Część V

SYSTEMY INFORMATYCZNE W ZARZĄDZANIU

WYKORZYSTANIE OTWARTEGO OPROGRAMOWANIA W INFORMATYCZNYCH SYSTEMACH ZARZĄDZANIA

WIESŁAW BARCIKOWSKI

WOJSKOWA AKADEMIA TECHNICZNA
WYDZIAŁ CYBERNETYKI

Wstęp

W dzisiejszych czasach funkcjonowanie firmy na rynku wymaga szybkiego reagowania na zachodzące zmiany i stałego dostosowywania się do nowych wyzwań płynących zarówno ze strony konkurencji, jak i przede wszystkim coraz bardziej wymagającego klienta. Dodatkowo, konieczność prowadzenia działalności w warunkach globalizacji dotyczy już nie tylko wielkich korporacji od lat funkcjonujących na rynku światowym, ale również firm sektora MŚP. Stało się to możliwe między innymi dzięki rozwojowi technologii teleinformatycznych – to te technologie sprawiły, że dotychczasowe granice i odległości stały się nieistotne.

W takiej sytuacji, bez informatycznego wspomagania, prowadzenie działalności jest niezwykle utrudnione, a w zasadzie niemożliwe – informatyzacja firm stała się koniecznością. Trend ten daje się zaobserwować nie tylko w biznesie, ale również w innych obszarach, takich jak edukacja czy przede wszystkim administracja publiczna – obywatel (czyli klient-usługobiorca) stawia podobne wymagania co do sposobu i jakości obsługi jednostkom administracji publicznej (czyli usługodawcom).

Współczesne systemy informatyczne mogą ułatwiać prowadzenie nie tylko działalności podstawowej, specyficznej dla danej firmy, ale również wspomagać obszary zabezpieczające tę działalność, a w konsekwencji zarządzanie całą firmą. Kompleksowa informatyzacja pozwala firmie osiągnąć najwięcej korzyści. Najłatwiej jest to osiągnąć poprzez wdrożenie zintegrowanego informatycznego systemu zarządzania. Niestety, mimo stałego spadku cen elementów technologii informatycznych, informatyczne systemy zarządzania w dalszym ciągu są niezwykle kosztowne. Po zakończeniu wdrożenia, należy liczyć się ze stałymi kosztami związanymi z utrzymaniem i pielęgnacją systemu. Istotnym elementem są koszty nabycia i utrzymania licencji na wykorzystywane oprogramowanie (dotyczy zarówno oprogramowania systemowego, jak i użytkowego). Dla wielu małych firm, w szczególności rozpoczynających działalność, może to stanowić barierę uniemożliwiającą wdrożenie informatycznego systemu zarządzania. Jednym ze

sposobów poradzenia sobie z dużymi kosztami licencji jest wykorzystanie wolnego i otwartego oprogramowania.

1. Wolne i otwarte oprogramowanie – definicja

Najprościej mówiąc, wolne i otwarte (o otwartych źródłach) oprogramowanie (ang. *Free and Open Source Software* – FOSS) jest rodzajem oprogramowania rozpowszechnianego na zasadzie specyficznej licencji dającej użytkownikowi prawo do jego bezpłatnego użytkowania. Zakres wykorzystania wolnego i otwartego oprogramowania określają szczegółowo tzw. zasady wolności:

- uruchamianie programu w dowolnym celu,
- analizowanie, jak program działa i dostosowywanie go do własnych potrzeb,
- rozpowszechnianie kopii programu,
- udoskonalanie programu i publiczne rozpowszechnianie zmian.

Warunkiem koniecznym do zrealizowania tych wolności jest pełny i nieograniczony dostęp do kodu źródłowego.

Definicja otwartego oprogramowania, a w zasadzie oprogramowania o otwartym kodzie źródłowym (ang. *Open Source Software* – OSS), została zaproponowana pod koniec lat 90. XX wieku przez powstałą wówczas organizację o nazwie Open Source Initiative (OSI)[1]. U podstaw idei wolnego i otwartego (o otwartych źródłach) oprogramowania leży również definicja wolnego oprogramowania (ang. *free software*)[2] przedstawiona w połowie lat 80. XX wieku przez organizację Free Software Foundation, według której termin „wolny" (ang. *free*) należy rozpatrywać bardziej w kategoriach wolności użytkowania i kopiowania, niż ceny oprogramowania.

Twórcami programów OSS są zwolennicy i entuzjaści idei otwartości oprogramowania, którzy pracują przede wszystkim w ramach zespołów społecznościowych mających na celu stworzenie i rozwijanie danego typu programu/systemu. Bardzo często są to wysokiej klasy fachowcy, którzy oprócz pracy wykonywanej w ramach wynagrodzenia, w ten sposób realizują swoje zainteresowania i pasje. Istotny udział w rozwoju oprogramowania OSS mają również komercyjne firmy informatyczne, które często sprawują opiekę nad projektami otwartego oprogramowania, np. język programowania Java był rozwijany za pomocą firmy SUN Microsystems, a rozwojem bazy danych MySQL aktualnie zajmuje się firma Oracle. Należy dodać, że również firmy komercyjne coraz częściej zajmują się utrzymaniem otwartego oprogramowania, oferując odpłatne usługi wsparcia jego użytkownikom. Daje to użytkownikom dodatkową gwarancję bezpiecznej eksploatacji takiego programu/systemu w dłuższej perspektywie czasowej.

[1] http://www.opensource.org
[2] http://www.gnu.org/philosophy/free-sw.pl.html

Aktualnie główną organizacją koordynującą ruch OSS na świecie jest Open Source Initiative. Na stronach tej organizacji zamieszczona jest definicja oprogramowania o otwartym kodzie[3]:

1. swobodna redystrybucja: oprogramowanie może być swobodnie przekazywane lub sprzedawane,
2. kod źródłowy: musi być dołączony lub dostępny do pobrania,
3. programy pochodne: musi być dozwolona redystrybucja modyfikacji,
4. integralność autorskiego kodu źródłowego: licencje mogą wymagać, aby modyfikacje były redystrybuowane jedynie jako tzw. łatki uaktualniające,
5. niedyskryminowanie osób i grup: nikt nie może zostać wykluczony,
6. niedyskryminowanie obszarów zastosowań: nie wolno wykluczać komercyjnych zastosowań,
7. dystrybucja licencji: prawa dołączone do oprogramowania muszą się odnosić do wszystkich odbiorców programu, bez konieczności nabywania przez nich dodatkowej licencji,
8. licencja nie może być specyficzna dla produktu: program nie może być licencjonowany tylko jako część szerszej dystrybucji,
9. licencja nie może ograniczać innego oprogramowania: np. licencja nie może wymagać, aby inne dystrybuowane z pakietem oprogramowanie było typu OSS,
10. licencja musi być technicznie neutralna.

Należy podkreślić, że – jak pokazuje zasada podana w p. 6 – oprogramowanie OSS może być wykorzystywane również do zastosowań komercyjnych, co powinno szczególnie zainteresować ten rodzaj użytkowników.

Na stronach OSI można znaleźć ponadto opisy kilkudziesięciu rodzajów licencji, według których można dystrybuować oprogramowanie OSS, w tym m.in. GNU General Public License (jedna z najpopularniejszych). Wszystkie rodzaje licencji łączy zgodność z definicją oprogramowania o otwartym kodzie. Należy również dodać, że jeden z rodzajów licencji: European Union Public Licence (EUPL)[4], został zdefiniowany przez Komisję Europejską na potrzeby współdzielenia oprogramowania o otwartym kodzie w ramach Unii Europejskiej, co powinno szczególnie zainteresować użytkowników (firmy i jednostki administracji publicznej) również z Polski.

2. Uniwersalne zastosowania otwartego oprogramowania

W początkowym okresie rozwoju oprogramowania OSS głównymi jego odbiorcami były osoby wykorzystujące je do celów prywatnych. Głównym powodem były względy finansowe – możliwość skorzystania z bezpłatnej alternatywy dla

[3] http://opensource.org/docs/osd

[4] http://www.osor.eu/eupl/european-union-public-licence-eupl-v.1.1

płatnych rozwiązań komercyjnych. Odbiorcy instytucjonalni (publiczni i komercyjni) zachowywali się wstrzemięźliwie, głównie z powodu obaw o bezpieczeństwo i stabilność oferowanych rozwiązań. W miarę upływu lat i angażowania się coraz lepiej przygotowanych zespołów wytwórczych, oprogramowanie OSS stopniowo uzyskało taki stan dojrzałości, że aktualnie jest już powszechnie akceptowane przez jednostki administracji publicznej oraz coraz częściej przez firmy komercyjne, stanowiąc rozsądną alternatywę dla rozwiązań komercyjnych.

Aktualnie dostępne są programy/systemy (pakiety oprogramowania) OSS pokrywające praktycznie wszystkie obszary zastosowań istotne dla wspomagania działalności firm i instytucji (a także dla użytku domowego). Poniżej przedstawiona jest lista wybranych obszarów zastosowań i odpowiadających im przykładowych programów typu OSS:

- programy użytkowe:
  - pakiet oprogramowania biurowego, np. O*penOffice*,
  - przeglądarka internetowa, np. *Firefox, Chrome*,
  - poczta elektroniczna (klient), np. *Thunderbird*,
  - planowanie spotkań i kalendarz, np. *Lightning*,
  - obróbka grafiki rastrowej, np. *Gimp*
  - obróbka grafiki wektorowej, np. *Inscape*,
  - przygotowanie materiałów wydawniczych (DTP), np.: *Stylus*,
  - zarządzanie projektami, np. *OpenProj, Codendi*;
- oprogramowanie systemowe:
  - system operacyjny, np. *Linux,*
  - serwer aplikacji, np. *Apache*,
  - serwer bazy danych, np. *Mysql, Postgresql*,
  - serwer poczty elektronicznej, np. *Sendmail*,
  - monitorowanie sieci i systemów, np. *Nagios;*
- systemy wspomagające zarządzanie:
  - zarządzanie treścią portali (CMS) , np. *Joomla, Drupal*
  - zarządzanie zasobami informatycznymi, np. *Open-Audit,*
  - zarządzanie nauczaniem na odległość (e-Learning), np. *Moodle*,
  - zarządzanie obiegiem dokumentów, np. *Alfresco*,
  - zarządzanie relacjami z klientami (CRM), np. *SugarCRM*,
  - informowanie kierownictwa/wspomaganie decyzji (BI), np. *Pentaho*,
  - zarządzanie przedsiębiorstwem (ERP), np. *OpenERP, OpenBravo*.

Wymienione powyżej przykładowe programy typu OSS mają charakter uniwersalny, gdyż wspierają realizację powszechnych i typowych potrzeb firm/instytucji, takich jak wytwarzanie i obieg dokumentów, obsługa portali informacyjnych czy wreszcie zarządzanie relacjami z klientami. Dzięki temu mogą być stosowane praktycznie w każdym sektorze gospodarki i administracji. Poprzez właściwy dobór i umiejętną integrację takich programów/systemów można doprowadzić w zasadzie do pełnej informatyzacji firm/instytucji, których potrzeby są w miarę

typowe i uniwersalne. Oczywiście niezbędne jest odpowiednie skonfigurowanie czy zmodyfikowanie pod kątem konkretnych potrzeb danej firmy czy instytucji, natomiast główna część (rdzeń) programu/systemu pozostaje taka sama. W przypadku zaistnienia potrzeby wykonania większej adaptacji, jest to również możliwe, gdyż dostępny jest kod źródłowy programu i użytkownik (firma, instytucja) ma prawo do jego dowolnej modyfikacji. Oczywiście, rozbudowa systemu polegająca na zwiększeniu liczby stanowisk pracy wynikającej ze wzrostu liczby użytkowników jest praktycznie bezkosztowa, gdyż licencje na oprogramowanie typu OSS są po prostu bezpłatne.

Uniwersalność takich programów/systemów powoduje zwiększenie liczby użytkowników. Z kolei zwiększona popularność bezpośrednio wpływa na wzrost zainteresowania środowiska OSS utrzymaniem i rozwojem tych programów/systemów. Przekłada się na wzrost poczucia bezpieczeństwa użytkowników w zakresie trwałości inwestycji w wybrany program/system typu OSS. Jest to szczególnie istotne w przypadku systemów, które muszą być ciągle modyfikowane np. ze względu na konieczność dostosowywania do zmieniającego się otoczenia. Aczkolwiek należy zaznaczyć, że w przypadku systemów, których poprawność funkcjonowania jest uzależniona od uwarunkowań prawnych specyficznych dla konkretnego kraju (np. systemy finansowo-księgowe czy kadrowo-płacowe) możliwości adaptacji nadążającej za zmianami prawnymi są bardziej ograniczone (mniejsza liczba użytkowników i potencjalnych deweloperów w danym kraju).

Z punktu widzenia potrzeb firm komercyjnych w zakresie wspomagania zarządzania, bardzo interesującą propozycją jest wymieniony w zestawieniu system SugarCRM[5]. Według informacji zawartych na polskiej stronie tego projektu, „jeżeli chodzi o funkcjonalność standardowej wersji SugarCRM, jest ona idealnym rozwiązaniem dla sektora małych i średnich przedsiębiorstw (po dokonaniu odpowiednich konfiguracji). Pozwala ona m.in. na: kompleksowe zarządzanie relacjami z klientami (namiarami, kontaktami, kontrahentami oraz partnerami biznesowymi), zarządzanie szansami sprzedażowymi oraz procesem sprzedaży, zarządzanie projektami wewnętrznymi oraz zewnętrznymi, a także zarządzanie kampaniami reklamowymi (marketing mailingowy). Dodatkowo SugarCRM udostępnia liczne narzędzia do tworzenia raportów oraz analizy sprzedaży i rezultatów przyjętych strategii. System może także zostać całkowicie dopasowany do specyficznej branży przedsiębiorstwa lub stanowić podstawę dla rozwiązania dedykowanego (stworzonego od podstaw dla klienta)”[6].

Należy wspomnieć, że użytkownikami tego systemu są również wielkie korporacje światowe (np. Coca-Cola, Toyota czy Axa) oraz że nad rozwojem oprogramowania czuwa amerykańska firma (oferująca również komercyjną wersję systemu o zwiększonej funkcjonalności), co powinno gwarantować istnienie

[5] http://www.sugarcrm.com

[6] http://sugarcrm.com.pl/systemy-crm-typu-open-source/

systemu w przyszłości. Ponadto, istnieją (również w Polsce) firmy komercyjne, które są w stanie przeprowadzić wdrożenie tego systemu i zaoferować wsparcie serwisowe. Ten element całkowitych kosztów posiadania systemu (ang. *Total Cost of Ownership* – TCO) jest oczywiście odpłatny, natomiast odpadają koszty nabycia i rocznych opłat licencyjnych za oprogramowanie, co stanowi istotną oszczędność dla użytkownika.

3. Specjalistyczne zastosowania otwartego oprogramowania

Obok oprogramowania o otwartym kodzie przeznaczonego dla uniwersalnych zastosowań, powstaje również oprogramowanie dedykowane dla odbiorców reprezentujących specyficzne środowiska, ale również liczne (w szczególności w skali świata).

Takim środowiskiem jest np. środowisko naukowe, którego przedstawiciele tworzą specjalistyczne aplikacje wspomagające prowadzenie badań i analiz naukowych, a następnie udostępniają je innym zainteresowanym w sieci Internet. Z czasem, po osiągnięciu niezbędnej dojrzałości, takie programy/systemy są wykorzystywane w instytucjach administracji publicznej, a także w firmach komercyjnych. Ilustruje to bardzo dobrze rozwój systemu R, specjalizowanego środowiska do przetwarzania i analizowania danych statystycznych. System R powstał na University of Auckland w Nowej Zelandii i bazował na języku S stworzonym w Bell Laboratories (należącym do amerykańskiej korporacji AT&T). Dalszy rozwój jest już udziałem międzynarodowego środowiska[7], a dystrybucja jest realizowana zgodnie z otwartą licencją GNU General Public License[8]. Aktualnie system R jest powszechnie wykorzystywany nie tylko przez środowiska naukowe, ale również przez rządowe organizacje statystyczne wielu państw, stanowiąc bezpłatną konkurencję dla produktów komercyjnych, takich jak SAS czy SPSS. Wybrane elementy systemu R są również adaptowane do zastosowań w firmach komercyjnych, prowadzących zaawansowane analizy statystyczne.

Innym przykładem specjalistycznych systemów typu OSS są systemy wspomagające zarządzanie służbą zdrowia. Wobec postępującej standaryzacji działalności operacyjnej (procedury medyczne, ścieżki kliniczne, rejestry leków itp.), coraz więcej jednostek służby zdrowia (przychodnie, szpitale) może funkcjonować w bardzo podobny sposób. Oznacza to, że również systemy informatyczne wspomagające ich działalność mogą być bardzo podobne (a w wielu obszarach – identyczne). W takiej sytuacji raz stworzony system dla jednej jednostki medycznej, może być udostępniony innym. Zasada powszechnego współdzielenia (ang. *common-share*) i ponownego użycia (ang. *re-use*) kodu źródłowego, zgodna i wynikająca z podstawowych idei ruchu OSS, oznacza konkretne oszczędności dla systemu ochrony zdrowia

[7] http://www.r-project.org/

[8] http://www.gnu.org/licenses/gpl.html

w skali państwa. Przykładem takiego działania jest decyzja szpitala St. Antonius w Utrechcie (Holandia) o udostępnieniu na licencji open source własnego systemu IntraZis, zbudowanego w oparciu o oprogramowanie systemowe typu open source (np. baza danych MySQL), służącego do zarządzania informacjami medycznymi[9]. Inicjatywa została zaakceptowana przez kilka jednostek służby zdrowia w Holandii, które są zainteresowane wdrożeniem systemu.

Na szczególną uwagę zasługuje również projekt GNU Health[10], którego wynikiem jest system informatyczny wspomagający zarządzanie ochroną zdrowia, obejmujący swym zakresem zarówno zarządzanie informacjami medycznymi (ang. *Electronic Medical Record* – EMR), jak i zarządzanie jednostką ochrony zdrowia (ang. *Hospital Information System* – HIS). Rozwój systemu jest realizowany przez międzynarodową grupę deweloperów i wspierany m.in. przez Komisję Europejską (portal OSOR[11]) i rząd Brazylii. System jest bezpłatny i jest udostępniany na zasadach otwartej licencji GPL. Według informacji dostępnych na portalu OSOR, system GNU Health jest już używany przez kilka szpitali w Indonezji[12] i został wybrany przez ONZ (United Nations University – International Institute for Global Health) jako system wspierający nauczanie w zakresie systemów zarządzania jednostkami ochrony zdrowia[13]. Wydaje się, że GNU Health jest szczególnie interesujący dla krajów, które do dziś nie rozwinęły odpowiednich systemów informatycznych wspierających ochronę zdrowia i nie dysponują wystarczającymi środkami do wdrożenia płatnych systemów komercyjnych.

4. Upowszechnianie otwartego oprogramowania w systemach zarządzania

Zalety wolnego i otwartego oprogramowania są nie do przecenienia przede wszystkim z punktu widzenia indywidualnych oczekiwań pojedynczego użytkownika (firmy, instytucji czy osoby prywatnej). Jest to głównie brak opłat licencyjnych i możliwość dowolnej modyfikacji kodu pod kątem spełnienia własnych potrzeb, a także zmniejszenie (lub brak) uzależnienia od jednego dostawcy (ang. *vendor lock-in*).

Idea wolnego i otwartego oprogramowania jest również atrakcyjna z perspektywy globalnej. W interesie państwa czy lokalnych społeczności leży współdzielenie takich samych rozwiązań (co pomniejsza koszty informatyzacji), jak również budowanie środowisk społecznościowych wokół projektu (dzielenie się wiedzą, wzrost kompetencji, przesunięcie aktywności z czystej konsumpcji w kierunku udziału

[9] http://www.osor.eu/news/nl-hospital-considers-publishing-medical-record-system-as-open-source
[10] http://health.gnu.org
[11] http://www.osor.eu/projects/medical
[12] http://forge.osor.eu/forum/forum.php?forum_id=827
[13] http://forge.osor.eu/forum/forum.php?forum_id=878

w tworzeniu). W konsekwencji stymuluje to w poszczególnych krajach powstawanie rodzimych firm komercyjnych zajmujących się wsparciem tego typu rozwiązań, czyli rozwój własnego przemysłu informatycznego. Tworzy to przeciwwagę dla modelu opartego o dystrybucję i wsparcie płatnych produktów wytworzonych w innych krajach. Powinno to być szczególnie interesujące dla krajów, które nie są światowymi liderami w produkcji oprogramowania.

Niestety, należy zauważyć, że stopień akceptacji tego typu rozwiązań jest daleko mniejszy od spodziewanego (wynikającego z otrzymywanych korzyści). Głównymi obawami ze strony potencjalnych użytkowników były wątpliwości co do funkcjonalności i jakości oferowanych produktów, jak również bezpieczeństwa ich stosowania (zarówno w kontekście cech produktu, jak i trwałości zespołów wytwórczych).

Oczywiście faktem jest, że są sytuacje, gdy programy OSS oferują mniejszą funkcjonalność niż ich komercyjne odpowiedniki. Najczęściej dotyczy to zaawansowanych funkcji, rzadko lub w ogóle nie wykorzystywanych przez większość użytkowników.

Jeżeli chodzi o jakość oprogramowania OSS, to należy zauważyć, że dzięki stosowaniu powszechnie dostępnych metod i narzędzi (najczęściej takich samych jak przy wytwarzaniu produktów komercyjnych) przez coraz lepiej przygotowane zespoły wytwórcze funkcjonujące w ramach projektów OSS, powstają produkty dobrej jakości, akceptowanej nie tylko przez typowych użytkowników, ale również przez bardziej wymagających (np. Europejska Agencja Kosmiczna).

Z kolei obawy co do trwałości projektu i dostępu do usług serwisowych są stopniowo rozwiewane poprzez powstawanie firm komercyjnych specjalizujących się we wsparciu oprogramowania OSS. Jednak nawet w sytuacji, gdy dany produkt nie ma dostępnego komercyjnego wsparcia, w dalszym ciągu pozostaje możliwość uzyskania pomocy od społeczności skupionej wokół projektu (projektanci, programiści, zaawansowani testerzy czy wreszcie inni użytkownicy). Jak pokazuje praktyka, reakcja społeczności na problemy z użytkowaniem programów OSS jest bardzo skuteczna i często szybsza niż w przypadku płatnego wsparcia oferowanego przez komercyjnego usługodawcę – w końcu do dyspozycji jest pomoc dostępna 24 godziny na dobę, gdyż osoby związane z danym projektem OSS można znaleźć we wszystkich strefach czasowych!

Stopień akceptacji rozwiązań informatycznych opartych o otwarte oprogramowanie jest różny w różnych krajach i różnych sektorach gospodarki. Duża popularność tych rozwiązań tradycyjnie była obserwowana w europejskich krajach nie-anglojęzycznych, takich jak Francja, Hiszpania czy Niemcy. Wynikało to często z próby szukania własnej, narodowej alternatywy dla, dominującego na rynku komercyjnym, oprogramowania wytwarzanego głównie przez firmy amerykańskie. Nasilający się kryzys finansowy skłonił do korzystania z oprogramowania OSS również kraje nordyckie i anglosaskie. W Polsce obserwuje się jak dotąd umiarkowane zainteresowanie rozwiązaniami OSS.

Analizując z kolei stopień wykorzystania oprogramowania OSS w różnych sektorach gospodarki (w szczególności w krajach zachodnich), można zaobserwować, że głównym odbiorcą tych rozwiązań jest sektor edukacyjny i administracja publiczna. Dla tych sektorów poza oczywistym zmniejszeniem kosztów informatyzacji, istotna jest również realizacja zasady reużywalności i promowanie zasady partycypowania w rozwoju, co jest szczególnie istotne również z punktu widzenia celów edukacyjnych. Nie bez znaczenia jest fakt, że te sektory finansują swoją działalność w większości za pomocą środków publicznych, co powinno prowadzić do ich oszczędnego wykorzystania.

W przypadku firm komercyjnych prowadzących działalność gospodarczą, stopień wykorzystania rozwiązań OSS jest trudny do oszacowania. Często firmy nie podają takich informacji, traktując je jako tajemnicę przedsiębiorstwa. U podstaw takich decyzji leżała czasami obawa przed ujawnieniem potencjalnym konkurentom szczegółów, które mogłyby ułatwić penetrację systemów firmowych (z racji otwartości, prawdopodobnie bardziej podatnych na ingerencję). Niekiedy przyczyną mogła być obawa o pogorszenie wizerunku firmy, skoro panowała opinia, że rozwiązania OSS jako mniej „zaawansowane" niż komercyjne, raczej nie powinny byś stosowane do wspomagania działalności gospodarczej.

Dzisiaj należy zauważyć, że opisane powyżej obawy nie są już powszechnie podzielane przez firmy komercyjne. Znaczne polepszenie jakości i bezpieczeństwa rozwiązań OSS stopniowo przekonuje coraz więcej firm, i to nie tylko z sektora MSP. Problemy związane z dużymi kosztami informatyzacji oraz uzależnieniem od jednego dostawcy dotykają wszystkich, również wielkie korporacje o zasięgu światowym. Stąd obserwuje się rosnące zainteresowanie firm komercyjnych oprogramowaniem OSS, coraz częściej skutkujące podejmowaniem decyzji o wdrożeniu takich rozwiązań głównie w systemach wspierających prowadzenie działalności, takich jak portale komunikacyjne czy systemy zarządzania dokumentami. Należy dodać do tego coraz powszechniejszą akceptację dla wykorzystania w rozwiązaniach korporacyjnych również oprogramowania systemowego typu OSS (np. system operacyjny klasy Linux), które umożliwia funkcjonowanie systemów użytkowych. Podany wcześniej przykład wykorzystania systemu SugarCRM przez wielkie światowe korporacje pokazuje, że również w obszarze wspomagania kluczowej działalności, firmy coraz częściej wykorzystują systemy OSS.

Na zwiększenie akceptacji rozwiązań OSS i ich upowszechnienie w gospodarce istotny wpływ mogą mieć wspomniane wcześniej dwa sektory: edukacyjny i administracji publicznej. Pierwszy, poprzez edukację uczniów i studentów w zakresie wykorzystania oprogramowania otwartego oraz korzyści z tego płynących, zarówno dla użytkowników indywidualnych, jak i całej gospodarki. Jedną z barier w upowszechnieniu rozwiązań OSS jest właśnie brak wiedzy wśród pracowników firm i instytucji, skutkujący czasem biernym oporem przed ich wdrażaniem.

Z kolei przed administracją publiczną stoi zadanie instytucjonalnego wsparcia upowszechniania rozwiązań OSS, głównie poprzez przejęcie roli koordynacyjnej w zakresie standaryzacji i promowania (np. poradniki, jak zamawiać i wdrażać), jak również poprzez wprowadzanie rozwiązań prawnych ułatwiających stosowanie systemów OSS.

Podsumowanie

Otwarte oprogramowanie oparte na otwartym kodzie osiągnęło odpowiedni poziom dojrzałości, pozwalający na jego wykorzystanie w informatyzacji firm i instytucji. Oferowana funkcjonalność w większości przypadków jest wystarczająca dla spełnienia wymagań zarówno instytucji publicznych, jak i firm komercyjnych, a stopniowo rosnąca liczba firm oferujących usługi wsparcia w zakresie oprogramowania OSS, zwiększa gwarancję ciągłości użytkowania takich systemów.

Głównym obszarem wykorzystania są systemy wspomagające prowadzenie działalności, takie jak systemy przygotowania i obiegu dokumentów czy portale korporacyjne. Obserwuje się również stosowanie rozwiązań OSS we wspieraniu kluczowej działalności przedsiębiorstw, np. w systemach zarządzania relacjami z klientami czy wspomagania podejmowania decyzji.

Należy się spodziewać, że stała konieczność (nie tylko w dobie kryzysu gospodarczego) optymalizacji działalności przedsiębiorstw i instytucji, skutkująca często koniecznością oszczędności finansowych, będzie prowadziła do większego zainteresowania otwartym oprogramowaniem, które oferuje (oprócz innych korzyści) niższe koszty wdrażania i użytkowania informatycznych systemów zarządzania.

USING OPEN SOFTWARE IN MANAGEMENT INFORMATION SYSTEMS

Summary: The paper describes types and features of open software distributed under the open license, what gives users free possibility to use and modify. Types and examples of software devoted to universal management systems as well as to address special user needs are presented. The author describes benefits of using open software in economy and public administration. The result of the analysis is presented: what are the main reasons that there can be observed still too small application of open software in companies and institutions. The author shows propositions of main activities to change this state as well.

Keywords: open software, open source, management information systems.

LITERATURA (NETOGRAFIA)

[1] www.opensource.org/docs/osd
[2] www.gnu.org/philosophy/free-sw.pl.html
[3] www.gnu.org/licenses.gpl.html

[4] www.osor.eu/eupl/european-union-public-licence-eupl-v.1.1
[5] www.osor.eu/news/more-open-source-software-at-european-space-agency
[6] www.osor.eu/news/nl-hospital-considers-publishing-medical-record-system-as-open-source
[7] www.osor.eu/projects/medical
[8] health.gnu.org
[9] forge.osor.eu
[10] sugarcrm.com.pl/systemy-crm-typu-open-source/
[11] www.r-project.org

O ZNACZENIU RZETELNEGO UDOKUMENTOWANIA SYSTEMU BEZPIECZEŃSTWA INFORMACYJNEGO DLA ZARZĄDZANIA RYZYKIEM INFORMACYJNYM

KRZYSZTOF LIDERMAN

WOJSKOWA AKADEMIA TECHNICZNA
WYDZIAŁ CYBERNETYKI

Wstęp

Zarządzanie ryzykiem to systematyczne stosowanie polityki, procedur i praktyki zarządzania do ustalania kontekstu ryzyka, jego identyfikowania, analizowania, wyznaczania, postępowania z ryzykiem oraz monitorowania i komunikowania ryzyka (definicja za PN-IEC 62198 [8]). Zagadnienia zarządzania ryzykiem nabierają coraz większego znaczenia w działalności biznesowej organizacji na całym świecie, czego przykładem jest pojawienie się nowej specjalności zawodowej „menedżera ryzyka"[1] oraz różnego rodzaju stowarzyszeń tej grupy zawodowej (jak np. FERMA – ang. *Federation of European Risk Management Associations*). Można chyba stwierdzić, że obecnie mamy do czynienia ze swoistą modą na widzenie wszystkich aspektów działalności biznesowej organizacji przez pryzmat ryzyka. Ma to przełożenie również na problematykę bezpieczeństwa informacyjnego, niezmiernie istotną we współczesnych, wysoce zinformatyzowanych organizacjach różnego rodzaju. Obecną modę na ryzyko poprzedziła moda z przełomu XX/XXI wieku na „widzenie" działalności biznesowej przez pryzmat procesów biznesowych – przykładem są chociażby zmiany zachodzące w kolejnych wydaniach serii norm z zakresu jakości, tj. ISO/IEC 900x.

Dobrym przykładem uzasadniającym stwierdzenie o nowym paradygmacie postrzegania działalności biznesowej są zmiany wprowadzone w 2010 roku do ustawy o ochronie informacji niejawnej [14] oraz treść normy [6]. Norma ta jest przeznaczona dla kadry kierowniczej organizacji oraz jej personelu w celu przedstawienia modelu oraz ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymywania i doskonalenia systemu zarządzenia bezpieczeństwem

[1] Przynajmniej w krajach innych niż Polska – w Polsce jest to specjalność nieformalna, nie ujęta w Rozporządzeniu Ministra Pracy i Polityki Społecznej z dnia 27 kwietnia 2010 r. w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz zakresu jej stosowania (publikacja: Dz.U. z 2010 r., nr 82, poz. 537).

informacji (dalej w skrócie SZBI). Do podstawowych elementów takiego modelu należą (za normą [6], podkreślenia własne):

- *system zarządzania bezpieczeństwem informacji* (SZBI) – ta część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. SZBI obejmuje strukturę organizacyjną, polityki, działania planistyczne, zakresy odpowiedzialności, praktyki, procedury, procesy i zasoby;
- *deklaracja stosowania* (ang. *statement of applicability*) – dokument, w którym opisano cele stosowania zabezpieczeń oraz zabezpieczenia, które odnoszą się i mają zastosowanie w SZBI danej organizacji, oparte o rezultaty i wnioski z procesów szacowania i postępowania z ryzykiem.

Jak można zauważyć, kluczowym elementem proponowanego w normie modelu jest zarządzanie ryzykiem. Gdy mowa o analizie ryzyka w kontekście bezpieczeństwa informacyjnego, należy mieć na uwadze m.in. jej związki z analizą ryzyka biznesowego oraz zależności między osobami zaangażowanymi w ocenę (i zarządzanie) ryzyka biznesowego i ryzyka związanego z bezpieczeństwem informacji przetwarzanych, przesyłanych i przechowywanych w systemach teleinformatycznych organizacji, a także zakresy odpowiedzialności tych osób.

Dla menedżera zajmującego się ryzykiem biznesowym, ryzyko związane z przetwarzaniem informacji w systemach informacyjnych (w tym w teleinformatycznych) organizacji, będzie tylko jednym z wielu mogących mieć wpływ na osiąganie celów biznesowych wyznaczonych przez kadrę zarządzającą. Dla osoby odpowiedzialnej za bezpieczeństwo informacyjne i, w szczególności, teleinformatyczne[2] i zwykle będącej tzw. *właścicielem ryzyka IT* w kontekście całościowego ryzyka biznesowego, to „ryzyko IT" jest jedyne i najważniejsze, ponieważ ma wpływ na skuteczne zarządzanie bezpieczeństwem informacyjnym (co jest podstawowym zadaniem służbowym takiej osoby).

Zarządzanie ryzykiem (na potrzeby bezpieczeństwa informacyjnego) ma na celu:

- wykazanie, którego ryzyka i jak można uniknąć, stosując rozwiązania organizacyjne i techniczne w zakresie przetwarzania, przesyłania i przechowywania informacji w systemach informacyjnych organizacji;
- zapewnienie optymalnego, ze względu na koszty i znane/zadane ograniczenia, stanu ochrony takich informacji;
- zminimalizowanie ryzyka szczątkowego tak, aby stało się akceptowalne.

Pożądany poziom odporności na zagrożenia zapewnia zwykle tzw. *system bezpieczeństwa informacyjnego*, na który składają się powiązane i oddziałujące na siebie w różny sposób elementy[3] organizacyjne, techniczne (w tym programowe)

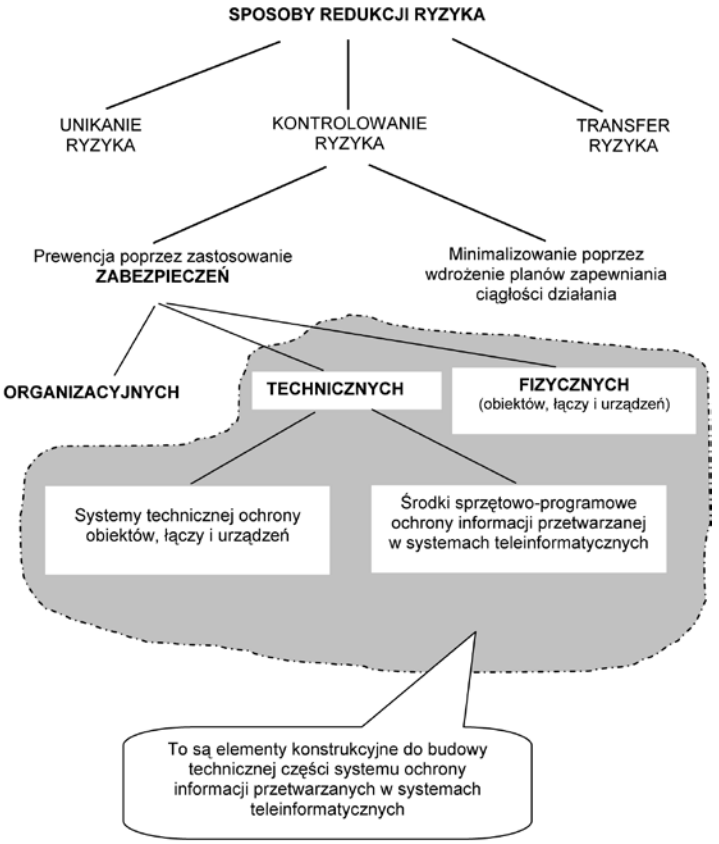
[2] Na przykład pełnomocnika ds. bezpieczeństwa lub administratora bezpieczeństwa teleinformatycznego.

[3] Nazywane zwykle zabezpieczeniami.

i ludzkie. Z perspektywy zarządzania ryzykiem, system ten służy do minimalizowania (redukcji) ryzyka – patrz rysunek 1.

Taki system, dla wszystkich wymienionych elementów składowych, powinien być dobrze udokumentowany. Jest to niezbędne dla:

- właściwej implementacji a potem eksploatacji zabezpieczeń (czyli, z perspektywy zarządzania ryzykiem, środków do minimalizacji ryzyka),
- utrzymania pod kontrolą zmian w tym systemie (czyli, z perspektywy zarządzania ryzykiem, minimalizacji ryzyka związanego z wprowadzeniem nie rozpoznanych podatności na zagrożenia),
- spełnienia wymogów różnych przepisów prawnych, które w sposób jawny nakładają obowiązek posiadania przez organizacje (o ile są przez nie przetwarzane i przechowywane określone klasy informacji) dokumentów nazywanych „polityka bezpieczeństwa", „instrukcje i procedury bezpieczeństwa" lub podobnie (patrz przykład 1). Czyli – z perspektywy zarządzania ryzykiem – minimalizacji ryzyka prawnego.



Rys. 1. Sposoby redukcji ryzyka
Źródło: opracowanie własne

Przykład 1:

I. Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. *w sprawie minimalnych wymagań dla systemów teleinformatycznych*: § 3.
   1. Podmiot publiczny opracowuje, modyfikuje w zależności od potrzeb oraz wdraża politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez ten podmiot do realizacji zadań publicznych.
   2. Przy opracowywaniu polityki bezpieczeństwa, o której mowa w ust. 1, podmiot publiczny powinien uwzględniać postanowienia Polskich Norm z zakresu bezpieczeństwa informacji.

II. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z kwietnia 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz.U. z 2004 r., nr 100, poz. 1024):

   § 3. 1. Na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją". 2. Dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej.

   3. Dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

   § 4. Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności:

   1. wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
   2. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
   3. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
   4. sposób przepływu danych pomiędzy poszczególnymi systemami;
   5. określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

***

Uważam, że system bezpieczeństwa może być w pełni udokumentowany przez następujące, dobrze opracowane i poprawnie wdrożone[4] dokumenty:

1. „Politykę bezpieczeństwa informacyjnego" – zawiera najważniejsze, ogólne ustalenia dotyczące działania organizacji w zakresie ochrony informacji i zasad jej przetwarzania; powinien być udostępniany wszystkim zainteresowanym.

[4] „Wdrożone" oznacza, że dokumenty te muszą zostać wprowadzone w organizacji odpowiednim zarządzeniem naczelnego kierownictwa oraz muszą zostać wykonane odpowiednie czynności administracyjne, jak np. szkolenia, zakupy czy zmiany w obiegu dokumentów oraz techniczne, jak np. instalacja sprzętu komputerowego i oprogramowania.

2. „Plan bezpieczeństwa informacyjnego" – zawiera szczegóły budowy systemu bezpieczeństwa informacyjnego; powinien być udostępniany zgodnie z zasadą „wiedzy koniecznej".
3. „Instrukcje i procedury bezpieczeństwa teleinformatycznego" – zawiera zasady i sposób postępowania w zakresie bezpieczeństwa teleinformatycznego dla osób korzystających z systemów teleinformatycznych; dokument do użytku wewnętrznego.
4. „Plan zapewniania informacyjnej ciągłości działania" – zawiera instrukcje i procedury postępowania w przypadku wystąpienia tzw. zdarzeń kryzysowych naruszających informacyjną ciągłość działania; dokument do użytku wewnętrznego, podlegający specjalnej ochronie.

Podstawowym z wymienionych czterech dokumentów jest „polityka bezpieczeństwa informacyjnego". W dalszej części artykułu, ze względu na ograniczone ramy publikacji, zostanie bardziej szczegółowo opisany tylko ten dokument. Informacje nt. planu zapewniania ciągłości działania zainteresowany Czytelnik znajdzie w publikacjach [1] i [2] oraz w normach i standardach [3, 4, 7, 10, 11].

1. Dokument „polityka bezpieczeństwa informacyjnego"

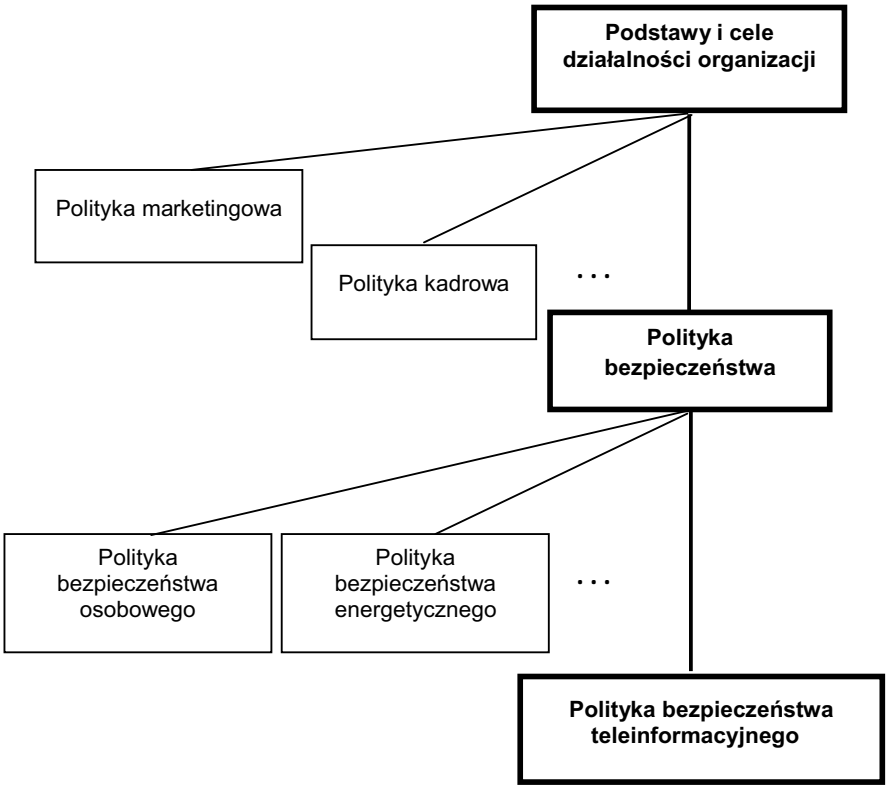
Potocznie termin „polityka" określa zorganizowane działania mające doprowadzić do osiągnięcia założonego celu(-ów)[5]. Na terenie konkretnej organizacji realizowane są zwykle różnorodne działania określane mianem „polityki", np.: polityka finansowa, polityka kadrowa, polityka marketingowa itd. (por. rys. 2). Zwykle te działania (określane tutaj mianem polityki) są wzajemnie powiązane, a zasady przeprowadzenia tych działań są spisane w odpowiednich dokumentach zatytułowanych „Polityka...". Podstawą dla wszelkiego rodzaju polityk realizowanych na terenie organizacji jest zazwyczaj jej statut, zawierający podstawę prawną i cele działalności[6].

Zdaję sobie w pełni sprawę z tego, że tak prymitywna definicja polityki może razić politologów czy przedstawicieli nauk społecznych. Jednak w dziedzinie, w której stosuję to pojęcie (bezpieczeństwo informacyjne), jest ono tak interpretowane. Uważam także, że jest ono zgodne z uznanymi interpretacjami – patrz znaczenie 3 w podanej w przypisie 5 definicji. Warto zwrócić także uwagę, że w języku angielskim opisywane pojęcie to „policy", nie mające odpowiednika w języku polskim,

[5] **Polityka** (gr. *politiké* 'sztuka rządzenia państwem', *tá politiká* 'sprawy publiczne, rządzenie') **1.** prowadzenie przez administrację rządową, samorządową działań zmierzających do określonej organizacji społeczeństwa w państwie oraz kierowania nim w kontaktach międzypaństwowych. **2.** działalność ugrupowań politycznych i społecznych mająca na celu zdobycie i sprawowanie władzy w państwie celem realizacji własnych celów programowych; także ogół działań prowadzonych dla osiągnięcia tego celu. **3.** *przen.* konsekwentne działanie w stosunku do jakiejś osoby lub grupy.
Na podstawie *Słownika Wyrazów Obcych,* Wydawnictwa Europa, M. Jarosz i zespół pod red. nauk. I. Kamińskiej-Szmaj, 2001.

[6] Często w tym kontekście pisze się o „misji" (ang. *mission*) organizacji.

różniące się od „politics" odpowiadającego rozumieniu polityki przez politologów i humanistów (polityka międzynarodowa, polityka obronna państwa itp.).



Rys. 2. „Polityki" w organizacji
Źródło: opracowanie własne

Dokumenty zatytułowane „Polityka..." wytwarza się m.in. w celu spełnienia wymogów różnych przepisów prawnych, które w sposób jawny nakładają obowiązek posiadania przez organizację takich dokumentów. Niestety, informacje zawarte w takich przepisach, a dotyczące konstrukcji i zawartości wymienionych dokumentów, są zwykle bardzo ogólnikowe, a nieraz także sprzeczne. Chaos w tym zakresie pogłębiają jeszcze różne interpretacje terminu „polityka". Normy i standardy odpowiednie dla bezpieczeństwa teleinformatycznego często ten chaos pogłębiają. Dlatego proponuję przyjęcie następujących ustaleń:

1) politykę (rozumianą jako sposób i zakres działania) kształtuje naczelne kierownictwo organizacji;
2) polityka w zakresie bezpieczeństwa informacyjnego jest realizowana przez ogół pracowników organizacji;
3) polityka w zakresie bezpieczeństwa teleinformatycznego jest nadzorowana przez osoby, które takie zadanie mają wpisane w swój zakres obowiązków

(głównie dotyczy to kierownictwa działów IT i osób z komórek organizacyjnych lub stanowisk związanych z bezpieczeństwem);

4) żeby politykę można było skutecznie realizować (czyli prowadzić działania mające doprowadzić do określonego celu – w tym przypadku zapewnienia odpowiedniego poziomu bezpieczeństwa informacyjnego) oraz nadzorować i w razie potrzeby aktualizować, polityka powinna być spisana w postaci dokumentu zatytułowanego (zwykle) „Polityka bezpieczeństwa informacyjnego”[7];
5) dokument, o którym mowa w punkcie 4), musi być wdrożony (por. przypis 4).

Dokument „Polityka bezpieczeństwa informacyjnego” (dalej w tekście PBI) to opis najważniejszych, ogólnych zamiarów działań i deklaracji najwyższego kierownictwa organizacji w zakresie zapewniania w niej odpowiedniego poziomu bezpieczeństwa informacyjnego. Przeznaczony jest do uzasadnienia zaufania klientów i partnerów biznesowych do powierzenia swoich informacji tej organizacji oraz stanowi podstawę do opracowania szczegółowych rozwiązań organizacyjnych i technicznych w zakresie ochrony informacji. PBI powinna być dokumentem jawnym, ogólnie dostępnym i powinna zawierać następujące informacje[8]:

1) słownik używanych pojęć i skrótów, w tym definicję bezpieczeństwa informacji oraz ról w systemie (właściciel, użytkownik, operator, administrator itp.);
2) wykaz dokumentów normatywnych (przepisów prawnych, jak np. ustawy, oraz standardów i norm technicznych), z których zapisami jest zgodny system ochrony informacji w organizacji[9] (patrz przykład 6.3);
3) wykaz aktów normatywnych, zgodnie z którymi należy rozstrzygać kwestie nieujęte w PBI i dokumentach pochodnych;
4) zakres (terytorialny i organizacyjny) i cel PBI;
5) deklarację priorytetów wartości dla organizacji, np.: życie i zdrowie klientów, życie pracowników i ich rodzin, zasoby powierzone, zasoby niezbędne dla utrzymania ciągłości działania itd.;
6) cel(-e) budowania systemu ochrony informacji;
7) deklarację zarządu organizacji odnośnie do środków finansowych przeznaczanych na bezpieczeństwo informacyjne;
8) opis zasobów informacyjnych organizacji, w tym:
   – specyfikację grup informacji podlegających szczególnej ochronie,
   – wymagany poziom ochrony dla każdej z grup informacji,

[7] W dalszej części termin „polityka” (domyślnie: w zakresie bezpieczeństwa informacyjnego) będzie używany wyłącznie jako nazwa dokumentu wymienionego w tym punkcie.

[8] Zapisy na temat polityki bezpieczeństwa informacyjnego oraz zawartości dokumentu, w zasadzie zgodne z przedstawionymi tutaj poglądami autora, można znaleźć także w normie PN-ISO/IEC-17799:2007, punkty: 5.1.1, 5.1.2, 6.1.1, 6.1.2.

[9] Wtedy w tekście PBI muszą być umieszczone zapisy wymagane prawem i, w razie umieszczenia takich odwołań, warunki zgodności z podstawowymi normami bezpieczeństwa.

- w razie potrzeby – system klasyfikacji i kategoryzacji informacji,
- znaczenie poszczególnych systemów informacyjnych (w szczególności teleinformatycznych) organizacji dla realizacji zadań statutowych,
- opis otoczenia informacyjnego organizacji, z dokładnym wskazaniem miejsc wejścia i wyjścia informacji do/z jej systemów informacyjnych,
- zasady dokumentowania systemu ochrony informacji;

9) ogólną zasadę podjęcia stosownych działań (także spoza zakresu kompetencji) oraz odstąpienia od działania (także należącego do obowiązków), z inicjatywy własnej lub na wezwanie (także w przypadku braku podległości służbowej) – w przypadku stwierdzenia zagrożenia interesów organizacji, w szczególności wartości priorytetowych dla organizacji (patrz punkt 5);
10) obowiązki i zakresy odpowiedzialności kierownictwa i pracowników organizacji w procesie ochrony zasobów informacyjnych oraz konsekwencje w przypadku nieprzestrzegania zasad zawartych w PBI;
11) ogólne zasady organizacyjne dotyczące dokumentu PBI, np.:
    - zapis o nadrzędności wobec innych dokumentów z zakresu bezpieczeństwa,
    - kto odpowiada za dokument PBI,
    - kto, kiedy i w jakim trybie może zmienić zapisy w PBI,
    - sposób przeglądu i aktualizacji PBI,
    - powiązania z regulacjami prawnymi i wewnętrznymi organizacji;
12) zasady nadawania uprawnień do działania na zasobach informacyjnych, w tym:
    - kto (na jakim stanowisku służbowym) i w jakim zakresie ma prawo do występowania o nadanie pracownikom uprawnień do zasobów informacyjnych,
    - kto, kiedy i w jakim zakresie ma prawo do występowania o nadanie uprawnień do zasobów informacyjnych w sytuacjach doraźnych (np. konsultantom zewnętrznym) lub wyjątkowych (np. w przypadku śmierci odpowiedzialnego za zasób pracownika lub żądania uprawnionych organów: policji, GIODO, kontroli skarbowej itd.),
    - sposób przekazywania i przechowywania informacji uwierzytelniających i autoryzacyjnych,
    - wzór (jako załącznik do PBI) dokumentu o nadanie uprawnień lub wskazanie aplikacji, za pomocą której takie zadanie jest realizowane w systemie informatycznym;
13) zasady dostępu do zasobów informacyjnych organizacji;
14) zasady przetwarzania informacji w systemach teleinformatycznych (zwykle poprzez odwołanie do innych dokumentów szczegółowych typu instrukcje i procedury) oraz przechowywania zbiorów informacyjnych (w tym komputerowych nośników informacji);

15) zasady ochrony zasobów informacyjnych niezbędnych do realizacji kluczowych procesów biznesowych;
16) zasady nadzoru nad wykorzystaniem zasobów informacyjnych zgodnie z obowiązującym prawem i wewnętrznymi przepisami organizacji;
17) zasady usuwania informacji z nośników komputerowych i niszczenia dokumentów papierowych;
18) koncepcję szkolenia pracowników organizacji w zakresie ochrony informacji;
19) zarys systemu kontroli, w tym audytów, w toku normalnej pracy organizacji;
20) ogólne wytyczne do sposobu reakcji na zdarzenia naruszające bezpieczeństwo informacyjne oraz wskazanie dokumentów zawierających szczegóły postępowania w takich przypadkach;
21) załączniki różne (np. schemat klasyfikacji informacji, schemat organizacyjny, wzory dokumentów itp.).

Warunkami i działaniami, bez których osiągnięcie sukcesu w opracowywaniu i wdrażaniu polityki bezpieczeństwa nie wydaje się możliwe, są:

1) świadomość najwyższej kadry kierowniczej znaczenia bezpieczeństwa informacyjnego dla działalności biznesowej organizacji;
2) chęć i jawna deklaracja najwyższej kadry kierowniczej wsparcia działań podnoszących poziom bezpieczeństwa informacyjnego, w tym zapewnienia odpowiednich środków finansowych;
3) sformułowanie celu budowy systemu bezpieczeństwa;
4) powołanie zespołu ds. zarządzania bezpieczeństwem informacyjnym, który będzie opracowywał (bądź nadzorował opracowanie) politykę bezpieczeństwa informacyjnego dla swojej organizacji;
5) podjęcie decyzji co do sposobu budowy (lub zmiany) systemu bezpieczeństwa informacyjnego – własnymi siłami organizacji lub wynajęcie do wykonania tej pracy wyspecjalizowanego zespołu z zewnątrz organizacji (rozwiązanie częściej spotykane);
6) zidentyfikowanie kluczowych dla działania organizacji procesów biznesowych (i związanych z nimi systemów teleinformatycznych);
7) zidentyfikowanie grup informacji, których ochrona jest szczególnie pożądana i określenie wymaganego poziomu ich ochrony (również ze względu na spełnienie wymagań ustawowych);
8) wstępne oszacowanie możliwych kosztów strat w przypadku utraty poufności, integralności lub dostępności informacji (również pod względem naruszenia przepisów prawnych państwowych lub resortowych, np. naruszenie przepisu o ochronie danych osobowych).

Należy zwrócić uwagę, że dla punktów 1-5 wymagane jest zaangażowanie najwyższego kierownictwa organizacji. W realizację punktów 6-8, wykonywanych najczęściej pod kierunkiem zewnętrznych ekspertów, są także zaangażowani przed-

stawiciele najwyższego kierownictwa, jako kompetentne osoby mające prawo do zajmowania oficjalnego stanowiska w imieniu organizacji.

Określenie niezbędności systemów teleinformatycznych w wypełnianiu zadań służbowych można przeprowadzić, stosując np. następującą opisową skalę ocen:

- **wspomagające** – zadania służbowe przy niewielkim dodatkowym nakładzie sił i środków mogą być wykonane innymi środkami (np. ręcznie);
- **ważne** – zadania służbowe mogą być wykonane innymi środkami tylko znacznym dodatkowym nakładem sił i środków;
- **zasadnicze** – ze względu na dużą ilość informacji, zadania służbowe mogą być wykonane innymi środkami tylko częściowo;
- **niezbędne** – zadania służbowe nie mogą być wykonane bez wykorzystania systemów teleinformatycznych.

Oszacowanie pożądanego poziomu ochrony informacji dotyczy wymaganej siły zabezpieczeń zastosowanych w konkretnych systemach teleinformatycznych i zwykle jest określane na podstawie skutków biznesowych (jako wynik tzw. *business impact analysis*), które miałyby miejsce, gdyby tych zabezpieczeń nie było. Poziom ten można określić na przykład według następującej skali:

- **bardzo wysoki** – gdy błędy w ochronie informacji przetwarzanych w systemach teleinformatycznych organizacji prowadzą do jej bankructwa lub wywierają szerokie niekorzystne skutki społeczne lub gospodarcze;
- **wysoki** – gdy błędy w ochronie informacji przetwarzanych w systemach teleinformatycznych organizacji naruszają zdolność do działania jej kluczowych elementów, a szkody z tego wynikłe dotyczą jej i podmiotów trzecich;
- **średni** – gdy błędy w ochronie informacji przetwarzanych w systemach teleinformatycznych organizacji przynoszą straty tylko tej organizacji;
- **niski** – jw., ale gdy straty są niewielkie.

W niektórych przypadkach (patrz przykład 2) poziomy ochrony mogą być jawnie wyspecyfikowane w przepisach prawnych. Natomiast cele budowania bezpieczeństwa teleinformatycznego będą zwykle następujące:

- zapewnienie dobrej marki organizacji na rynku;
- zapewnienie ciągłości pracy w organizacji;
- zapewnienie realizacji wymagań przepisów prawnych np. o ochronie tajemnicy przedsiębiorstwa;
- zagwarantowanie niezawodności procesów biznesowych z punktu widzenia zarówno ich terminowości (dostępność informacji), dokładności (integralność informacji), jak i poufności.

Przykład 2:

Wymagania bezpieczeństwa wynikające z rozporządzenia MSWiA z dnia 29 kwietnia 2004 r. „w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać

urządzenia i systemy informatyczne służące do przetwarzania danych osobowych" (Dz.U. z 2004 r., nr 100, poz. 1024):

1. Zróżnicowanie wymaganego poziomu ochrony przetwarzania danych w zależności od kategorii przetwarzanych danych oraz występujących zagrożeń:
   - **poziom podstawowy** – gdy **nie są** przetwarzane dane, o których mowa w art. 27[10] ustawy, oraz żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych **nie jest połączone** z siecią publiczną;
   - **poziom podwyższony –** gdy **są** przetwarzane dane, o których mowa w art. 27 ustawy oraz żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych **nie jest połączone** z siecią publiczną;
   - **poziom wysoki –** gdy przynajmniej jedno z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych jest połączone z siecią publiczną.

   W rozporządzeniu są wyspecyfikowane stosowane obligatoryjnie środki ochronne, bez określenia sposobu implementacji tych środków.

   Na poziomie wysokim wymagane jest stosowanie środków ochrony kryptograficznej nie tylko wobec danych osobowych przesyłanych w publicznej sieci telekomunikacyjnej, ale również wobec informacji wykorzystywanych do uwierzytelniania się w systemie.
2. Obowiązek prowadzenia dokumentacji przetwarzania danych osobowych:
   - polityki bezpieczeństwa;
   - instrukcji zarządzania systemem informatycznym.
3. W odniesieniu do przetwarzania danych osobowych przez instytucje i organy ustanowione przez lub na podstawie traktatów ustanawiających Wspólnoty Europejskie, dodatkowo obowiązują wymagania wynikające z przepisów prawa UE.

***

Wdrożenie w organizacji dokumentów opisujących system bezpieczeństwa (patrz przypis 4) jest jednym z etapów wdrażania systemu bezpieczeństwa informacyjnego. W skład tego etapu wchodzą m.in. dwa przedsięwzięcia organizacyjne:

1) wprowadzenie do użytku w organizacji, odpowiednim zarządzeniem naczelnego kierownictwa, dokumentów opisujących system bezpieczeństwa informacyjnego,
2) przeprowadzenie szkolenia personelu organizacji (podstawą szkolenia są ww. dokumenty).

[10] Art. 27 ust. 1 (ust. 2 precyzuje, kiedy takie przetwarzanie jest dopuszczalne):
„Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym".

Kształtowanie świadomości kierownictwa i pracowników w zakresie bezpieczeństwa informacyjnego uważa się za jeden z kluczowych elementów zapewniania tego bezpieczeństwa. Praktyczne wskazówki dotyczące prowadzenia szkoleń z ochrony informacji niejawnych[11] i bezpieczeństwa informacyjnego można sformułować następująco:

1. Szkolenia personelu powinny obejmować cały związany z systemami informacyjnymi personel – od członków zarządu do zwykłego użytkownika systemu teleinformatycznego. Wymóg przeszkolenia dotyczy także pracowników okresowych (np. praktykantów, pracowników outsourcingowych itp.).
2. Merytoryczną podstawą szkolenia są wdrożone w organizacji, wymienione we wstępie niniejszego rozdziału, dokumenty (głównie dokument „Instrukcje i procedury...").
3. Szkolenie powinno być przeprowadzone, zanim zostaną w pełni wdrożone techniczne i organizacyjne przedsięwzięcia związane z systemem bezpieczeństwa.
4. Szkolenia powinny być powtarzane w regularnych odstępach czasu.
5. Tematyka szkolenia powinna uwzględniać również zagadnienia ogólne, takie jak:
   – cele wdrażania systemu bezpieczeństwa informacyjnego,
   – wybrane elementy obowiązującej w organizacji koncepcji bezpieczeństwa informacyjnego (w szczególności wskazanie osób odpowiedzialnych za poszczególne elementy tego bezpieczeństwa),
   – sposoby postępowania w przypadkach naruszania bezpieczeństwa.
6. Wszyscy pracownicy powinni poświadczyć własnoręcznym podpisem odbycie szkoleń z zakresu bezpieczeństwa informacyjnego, a fakt odbycia szkolenia powinien być odnotowany w aktach personalnych pracownika.
7. Szkolenia z podstaw bezpieczeństwa informacyjnego powinny zawierać elementy ochrony informacji niejawnych (w szczególności obowiązujący w organizacji system klasyfikowania informacji), nie pomijając informacji o konsekwencjach karnych i dyscyplinarnych ponoszonych przez pracownika naruszającego zasady tego bezpieczeństwa.

Dla osiągnięcia pożądanych rezultatów, szkolenia prowadzone są zwykle w następujących grupach:

1) najwyższej kadry kierowniczej organizacji;
2) personelu kierowniczego średniego szczebla;
3) pracowników biurowych;
4) personelu technicznego i pomocniczego;
5) administratorów sieci, serwerów, stacji roboczych i systemów.

[11] W przypadku informacji niejawnych w rozumieniu ustawowym, tryb i zakres prowadzonych szkoleń jest szczegółowo regulowany odpowiednimi przepisami.

Najwyższą kadrę kierowniczą należy przeszkolić, ponieważ to ona decyduje, na co i jak wydać pieniądze organizacji. W szczególności to spośród niej będzie się rekrutował tzw. *właściciel ryzyka* (tutaj: informacyjnego). Kadra ta powinna zatem zostać przekonana o słuszności inwestowania w „bezpieczeństwo" oraz muszą jej zostać dostarczone niezbędne informacje do podejmowania prawidłowych decyzji w zakresie bezpieczeństwa informacyjnego, w tym minimalizacji ryzyka. Poza tym, to na VIP-owskich notebookach znajdują się zwykle informacje szczególnie wrażliwe.

Personel kierowniczy średniego szczebla należy przeszkolić, ponieważ to on będzie w dużej mierze decydował o powodzeniu organizacyjnej strony przedsięwzięć bezpieczeństwa. To kierownicy komórek organizacyjnych występują o nadanie uprawnień w systemie dla podległych pracowników (a zatem powinni znać zasady „wiedzy koniecznej" i „minimalnego środowiska pracy"), to oni bezpośrednio nadzorują tzw. politykę „czystego biurka" i „czystego ekranu", to oni decydują o skierowaniu swoich pracowników na szkolenia itd. To personel kierowniczy średniego szczebla jest w głównej mierze nosicielem szczególnie groźnego dla skuteczności systemu bezpieczeństwa „syndromu kelnera": „Bezpieczeństwo sieci i komputerów? To nie ja (my), to dyrektor działu IT i jego ludzie!".

Szczególną uwagę należy zwrócić także na podnoszenie kwalifikacji przez administratorów technicznych w zakresie zarządzanych przez nich systemów i urządzeń. Im bowiem więcej administrator wie o systemie (urządzeniu, oprogramowaniu), tym lepiej może zrozumieć jego działanie i skuteczniej nim zarządzać, również pod względem bezpieczeństwa informacyjnego.

Przykład 3:

Kształtowanie świadomości w zakresie bezpieczeństwa teleinformatycznego według normy PN-ISO/IEC 27001:2007 (załącznik A.6.2.1: Szkolenie i kształcenie w zakresie bezpieczeństwa informacji): „Wszyscy pracownicy instytucji, a jeśli to konieczne, także użytkownicy – osoby trzecie – pochodzący spoza instytucji, powinni przejść właściwe, okresowo uaktualniane, przeszkolenie w zakresie polityk i procedur obowiązujących w instytucji, zanim zostanie im przyznany dostęp do informacji lub usług".

Norma PN-ISO/IEC-17799:2007 precyzuje w punkcie 6.2.1: „Przeszkolenie takie obejmuje wymagania bezpieczeństwa, odpowiedzialność prawną i zabezpieczenia wewnętrzne, jak również przeszkolenie w zakresie prawidłowego korzystania z urządzeń przetwarzania informacji, np. procedur rejestrowania w systemie, używania pakietów oprogramowania".

Podsumowanie

Znaczenie dokumentu „Polityka bezpieczeństwa informacyjnego" wynika z faktu, że jego posiadanie:

– świadczy o „należytej staranności" organizacji w zakresie ochrony informacji i daje **podstawy do rzetelnego zarządzania ryzykiem informacyjnym**;

- stanowi podstawę zaufania potencjalnych klientów lub partnerów biznesowych do powierzenia swoich dóbr informacyjnych takiej organizacji;
- dla audytora stanowi dowód, że koncepcja ochrony informacji jest przemyślana i spisana;
- dla inżynierów budujących system ochrony informacji (lub, patrząc na problem z perspektywy zarządzania ryzykiem, system minimalizacji ryzyka) zawiera podstawowe wymagania projektowe i operacyjne (wytyczne) na taki system;
- dla pracowników zaangażowanych w ochronę informacji stanowi podstawowy zbiór zasad pozwalających im na skuteczne pełnienie obowiązków służbowych;
- jest wymagane przez przepisy prawa (np. ustawę o ochronie danych osobowych i stosowne rozporządzenie) – patrz przykład 1.

Do efektywnego zarządzania ryzykiem potrzebne będą także pozostałe, wymienione pod koniec rozdziału 1, dokumenty:

- instrukcje i procedury z zakresu bezpieczeństwa teleinformatycznego są niezbędne do minimalizowania ryzyka związanego z błędami ludzkimi i proceduralnymi;
- „Plan bezpieczeństwa informacyjnego" jest niezbędny do minimalizowania ryzyka niewłaściwego zaprojektowania systemu ochrony oraz ryzyka jego niewłaściwej eksploatacji;
- „Plan zapewniania informacyjnej ciągłości działania" jest niezbędny do minimalizowania ryzyka związanego z wystąpieniem zdarzeń naruszających ciągłość pracy systemu informacyjnego lub integralność albo dostępność zbiorów danych.

ABOUT SIGNIFICANT RELIABLE INFORMATION SECURITY SYSTEM DOCUMENTATION FOR INFORMATION RISK MANAGEMENT

Summary: The paper presents author's view for significant reliable information security system documentation for information risk management. It presents an outline of activity assembled on information risk management. It explains the way of understanding the term "policy" in information security area. In details there is described the content of information security policy document.

Keywords: information risk management, information security, information security policy.

LITERATURA

[1] Liderman K., *Plan ciągłości działania elementem dokumentowania ładu korporacyjnego*, [w:] Gonciarski W., Zaskórski P. (red.), *Wybrane koncepcje i metody zarządzania na początku XXI wieku***,** WAT, Warszawa 2009, s. 147-159.
[2] Liderman K., *Bezpieczeństwo informacyjne*, PWN, Warszawa 2012.
[3] BS 25999-1: 2006: *Business continuity management. Code of practice*.
[4] BS 25999-2: 2007: *Specification for business continuity management*.

[5] PN-ISO/IEC-17799:2007: *Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji*.
[6] PN-ISO/IEC 27001:2007: *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*.
[7] PN-ISO/IEC 24762:2010: *Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.*
[8] PN-IEC 62198:2005: *Zarządzanie ryzykiem przedsięwzięcia – Wytyczne stosowania*.
[9] PN-ISO/IEC 27005:2010: *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.*
[10] NFPA 1600: *Standard on Disaster/Emergency Management and Business Continuity Programs*, 2007 Edition.
[11] NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, June 2002.
[12] Rozporządzenia MSWiA z dnia 29 kwietnia 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz.U. z 2004 r., nr 100, poz. 1024).
[13] Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. *w sprawie minimalnych wymagań dla systemów teleinformatycznych* (Dz.U. z 2005 r., nr 212, poz. 1766).
[14] Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnej* (Dz.U. z 2010 r., nr 182, poz. 1228).

WYKORZYSTANIE TECHNOLOGII CYFROWEJ W POLSKICH ORGANIZACJACH. NIEKTÓRE WYNIKI BADAŃ ANKIETOWYCH

WIESŁAW GONCIARSKI

WOJSKOWA AKADEMIA TECHNICZNA
WYDZIAŁ CYBERNETYKI
INSTYTUT ORGANIZACJI I ZARZĄDZANIA

Wstęp

Obserwowany od kilku już dziesięcioleci dynamiczny rozwój technologii cyfrowej[1] w zasadniczy sposób zmienia warunki funkcjonowania współczesnego rynku. Widać to zarówno wtedy, gdy analizuje się funkcjonowanie globalnego rynku, jak i wtedy, gdy obserwuje się podmioty gospodarcze, gospodarstwa domowe, instytucje państwowe oraz inne organizacje. Oczywiście, postęp technologiczny nie jest równomierny i zarówno w skali świata, jak i poszczególnych państw mamy obszary, na których technologia cyfrowa jest powszechnie dostępna i wykorzystywana, jak również takie, które można określić mianem wykluczenia cyfrowego.

Zarządzanie organizacjami w XXI wieku wymaga stosowania technologii teleinformatycznej praktycznie we wszystkich obszarach aktywności i prawie wszystkich funkcjach oraz procesach organizacyjnych. Stosowanie zaawansowanych systemów teleinformatycznych jest dowodem nowoczesności zarządzania, a ich brak w organizacji sugeruje egzystowanie na obrzeżach nowoczesnej gospodarki. Jest jednak oczywiste, że poziom wykorzystywania technologii teleinformatycznej w zarządzaniu nie jest taki sam na całym świecie. W państwach wysokorozwiniętych technologia teleinformatyczna wykorzystywana jest powszechnie i to w zaawansowanych aplikacjach, a w znacznej części świata rozwijającego się jest ona stosowana w znacznie mniejszym stopniu.

Gdy jednak ograniczymy analizę do państw wysoko i średnio rozwiniętych, to możemy stwierdzić, że technologia teleinformatyczna jest na początku XXI wieku wszechobecna. W konsekwencji coraz trudniej sobie wyobrazić możliwość funkcjonowania wielu podmiotów (np. banków, firm ubezpieczeniowych, firm logistycznych) bez wykorzystywania zaawansowanych rozwiązań technologii teleinformatycznej. Oczywiście, ciągle też wiele firm wykorzystuje tylko część możliwości,

[1] Terminy „technologia teleinformatyczna" i „technologia cyfrowa" w tym artykule będą traktowane jak synonimy, pomimo tego, że formalnie rzecz ujmując występują między nimi pewne różnice.

jakie daje dzisiejsza technologia cyfrowa i wiele z nich wdraża tylko podstawowe jej rozwiązania. W tym kontekście interesującym problemem wydaje się analiza wykorzystania technologii teleinformatycznej przez polskie organizacje.

Konstatacja powyższa skłoniła autora tego artykułu do przeprowadzenia badań pilotażowych, których celem było zbadanie: jak pracownicy danych organizacji oceniają wykorzystanie technologii teleinformatycznej w swoich firmach. A w dalszej kolejności celem badań było skonfrontowanie uzyskanych wyników z analizami statystycznymi przeprowadzonymi przez polskie i zagraniczne instytucje statystyczne (np. GUS, Eurostat).

Podstawowym celem tego artykułu jest przedstawienie niektórych wyników przeprowadzonych badań ankietowych, gdyż ograniczone ramy objętościowe artykułu uniemożliwiają przedstawienie całości.

1. Znaczenie technologii teleinformatycznej we współczesnym zarządzaniu

Postęp technologiczny jest dość oczywistym zjawiskiem cywilizacyjnym, chociaż przez znaczną część rozwoju cywilizacji ludzkiej jego konsekwencje były słabo zauważalne[2]. Analizując rozwój gospodarczy na przestrzeni wieków, G. Hamel podkreśla, że od 1000 do 1820 roku dochód *per capita* wzrósł jedynie o 50%. Natomiast w ciągu ostatnich dwustu lat skoczył o 800%. Oznacza to, mówiąc najprościej, że innowacyjność napędzana technologiami wydobyła ludzkość z niedostatku[3]. Rozwój cywilizacji ludzkiej nie jest oczywiście wynikiem wyłącznie doskonalenia technologii, ale nie ulega wątpliwości, że technologia odgrywa tu rolę znaczącą. Ale zgodnie z sugestią M. Castellsa[4] należy odrzucać determinizm technologiczny, co jednak nie może prowadzić do poglądu – jak trafnie zauważa Y. Benkler[5] – że technologie są tylko narzędziami w rękach poszczególnych społeczeństw. Pomimo tego, że „nie ma ustalonego kanonu wiedzy dotyczącej roli nowych technologii w zarządzaniu"[6], gotowość i umiejętność wykorzystywania istniejącego potencjału nowej technologii jest dowodem na nowoczesność danego społeczeństwa.

Obecnie jesteśmy świadkami i uczestnikami procesu przekształceń technologicznych, które przez wielu określane są mianem trzeciej rewolucji przemysłowej[7]. Pierwsza kojarzona była z wynalezieniem silnika parowego, symbolem drugiej była

[2] R.E.S. Boulton, B.D. Libert, S.M. Samek, *Odczytując kod wartości*, WIG-Press, Warszawa 2001, s. 37.
[3] G. Hamel, *Ce qui compie vraiment. Le 5 défis pour l'entreprise*, Éditions. Eyrolles, Paris 2012, s. 66.
[4] M. Castells, *Społeczeństwo sieci*, PWN, Warszawa 2007, s. 22-23.
[5] Y. Benkler, *Bogactwo sieci*, Wyd. Akademickie i Profesjonalne, Warszawa 2008, s. 34.
[6] J. Kociatkiewicz, *Nowe technologie w organizacjach*, [w:] M. Kostera (red.), *Nowe kierunki w zarządzaniu*, Wyd. Akademickie i Profesjonalne, Warszawa 2008, s. 321.
[7] J. Rifkin, *Trzecia rewolucja przemysłowa*, Sonia Draga, Katowice 2012, s. 60-61; L. Thurow, *Fortuna sprzyja odważnym*, Muza, Warszawa 2007, s. 46-50; J.-P. Mongand, *Le manager dans la nouvelle économie*, Éditions d'Organisation, Paris 2001, s. 18.

elektryczność, a trzecia utożsamiana jest z rozwojem informatyki[8]. I chociaż można zgodzić się z R. Cameronem, że termin rewolucja nie jest najtrafniejszy dla opisywania przemian wywołanych ujarzmieniem pary i wykorzystaniem elektryczności[9], to w odniesieniu do technologii cyfrowej i jej wpływu na przekształcania różnych wymiarów funkcjonowania systemów ekonomicznych i społecznych pasuje zdecydowanie lepiej. Zakres i tempo zmian są bowiem tak duże, że na oczach współczesnych burzą dotychczasowy porządek. R. Normann zauważa, że prowadzi to do formułowania nowego paradygmatu strategicznego, a siłą napędową zmian, tak jak wcześniej, znów jest technologia, z tym że obecnie jest to technologia cyfrowa[10]. W efekcie tworzy się nowy porządek świata, który rewolucjonizuje dotychczasowe reguły gospodarcze[11]. A szczególny wkład w tym zakresie – na podobieństwo elektryczności w wieku poprzednim – wnosi Internet[12]. W szczególności technologia ta wpływa lub może wpływać na zarządzanie. Jej oddziaływanie zależy oczywiście od ludzi, ich wiedzy, umiejętności i gotowości wykorzystywania jej w życiu prywatnym i zawodowym. Potencjał, jaki ona dostarcza, może pozwalać na osiąganie wspaniałych wyników, ale równie dobrze może być niedostrzegany lub marnotrawiony.

Niedocenianie lub wręcz lekceważenie znaczenia technologii teleinformatycznej we współczesnym zarządzaniu jest – jak się wydaje – związane przede wszystkim z wykluczeniem cyfrowym, którego powodem może być brak wiedzy, wiek osoby wypowiadającej się na ten temat lub trudność uzyskania dostępu do technologii spowodowana czy to ograniczeniami finansowymi, czy też techniczno-terytorialnymi. Wydaje się jednak, że szczególnie niebezpieczne jest tzw. wykluczenie mentalne. W tym kontekście warto odnotować stanowisko H. Mintzberga, który w ostatnio wydanej książce[13] wyraźnie nie docenia technologii cyfrowej, a zwłaszcza Internetu. Ten skądinąd wybitny, znany i ceniony profesor zarządzania formułuje swoje opnie o tej technologii na skojarzeniu, że najważniejszym narzędziem komunikacji internetowej jest poczta elektroniczna, która – jak twierdzi – jest ograniczona zarówno ubóstwem słowa pisanego, jak i tym, że „nawet dodawanie obrazów do e-maili bywa nieraz kłopotliwe"[14]. Tego typu poglądy prezentowane w dobie technologii Web 2.0 (blogów, portali społecznościowych, technologii Wiki, *cloud compating'u*) wydają się, delikatnie mówiąc, nieporozumieniem. Jak na przykład podaje J. Gleick[15] w 2010 r. tylko przez YouTube przepływało dziennie ponad miliard nagrań wideo. Przywołuję i komentuję powyższe stanowisko w przekonaniu, że zbyt wiele

[8] B. Jarrosson, *Vers l'economie 2.0*, Éditions d'Organisation, Paris 2009, s. 37-46; J. Papińska-Kacperek, *Nowa epoka – społeczeństwo informacyjne*, [w:] J. Papińska- Kacperek (red.), *Społeczeństwo informacyjne*, PWN, Warszawa 2008, s. 19-21.

[9] R. Cameron, *Historia gospodarcza świata*, KiW, Warszawa 1996, s. 181-183.

[10] R. Normann, *Przeformułowanie w biznesie*, GWP, Gdańsk 2012, s. 35.

[11] D. Tapscott, *Gospodarka cyfrowa*, Business Press, Warszawa 1998, s. 6-7.

[12] D. Cohen, *Trois leçons sur la société post-industrielle*, Éditions Seuil, Paris 2006, s. 21.

[13] H. Mintzberg, *Zarządzanie*, Wolters Kluwer Polska, Warszawa 2012 (oryg. 2009), s. 54-58.

[14] Ibidem, s. 55.

[15] J. Gleick, *Informacja – bit, wszechświat, rewolucja*, Znak, Kraków 2012, s. 367.

wypowiedzi teoretyków i praktyków zarządzania – w których technologii cyfrowej w ogóle się nie dostrzega lub nie docenia – formułowanych jest w całkowitym oderwaniu od rzeczywistości.

Świat dzisiejszego nowoczesnego zarządzania nie może bowiem obejść się bez technologii teleinformatycznej[16]. Wikinomia, społeczeństwo sieci czy struktury wirtualne to nie fantasmagorie cybermaniaków, ale dzisiejsza rzeczywistość, w której organizacja, jeśli chce przetrwać, musi znaleźć dla siebie jakieś miejsce. Chociaż pamiętać też należy, że np. „wikinomia sama w sobie nie stanowi antidotum na wszelkie dolegliwości świata"[17] i w efekcie jest tylko platformą pozwalającą doskonalić różne wymiary życia organizacyjnego. W szczególności nowe technologie teleinformatyczne zmieniają metody prowadzenia biznesu[18], pozwalają na kształtowanie nowych modeli biznesowych[19], przekształcają zarządzanie organizacjami[20] i umożliwiają globalną, prawie niczym nieograniczoną współpracę.

Analizując problem wykorzystania technologii teleinformatycznej w organizacjach, zauważyć jednak należy, że chodzi tu zarówno o tak banalną kwestię jak dostęp do Internetu, jak i o zaawansowane rozwiązania technologiczne, takie jak *cloud compating* czy oprogramowanie CRM, ERP, SCM, KM i wiele innych[21]. Technologie te pozwalają organizacjom normalnie funkcjonować na rynku, zwiększać efektywność, podnosić jakość działań, lepiej komunikować się z klientami, zarządzać wiedzą, wykorzystywać możliwości współpracowników, sięgać po potencjał globalnego rynku.

2. Niektóre założenia metodologiczne badań ankietowych

Ocena wykorzystania technologii cyfrowej przez organizacje może być dokonywana z różnych perspektyw. Można analizować wyposażenie organizacji w sprzęt teleinformatyczny i oprogramowanie, można oceniać działanie organizacji w zakresie ogólnego wykorzystywania tej technologii, można badać wykorzystywanie technologii w odniesieniu do poszczególnych funkcji (marketing, logistyka, procesy,

[16] Szerzej: W. Gonciarski, *Specyficzne aspekty zarządzania w warunkach gospodarki cyfrowej*, [w:] W. Gonciarski (red.), *Poszukiwanie nowych koncepcji i metod zarządzania*, WAT, Warszawa 2008, s. 17-22; R. Orzechowski, *Budowanie wartości przedsiębiorstwa z wykorzystaniem IT*, SGH, Warszawa 2008, s. 26-41.

[17] D. Tapscott, A.D. Williams, *Makrowikinomia. Reset świata i biznesu*, Studio Emka, Warszawa 2011, s. 31.

[18] W. Szpinger, *Wpływ wirtualizacji przedsiębiorstw na modele e-biznesu*, SGH, Warszawa 2008, s. 58.

[19] Szerzej: M. Poniatowska-Jaksch, *Modele biznesu w epoce network economy*, [w:] M. Duczkowska-Piasecka, *Model biznesu w zarządzaniu przedsiębiorstwem*, SGH, Warszawa 2012, s. 89-122.

[20] Szerzej: W. Gonciarski, *Zarządzanie 2.0 – przyczyny powstania i główne założenia*, [w:] Z. Dworzecki, B. Nogalski, *Przełomy w zarządzaniu. Kontekst strategiczny,* Wyd. „Dom Organizatora", Toruń 2011, s. 211-217.

[21] W. Gonciarski, *Management challenges in the era of digital technology*, [w:] C. Sołek (red.), *Management dilemmas in the information technology era*, WAT, Warszawa 2012, s. 14-15.

działalność operacyjna itp.), można też oceniać wykorzystywanie tej technologii z punktu widzenia klientów czy też innych interesariuszy. Interesującą perspektywą oceny jest porównywanie wykorzystania technologii teleinformatycznej w danej organizacji z innymi podmiotami, ocena nowoczesności rozwiązań, czy też ocena efektywności wdrożonych rozwiązań.

W przedstawionej w dalszej części opracowania analizie wyników badań ankietowych wykorzystano spojrzenie na technologię teleinformatyczną ze strony pracowników organizacji. Podstawowym celem badań ankietowych było zidentyfikowanie wykorzystania technologii teleinformatycznej w różnorodnych organizacjach (zarówno w przedsiębiorstwach, jak i organizacjach sektora publicznego oraz społecznego). Celem dodatkowym była ocena zaangażowania badanych organizacji w technologię cyfrową, dokonana przez pracowników tych organizacji. A jednym z następnych celów było skonfrontowanie uzyskanych wyników z danymi statystycznymi dotyczącymi całej Polski oraz wybranych państw europejskich.

Badania zostały przeprowadzone na grupach respondentów będących studentami różnych kierunków studiów oraz słuchaczami Podyplomowych Studiów Zarządzania Zasobami Ludzkimi. Respondentami byli studenci i słuchacze dwóch warszawskich uczelni: publicznej – Wojskowej Akademii Technicznej (ale bez studentów będących żołnierzami) oraz niepublicznej – Almamer Szkoły Wyższej. Ankietę wypełniały wyłącznie osoby pracujące w jakichś organizacjach i przez ten fakt dysponujące wiedzą dotyczącą technologii cyfrowej wykorzystywanej w działaniach organizacyjnych. Dobór próby badawczej nie był przeprowadzony metodą reprezentatywną, ale wydaje się, że zgodnie z sugestią metodologii grupa była odpowiednio heterogeniczna[22], by dokonywać na jej podstawie pewnych uogólnień. Zaletą tej grupy było to, że składała się ona z osób bądź posiadających wyższe wykształcenie, bądź w trakcie jego uzyskiwania. W większości przypadków byli to młodzi ludzie dość dobrze obeznani z technologią teleinformatyczną, choć oczywiście w różnym stopniu z nią zaznajomieni. Dzięki temu uzyskano możliwość – sugerowaną przez Ph. Baumgarda i J. Iberta[23] – różnorodnego spojrzenia na rzeczywistość, a w tym przypadku wykorzystania technologii cyfrowej w różnych polskich organizacjach.

Podstawowymi hipotezami badawczymi weryfikowanymi w trakcie tego badania były przypuszczenia, że:

1. zdecydowana większość polskich organizacji wykorzystuje technologię teleinformatyczną w trakcie typowych działań organizacyjnych;
2. większość polskich organizacji wykorzystuje jednak wyłącznie proste rozwiązania teleinformatyczne;

[22] C. Frannkfort-Nachmias, D. Nachmias, *Metody badawcze w naukach społecznych*, Zysk i S-ka, Poznań 2001, s. 247.

[23] Ph. Baumgard, J. Ibert, *Quelles approches avec quelles donnees?,* [w:] R.-A. Thietard (red.), *Méthodes de recherche en management*, Éditions Dunod, Paris 2007, s. 86.

3. polskie organizacje w zdecydowanie mniejszym stopniu wykorzystują zaawansowane rozwiązania teleinformatyczne, niż ich odpowiedniki z państw Unii Europejskiej.

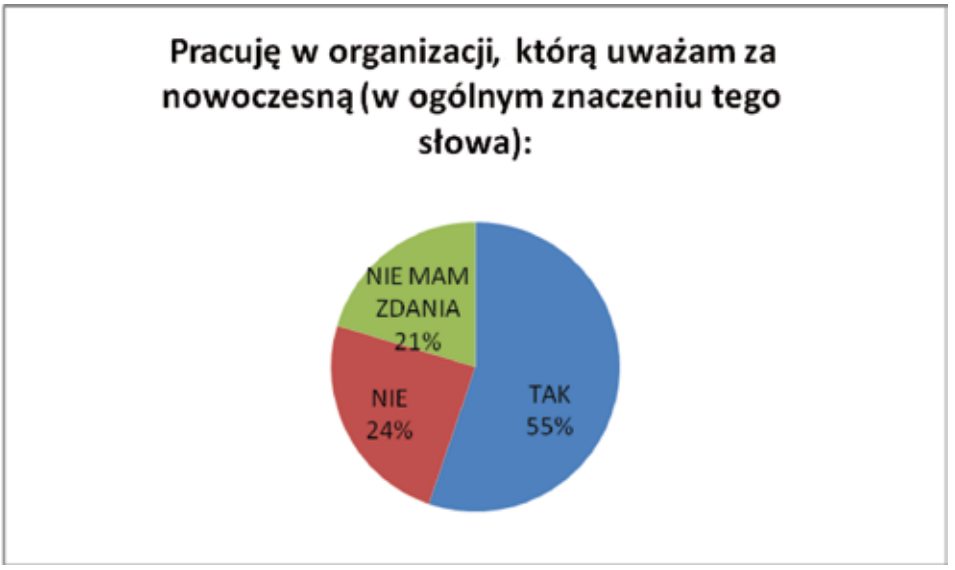
Badania ankietowe przeprowadzone zostały na grupie 201 respondentów, którzy wypełniali ankietę składającą się z 20 pytań zamkniętych. W pojedynczych przypadkach respondenci nie odpowiedzieli na niektóre pytania, co zostało uwzględnione w opisie każdego wykresu. W dalszej części artykułu – ze względu na ograniczenia objętościowe tekstu – przedstawiono analizę zebranych wyników dotyczącą tylko niektórych z zadawanych pytań. Jak wynika z deklaracji respondentów, zdecydowana większość z nich (63%) pracowała w przedsiębiorstwach komercyjnych, 32% było zatrudnionych z sektorze publicznym, a tylko 5% pracowało w sektorze społecznym. Oceniając typ swojej organizacji, 52% respondentów zadeklarowało, że pracuje w organizacji usługowej, 25% – w usługowo-produkcyjnej, 11% – handlowej, a tylko 12% – produkcyjnej. Interesujące są także dane dotyczące pochodzenia kapitału organizacji, w których pracowali respondenci. Większość, bo 58% procent, pracowała w organizacjach utożsamianych z polskim kapitałem, 22% – z kapitałem mieszanym, a 20% – z kapitałem obcym. W tym zakresie dostrzec można pewną nadreprezentatywność kapitału obcego w stosunku do średniej krajowej. Wynika to, jak się wydaje, z faktu, że większość respondentów zatrudniona była w organizacjach umiejscowionych w Warszawie i jej okolicach, gdzie często lokują swoje biznesy przedsiębiorcy zagraniczni.

3. Analiza wyników badań ankietowych

Pierwsze pytanie ankiety miało na celu skłonienie respondentów do oceny nowoczesności organizacji, w której pracują. Parametry tej nowoczesności nie były określone, więc respondenci mieli swobodę w zakresie tej oceny. Wyniki ankiety (wykres 1) są jednak nieco zaskakujące, gdyż aż 21% respondentów nie było w stanie zająć stanowiska w tej kwestii. Natomiast 55% uważało, że pracują w organizacjach nowoczesnych, ale też 24% było skłonnych uznawać swoją organizację za nienowoczesną. Ogólne znaczenie terminu „nowoczesność" może prowadzić do poszukiwania różnych jej parametrów, można jednak założyć, że jednym z ważniejszych branych pod uwagę przez respondentów było wykorzystywanie technologii teleinformatycznej.

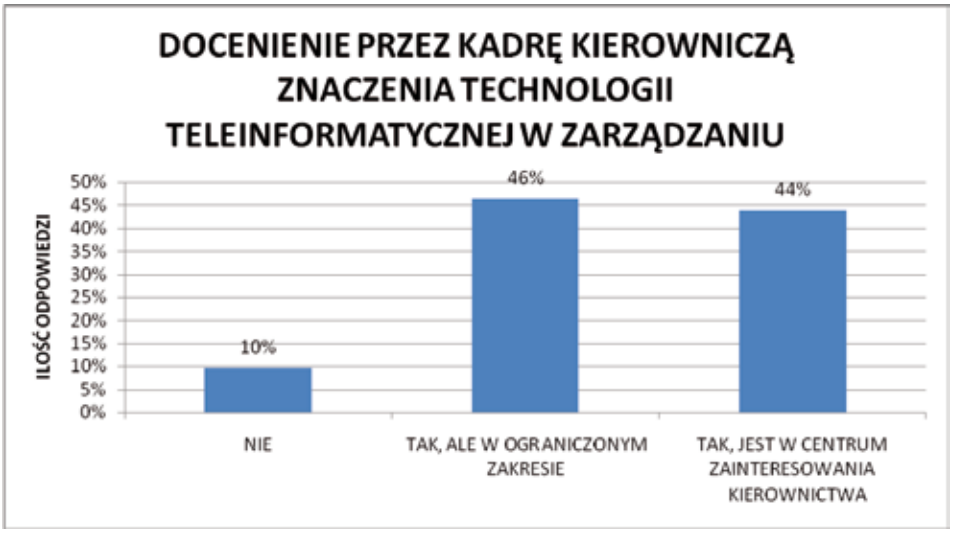
Kolejne pytanie ankiety dotyczyło oceny, jak kadra kierownicza organizacji traktuje technologię teleinformatyczną w zakresie zarządzania. Z zestawienienia przedstawionego na wykresie 2 wynika, że 44% respondentów uważa, iż technologia ta jest w centrum zainteresowania kierownictwa. Jeszcze więcej respondentów, bo 46%, skłania się ku ocenie, że co prawda kadra kierowniczna, chociaż docenia znaczenie technologii teleinfromatycznej, lecz czyni to w ograniczonym zakresie. Jak z tego wynika, tylko w 10% organizacji – w opinii respondentów – technologia ta nie jest odpowiednio doceniana przez kadrę kierowniczą.

Wykres 1. Ocena nowoczesności organizacji (N = 201, w %)



Źródło: opracowanie własne

Wykres 2. Docenianie przez kadrę kierowniczną znaczenia technologii teleinfromatycznej w zarządzaniu (N = 196, w %)

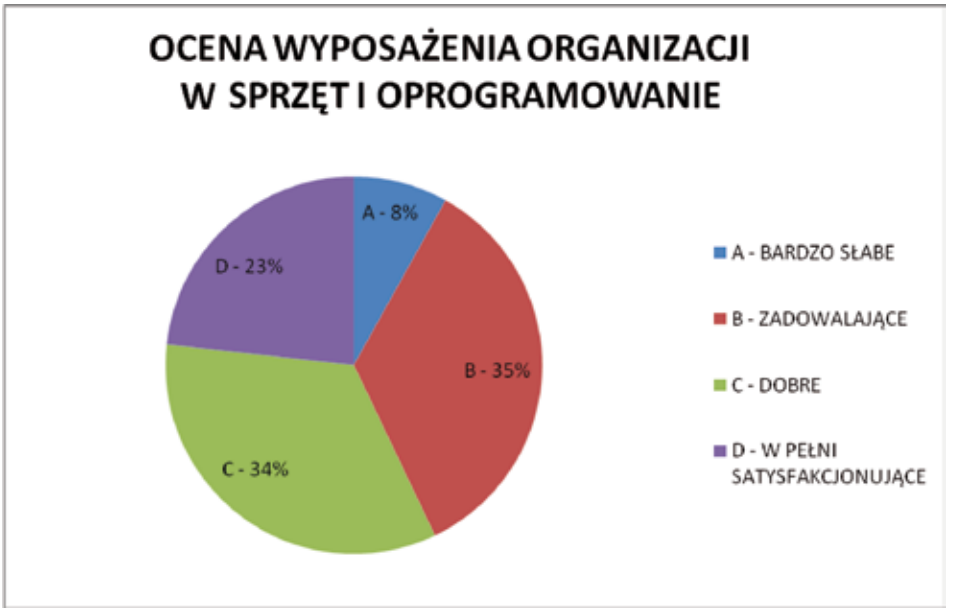


Źródło: opracowanie własne

Uszczegółowiem stanowiska charakteryzowanego w poprzednim pytaniu jest pytanie kolejne dotyczące oceny wyposażenia organizacji w sprzęt i oprogramowanie teleinformatyczne. Jak wynika z analizy wyników zaprezentowanych na wykresie 3,

tylko 23% organizacji dysponuje sprzętem i oprogramowaniem w pełni satysfakcjonującym respondentów. Można na tej podstawie wnioskować, że w tych organizacjach pracownicy nie mają problemu z realizowaniem zadań organizacyjnych za pomocą technologii teleinformatycznej. Co jednak nie oznacza, że we wszystkich organizacjach zaliczanych do tej kategorii technologia ta jest na najwyższym poziomie. W praktyce technologia może być bowiem pochodną realizowanych zadań i zależeć od specyfiki organizacji. Dobrym i zadowalającym wyposażeniem dysponowało 58% organizacji, a zaledwie w 8% organizacji wyposażenie było ocenione jako bardzo słabe.

Wykres 3. Ocena wyposażenia organizacji w sprzęt i oprogramowanie teleinfromatyczne (N = 198, w %)



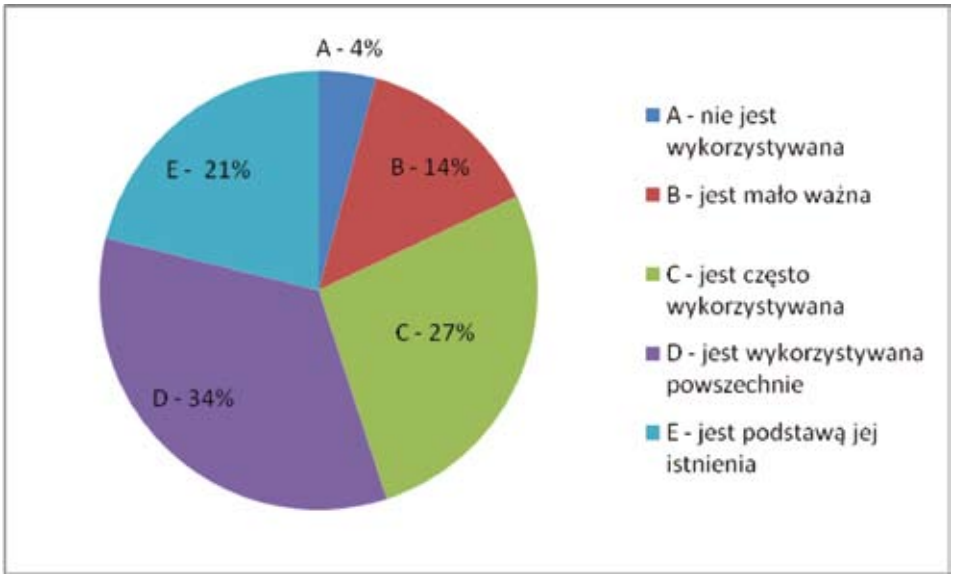
Źródło: opracowanie własne

W następnym pytaniu podjęto próbę określenia znaczenia technologii teleinformatycznej w działaniach organizacyjnych. Wyniki odpowiedzi respondentów zostały przedstawione na wykresie 4. Analiza danych sugeruje, że dla 21% organizacji technologia teleinformatyczna jest podstawą ich istnienia, co oznacza, że możliwość realizowania zadań jest determinowana istnieniem i sprawnością tej technologii. Duże znaczenie technologia teleinformatyczna ma także dla ponad 60% organizacji, w których wykorzystywana jest powszechnie (34%) lub jest często stosowana (27%). W tym kontekście należy zauważyć, że w prawie 20% organizacji technologia ta jest mało ważna (14%) lub nie jest wykorzystywana (4%).

Dość powszechnie uznaje się, że jednym z podstawowych mierników wykorzystania technologii teleinformatycznej jest korzystanie z Internetu w działaniach

organizacyjnych. Problem ten weryfikowany był w pytaniu: *Czy w Państwa organizacji pracownicy mają dostęp do Internetu?* Procentowe zestawienie odpowiedzi respondentów zostało przedstawione na wykresie 5. Wynika z niego, że w połowie organizacji pracownicy dysponują bez ograniczeń możliwością dostępu do Internetu, natomiast w 29% organizacji dostęp ten jest ograniczony wyłącznie do zastosowań służbowych. Należy też zauważyć, że w 14% organizacji dostęp ten jest niezwykle ograniczony, a w 6% organizacji pracownicy nie mają takiego dostępu.

Wykres 4. Ocena wykorzystywania technologii teleinformatycznej w organizacjach (N = 198, w %)

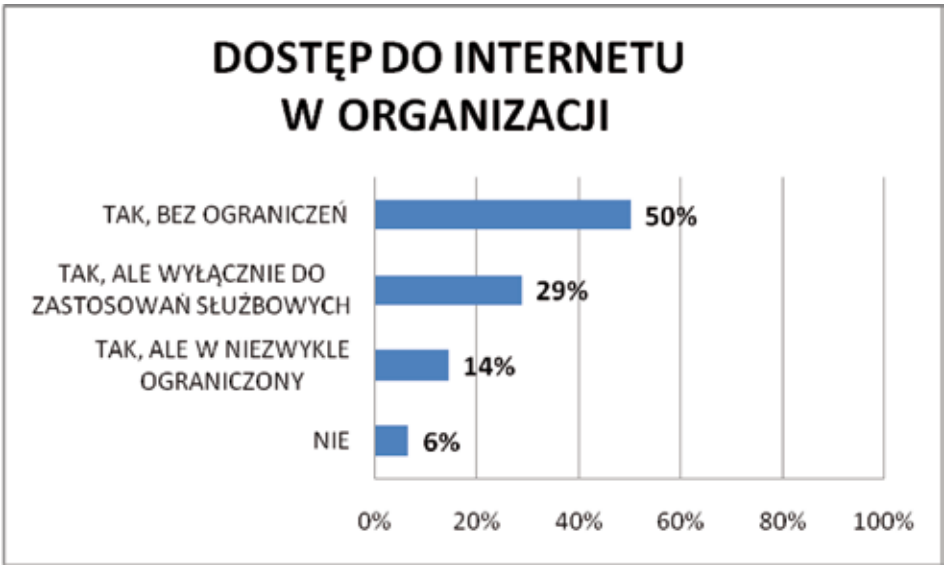


Źródło: opracowanie własne

Dane uzyskane od respondentów tylko w niewielkim zakresie odbiegają od danych prezentowanych przez Główny Urząd Statystyczny. W raporcie „Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2004-2008" czytamy, że w 2008 r. w zakresie dostępu przedsiębiorstw do Internetu przedsiębiorstwa w Polsce osiągnęły poziom średniej unijnej wynoszący 93%. Zauważyć przy tym należy, że dystans dzielący Polskę od państw z czołówki europejskiej (Islandia, Holandia i Finlandia) wynosił wtedy 5-6 punktów procentowych, ale za to zdecydowanie wyprzedzaliśmy takie kraje, jak Rumunia, Bułgaria, Węgry, Łotwa i Cypr, a nieznacznie Maltę i Portugalię. Jednocześnie taki sam jak Polska dostęp do Internetu miały przedsiębiorstwa Grecji i Wielkiej Brytanii[24].

[24] *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2004-2008,* GUS, Warszawa 2010, s. 33.

Wykres 5. Dostęp do Internetu w organizacji (N = 201, w %)



Źródło: opracowanie własne

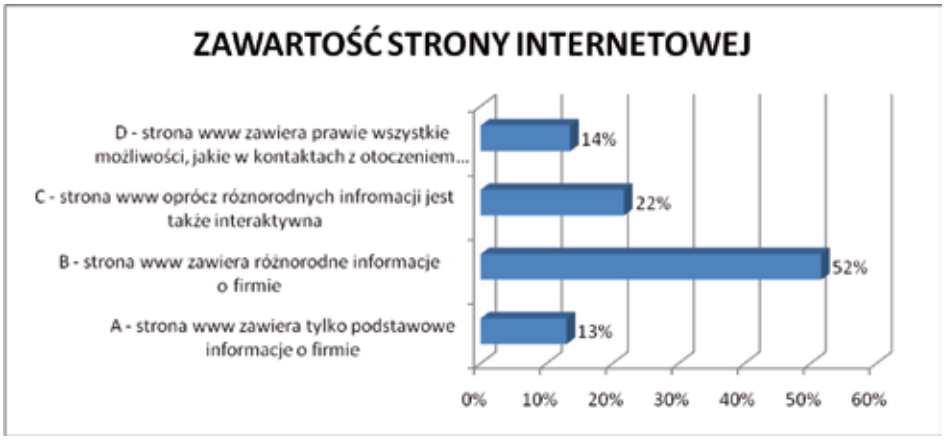
W kolejnych pytaniach respondenci wypowiadali się na temat stron internetowych organizacji, w których pracują. Według ich deklaracji strony takie posiadało 184 podmiotów, czyli 92% z grupy badawczej. Ale istotne jest również to, jakiego rodzaju są to strony, co zostało przedstawione na wykresie 6. Tylko 14% respondentów oceniło, że strony internetowe ich organizacji posiadają prawie wszystkie możliwości, jakie w kontaktach z otoczeniem zewnętrznym oferuje współczesna technologia sieciowa. Większość organizacji (52%) dysponuje stosunkowo prostymi stronami WWW, które zawierają podstawowe informacje o firmie, ale licząca się grupa 22% organizacji posiada strony, które oprócz różnorodnych informacji są także interaktywne. Natomiast strony WWW w 13% organizacji zawierają tylko podstawowe informacje o firmach.

Niezwykle symptomatyczne są odpowiedzi na pytanie dotyczące posiadania przez organizację rozwiniętych informatycznych systemów zarządzania, typu: hurtownie danych, platformy B2B, B2C, MRP, ERP itp. Jak wynika z odpowiedzi respondentów, które zostały przedstawione na wykresie 7, zaledwie 37% organizacji dysponuje takimi zaawansowanymi systemami informatycznymi. Ocenić należy, że świadczy to o słabości polskich organizacji w zakresie wykorzystnia pełnych możliwości współczesnej technologii cyfrowej. W ten sposób dane te korespondują z badaniami przeprowadzonymi przez The Boston Consulting Grup[25], z których wynika, że poziom wykorzystania systemów informatycznych wspomagających zarządzanie zasobami

[25] G. Cimochowski, F. Hutten-Czapski, M. Rał, W. Sass, *Polska Internetowa. Jak Internet dokonuje transformacji polskiej gospodarki*, BCG, Warszawa 2011, s. 17.

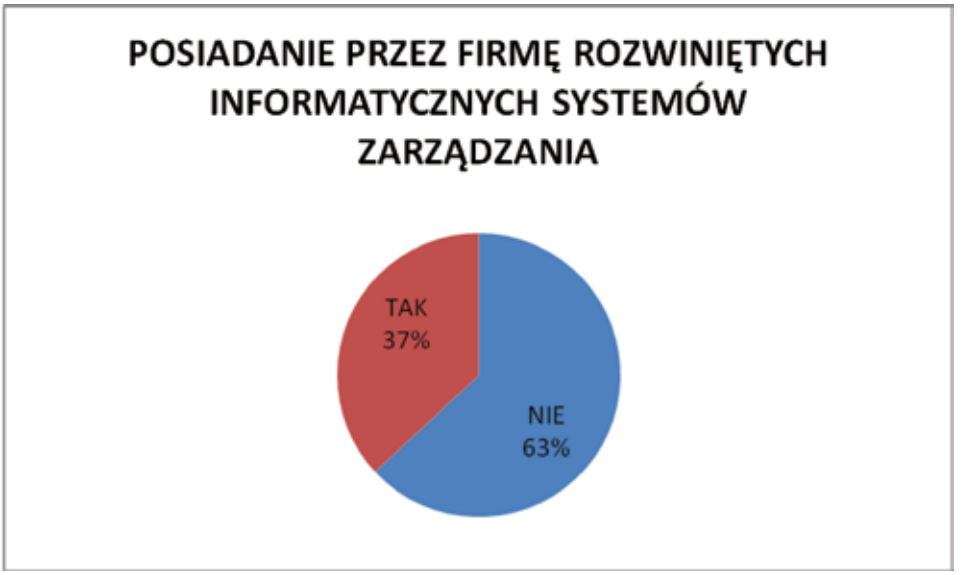
przedsiębiorstwa – tzw. ERP (*Enterprise Resource Planning*) przez małe i średnie firmy sytuuje Polskę na 26. miejscu w rankingu państw Unii Europejskiej.

Wykres 6. Ocena strony internetowej organizacji (N = 184, w %)



Źródło: opracowanie własne

Wykres 7. Posiadanie przez firmę rozwiniętych informatycznych systemów zarządzania (N = 195, w %)

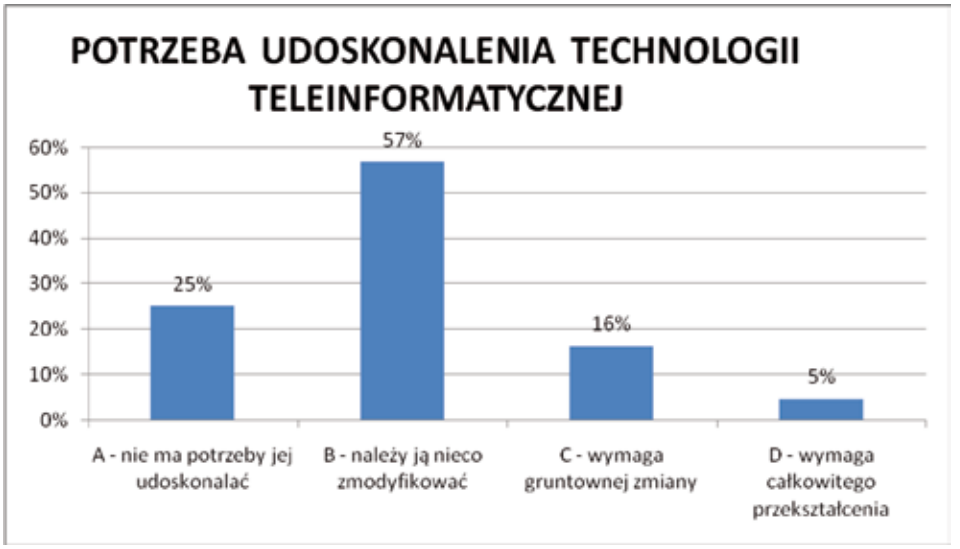


Źródło: opracowanie własne

Równie symptomatyczne są odpowiedzi respondentów na pytanie o potrzebę udoskonalenia i lepszego wykorzystania technologii teleinformatycznej w organizacjach, w których pracują. Tym razem wydaje się jednak, że ocena ta

– przedstawiona na wykresie 8 – dotyczy nie tylko samych organizacji, ale także podejścia do tej problematyki, jakie prezentują respondenci. Zastanawiać bowiem może stanowisko aż 25% respondentów, którzy uważają, że w ich organizacjach nie ma potrzeby doskonalenia systemów teleinformatycznych. Wątpliwości związane są z dość banalną konstatacją, iż ciągły postęp w szeroko rozumianej informatyce prowadzi do konieczności równie ciągłego doskonalenia systemów teleinformatycznych wykorzystywanych przez organizacje. W efekcie trudno sobie nawet wyobrazić taką organizację, która dysponuje tak doskonałą technologią, że niczego w niej nie trzeba zmieniać. W tym kontekście należy też widzieć pozostałe grupy odpowiedzi respondentów. Zdecydowana większość (57%) odpowiada bowiem, że technologię teleinformatyczną stosowaną w ich organizacjach należy nieco zmodyfikować, a 16% – że wymaga ona gruntownej zmiany. Świadczyłoby to o dobrym poziomie zaawansowania rozwiązań teleinformatycznych stosowanych w polskich organizacjach co – jak się wydaje – nie jest w pełni uprawnione. Prowadzi to do wniosku, iż ocena, że technologia teleinformatyczna tylko 5% polskich organizacji wymaga całkowitego przekształcenia jest – jak się wydaje i jak wynika to z innych badań – zdecydowanie zaniżona.

Wykres 8. Ocena potrzeby udoskonalenia technologii teleinformatycznej organizacji (N = 198, w %)



Źródło: opracowanie własne

Podsumowanie

Konieczność stosowania technologii teleinformatycznej w organizacjach funkcjonujących w warunkach drugiej dekady XXI wieku wydaje się bezdyskusyjna.

Nie sposób wręcz wyobrazić sobie nowoczesną organizację, w której technologia teleinformatyczna byłaby niedoceniona. W Polsce technologia ta jest coraz łatwiej dostępna i coraz częściej stosowana, zarówno w celach prywatnych, jak i zawodowych. Co jednak nie oznacza, że z osiągniętego poziomu wdrożonych i wykorzystywanych w praktyce rozwiązań możemy być w pełni zadowoleni. Faktem jest, że stopniowo odrabiamy zaległości w stosunku do państw wysokorozwiniętych. Opóźnienie rozwoju w tym zakresie związane było z problemami natury politycznej i gospodarczej. Przyczyny polityczne to przede wszystkim to, że w czasie, gdy na Zachodzie firmy wdrażały nowoczesne rozwiązania, w Polsce stopnio upadał system komunistyczny i dopiero od początku lat 90. XX wieku odtwarzany jest system demokratyczny i gospodarka rynkowa. Gospodarcze przyczyny opóźnień wiązać należy z problemami transformacji gospodarczej oraz słabością finansową znacznej części polskich organizacji.

Po przystąpieniu Polski do Unii Europejskiej w 2004 roku stopniowo wzmacnia się polska gospodarka, co odzwierciedla się także w upowszechnieniu technologii teleinformatycznej. Jednak jak pokazują różnorodne badania – a w tym to, którego niektóre wyniki przedstawiono w tym artykule – postęp w zakresie stosowania technologii cyfrowej chociaż jest odczuwany, to jednak nie może satysfakcjonować. W organizacjach dominują stosunkowo proste rozwiązania, a wdrażanie nowatorskich technologii napotyka na różnorodne przeszkody, począwszy od ograniczeń finansowych, poprzez bariery prawne, a na barierach mentalnych kończąc. Wydaje się jednak, że wraz z rozwojem cywilizacyjnym oraz naturalną zmianą pokoleniową znaczenie technologii teleinformatycznej będzie się stopniowo zwiększało. W związku z tym wydaje się, że problematyka ta będzie w najbliższym czasie interesującym obszarem badawczym.

THE USE OF DIGITAL TECHNOLOGY IN POLISH ORGANIZATIONS. SOME RESULTS OF QUESTIONNAIRE INVESTIGATIONS

Summary: In 21th century, running organizations needs using digital technology, practically in all of organizational processes. Using advanced IT systems is the proof of novelty (modernity) of management. Their lack in the organization suggests that it merely exists on periphery of modern market. The basic goal of this article is to present the results of survey studies, whose purpose was to research into way how the employees judge the use of IT technology in their organizations. As a consequence the knowledge about using digital technology in polish organizations was obtained.

Keywords: management, organizations, digital technology, the respondents.

LITERATURA

[1] Baumgard Ph., Ibert J., *Quelles approches avec quelles donnees?,* [w:] Thietard R.-A. (red.), *Méthodes de recherche en management*, Ed. Dunod, Paris 2007.
[2] Benkler Y., *Bogactwo sieci*, Wyd. Akademickie i Profesjonalne, Warszawa 2008.
[3] Boulton R.E.S., Libert B.D., Samek S.M., *Odczytując kod wartości*, WIG-Press, Warszawa 2001.

[4] Cameron R., *Historia gospodarcza świata*, KiW, Warszawa 1996.
[5] Castells M., *Społeczeństwo sieci*, PWN, Warszawa 2007.
[6] Cimochowski G., Hutten-Czapski F., Rał M., Sass W., *Polska Internetowa. Jak Internet dokonuje transformacji polskiej gospodarki*, BCG, Warszawa 2011.
[7] Cohen D., *Trois leçons sur la société post-industrielle*, Éditions Seuil, Paris 2006.
[8] Frannkfort-Nachmias C., Nachmias D., *Metody badawcze w naukach społecznych*, Zysk i S-ka, Poznań 2001.
[9] Gleick J., *Informacja – bit, wszechświat, rewolucja*, Znak, Kraków 2012.
[10] Gonciarski W., *Management challenges in the era of digital technology*, [w:] Sołek C. (red.), *Management dilemmas in the information technology era*, WAT, Warszawa 2012.
[11] Gonciarski W., *Specyficzne aspekty zarządzania w warunkach gospodarki cyfrowej*, [w:] Gonciarski W. (red.), *Poszukiwanie nowych koncepcji i metod zarządzania*, WAT, Warszawa 2008.
[12] Gonciarski W., *Zarządzanie 2.0 – przyczyny powstania i główne założenia*, [w:] Dworzecki Z., Nogalski B. (red.), *Przełomy w zarządzaniu. Kontekst strategiczny,* Wyd. „Dom Organizatora", Toruń 2011.
[13] Hamel G., *Ce qui compie vraiment. Le 5 défis pour l'entreprise*, Éditions Eyrolles, Paris 2012.
[14] Jarrosson B., *Vers l'economie 2.0*, Éditions d'Organisation, Paris 2009.
[15] Kociatkiewicz J., *Nowe technologie w organizacjach*, [w:] Kostera M. (red.), *Nowe kierunki w zarządzaniu*, Wyd. Akademickie i Profesjonalne, Warszawa 2008.
[16] Mintzberg H., *Zarządzanie*, Wolters Kluwer Polska, Warszawa 2012.
[17] Mongand J.-P., *Le manager dans la nouvelle économie*, Éditions d'Organisation, Paris 2001.
[18] Normann R., *Przeformułowanie w biznesie*, GWP, Gdańsk 2012.
[19] Orzechowski R., *Budowanie wartości przedsiębiorstwa z wykorzystaniem IT*, SGH, Warszawa 2008.
[20] Poniatowska-Jaksch M., *Modele biznesu w epoce network economy*, [w:] Duczkowska-Piasecka M., *Model biznesu w zarządzaniu przedsiębiorstwem*, SGH, Warszawa 2012.
[21] Rifkin J., *Trzecia rewolucja przemysłowa*, Sonia Draga, Katowice 2012.
[22] *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2004-2008,* GUS, Warszawa 2010.
[23] Tapscott D., *Gospodarka cyfrowa*, Business Press, Warszawa 1998.
[24] Tapscott D., Williams A.D., *Makrowikinomia. Reset świata i biznesu*, Studio Emka, Warszawa 2011.
[25] Thurow L., *Fortuna sprzyja odważnym*, Muza, Warszawa 2007.

MARKETING INTERNETOWY W WYSZUKIWARKACH I SIECIACH INTERNETOWYCH – PRÓBA PORÓWNANIA

KRZYSZTOF MARUDA, KRZYSZTOF SOŁODUCHA

WOJSKOWA AKADEMIA TECHNICZNA
WYDZIAŁ CYBERNETYKI

Wstęp

W tej chwili najpopularniejsze są dwie metody realizacji modelu pull w komunikacji wykorzystującej hipertekstowy model „wielu do wielu" – komunikacja w wyszukiwarkach internetowych oraz komunikacja w sieciach społecznościowych. Artykuł próbuje odpowiedzieć na pytanie, jakie zadania powinny spełniać te metody w sieciowej strategii komunikacji organizacji.

1. Krótka historia sieci

Mimo że wiele osób za datę powstania Internetu uważa koniec XX wieku, jego początki sięgają pierwszej połowy ubiegłego stulecia. Większość źródeł zgadza się co do tego, że za powstanie fundamentów Internetu odpowiada amerykański uczony Vannevar Bush, który był m.in. doradcą do spraw nauki prezydenta Roosvelta w czasie II wojny światowej. Zaprezentował on koncepcję „Memeksa, protoplasty czegoś, co dziś można określić mianem „osobistego asystenta informacyjnego", urządzenia przechowującego książki, osobiste zapiski i notatki użytkownika. Bush przy tym zauważał potrzebę modyfikacji i rozszerzenia tradycyjnych metod indeksowania i wyszukiwania informacji. Zamiast hierarchii klasyfikacyjnej, pozwalającej na przeglądanie kolejnych podkategorii, postulował wprowadzenie mechanizmów wyszukiwania skojarzeniowego, wzorowanych na działaniu mózgu ludzkiego. Pozwalałyby one użytkownikowi przemieszczać się po ścieżkach powiązanych ze sobą fragmentów informacji"[1]. Pomimo że poziom ówczesnej technologii nie pozwalał na wprowadzenie koncepcji Busha w życie, to jednak jego idea automatycznego zarządzania rozrastającymi się przestrzeniami informacyjnymi zainspirowała wiele osób tworzących podwaliny dzisiejszego Internetu.

Rozwijali ją m.in. Joseph Carl Robnett Lickrider (twórca idei globalnej sieci komputerowej – tzw. „galaktycznej sieci"), Douglas Engelbart (implementator

[1] J. Papińska-Kacperek (red.), *Społeczeństwo informacyjne*, PWN, Warszawa 2008, s. 137.

jednego z pierwszych systemów hipertekstowych On Line System – tzw. NLS), czy Ted Nelson (twórca pojęcia „hipertekst").

Lata 60. XX wieku to z kolei intensywne prace nad technicznymi aspektami działania Internetu. „W 1961 Leonard Kleinrock opublikował pierwszy artykuł na temat komunikacji sieciowej wykorzystującej przełączanie pakietów, a w 1964 roku pierwszą książkę na ten temat. (…) W 1964 roku Paul Baran przedstawił koncepcję sieci komputerowej bez wyróżnionych punktów centralnych"[2].

Jednakże powstanie samego Internetu zawdzięcza się Agencji Departamentu Obrony USA (ARPA), organizacji zajmującej się rozwojem i wykorzystaniem nowych technologii do celów wojskowych[3]. Początkowo zasponsorowała ona sieć komputerową łączącą dwa komputery (jeden z System Development Corporation, a drugi z Massachusetts Institute of Technology) za pomocą linii telefonicznej. Po jakimś czasie do tej prowizorycznej sieci dołączono jeszcze jeden komputer, tym razem z samej ARPA.

Za narodziny Internetu uznaje się jednak rok 1969, kiedy to w tej samej agencji uruchomiono sieć ARPANET, tym razem złożoną z 4 komputerów. „Pierwszy węzeł został uruchomiony 2 września na Uniwersytecie Kalifornijskim w Los Angeles (UCLA). 1 października podłączono drugi węzeł w Stanford Research Institute (SRI). Wkrótce potem, bo 29 października, nastąpiła pierwsza próba transmisji danych między tymi węzłami (…). W listopadzie i grudniu do sieci ARPANET dołączono węzły Uniwersytetu Kalifornijskiego w Santa Barbara (USCB) oraz Uniwersytetu Utah"[4]. Od tej pory można mówić o stopniowym rozwoju sieci Internet przejawiającym się głównie w dołączaniu do ARPANET-u kolejnych komputerów, jak również poprawie jakości łącza.

Za kamienie milowe ewolucji ówczesnego Internetu należy uznać m.in. powstanie pierwszych radiowych sieci komputerowych na początku lat 70., stworzenie tzw. protokołu TCP oraz TCP/IP odpowiednio w 1974 i 1983 roku, wprowadzenie systemu Domain Name Server (DNS) służącego do identyfikacji komputerów podłączonych do sieci oraz udostępnienie usług telnet (w 1972 r.) i ftp (w 1973 r.). Stopniowo do sieci ARPANET dołączano również kolejne, np. BITNET, czy CSNET.

W końcu bardzo dynamiczny przyrost użytkowników sieci doprowadził do tego, że ARPA musiała wydzielić w 1983 roku z planowo przeznaczonego do celów wojskowych ARPANET-u sieć typowo komercyjną – MILNET. Wtedy to również w odniesieniu do obydwu sieci zaczęto używać nazwy Internet. Sieć ta stawała się coraz bardziej powszechna i wykorzystywana w celach komercyjnych. Jednakże jej rozkwit miał dopiero nastąpić.

---

[2] Ibidem, s. 139.

[3] http://portalwiedzy.onet.pl/135085arpa,haslo.html

[4] J. Papińska-Kacperek (red.), op. cit., s. 140.

1.1. Ekspansja w latach 90.

Stało się to za sprawą Tima Bernersa-Lee, który w 1990 roku zaprojektował rozproszoną hipertekstową bazę danych dla CERN (centrum badań jądrowych)[5]. Baza ta stała się zaczątkiem dzisiejszego WWW (World Wide Web), a więc bodajże najbardziej rewolucyjnego odkrycia w historii Internetu. Pajęczyna WWW pozwoliła na powiązanie ze sobą poszczególnych dokumentów umieszczonych w sieci za pomocą tzw. łączy hipertekstowych. Rok później Berners-Lee opracował pierwszą przeglądarkę tekstową, dzięki czemu użytkownicy mogli przemieszczać się pomiędzy poszczególnymi dokumentami w sieci WWW. Jednakże wynalezienie WWW samo w sobie nie wywołało kolejnej wielkiej rewolucji w świecie Internetu. Z sieci tej bowiem korzystały najczęściej jedynie środowiska akademickie, naukowcy i informatycy, natomiast zwykli użytkownicy najzwyczajniej nie mieli w niej czego szukać.

Rewolucja taka nastąpiła w 1993 roku, kiedy to dwóch zafascynowanych siecią WWW studentów Uniwersytetu Illinois – Marc Andressen i Eric Bin – opracowało pierwszą graficzną przeglądarkę internetową – Mosaic. To właśnie dzięki niej Internet z narzędzia dla fascynatów powoli stawał się ogólnodostępnym medium. W 1994 przy udziale m.in. Andressena i Bina, a także amerykańskiego inwestora Jima Clarka powstała firma Netscape, która opracowała przeglądarkę Netscape Navigator, czym zdominowała WWW w pierwszych latach jej istnienia. To właśnie dzięki przeglądarkom firmy Netscape nastąpił gigantyczny przyrost użytkowników Internetu. Firma ta stanęła na drodze samemu Microsoftowi, którego zamiarem było utworzenie płatnej infostrady i zdominowanie sieci w taki sposób, jak rynek oprogramowania do komputerów PC. Tymczasem Netscape udostępniało swoją przeglądarkę zupełnie bezpłatnie. Dlatego też w pierwszych latach istnienia Internetu firma ta pozostawiała swojego wielkiego rywala w tyle, jeśli chodzi o liczbę użytkowników przeglądarek.

Niestety, dla Netscape ostatecznym zwycięzcą tej „wojny przeglądarek" okazał się Microsoft, który wykorzystał swoją przewagę wynikającą z praktycznego monopolu w dostarczaniu systemów operacyjnych i dołączył przeglądarkę Internet Explorer 4.0 do systemu operacyjnego Windows 95, co doprowadziło w końcu do upadku Netscape w 1997 roku.

Kolejnym narzędziem, które zrewolucjonizowało WWW, okazały się wyszukiwarki internetowe. W Internecie pojawiało się coraz więcej informacji dostępnych dla coraz większej liczby użytkowników, niemniej jednak w celu znalezienia ich niezbędne było ręczne przeszukiwanie poszczególnych witryn. Dlatego też znalezienie interesującej informacji bardzo często nieomal graniczyło z cudem, a już na pewno zajmowało mnóstwo czasu. Zmieniło się to dzięki dwóm studentom Uniwersytetu Stanford – Jerry'emu Yang i Davidowi Filo, którzy utworzyli pierwszy ręczny katalog stron WWW, znany dzisiaj, jako Yahoo! Twórcy Yahoo! Postanowili

[5] Ibidem, s. 148.

ręcznie pogrupować strony WWW według przeróżnych kategorii, dzięki czemu użytkownicy sieci mogli w łatwiejszy sposób pozyskać poszukiwane informacje. Yahoo! stało się również pierwszą firmą, która zaczęła zarabiać na Internecie, sprzedając na swojej witrynie reklamy bannerowe.

W 1996 roku na horyzoncie pojawiła się firma Excite, która opracowała pierwowzór teraźniejszych wyszukiwarek i stała się poważnym konkurentem dla Yahoo! Obydwie firmy stoczyły pomiędzy sobą kolejną w historii Internetu wojnę o jego użytkowników i jak największe wpływy z reklam, zapominając jednak o swoich początkowych założeniach, a więc ułatwianiu internautom wyszukiwania informacji w sieci.

Wtedy to kolejni studenci z Uniwersytetu Stanford – Larry Page i Sergey Brin, wpadli na, jak się później okazało, rewolucyjny pomysł stworzenia algorytmu wyszukiwania. Poszczególne strony w wyszukiwarce Page'a i Brina były rankowane według liczby odnośników do ich adresów pojawiających się na innych stronach. Przykładowo, w przypadku gdy adres do strony A znajduje się na kilkudziesięciu stronach, to według tego algorytmu jest ona lepiej oceniana niż strona B, do której odniesienia znajdują się na zaledwie kilku stronach. Tak właśnie powstała dobrze znana dzisiaj wyszukiwarka Google. Dzięki niej, po wpisaniu interesującego hasła, w mgnieniu oka można otrzymać poszukiwane informacje, o czym internauci jeszcze 15 lat temu mogli jedynie pomarzyć.

1.2. Od strony technicznej

Czym jest Internet od strony technicznej? Słownik języka polskiego wydawnictwa PWN definiuje ten termin jako „ogólnoświatową sieć komputerową"[6]. Bardzo często używa się również określenia „sieć sieci"[7]. Bardziej rozbudowana definicja przytoczona została w *Wielkim słowniku wyrazów obcych i trudnych*, który określa Internet jako „system wielu sieci komputerowych łączący wiele milionów systemów komputerowych na całym świecie, umożliwiający użytkownikom wymianę różnorodnych informacji, a także np.: wysyłanie i otrzymywanie korespondencji. (…) Dzięki Internetowi możliwe jest błyskawiczne uzyskiwanie aktualnych informacji z całego świata, uczestnictwo w międzynarodowym życiu zawodowym i towarzyskim, przesyłanie danych, a nawet prowadzenie spekulacji na giełdzie"[8].

Wszystkie z powyższych definicji zgodnie przedstawiają Internet jako swego rodzaju sieć komputerową, a więc „zespół oddalonych od siebie komputerów, urządzeń peryferyjnych, a także urządzeń o specjalnych funkcjach, połączonych liniami transmisji danych"[9] o zasięgu międzynarodowym.

---

[6] http://sjp.pwn.pl/szukaj/internet

[7] J. Papińska-Kacperek (red.), op. cit., s. 136.

[8] A. Markowski, R. Pawelec, *Wielki słownik wyrazów obcych i trudnych*, WILGA, Warszawa 2001, s. 335.

[9] http://sjp.pwn.pl/szukaj/sie%C4%87

Elementami Internetu mogą być zarówno mniejsze sieci lokalne (LAN), sieci bardziej rozległe (WAN), jak i pojedyncze jednostki komputerowe. Podłączając się do tej sieci, nasz komputer staje się jednym z jej elementów, posiadającym swój indywidualny adres. Wyróżnia się dwa typy komputerów podłączonych do sieci[10]:

- serwery – komputery udostępniające dokumenty innym komputerom,
- klienci – komputery korzystające z zasobów serwerów.

Struktura Internetu oparta jest o tzw. protokoły internetowe, a więc „algorytmy komunikowania się komputerów – zespoły norm, standardów i oprogramowania, dzięki którym komputery działające w różnych systemach mogą współpracować"[11]. W Internecie używany jest tzw. protokół TCP/IP (Transmission Control Protocol/ Internet Protocol), powstały z połączenia protokołów TCP i IP. Pierwszy z nich odpowiada za przydzielanie poszczególnym elementom sieci unikatowych adresów, natomiast drugi czuwa nad kierowaniem komunikatów do właściwych miejsc. Dzięki protokołom internetowym, dane mogą być przesyłane pomiędzy poszczególnymi elementami Internetu. Na internetowy protokół TCP/IP składają się 4 warstwy[12]:

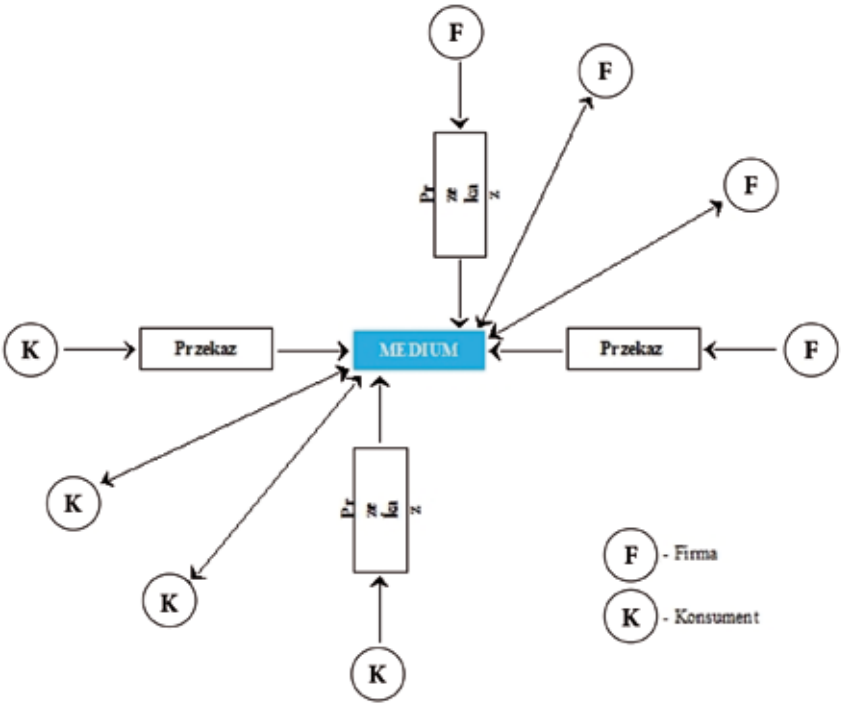
- warstwa aplikacji, zwana też procesową (ang. *process layer*) to poziom, który tłumaczy odbierane dane na postać zrozumiałą dla człowieka (aplikacje – np. przeglądarka internetowa, serwer WWW),
- warstwa sieciowa (warstwa protokołu) – ustala drogę do komputera docelowego (protokół http),
- warstwa transportowa – odpowiada za pewność transmisji, nawiązywanie i zrywanie połączenia pomiędzy poszczególnymi komputerami, a także tłumaczy adres zrozumiały dla ludzi – domenę, na adres zrozumiały dla komputera – IP (protokół DNS),
- warstwa dostępu do sieci (warstwa fizyczna) – odpowiada za transmitowanie danych poprzez fizyczne połączenia (np. kabel) pomiędzy poszczególnymi urządzeniami. Warstwę tę stanowi najczęściej karta sieciowa lub modem (coraz rzadziej).

1.3. Wykorzystanie komercyjne

Internet powstał początkowo jako marzenie o alternatywnym świecie, w którym będzie możliwe porozumiewanie się i funkcjonowanie bez ograniczeń istniejących „w realu". Szybko jednak okazało się, że sukces i powszechność używania tego narzędzia predestynuje go do wykorzystania komercyjnego. Jednym ze sposobów jest tutaj wykorzystanie do celów komunikacji marketingowej. Co więcej, wraz z rozwojem tej dziedziny okazało się, iż to wykorzystanie generuje nowe modele teoretyczne komunikacji marketingowej. Model ten nazwano modelem hipertekstowym.

[10] http://www.mapainternetowa.com/struktura-internetu.html
[11] P. Gilster, *Internet. Przewodnik użytkownika*, WNT, Warszawa 1995, s. 672.
[12] http://www.mapainternetowa.com/struktura-internetu.html

Jego podstawą jest relacja typu „wiele do wielu", w której zróżnicowane formy przekazu umożliwiają zarówno interakcje osobowe, jak i „maszynowe". W porównaniu z pozostałymi modelami zmienia się również rola medium – z łącznika pomiędzy nadawcą a odbiorcą, na „zupełnie nowe środowisko komunikowania o dwóch wymiarach: rzeczywistym i hipermedialnym". W relacje z medium mogą wchodzić zarówno sprzedawcy, jak i nabywcy. Pierwsi z nich, za pomocą różnego rodzaju środków przekazują swój komunikat do medium. Drudzy natomiast mogą być zarówno odbiorcami tegoż komunikatu, jak i nadawcami innych. Wyróżnikiem staje się to, że to nabywcy sami decydują o wyborze komunikatów, które chcą odebrać. W przeciwieństwie np. do reklamy telewizyjnej, gdzie odbiorca nie ma bezpośredniego wpływu na jej emisję (komunikacja typu „push"), w sieci odbiorca może wybrać ten przekaz, który okaże się interesujący z jego perspektywy.



Rys. 1. Model komunikacji marketingowej w hipermedialnym środowisku komputerowym
Źródło: J.W. Wiktor, *Teoretyczne podstawy systemu komunikacji marketingowej*, Akademia Ekonomiczna w Krakowie, 2001

2. Komunikacja marketingowa w wyszukiwarkach internetowych

Formą komunikacji marketingowej rozpowszechnioną za czasów Web 1.0 jest marketing w wyszukiwarkach internetowych, zwany również SEM (*search en-*

gine marketing). Jak podaje J. Reed w swojej publikacji poświęconej marketingowi internetowemu, „marketing w wyszukiwarkach internetowych ma na celu maksymalizację prawdopodobieństwa, że potencjalny klient odnajdzie Cię w Google lub w innej wyszukiwarce"[13]. W Polsce dominacja Google jest całkowita i przekracza 90% udziału w rynku. Oczywiste jest więc to, że przedsiębiorcy poszukują klientów tam, gdzie jest ich najwięcej, dlatego też rynek marketingu w wyszukiwarkach skupia się wokół narzędzi oferowanych przez Google.

Upraszczając zasadę działania największej na świecie wyszukiwarki, opiera się ona na pełnieniu dwóch podstawowych funkcji:

- automatyczne przeszukiwanie zasobów sieci przez tzw. roboty w celu poszukiwania stron internetowych i indeksowania ich w katalogu Google,
- wartościowanie poszczególnych stron poprzez badanie ich trafności w stosunku do poszczególnych słów kluczowych, jak również przydzielanie im odpowiedniego wskaźnika PageRank na podstawie ich popularności wśród użytkowników.

Istotą działań komunikacyjnych związanych z wyszukiwarkami internetowymi jest zapewnienie stronie internetowej jak najwyższych pozycji w wynikach wyszukiwania dla określonych słów kluczowych. Wyodrębnia się trzy główne sposoby na osiągnięcie tego celu[14]:

- optymalizacja w wyszukiwarkach internetowych (tzw. SEO – *search engine optimalization*),
- pozyskiwanie płatnych pozycji,
- pozyskiwanie odnośników przychodzących.

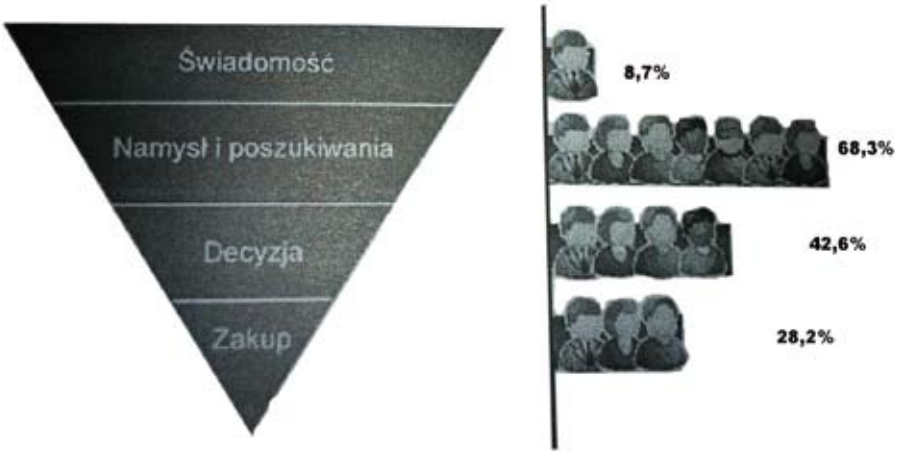
Istnieje wiele metod SEO, a wszystkie je łączy jeden cel – znalezienie się strony na jak najwyższej pozycji w wynikach tzw. wyszukiwania organicznego (nieobejmującego linków sponsorowanych). To właśnie ten rodzaj wyszukiwania jest podstawą działania Google. Po wpisaniu przez internautę odpowiedniego słowa kluczowego, wyszukiwarka wyświetla wiele linków do stron z nim powiązanych. O pozycji poszczególnych stron w wynikach decyduje wskaźnik PageRank. Im wyżej w wynikach pojawi się strona danej firmy, tym większe prawdopodobieństwo, że użytkownik „kliknie" na nią w celu poszukiwania informacji, której poszukuje.

Praktyka dowodzi, że zdecydowanie największą popularnością cieszą się pierwsze trzy witryny wyświetlone w wynikach, z drugiej strony jedynie nieliczni (ok. 10%) decydują się na sprawdzenie wyników spoza pierwszej strony (na każdą ze stron przypada 10 wyników). Konkurencja jest więc ogromna, szczególnie w przypadku najbardziej popularnych słów kluczowych. Dlaczego więc ta forma SEM jest tak bardzo popularna? Po pierwsze, wyniki wyszukiwania organicznego cieszą się zdecydowanie większą popularnością od wyników płatnych wśród samych

[13] J. Reed, *Marketing internetowy. Szybkie łącze z klientami*, Helion, Gliwice 2012, s. 65.
[14] Ibidem.

użytkowników (ok. 75% internautów klika naturalne wyniki wyszukiwania). Po drugie, działania z zakresu SEO nie są związane z ponoszeniem praktycznie żadnych nakładów finansowych, o ile przedsiębiorstwo dysponuje zasobami będącymi w stanie wykonać odpowiednie działania.

W przeciwieństwie do optymalizacji w wyszukiwarkach internetowych, pozyskiwanie płatnych pozycji wiąże się z poniesieniem sporych nakładów finansowych. Nie jest ono również tak skuteczne jak SEO, gdyż według statystyk sponsorowane wyniki wyszukiwania są otwierane przez około 25% internautów (choć ostatnio te proporcje korzystnie się zmieniają). Ponadto, przy odpowiednim przeprowadzeniu kampanii, reklama tego typu nie musi być wcale dużym wydatkiem dla organizacji. Istotą płatnej reklamy w wyszukiwarkach jest umieszczenie za odpowiednią opłatą tzw. linków sponsorowanych pojawiających się w płatnych wynikach wyszukiwania dla odpowiednich słów kluczowych, które mogą zostać wskazane przez firmę. Kampanie takie są rozliczanie według systemu CPC (*cost per click* – koszt za kliknięcie), dlatego też podmiot ponosi koszt tylko wówczas, gdy użytkownik „kliknie" w jego reklamę.



Rys. 2. Lejek sprzedaży
Źródło: T. Frontczak, *Marketing internetowy w wyszukiwarkach,* Helion, Gliwice 2006, s. 67

Trzeci z elementów marketingu w wyszukiwarkach – pozyskiwanie odnośników przychodzących jest bardzo często zaliczane do działań z zakresu SEO (takie połączenie ma również miejsce w dalszej części niniejszej publikacji). Algorytm Google opiera się na wartości wskaźnika PageRank przypisanej do poszczególnych stron internetowych. Jest on naliczany m.in. na podstawie liczby odwołań do danej strony występujących w sieci, jak również jakości stron, na których odwołania te występują. Dlatego też działania takie, jak pozyskanie linków ze stron cieszących się dużym wskaźnikiem PageRank mają pozytywny wpływ na wartość tegoż parametru w przypadku strony docelowej.

Wyszukiwarki są narzędziem, za pomocą którego internauci głównie poszukują informacji oraz dokonują porównania znalezionych ofert, na bazie czego podejmują decyzję zakupową. Ilustruje to raport przeprowadzony przez Enquiro, którego wyniki zaprezentowano na rysunku 2, a który przedstawia znaczenie wyszukiwarek w poszczególnych etapach – tzw. „lejka sprzedaży".

Okazuje się, że wyszukiwarki internetowe najczęściej używane są na etapie poszukiwania przez internautów informacji o produkcie. Aż 68,3% badanych twierdzi, że korzysta w tym celu z wyszukiwarek internetowych. Ponadto wyszukiwarki są wykorzystywane stosunkowo często na etapie podejmowania decyzji (korzysta z nich 42,6% badanych). Rzadziej używa się ich w fazie samego zakupu, a minimalnie na etapie budowania świadomości.

Istnieje wiele metod pozyskiwania linków zewnętrznych, a ich skuteczność jest różna. Najpopularniejsze z nich to:

1. Katalogowanie QIWeb

Metoda ta polega na indeksowaniu linków do danej strony internetowej w specjalnych katalogach skupiających strony z danego zakresu tematycznego, które można podzielić na bezpłatne oraz płatne. Zaletą katalogów bezpłatnych jest to, że firma nie ponosi kosztów indeksowania, jednakże wyszukiwarki internetowe przypisują im coraz mniejszą wagę ze względu na częste nadużywanie w ich przypadku metod spamerskich. Z racji konieczności opłaty za indeksowanie, katalogi płatne nie są tak ogólnodostępne, dlatego też uważane są za bardziej wartościowe, a wyszukiwarki przypisują im większą wagę niż ich bezpłatnym odpowiednikom. Firma prowadząca proces katalogowania powinna pamiętać, aby wybierać tylko katalogi z jak największym wskaźnikiem PageRank. Ponadto zbyt duża aktywność w tym zakresie może zostać potraktowana przez wyszukiwarki jako działania spamerskie, a co za tym idzie – doprowadzić do usunięcia danej strony z wyników wyszukiwania.

2. Pressel Pages

„To strony stworzone w celu umożliwiania innym wstawienia artykułów z linkami do ich stron"[15], które powstały na skutek słabnącej skuteczności katalogów, zwłaszcza tych bezpłatnych. Na stronach tego rodzaju, poświęconych określonej tematyce, poszczególne jednostki mogą publikować treść (np. w postaci artykułów), a przy okazji zamieszczać linki do swoich stron. Podobnie jak w przypadku katalogów, należy jednak mieć na uwadze to, że zbyt duża aktywność na stronach tego typu, szczególnie nie powiązanych tematycznie z działalnością firmy, może zostać zakwalifikowana przez wyszukiwarki do działań spamerskich.

3. Pingowanie

„Pingowanie w znaczeniu SEO opiera się na protokole RPC (*Remote Procedure Call*). Protokół ten umożliwia zdalne wywołanie procedur. Klient wysyła żądanie wykonania metody weblogUpdates.ping do serwera pingującego, podając mu od-

[15] http://www.lexy.com.pl/blog/presell-pages.html

powiednie parametry, a następnie dostaje odpowiedź z wynikiem działania funkcji"[16]. Innymi słowy, celem pingowania jest przyspieszenie procesu indeksowania nowych podstron przez roboty wyszukiwarek, poprzez przesłanie swego rodzaju „zlecenia" ich przeszukania.

4. Posiadanie „Zaplecza"

Mianem tym określa się różnego rodzaju miejsca w sieci, gdzie można publikować wybrane treści związane z pozycjonowaną stroną. Szczególnie dobrze spisują się w tej roli media społecznościowe. Przykładami zaplecza są firmowe blogi, strony informacyjne, fora, strony, czy profile w mediach społecznościowych, na których można publikować treść z odnośnikami do danej strony.

5. Płatne linki

Metoda polegająca na płaceniu innym serwisom, najlepiej z jak największym wskaźnikiem PageRank za zamieszczenie na nich linków do pozycjonowanej strony. Linki takie są wykupywane na określony czas, łączy się to więc z ponoszeniem stałych kosztów ich utrzymania.

Przy każdej z powyższych metod najważniejszą zasadą jest zachowanie umiaru. Nadużywanie tych sposobów jest niezgodne z zasadami etyki pozycjonowania, a poza tym może doprowadzić do czasowego lub – w skrajnych przypadkach – stałego usunięcia danej strony z wyników wyszukiwania, co jest odwrotnością celu zamierzonego przy pozycjonowaniu.

3. Komunikacja marketingowa w mediach społecznościowych

Rozwój mediów, jak również częste negatywne doświadczenia z przeszłości sprawiają, że dla dzisiejszego konsumenta tradycyjna reklama i opinia przedsiębiorcy staje się stopniowo coraz mniejszym autorytetem, kosztem opinii o produkcie bądź marce, której źródłem są inni członkowie informacyjnej społeczności. Dzisiaj, kiedy konsument chce kupić produkt czy też usługę, przed podjęciem decyzji zakupowej bardzo często sprawdza, jakie zdanie na ten temat mają inni konsumenci. Mogą to być np. osoby, które wcześniej zdecydowały się na zakup, czy też mają innego rodzaju doświadczenia związane z danym produktem/usługą. Informacja o produkcie pochodząca od innych użytkowników jest uważana za bardziej cenną od tej, której źródłem jest producent. Media społecznościowe stają się w tym przypadku ważnym kanałem wymiany informacji pomiędzy konsumentami. „(...) już nie wystarczy mówić, teraz trzeba rozmawiać, nie wystarczy ogłaszać, teraz trzeba słuchać, nie wystarczy pokazywać, teraz trzeba angażować, a na dodatek przejmować się każdym z osobna (zamiast mówić do wszystkich naraz) i podlegać weryfikacji 24 h na dobę"[17].

[16] http://reklama24online.pl/?p=140

[17] J. Namedyński, *Zanim organizacja zacznie rozmawiać*, [w:] Social media manual, 2010, s. 24-26, http://www.slideshare.net/IRCenter/social-media-manual-2010

Wyróżnia się następujące formy komunikacji marketingowej realizowanej w modelu społecznościowym:

- wykorzystanie portali społecznościowych, takich jak Facebook lub Nasza Klasa,
- marketing na blogach,
- udostępnianie społeczne takich treści, jak filmy, zdjęcia, podcasty lub pliki,
- marketing na forach internetowych.

Najczęściej realizowane są one dzisiaj w ramach tzw. strategii ROPO – *Research Online, Purchase Offline* – będących odpowiedziami na zmieniające się zachowania konsumentów na rynku.

4. Porównanie zadań komunikacji w wyszukiwarkach i mediach społecznościowych

Kluczem do porównania komunikacji marketingowej w social media oraz wyszukiwarkach jest rola, jaką odgrywają te formy w procesie sprzedaży zobrazowanym przez tzw. „lejek sprzedaży" zaprezentowany wyżej.

Zgodnie z tymi informacjami, internauci wykorzystują wyszukiwarki najczęściej w fazie poszukiwań i namysłu oraz, w drugiej kolejności, do podejmowania decyzji. Ujmując to w inny sposób, osoba zainteresowana konkretnym produktem wykorzystuje wyszukiwarki do znalezienia konkretnych ofert. Następnie porównuje ze sobą znalezione wyniki, klikając w poszczególne linki (najczęściej nie wykraczając poza pierwszą stronę) w celu pozyskania większej ilości informacji o poszczególnych ofertach czy produktach oraz zestawiania ich ze sobą. Na podstawie tego porównania stosunkowo często podejmowana jest decyzja użytkownika np. co do wyboru konkretnego produktu lub usługi. Dlatego też dobre pozycjonowanie oferty w wyszukiwarkach internetowych ma najczęściej spore przełożenie na konkretną aktywność zakupową konsumentów, przy czym nie musi być to zakup za pośrednictwem Internetu, bowiem spora grupa internautów sprawdza informacje w Internecie po to, żeby później zakupić produkt w zwykłym sklepie. Wyszukiwarki raczej słabo spisują się jako narzędzie budowania świadomości marki.

W przypadku mediów społecznościowych sytuacja przedstawia się niemal całkowicie odwrotnie. Dzięki swojej specyfice są one świetnym sposobem na budowanie świadomości marki. Dzięki prowadzeniu dialogu ze społecznością firma może przekazywać jej swoje wartości, tożsamość marki, czy ludzki wymiar organizacji, w celu budowania odpowiednich relacji i budowania zaufania. Jest to więc proces wysoce długoterminowy nienastawiony na uzyskanie bezpośrednich korzyści sprzedażowych w krótkim czasie.

Oczywiście internauci szukają również np. na forach internetowych informacji potrzebnych do dokonania decyzji zakupowych, jednak nie występuje tu

zjawisko przełożenia na konkretne decyzje zakupowe w takim stopniu, w jakim to ma miejsce w wyszukiwarkach. Ponadto, jak wcześniej wspomniano, reklama sprzedażowa w mediach społecznościowych jest najczęściej odbierana negatywnie przez internautów, ponieważ nie tego rodzaju informacji poszukują oni w serwisach.

Podsumowanie

Rozwój technik komunikacji przy wykorzystaniu modelu hipermedialnego spowodował znaczne zmiany sposobów zachowania się konsumentów na rynku. Ponad 60% decyzji zakupowych odbywa się dzisiaj w modelu ROPON i ROPOF (*Research Online Purchase Online i Research Online Purchase Offline*). Techniki komunikacji za pomocą wyszukiwarek internetowych i sieci społecznościowych zaczynają odgrywać coraz większą rolę w stategiach ROPON i ROPOF. Ze względu na swoje własności wykorzystywane są jednak w odmienny sposób: komunikacja w wyszukiwarkach ma ułatwiać gromadzenie informacji w sieci, a komunikacja w sieciach społecznościowych – budowanie świadomości marki, czyli wprowadzenie jej do tzw. zbioru marek znanych. Artykuł pokazuje, jakie argumenty kryją się za takim określeniem celów stawianych przed komunikacją realizowaną za pośrednictwem wyszukiwarek internetowych i sieci społecznościowych.

SEARCH ENGINE MARKETING OR SOCIAL MEDIA MARKETING – GOALS AND TASKS – COMPARISION ATTEMPT

Summary: Rapid development of internet as a tool of communication has huge influence on consumers market behaviour. More than 60% of purchase decisions are made at the moment in ROPON or ROPOF model (Research Online Purchase Online i Research Online Purchase Offline). It is a big challenge for marketing communication theory to develop proper tools and methods which would be able to face this new situation. Search engine marketing or social media marketing there are classical web merketing tools which should play a different role in na coplex on line communication strategy of an contemporary organisation. The text is an attempt to answer this question – what should be a special task for SEM (search engine marketing) and SMM (social media marketing) tools in current web communication strategy of an organisation.

Keywords: search engine marketing, social media marketing, marketing communication, marketing strategy, research online purchase online model, research online purchase offline model.

LITERATURA

[1] Berners Lee T., Hendler J., Lassila O., *Sieć semantyczna*, „Świat nauki", nr 7/2001.

[2] Bickerton P., Bickerton M., Pardesi U., *Marketing w Internecie. Jak najlepiej wykorzystać sieć w sprzedaży produktów i usług?,* Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2006.

[3] Dębski Ł., *Jak umiejętnie wykorzystać serwisy społecznościowe do rozwoju naszego biznesu?*, [w:] Social media manual, 2010, http://www.slideshare.net/IRCenter/social-media-manual-2010
[4] Evans L., *Social media marketing*, Helion, Gliwice 2011.
[5] Gilster P., *Internet. Przewodnik użytkownika*, WNT, Warszawa 1995.
[6] Frontczak T., *Marketing internetowy w wyszukiwarkach*, Helion, Gliwice 2006.
[7] Gąsiewski M., *Przewodnik SEO-SEM, czyli jak promować stronę małej firmy w Internecie*, http://www.ittechnology.us
[8] Joel M., *Sześć pikseli oddalenia. Zarabiaj dzięki sieci Web 2.0*, Helion, Gliwice 2010.
[9] Jopek J., *Promocje i konkursy na Facebooku*, www.aplikacjakonkusowa.pl
[10] Kaznowski D., *Nowy marketing*, VFP Communications, Warszawa 2008.
[11] Kotler P., Kartajaya H., Setiawan I., *Marketing 3.0*, MT Biznes Sp. Z o.o., Warszawa 2010.
[12] Markowski A., Pawelec R., *Wielki słownik wyrazów obcych i trudnych*, WILGA, Warszawa 2001.
[13] Mullen J., Daniels D., *Godzina dziennie z e-mail marketingiem*, Helion, Gliwice 2010.
[14] Namedyński J., *Zanim organizacja zacznie rozmawiać*, [w:] Social media manual, 2010, http://www.slideshare.net/IRCenter/social-media-manual-2010
[15] Niezgoda M., Świątkiewicz-Mośny M., Wagner A. (red.), *com.unikowanie w zmieniającym się społeczeństwie*, Nomos, Kraków 2010.
[16] Nowacki R., *Reklama*, Difin, Warszawa 2006.
[17] Papińska-Kacperek J. (red.), *Społeczeństwo informacyjne*, PWN, Warszawa 2008.
[18] Podlaski A., *Marketing społecznościowy. Tajniki skutecznej promocji w social media*, Helion, Gliwice 2011.
[19] *Podręcznik startowy optymalizacji pod kątem wyszukiwarki Google*, praca zbiorowa, Google 2008.
[20] Reed J., *Marketing internetowy. Szybkie łącze z klientami*, Helion, Gliwice 2012.
[21] Scott D.M., *Nowe zasady marketingu i PR*, Wolters Kluver business, Warszawa 2009.
[22] Treadaway Ch., Smith M., *Godzina dziennie z Facebook marketingiem*, Helion, Gliwice 2011.
[23] Wiktor J.W., *Teoretyczne podstawy systemu komunikacji marketingowej*, Akademia Ekonomiczna w Krakowie, Kraków 2001.