, jako drugie przedsiębiorstwo, wpisane do rejestru kwalifikowanych podmiotów, świadczących usługi certyfikacyjne. Procedura uzyskania wpisu trwała kilka miesięcy, mniej więcej od połowy zeszłego roku. Składało się na nią złożenie wniosku o wpis z podaniem wyczerpującego opisu działania ośrodka certfikacyjnego, w wyniku którego stosowne czynniki państwowe przeprowadziły audyt bezpieczeństwa. Signet uzyskałby wpis prawdopodobnie wcześniej, gdyby nie fakt odwołania ministra Jacka Piechoty i likwidacji Ministerstwa Gospodarki, które prowadzi rejestr. Procedurą finalizowało już Ministerstwo Gospodarki, Pracy i Polityki Socjalnej. Jako pierwszy na listę kwalifikowanych podmiotów wciągnięte zostało Unizeto. Wniosek składała również Państwowa Wytwórnia Papierów Wartościowych, ale nie został on rozpatrzony pozytywnie.

Podstawowe założenia, związane z rolą CC Unizeto Certum jako zaufanej strony trzeciej, zasadami bezpieczeństwa towarzyszącymi wydawaniu certyfikatów, obowiązkami subskrybentów oraz organizacją Centrum Certyfikacji określają Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego. Obydwa dokumenty, w obowiązującej aktualnie wersji, wraz z określeniem daty, od której obowiązują można znaleźć na stronach internetowych CC Unizeto Certum, pod adresem http://www.certum.pl.

CC Unizeto Certum wydaje ponad 50 typów certyfikatów do różnych zastosowań. Podstawowe produkty to:

- certyfikaty bezpiecznej poczty elektronicznej, służące do podpisywania i szyfrowania przesyłek ekspediowanych przez Internet. Stosowanie certyfikatów pozwala na osiągnięcie poufności przesyłanych danych oraz ich integralności,
- certyfikaty serwerów www, służące do zabezpieczenia dostępu do serwerów internetowych, bankowych serwerów dostępowych oraz hostów korporacyjnych WWW. Certyfikaty wymuszają silną kryptografię 128-bit SSL Server Gated Cryptography. Stosowane przede wszystkim w sytuacji, gdy użytkownicy zewnętrzni przekazują przez Internet dane personalne, hasła i inne poufne informacje,
- certyfikaty serwerów SSL/TLS, znajdujące zastosowanie dla serwerów pocztowych SMTP, serwerów odbioru poczty POP3, IMAP, korporacyjnych usług NNTP, hostów LDAP oraz serwerów SMB. Certyfikaty wymuszające silną kryptografię 128-bit SSL Server Gated Cryptography. Pozwalają na przepływ informacji między oddziałami firmy z wykorzystaniem mechanizmów szyfrowania i autoryzacji,
- certyfikaty do podpisywania kodu, dające pewność, że stworzone oprogramowanie dociera do odbiorców bez modyfikacji (hakerzy, infekcja wirusem),
- certyfikaty Strong Internet, służące do uwierzytelniania się i nawiązywania bezpiecznego połączenia między serwerem korporacyjnym (Enterprise Server) a klientem znajdującym się w dowolnej lokalizacji. Zastosowanie certyfikatu pozwala na zastąpienie klasycznej metody autoryzacji z użyciem hasła i nazwy użytkownika, umożliwia zastosowanie kart kryptograficznych zarówno do logowania się na stacje robocze, jak i silnej autoryzacji przez Internet. Pozwala na utworzenie sieci intranetowych, ekstranetowych oraz autoryzowanego dostępu do serwera WWW, SMTP, POP3 czy LDAP, do zasobów bazy danych bez obawy o naruszenie poufności przekazywanych informacji,
- certyfikaty VPN, służące do zabezpieczania przepływających danych w sieciach korporacyjnych VPN. Certyfikaty obsługujące routery i klientów, współpracujące z rozwiązaniami: Cisco, Windows 2000, VPN–1 Family, Contivity VPN.

CC Unizeto Certum składa się z 5 odrębnych urzędów certyfikacyjnych Certum Level I, Certum Level II, Certum Level III, Certum Level IV, CA–NAD, przeznaczonych do podpisywania certyfikatów i list CRL w różnych klasach wiarygodności.

Certyfikaty wystawiane przez urzędy poszczególnych poziomów (levels) różnią się między sobą procedurami weryfikacji tożsamości podmiotu (osoby, organizacji) ubiegającego się o przyznanie certyfikatu, okresem ważności certyfikatu oraz poziomem gwarancji finansowych ze strony Unizeto.

Gwarancje finansowe dotyczą sytuacji, w których użyty certyfikat:

- został wystawiony dla nieprawidłowego użytkownika – czyli wystąpiła sytuacja nieprawidłowej weryfikacji tożsamości osoby ubiegającej się o certyfikat;

- konkretna para kluczy prywatnego i publicznego została wystawiona dla więcej niż jednego użytkownika – czyli powstała możliwość odczytania treści korespondencji przez osobę nieuprawnioną (rozszyfrowanie własnym kluczem prywatnym treści przesyłki szyfrowanej kluczem publicznym innej osoby, identycznym z własnym kluczem publicznym);
- mimo zastosowania mechanizmów szyfrowania informacja została rozszyfrowana przez nieuprawnionego użytkownika (tzn. osobę inną, niż właściwy odbiorca przesyłki, dysponujący ważnym, własnym kluczem prywatnym wystawionym przez CC Unizeto Certum).

Dla każdego z poziomów certyfikatów różne są też opłaty za wystawienie i odnowienie certyfikatu.

W ramach Centrum Certyfikacji Unizeto Certum działa siedem pośrednich urzędów certyfikacyjnych dostarczających użytkownikom (subskrybentom) usługi dodatkowe:
- Kurier Elektroniczny, będący odpowiednikiem tradycyjnej przesyłki poleconej z potwierdzeniem odbioru. Klient usługi dysponuje przechowywanymi przez CC Unizeto Certum dowodami nadania przez nadawcę i odbioru przez adresata korespondencji elektronicznej. Wymienione dowody są niepodatne na próby modyfikacji przez strony korespondencji,
- Elektroniczny Datownik, będący usługą polegającą na znakowaniu czasem przesyłki lub innego obiektu, w sposób pozwalający na jednoznaczne stwierdzenie prób późniejszej modyfikacji lub antydatowania dokumentu. Dokładność czasu wykorzystywanego przez Elektroniczny Datownik zapewniana jest dzięki wykorzystaniu zegarów atomowych za pośrednictwem odbiornika satelitarnego,
- Skarbiec Elektroniczny, polegający na udostępnieniu użytkownikowi osobistej skrytki, w której przechowywane mogą być: certyfikaty osób trzecich wydane przez inne urzędy certyfikacyjne, podpisy elektroniczne, klucze i znaczniki czasu. Usługa gwarantuje integralność przechowywanych obiektów, a także ich bezpieczny transfer przez Internet,
- Elektroniczny Notariat, będący usługą poświadczania niezaprzeczalności wykorzystywaną w transakcjach elektronicznych w celu: poświadczenia dowodu posiadania danych i ich ważności, poświadczenia ważności identyfikatora cyfrowego (certyfikatu), poświadczenia ważności podpisu elektronicznego.

Jednym ze sposobów pozyskania certyfikatów, np. dla poczty e-mail, jest użycie typowej przeglądarki internetowej. Procedura jest w znacznym stopniu zautomatyzowana – odpowiednie formularze prowadzą użytkownika za pomocą czytelnych komunikatów. Rozwiązania dostarczane przez Unizeto są wspierane przez zdecydowaną większość popularnych, dostępnych na rynku aplikacji (serwerów, klientów poczty) i instrukcje uwzględniają ich specyfikę. W przypadku wykorzystywania rzadziej spotykanego oprogramowania oraz jakichkolwiek innych problemów, do dyspozycji klientów jest telefoniczna pomoc techniczna.

Wygenerowane certyfikaty są instalowane na komputerze, na którym była prowadzona procedura certyfikacji. Certyfikaty mogą być eksportowane na inne komputery, na dyskietkę lub na kartę mikroprocesorową.

W ramach działalności CC Unizeto Certum publikuje listy certyfikatów unieważnionych oraz daje możliwość zweryfikowania w trybie on-line statusu konkretnego certyfikatu.

2. System SET

Podamy tu bardziej szczegółowy opis architektury systemu SET. Warto go prześledzić, gdyż system ten daje dobre podstawy do zrozumienia zagadnień dotyczących płatności elektronicznych oraz podstawowe elementy technologiczne, z jakimi się tam spotykamy.

SET jest zbiorem technicznych unormowań, do których prawa mają wspólnie firmy Visa i Mastercard. Specyfikacje techniczne opracowano w firmach GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa i VeriSign. System SET korzysta w dużym stopniu z technologii zabezpieczeń, włączając w to certyfikację oraz podpisy cyfrowe.

2.1. Wymagania biznesowe systemu SET

SET identyfikuje siedem wymagań odnoszących się do biznesu, proponując rozwiązania techniczne zapewniające ich spełnienie.

l. Poufność informacji
SET identyfikuje potrzebę poufności informacji, zarówno dotyczącej zamówień, jak i towarzyszącej jej informacji odnoszącej się do płatności. Aby ją zaspokoić, stosuje się szyfrowanie wiadomości. Podejście to zakłada, co należy podkreślić, szyfrowanie samych wiadomości, a nie tylko zabezpieczenie kanałów służących do ich przesyłania.

Zaszyfrowany transport, jak warstwa zabezpieczenia łączy, służy utajnieniu treści przed szpiegami, lecz odbiorca wiadomości może odczytać ją w całości.

Szyfrując same komunikaty, można je potem bezpiecznie przesyłać za pośrednictwem różnych osób trzecich pełniących rozmaite role, będąc pewnym, iż każda z nich będzie w stanie odczytać jedynie tę część komunikatu, jaka jej dotyczy. Przykładowo: handlowiec będzie w stanie odszyfrować część informacji dotyczącą zamówienia, lecz nie odczyta towarzyszącej jej informacji na temat płatności.

2. Integralność wszystkich przesyłanych danych
Wszystkie strony zaangażowane w transakcję elektroniczną muszą być pewne, iż dane nie uległy manipulacji ze strony osób niepowołanych lub modyfikacji w czasie przesyłania. SET używa podpisów cyfrowych, za pomocą których podpisuje się dane przed ich wysłaniem.

3. Uwierzytelnienie faktu, że posiadacz markowej karty jest uprawnionym użytkownikiem konta płatniczego powiązanego z tą kartą.

Gdy ktoś płaci kartą kredytową, ważne jest, aby handlowiec mógł skojarzyć tę osobę z jej kontem kartowym. Przy transakcji w obecności klienta (np. w sklepie), handlowiec łączy posiadacza karty z kartą prosząc go o złożenie podpisu mającego pasować do znajdującego się na karcie, a następnie łączy kartę z kontem jej posiadacza. W tym celu ogląda kartę sprawdzając czy jest autentyczna, a w wielu przypadkach kontaktuje się z wydawcą karty, sprawdzając tym samym, czy konto jest ważne.

W transakcjach internetowych powszechnie stosuje się prosty sposób polegający na żądaniu od osoby dokonującej zakupu podania numeru swej karty, daty jej ważności oraz innej informacji osobistej. Sposób ten uznaje się za wystarczający do skojarzenia danej osoby z kontem bankowym, lecz nie jest to zbyt bezpieczne i umożliwia nadużycia. Jeśli uda mi się uzyskać numer czyjejś karty kredytowej i jej datę ważności (można tego dokonać szybko oglądając kartę), to mogę łatwo dokonać transakcji elektronicznej w imieniu posiadacza tej karty.

SET załatwia ten problem używając kombinacji certyfikatów posiadacza karty oraz podpisów elektronicznych. Certyfikaty posiadacza karty są w systemie SET e-biznesowym odpowiednikiem karty płatniczej. Przy ich wydawaniu są podpisywane cyfrowo przez bank, który je wydaje. Tym sposobem zostają zabezpieczone przed modyfikacją lub fałszerstwem. Jak podano w odniesieniu do fizycznych kart płatniczych, „tajna „ informacja na nich zapisana (która dlatego uwierzytelnia jej użycie w wielu praktycznych okolicznościach), to numer konta i data ważności karty. W przypadku certyfikatu posiadacza karty, informacja dotycząca konta oraz tajna wartość (tzn. PIN lub hasło) są zaszyfrowane przy użyciu jednostronnego algorytmu skrótu. Dane te są więc łatwe do weryfikacji przez porównanie z zawartością certyfikatu, lecz nie mogą zostać odtworzone na jego podstawie.

4. Uwierzytelnienie faktu, że handlowiec może zaakceptować transakcję dokonywaną za pomocą markowej karty płatniczej, na podstawie jej związku z bankiem obsługującym tego handlowca.

Posiadacze kart potrzebują sprawdzić, czy dany handlowiec posiada konto w banku, pozwalając mu tym sposobem na zaakceptowanie kart kredytowych. Ci posiadacze kart muszą być w stanie potwierdzić tożsamość handlowca. Oznacza to, że jeśli płacę firmie X, to muszę być pewien, iż dana strona internetowa jest rzeczywiście stroną jednej z tych firm, a nie inną witryną o podobnej nazwie, lecz zarządzaną przez jakiegoś oszusta bez skrupułów. SET załatwia ten problem używając podpisów cyfrowych i certyfikatów handlowca. Certyfikaty handlowca są w systemie SET e-biznesowym odpowiednikiem nalepki Visa, jaka widnieje często na szybach wystaw sklepowych, lecz ich zawartość, jest nieco bardziej bogata. Przy wydawaniu certyfikaty handlowca są podpisywane przez bank i dlatego gwarantują, iż handlowiec ma umowę z tym właśnie bankiem.

5. Zagwarantowanie użycia najlepszych zasad bezpieczeństwa i technik projektowania systemów do ochrony wszystkich stron uprawomocnionych do brania udziału w elektronicznej transakcji handlowej.

Jak już stwierdzono, SET oferuje pełną architekturę systemu płatniczego. W zgodzie z zasadami SET spełnił wymaganie zachowania najlepszych zasad bezpieczeństwa odwołując się do ekspertyz takich wiodących firm, jak GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa i VeriSign.

6. Stworzenie protokołu niezależnego od mechanizmów bezpieczeństwa transportu, lecz nie wykluczającego ich użycia.

Intencją SET jest raczej przestrzeganie zasad bezpieczeństwa w odniesieniu do aplikacji oraz komunikatów przekazywanych pomiędzy tymi aplikacjami niż poleganie na bezpiecznej infrastrukturze transportowej.

7. Ułatwienie i zachęta do współpracy pomiędzy operatorami softwarowymi i sieciowymi

SET definiuje w tym celu otwarty zbiór specyfikacji dotyczących przesyłanych wiadomości. Szczegółowe dane na ten temat podano w raporcie: SET Secure Electronic Transaction Specification Version 1.0.

2.2. Przykład transakcji SET

Architekturę SET omówimy na przykładzie posiadacza karty kupującego pewne dobra on-line i płacącego kartą kredytową. Ominiemy pewne złożone problemy, np. to, że wszyscy uczestnicy transakcji mogą akceptować płatności dokonywane przy użyciu różnych kart płatniczych wydanych przez różne instytucje handlowe. Będziemy więc zakładać, że płatność zostanie dokonana za pośrednictwem bramy płatniczej, której operatorem jest bank przyjmujący płatności. Od razu na początku przyjmiemy pewne założenia.

- Posiadacz karty ma już konto w banku wydającym karty i otrzymał certyfikat posiadacza karty.
- Handlowiec ma już konto w banku i otrzymał od niego certyfikat handlowca.
- Posiadacz karty i handlowiec mają już „klucz podpisujący" służący do podpisywania komunikatów. Każdy klucz podpisujący składa się z dwu części: klucza publicznego i klucza prywatnego.
- Brama płatnicza ma certyfikat, którego kopia znajduje się u handlowca. Ten certyfikat jest w istocie podpisaną kopią klucza publicznego bramy płatniczej.

Przebieg tej transakcji śledzimy od momentu, gdy posiadacz karty przeszukał witrynę internetową handlowca, wybrał produkty do zakupu, wypełnił on-line pewien formularz zamówienia, a teraz pragnie dokonać płatności.

Komunikat o zamówieniu wstępnym
Komputer posiadacza karty wysyła do komputera handlowca wiadomość zamówienie wstępne.

Komunikat o odpowiedzi wstępnej

l. Gdy komputer handlowca otrzymuje wiadomość zamówienie wstępne, generuje najpierw jeden unikalny identyfikator transakcji, który będzie odtąd używany w czasie całego procesu.
2. Następnie generuje on wiadomość odpowiedź wstępna (zawierającą identyfikator transakcji).
3. Komputer handlowca podpisuje cyfrowo komunikat odpowiedź wstępna (tworząc jego skrót i szyfrując go za pomocą prywatnego klucza podpisującego handlowca).
4. Komputer handlowca wysyła podpisany komunikat odpowiedź wstępna do posiadacza karty, razem z certyfikatem handlowca oraz certyfikatem bramy płatniczej.

Komunikat o zleceniu zakupu

1. Gdy komputer posiadacza karty otrzyma komunikat odpowiedź wstępna, sprawdza najpierw integralność komunikatu za pomocą podpisu handlowca, tzn. komputer posiadacza karty tworzy jego skrót i porównuje go z podpisem rozszyfrowanym za pomocą publicznego klucza podpisującego handlowca. Oba powinny być takie same, jeśli tylko wiadomości po drodze nie sfałszowano.
2. Komputer posiadacza karty weryfikuje certyfikaty handlowca i bramy płatniczej przechodząc (traversing) przez łańcuch zaufania (trust chain) do klucza głównego (root key). Zdobywa w ten sposób pewność, że handlowiec oraz brama są tymi, za których się podają, oraz że certyfikat handlowca wydał autentyczny bank.
3. Komputer posiadacza karty generuje następnie informację o zakupie (Order Information (0I) oraz instrukcje płatnicze (Payment Instructions (PI).
4. Generuje on podwójny podpis dla OI oraz PI tworząc ich skróty, dokonując złączenia (konkatenacji) obu liczb, tworząc skrót wyniku, szyfrując go prywatnym kluczem podpisującego posiadacza karty. Ten podwójny podpis będzie stosowany dla indywidualnej oraz łącznej ochrony integralności komunikatów OI oraz PI.
5. Komputer posiadacza karty generuje przypadkowy symetryczny klucz szyfrujący (K) stosując go następnie do zaszyfrowania komunikatu PI. Ten krok jest konieczny, aby zapewnić tajność informacji płatniczej, szczególnie gdy płatności dokonywane są poprzez pośredników, takich jak handlowiec.
6. Informacja o koncie posiadacza karty jest szyfrowana łącznie z kluczem K z użyciem publicznego klucza bramy płatniczej (wziętego z jej certyfikatu).
7. Komputer posiadacza karty generuje komunikat zlecenie zakupu zawierający OI, zaszyfrowane PI, skrót wiadomości PI oraz podwójny podpis.

Komunikat odpowiedzi na zlecenie zakupu

l. Gdy komputer handlowca otrzyma zlecenie zakupu, weryfikuje certyfikat podpisujący posiadacza karty przechodząc przez łańcuch zaufania do klucza głównego.
2. Następnie sprawdza on integralność zamówienia używając podwójnego podpisu. Można tego dokonać rozszyfrowując je kluczem publicznym posiadacza karty i porównując ten wynik z konkatenacją (złożeniem) skrótu OI (który handlowiec może obliczyć) ze skrótem PI (dołączonym do komunikatu zlecenia zakupu).
3. Komputer handlowca kieruje zaszyfrowaną informację płatniczą do bramy płatniczej.
4. Zamówienie jest przetwarzane przez handlowca zgodnie z zawartością komunikatu OI.
5. Komputer handlowca generuje i podpisuje cyfrowo komunikat odpowiedzi na zakup. Składa się on z kopii certyfikatu podpisującego handlowca oraz wiadomości, że zamówienie posiadacza karty zostało odebrane przez handlowca.

Komputer posiadacza karty

Zamówienie wstępne

1. Zweryfikować podpis handlowca.
2. Zweryfikować certyfikaty przechodząc przez łańcuch zaufania.
3. Utworzyć informację o zamówieniu (OI) oraz instrukcję płatniczą (PI).
4. Utworzyć podpis podwójny na podstawie OI oraz PI (konkatenacja obu skrótów, skrót wyniku zaszyfrować prywatnym kluczem podpisu posiadacza karty).
5. Utworzyć przypadkowy symetryczny klucz szyfrujący (K), zaszyfrować nim PI.
6. Zaszyfrować informację o stanie konta posiadacza karty wraz z K, za pomocą publicznego klucza bramy płatniczej, wziętego z jej certyfikatu.
7. Utworzyć komunikat zlecenie zakupu.

Zweryfikować certyfikat podpisu handlowca przechodząc przez łańcuch zaufania. Sprawdzić integralność komunikatu przy użyciu podpisu cyfrowego.

Odpowiedź wstępna + Certyfikat handlowca + Certyfikat bramy płatniczej
Zlecenie zakupu + OI + Zaszyfrowane PI
Odpowiedź na zakup

Komputer handlowca

1. Przyznać unikalny ID transakcji.
2. Wygenerować komunikat Odpowiedzi wstępnej (obejmujący ID).
3. Podpisać komunikat kluczem prywatnym.
4. Wysłać komunikat plus certyfikat handlowca i certyfikat bramy płatniczej.
5. Zweryfikować certyfikat podpisu posiadacza karty, przechodząc przez łańcuch zaufania.
6. Zweryfikować podpis podwójny.
7. Przekazać zaszyfrowany ID do bramy płatniczej.
8. Przetworzyć informacje o zamówieniu.
9. Utworzyć komunikat odpowiedź na zakup i podpisać go cyfrowo.
10. Gdy komputer posiadacza karty otrzyma odpowiedź na zakup od handlowca, sprawdza najpierw integralność komunikatu za pomocą podpisu cyfrowego handlowca. Weryfikuje następnie certyfikat podpisującego handlowca przechodząc przez łańcuch zaufania do klucza głównego.

2.3. Podsumowanie działania systemu SET

Opisany schemat działania jest dosyć złożony, ale ma zalety:
- Integralność komunikatów jest sprawdzana na wszystkich etapach poprzez zastosowanie podpisów cyfrowych.
- Odpowiednie poziomy tajności są zachowane poprzez szyfrowanie komunikatów (np. handlowiec nie może zobaczyć szczegółowych instrukcji płatniczych wysyłanych do banku przyjmującego zapłatę).
- Mimo niezależnego traktowania informacji dotyczących zamówienia i płatności, są one zintegrowane za pomocą „podwójnego klucza „chroniącego je łącznie, a integralność może zostać zweryfikowana nawet przez tych, którzy (jak handlowiec) nie mają dostępu do całej zawartości komunikatu.
- Tożsamość wszystkich stron jest zapewniona za sprawą certyfikatów (podpisanych przez zaufane strony trzecie).

W czasie pisania tej książki standardy SET nie były jeszcze zbyt rozpowszechnione i nic na przykład nie wiadomo o ich ewentualnym zastosowaniu gdziekolwiek w Wielkiej Brytanii. Prawdopodobnie podstawową przyczyną tego stanu jest konieczność uzyskania (i posługiwania się nim) certyfikatu i klucza podpisującego przez posiadacza karty.

Posługiwanie się kartą plastikową jest łatwe zarówno dla jej wydawcy, jak i dla posiadacza, inaczej jest w przypadku certyfikatów elektronicznych. Dane te mogą się np. znaleźć na komputerze używanym przez inne osoby; można je wówczas przypadkowo lub celowo skopiować. Nie nadają się też do wygodnego przenoszenia (np. między pracą a domem).

Prawdopodobnie najważniejszym warunkiem przyjęcia standardu SET okaże się wprowadzenie fizycznego sposobu przechowywania certyfikatów, takiego jak karty inteligentne oraz zintegrowanie używanych środków z komputerami PC tak, aby można było za ich pomocą odczytywać niezbędne dane. Ten ostatni warunek nie jest bez znaczenia, gdyż musi zostać zrealizowany za pośrednictwem godnych zaufania składników systemu.

3. „Instant office", czyli „gotowe biura" – nowy sposób prowadzenia biznesu

Na zachodzie Europy i w Stanach Zjednoczonych korzystanie z usług typu „instant office" jest tak popularne, jak rezerwacja pokoju hotelowego czy wynajęcie samochodu, w Polsce – prawie nikt o tym nie słyszał.

„Instant office" w wolnym tłumaczeniu: „biuro/siedziba firmy od ręki" jest to usługa umożliwiająca szybkie otwarcie i elastyczne prowadzenie działalności gospodarczej. Pod tym terminem kryje się kompleksowe wsparcie w postaci: w pełni wyposażonych pokoi biurowych, sal konferencyjnych, recepcji i sekretariatu, a także tzw. „consierge" – dostaw biurowych, cateringu, organizowania podróży oraz doradztwa biznesowego (obsługa prawna, finansowo-księgowa...).

Dla osób myślących o założeniu swojego interesu oznacza to możliwość natychmiastowego rozpoczęcia działania, bez konieczności zaciągania długoterminowych zobowiązań (jak to się ma chociażby w przypadku wynajmu powierzchni biurowej) oraz bez ponoszenia wysokich kosztów związanych z profesjonalnym wyposażeniem i utrzymaniem swojej siedziby. W dzisiejszych czasach, gdy wszyscy poszukują oszczędności, usługa „gotowe biuro" jest sposobem na optymalizację wydatków i podniesienie sprawności działania.

Z punktu widzenia organizacji działań, można powiedzieć, że jest to odmiana outsourcingu. W tym przypadku dostawcy zewnętrznemu przekazuje się prowadzenie biura i sprawowanie funkcji administracyjnych. Zgodnie z zasadą „niech każdy robi to, na czym zna się najlepiej", korzystanie z „instant office" niesie ze sobą wiele korzyści:
- umożliwia skoncentrowanie wysiłków na podstawowej działalności,
- obniża koszty,
- zwiększa elastyczność działania (umożliwia szybkie reagowanie na zmiany otoczenia,
- redukuje ryzyko,
- zapewnia profesjonalną obsługę, gwarantuje określony poziom jakości.

Badania przeprowadzone przez UK Chartered Institute of Purchasing and Supply wykazały, iż przedsiębiorcy korzystający z „gotowych biur" mogą oszczędzić nawet do 66% kosztów w porównaniu z tradycyjnym wynajmowaniem powierzchni biurowych.

Dla niewielkich firm rozpoczynających swój biznes i niepewnych sukcesu, podpisywanie długoterminowych umów najmu, inwestowanie w sprzęt i wyposażenie może być dużym obciążeniem. „Gotowe biuro" zapewnia niezbędną elastyczność oraz dostęp do szerokiej gamy usług wspomagających, co umożliwia szybkie rozpoczęcie działalności i natychmiastową reakcję na pojawiające się potrzeby.

Dodatkową wartością oferowaną przez firmy „instant office" jest „profesjonalny wizerunek". W dzisiejszym otoczeniu biznesowym jest to wymóg konieczny dla każdego, kto chce uchodzić za wiarygodnego i rzetelnego partnera. Siedziba firmy, adres i telefon, obsługa korespondencji i rozmów z klientami to podstawowe wyznaczniki, na podstawie których oceniamy, z kim mamy do czynienia. Dostawcy „gotowych biur" dysponują pomieszczeniami zlokalizowanymi w prestiżowych dzielnicach, dbają o ich nowoczesne i eleganckie wyposażenie, zatrudniają wykwalifikowany personel, który zapewni fachową obsługę klientów. Dzięki temu korzystający z ich usług pierwszy krok do stworzenia właściwego „image" mają już za sobą.

4. Czym są wyszukiwarki i katalogi

W katalogach możemy umieszczać adres swojej witryny wraz z krótkim opisem. Do najpopularniejszych katalogów światowych należy m.in. www.yahoo.com. Osoba szukająca informacji na dany temat wybiera z dostępnej listy po kolei słowa kluczowe, coraz bardziej zawężając dane, np. gdy szukamy informacji nt. przyrządzania wegetariańskiej pizzy, nasza droga może wyglądać następująco: jedzenie –> przepisy –> wegetariańskie –> pizza. Jest to oczywiście czysto hipotetyczna droga, ale uwidacznia,

w jaki sposób zawężamy poszukiwania. Należy pamiętać, że jeśli nie zarejestrowaliśmy naszej witryny, to nie pojawi się ona w katalogu.

Natomiast wyszukiwarki same znajdują informacje na dany temat (np. www.infoseek.com), bez konieczności rejestracji, po wpisaniu kilku słów.

Wyszukiwarki

Poniżej przedstawione zostały najbardziej popularne wyszukiwarki wraz z krótkim opisem.

Infoseek (www.infoseek.com)
Jest to obecnie jeden z lepszych serwisów wyszukiwawczych. Oferuje natychmiastowe umieszczenie danej witryny w swoim serwisie.

HotBot (www.hotbot.com)
Od czasu rejestracji do czasu umieszczenia naszej witryny nie powinno minąć więcej niż 48 godzin.

Altavista (www.altavista.com)
Jeden z bardziej zaawansowanych serwisów. Oferuje nawet tłumaczenie stron na wybrany język. Czas zarejestrowania nie powinien przekroczyć dwóch dni.

Onet (www.onet.pl)
Polski portal wraz z oprogramowaniem Infoseek'a. W Polsce tworzy zdecydowanie największą bazę danych. Połączony jednocześnie z katalogiem.

WP (www.wp.pl)
Zbliżony do Onetu, jednak o mniejszej skuteczności.

Słownik terminów e-gospodarki

CGI Common Gateway Interface (CGI) – wspólny interfejs bramkowy – standard opisujący, w jaki sposób serwery WWW zgodnie z HTTPD powinny się odwoływać do zewnętrznch programów, by zwracać użytkownikowi ich wyniki w formie automatycznie generowanych stron WWW.

COBRA Common Object Request Broker Architecture (COBRA) wspólna architektura komunikowania się obiektów – standard oprogramowania pośredniczącego, który pozwala obiektom komunikować się wzajemnie, nawet jeśli sieć łączy komputery o różnej architekturze, a obiekty napisane są w różnych językach programowania.

Cyfrowe pieniądze Metoda zapewniania poufności w świecie, w którym handel elektroniczny staje się powszechny. Polega ona na tym, że osoba mająca konto bankowe dokonuje zakupów przez sieć komputerową, a zapłata jest automatycznie przelewana z jej konta na konto sprzedawcy.

DES Data Encryption Standard (DES) – standard szyfrowania danych – opracowane przez IBM technologia szyfrowania danych, zaadaptowana przez rząd USA do szyfrowania danych nie opatrzonych klauzulą poufności i szeroko stosowana przez indtytucje finansowe do elektronicznego przesyłania dużych kwot pieniędzy.

DNS Domain Name Service (DNS) – domenowa usługa nazewnicza – program działający w systemie komuterowym podłączonym do internetu, wykonujący automatyczne tłumaczenie nazw domen na adresy IP.

DTD Document Type Definition (DTD) – definicja typu dokumentu – w SGML pełna definicja języka załączników, która definiuje elementy dokumentu oraz znaczniki używane do ich identyfikacji.

EDI Electronic Data Interchange (EDI) – elektroniczna wymiana danych – standard elektronicznej wymiany dokumentów handlowych, takich jak faktury i zlecenia zakupu. Standard ten opracowało Stowaryszenie ds. Normalizacji Wymiany Danych (DISA).

EDIFACT Electronic data interchange for administration, commerce and transport – standard elektronicznej wymiany danych (EDI) dla rozwiązań w administracji, handlu i transporcie.

Ethernet Standard sprzętu, okablowania i sposobu komunikowania się w sieci lokalnej (LAN), zaprojektowany przez Xerox Corporation.

Etyka hakerska Zbiór moralnych zasad wspólnych dla wczesnej generacji hakerów (w latach 1965–1982). Zgodnie z nim wszystkie informacje techniczne powinny być z zasady swobodnie dostępne. Z tego względu wchodzenie do jakiegoś systemu w celu przejrzenia danych i zwiększenia wiedzy nie może być nieetyczne.

Etyka komputerowa Gałąź etyki ukierunkowana specjalnie na problematykę etycznego wykorzystywania zasobów komputerowych.

FAQ Frequently Asked Questions (FAQ) – często zadawane pytania – w Usenecie dokument regularnie publikowany w grupie dyskusyjnej, mogący pomóc nowym użytkownikom.

FTP File Transfer Protocol (FTP) – protokół transmisji plików – internetowy standard przesyłania plików. Jest on zbiorem reguł opisujący konkretny protokuł transmisji plików. Do korzystania z FTP służy klient FTP, czyli program użytkowy, pozwalający na kontaktowanie się z innymi komputerami w Internecie i wymianę danych.

GPRS GPRS (General Packet Radio Service) to technologia transmisji danych metodą pakietową. Pozwala na przesyłanie danych z symetrycznie prędkością do 115 kb/s, jednak prędkość jest ograniczona możliwościami telefonu. Polega na pakietowym przesyłaniu danych – kanał jest wykorzystywany tylko w momencie transferu danych, a opłata pobierana za ilość przesłanych danych, a nie za czas trwania połączenia.

HTML HyperText Markup Language (HTML) – język znaczników hipertekstowych – język deklaratywny służący do opisu sposobu formatowania fragmentów dokumentu, tak aby wyświetlane za pomocą przeglądarki WWW zachowywały nadany format niezależnie od producenta komputera, systemu operacyjnego i systemu samej przeglądarki.

ISDN Integrated Services Digital Network (ISDN) sieć cyfrowa ze zintegrowanymi usługami – światowy standard obejmujący udostępnianie cyfrowych usług telefonicznych i transmisji danych do domów, biur i szkół.

LDAP Lightweight Directory Access Protocol (LDAP) – uniwersalny protokół dostępu do katalogu – internetowy standard umożliwiający przeszukiwanie – za pomocą przeglądarki WWW – katalogowych baz danych.

MRO ang. MRO (Maintenance, Repair, and Operating Equipment) system eksploatacji, napraw i obsługi kierowany przez nabywcę, rutynowe zakupu usług, takich jak dostawy materiałów biurowych, obsługa podróży służbowych.

Oracle Corporation Jeden z wiodących producentów UNIX'owych systemów zarządzania relacyjną bazą danych (RDBMS) przeznaczonych dla wielożytkownikowych środowisk obliczeniowych. Oracle był pierwszą dużą firmą, która zastosowała SQL jako standardowy język zapytań.

PDN Sieć prywatna – niezwykle bezpieczna, choć droga sieć rozległa (WAN) wykorzystująca linie dzierżawione, które służą do transmisji danych tylko jednego przedsiębiorstwa.

PSTN Public Switched Telephone Network (PSTN) – publiczna komutowana sieć telefoniczna – ogólnoświatowa sieć komutowanych łączy telefonicznych umożliwiających nawiązywanie bezpośrednich połączeń telefonicznych milionom użytkowników na świecie.

RDBMS Relational Database Management System (RDBMS) – system zarządzania relacyjną bazą danych – program do zarządzania relacyjną bazą danych dostarczony wraz z niezbędnym oprogramowaniem pomocniczym, narzędziami programistycznymi i dokumentacją potrzebnymi do tworzenia, instalowania i obsługi aplikacji bazy danych.

RSA Public Key Encryption Algorithm Algorytm szyfrowania RSA z kluczem publicznym – najbardziej popularny algorytm szyfrowania z kluczem publicznym – de facto ogólnoświatowy standard. Mimo swej poufności został włączony do wielu protokołów (między innymi SSL).

SDI Jest to stosunkowo nowa usługa oferowana między innymi przez TP SA, polegająca na udostępnieniu użytkownikowi nieograniczonego czasowo dostępu do Internetu. W dużym uproszczeniu polega ona na zainstalowaniu u użytkownika pewnego urządzenia (nieco podobnego do modemu), które za pomocą zwykłej linii telefonicznej przesyła dane pomiędzy centralą telefoniczną a komputerem.

Sieć publiczna PDN – sieć rozległa (WAN) udostępniająca firmom i użytkownikom indywidualnym daleko zasięgowe usługi transmisji danych. Sieci takie znajdują zastosowanie w dużych korporacjach, zapewniając bezpieczne komunikowanie się między oddziałami firmy, agencjami branżowymi a dostawcami.

SQL Structural Query Language (SQL) – strukturalny język zapytań – w systemie zarządzania bazą danych opracowany prze IBM język zapytań, który stał się standardem zapytań zadawanych bazom danych w sieciach klient–serwer.

SSL Secure Sockets Layer (SSL) – warstwa bezpiecznych gniazdek – standard zabezpieczeń internetowych zaproponowany przez Netscape Communication, włączony do przeglądarek Netscape. SSL jest nie-

zależny od aplikacji, współpracuje ze wszystkimi narzędziami internetowymi, nie tylko z siecią WWW. SSL działa w warstwie sieci, a nie w warstwie aplikacji i dzieki temu jest dostępny dla wszystkich aplikacji przystosowanych do współpracy z nim.

UMTS Uniwersalny System Komunikacji Ruchomej, UMTS (z języka angielskiego *Universal Mobile Telecommunications System*), to system komunikacji ruchomej i bezprzewodowej trzeciej generacji, umożliwiający w szczególności realizację nowatorskich usług multimedialnych w skali wykraczającej poza możliwości systemów drugiej generacji (GSM).

UMTS pozwala na szybki dostęp do Internetu (z prędkością do dwóch megabitów na sekundę), dokonywanie skomplikowanych operacji bankowych i zakupów. Właściciel telefonu – terminala UMTS będzie miał możliwość oglądania rozmówcy.

Uruchomienie pierwszych europejskich sieci planuje się w 2002 roku, a w Japonii już w 2001. Według prognoz Międzynarodowej Unii Telekomunikacyjnej (ITU) w 2005 roku 15 procent użytkowników telefonii komórkowej w Europie będzie korzystało z UMTS, a w 2010 nawet 45 procent.

WWW World Wide Web – ogólnoświatowa sieć WWW – globalny system hipertekstowy wykorzystujący Internet jako mechanizm transportowy.

X25 Międzynarodowy standard sieci z komunikacją pakietów, powszechnie stosowany w sieciach publicznych (PDN)

Literatura

1. Badanie użytkowników sieci Internet. Akademia Ekonomiczna w Krakowie, 1999.
2. Czechowicz T.: Modele biznesowe firm – czy to rzeczywiście działa? Forum Oracle: Internetowe aplikacje biznesowe jako czynnik przewagi konkurencyjnej, Warszawa 2001.
3. eHandel w Polsce. Informacja prasowa. Global eMarketing S.A., Warszawa 2001.
4. Garfinkel S., Spafford G.: WWW Bezpieczeństwo i handel. Helion, Gliwice 1999.
5. Kraszewski D.: Perspektywy eHandlu w Polsce. Arthur Andersen, Warszawa 2001. Gospodarka elektroniczna – perspektywy i bariery 345.
6. Piotrowski A.J: Zaplecze dla nowej i „starej" gospodarki. Forum Oracle: Internetowe aplikacje biznesowe jako czynnik przewagi konkurencyjnej, Warszawa 2001.
7. Piwowar P.: Przemówienie powitalne na konferencji Forum Oracle: Internetowe aplikacje biznesowe jako czynnik przewagi konkurencyjnej, Warszawa 2001.
8. Raport o Internecie w Polsce. Global eMarketing S.A., Warszawa, październik 1999. www.g-em.pl.
9. Smith N.: White Paper: The Internet Economy in Europe – from Revolution to Evolution. Raport Gartner Group, Inc. wykonany na zamówienie Cisco Corp. www.cisco.com/warp/public/3/emea/gartner.
10. Trepper C.: E-Commerce Strategies. Microsoft Press, Redmond, WA, USA, 2000.
11. Waszczyk M: Internet jako czynnik przewagi konkurencyjnej. Forum Oracle: Internetowe aplikacje biznesowe jako czynnik przewagi konkurencyjnej, Warszawa 2001.
12. www.covisint.com. Witryna www.