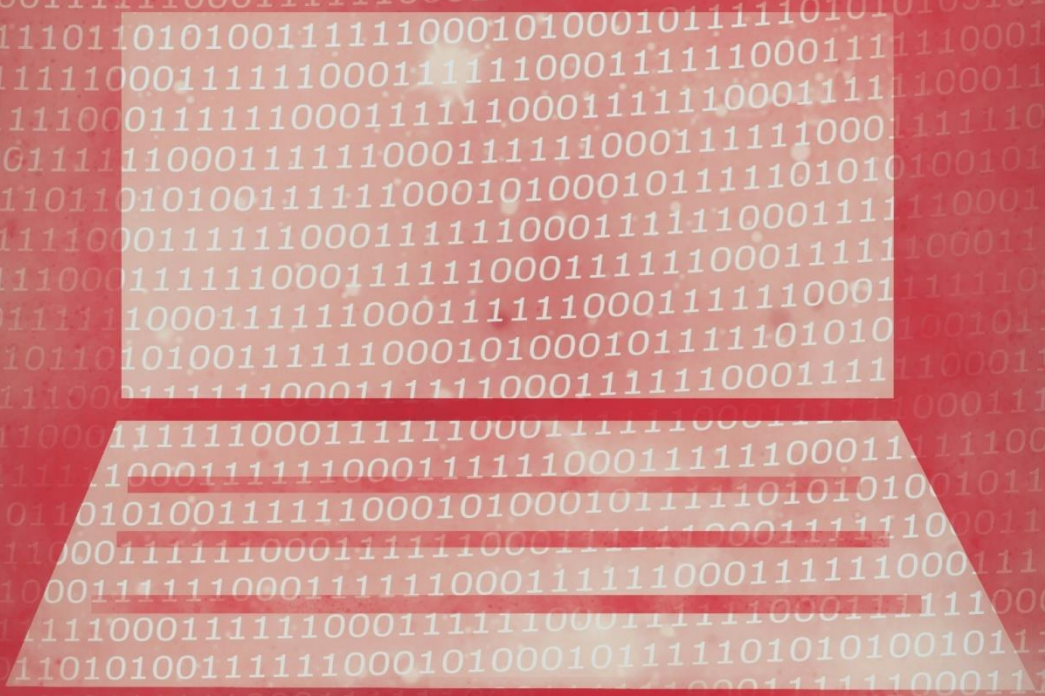
Fundacja Rozwoju Przedsiębiorczości w Suwałkach

Czy inwestować

w umiejętności informatyczne pracowników?



Suwałki 2013

Czy inwestować w umiejętności informatyczne pracowników?

Publikacja powstała w ramach autorskiego projektu Fundacji Rozwoju Przedsiębiorczości w Suwałkach pod nazwą „Akademia Cyfrowa" realizowanego na terenie województwa podlaskiego i warmińsko-mazurskiego od 15 października do 15 grudnia 2013 roku w ramach zadania publicznego „Upowszechnianie korzystania z Internetu i rozwój kompetencji cyfrowych" współfinansowanego ze środków Skarbu Państwa – Ministra Administracji i Cyfryzacji oraz środków własnych.

Autorzy

Agnieszka Bógdał-Brzezińska, Henryk Bednarczyk, Tomasz Frankowski, Ewa Serafin, Maciej Perkowski, Wojciech Zoń, Marzena Mażewska, Karol Wasilewski

Recenzja

Tomasz Kupidura

Projekt okładki

Joanna Maria Wierzbińska

Redakcja

Karol Wasilewski

Korekta i skład komputerowy

Karol Wasilewski, Justyna Harasim

Wsparcie merytoryczne

Jacek Anuszkiewicz, Barbara Bąkowska, Henryk Bednarczyk, Teresa Bogacka, Krzysztof Bondyra, Cezary Cieślukowski, Ilona Hofman, Monika Kraszewska, Krzysztof Krukowski, Andrzej Lewkowicz, Krzysztof Mika, Cezary Miżejewski, Dorota Ilona Niewińska, Maciej Perkowski, Anna Poźniak, Elżbieta Rosiak, Bożenna Rutkowska, Andrzej Wasilewski, Jerzy Wawruk, Marek Wierzbiński

ISBN 978-83-926117-1-4

Spis treści

Wstęp

E-book „Czy inwestować w umiejętności informatyczne pracowników?" jest kolejną publikacją, która została przygotowana przez Fundację Rozwoju Przedsiębiorczości w Suwałkach w ramach autorskiego projektu „Akademia Cyfrowa" i powstała dzięki finansowaniu ze środków Ministerstwa Administracji i Cyfryzacji. Choć w jego tytule postawione jest pytanie, w rzeczywistości autorzy przekonują, że szybko zmieniająca się cyfrowa rzeczywistość wymaga od przedsiębiorców inwestycji w kapitał ludzki, a od administracji różnych szczebli udoskonalania dotychczasowych i poszukiwania nowych form współpracy z sektorem prywatnym, w tym z organizacjami pozarządowymi.

Ta niezwykła potrzeba efektu synergii zaakcentowana jest gronem autorów, wśród których znajdują się przedstawiciele świata nauki. Warto zauważyć, że część z nich daje doskonały przykład łączenia teorii i praktyki. Niektórzy posiadają bowiem wieloletnie doświadczenie we współpracy z przedsiębiorcami, administracją rządową i samorządową oraz działają na rzecz rozwoju przedsiębiorczości i wprowadzania nowoczesnych rozwiązań technologicznych. Stwarza to nowe możliwości rozwoju polskiej gospodarki i zwiększa konkurencyjność rodzimych firm na rynku międzynarodowym.

Nasze przekonania w tej kwestii wynikają z wieloletniego doświadczenia w działaniach na rzecz rozwoju przedsiębiorczości. W ciągu dwudziestu lat istnienia Fundacja zrealizowała szereg projektów, których odbiorcami byli i są przedsiębiorcy. Do godnych zauważenia inicjatyw, przy których współpracowaliśmy również z zaangażowanymi w przygotowanie niniejszego e-booka autorami, można zaliczyć projekty realizowane w ramach instrumentów inżynierii finansowej takie jak: Fundusz Rozwoju Przedsiębiorczości (realizowany ze środków Banku Światowego w ramach projektu TOR#10 na zlecenie Ministerstwa Pracy i Polityki Społecznej oraz środków Unii Europejskiej na zlecenie Polskiej Agencji Rozwoju Przedsiębiorczości) i Podlaski Fundusz Przedsiębiorczości (realizowany ze środków Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007 - 2013). Warto wspomnieć również projekty „Przedsiębiorczość w sieci - Internet szansą na wzrost konkurencyjności", którego liderem był Instytut Technologii Eksploatacji – Państwowy Instytut Badawczy w Radomiu (realizowany w ramach Inicjatywy Wspólnotowej EQUAL) i „Akademia Augustowska" (realizowany na zlecenie British American Tobacco Polska S.A. w ramach społecznej odpowiedzialności w biznesie).

Fundacja Rozwoju Przedsiębiorczości od wielu lat współpracuje z ośrodkami na terenie całej Polski zrzeszonymi w Krajowym Systemie Usług, który działa przy Polskiej Agencji Rozwoju Przedsiębiorczości. Fundacja należała również do Związku Pracodawców Suwalskie Stowarzyszenie Pracodawców – członka Polskiej Konfederacji Pracodawców Prywatnych Lewiatan. Stowarzyszenie to zakończyło swoją misję w roku 2011. Jest także członkiem Stowarzyszenia Organizatorów Ośrodków Innowacji i Przedsiębiorczości w Polsce oraz Polskiego Związku Funduszy Pożyczkowych. Ze stowarzyszeniem tym współpracujemy od początku realizacji naszych celów statutowych. Pragnę zauważyć, że duży wpływ na kierunki naszego rozwoju miał zmarły w 2012 r. dr hab. Krzysztof B. Matusiak, wieloletni działacz i prezes stowarzyszenia. Fundacja jest również członkiem założycielem Polskiego Związku Funduszy Pożyczkowych. Prestiż związany z uczestnictwem w tych inicjatywach obliguje nas do stosowania wysokich standardów w działaniu i podejmowania coraz nowszych inicjatyw na rzecz przedsiębiorców i rozwoju przedsiębiorczości zarówno na terenie miasta Suwałk, województwa Podlaskiego, jak i całego kraju. Stąd też celem niniejszej publikacji jest podjęcie najważniejszych zagadnień związanych ze zmianami, które zachodzą w obrębie cyberprzestrzeni i rodzą konsekwencje dla wszystkich przedsiębiorców.

Zaproponowana tematyka nie wyczerpuje oczywiście w pełni kwestii związanych z wyzwaniami, jakie stawia przed przedsiębiorcami cyfrowy świat. W e-booku autorzy starali się jednak poruszyć najbardziej istotne ich zdaniem zagadnienia, które mogą zwrócić uwagę przedsiębiorców stanowiących docelową grupę odbiorców niniejszej publikacji na pewne zagadnienia związane z działaniem w cyberprzestrzeni. Przedstawili im nie tylko korzyści, jakie mogą wynikać ze świadomego funkcjonowania w jej obrębie, ale także zaprezentowali zagrożenia, które w konsekwencji mogą utrudniać im działanie, i sposoby ich neutralizowania. Wierzę, że wnikliwa lektura niniejszego e-booka będzie cennym źródłem informacji, która pozwoli przedsiębiorcom lepiej przystosować się do warunków funkcjonowania w dynamicznie zmieniającym się, cyfrowym środowisku i będzie pomocna w odpowiednim projektowaniu działań w przyszłości.

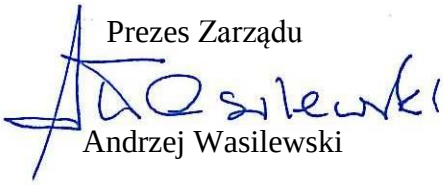
Na koniec chciałbym podziękować całemu zespołowi realizującemu projekt „Akademia Cyfrowa”. Przede wszystkim Markowi Wierzbińskiemu – dyrektorowi Ośrodka Transferu Wiedzy i Innowacji, który przygotował koncepcję projektu, Dorocie Ilonie Niewińskiej, która koordynowała całe przedsięwzięcia oraz Alicji Łabacz , która pomogła we właściwym zaksięgowaniu i rozliczeniu finalnym całego projektu. Na uznanie zasługuje także Joanna Maria Wierzbińska, która opracowała szatę graficzną, nawiązując do pierwszej

publikacji „Drzwi do świata cyfrowego” wydanej również w ramach projektu „Akademia Cyfrowa”. Szczególne ukłony należą się Justynie Harasim, która wsparła nas w przygotowaniu e-booków do właściwego internetowego wyglądu.

Wydanie publikacji, która skierowana jest przede wszystkim do przedsiębiorców, stanowi także doskonałą okazję do podziękowania tym, którzy wspierali Fundację w realizacji naszego projektu. Szczególne podziękowania należą się zatem Jerzemu Bartnikowi, prezesowi Zarządu Związku Rzemiosła Polskiego, Andrzejowi Lewkowiczowi, starszemu Cechu, i Bożennie Rutkowskiej, dyrektor biura Rzemieślników i Przedsiębiorców w Suwałkach. Dzięki okazanej pomocy mogliśmy dotrzeć do szerokiego grona przedsiębiorców z terenu województwa podlaskiego. Podziękowania kieruję także na ręce Anny Poźniak, kanclerz Państwowej Wyższej Szkoły Zawodowej im. prof. Edwarda F. Szczepanika w Suwałkach, dzięki której uprzejmości mogliśmy we właściwych warunkach przedstawić rezultaty naszego projektu. Na końcu zaś pragnę serdecznie podziękować autorom poszczególnych artykułów za chęć współpracy przy tworzeniu tej publikacji i współpracy z Fundacją Rozwoju Przedsiębiorczości w Suwałkach.

Zapraszam więc do e-lektury naszej e-publikacji, zapewniając że nie będzie to czas stracony, a treść zawarta w poszczególnych artykułach wesprze Państwa w codziennym rozwoju osobistym i własnej firmy dla pożytku ogółu.

Prezes Zarządu



Andrzej Wasilewski

Inwestycje oparte na wiedzy a społeczeństwo informacyjne w Polsce

Agnieszka Bógdał-Brzezińska[1]

1. Wiedza, innowacja, technologie – narzędzia postępu i nowoczesności

Rewolucja technologiczna, pogłębiająca się od połowy XX wieku, uległa gwałtownemu przyspieszeniu na przełomie lat 80. i 90. Duży wpływ wywarły na to przemiany międzynarodowe, które związane były z rozpadem porządku międzynarodowego opartego na rywalizacji między USA i ZSRR. Rywalizacja ta miała nie tylko wymiar polityczny i ideologiczny, lecz istniała również w sferze technologii, a to za przyczyną zimnowojennego wyścigu zbrojeń. Sprzyjał on tworzeniu nowych rozwiązań technicznych, które pierwotnie zaprojektowane dla celów wojskowych, stawały się po pewnym czasie narzędziami postępu społecznego. Tak było w przypadku Internetu, którego pierwociny – system połączeń zw. Arpanet – powstał w latach 60. XX wieku, by już w latach 70. przeobrazić się w środek służący komunikacji między ośrodkami naukowymi, a z czasem – w medium służące masowym użytkownikom komputerów. Rewolucja technologiczna wprowadziła społeczeństwa i gospodarki państw w erę informacyjną. Społeczeństwa zyskały nowe możliwości pozyskiwania informacji i gromadzenia wiedzy, stając się potencjalnie o wiele bardziej wyedukowane, a w konsekwencji – emancypując się spod kontroli i kurateli władz publicznych. Proces permanentnej edukacji, czyli kształcenie ustawiczne, stał się nowym modelem zachowań jednostki jako obywatela i pracownika.

Inwestowanie w kompetencje i umiejętności zaczęło przynosić korzyści różnego rodzaju: zwiększyło elastyczności i mobilność osób fizycznych na rynku pracy, sprzyjało kumulowaniu przez nie doświadczenia zawodowego z różnych branż i obszarów gospodarki, zapobiegało marginalizacji i wykluczeniu na rynku pracy, sprzyjając utrzymaniu ciągłości zatrudnienia i pogłębiając poczucie sprawczości oraz kompetencji zawodowej. Walor współczesnego pracownika – jego przygotowanie do wykonywania różnorodnych czynności zawodowych – sytuuje go pomiędzy tradycyjnym dostawcą usług a typowym robotnikiem. Zmiana w strukturach zatrudnienia, związana z wiedzą jako czynnikiem produkcji, prowadzi

[1] Pracownik naukowy Instytutu Stosunków Międzynarodowych Uniwersytetu Warszawskiego. Specjalizuje się m. in. w problemach globalnego społeczeństwa informacyjnego i bezpieczeństwa teleinformatycznego.

do powstania nowych klas społecznych, w tym klasy zwanej *information workers*, których miarodajnym przykładem są współcześnie pracownicy świadczący usługi *offsourcingu* i *offshoringu*, jak też nowe elity wiedzy zwane kognitariatem, wśród nich menedżerowie zarządzania informacją i naukowcy.

Współczesne kraje zaawansowane technologicznie muszą skłaniać rodzimy biznes do inwestycji w wiedzę i kompetencje pracownicze, by utrwalić przekonanie przedsiębiorców, że kapitał ludzki staje się równie ważny jak kapitał finansowy i potencjał logistyczny. W ten sposób tworzy się system innowacyjności firm, czyli całokształt działań od powstania projektu do jego realizacji w obrębie przedsiębiorstwa, oparty na kształceniu kadr jako „najważniejszym długoterminowym czynniku rozwoju społeczeństwa ukierunkowanego na wiedzę i konkurencję”[2]. Kolejnym kluczowym elementem budowania potencjału firm w warunkach nowoczesnej gospodarki opartej na wiedzy (KBE) jest efektywne zarządzanie zasobami wiedzowymi w połączeniu z inwestowaniem w technologie informacyjno-komunikacyjne (ICT). Niezbędne wydaje się w tym miejscu przybliżenie fundamentalnych pojęć związanych z KBE, tj. danych, wiedzy i informacji. Triada ta przyjmuje postać piramidy logicznej. Jej podstawę stanowią dane: rozproszone, zdezintegrowane, cząstkowe, nieuporządkowane, wybiórcze, zróżnicowane w chaosie, w masie. Są liczne, ale cechuje je mała wartość wyjaśniająca. Gromadzenie danych nie przesądza jeszcze w żadnej mierze o potencjale czy konkurencyjności podmiotów gospodarczych. Wartości rynkowej nabiera już natomiast informacja – zestawiona z danych w usystematyzowany, całościowy sposób, skonstruowana wg obranego przez firmę kryterium użyteczności. Informacja jest selektywna, ale nie chaotyczna. Wyjaśnia wybrany problem, nie przedstawiając go w szerszym kontekście przestrzennym ani czasowym. Wreszcie na szczycie omawianej piramidy logicznej sytuuje się wiedza, którą A. Toffler określił jako podstawę wszelkich systemów ekonomicznych, a wszelkie przedsięwzięcia gospodarcze zależą od jej społecznie nagromadzonych zasobów. Wiedza jest substytutem wszelkich czynników produkcji, dlatego jak słusznie zauważa amerykański badacz M. Castells: „informacja stanowi surowiec: są technologie działające na informację, tak jak istnieją technologie działające na węgiel”[3]. Nowoczesne przedsiębiorstwo staje więc przed koniecznością inwestowania w wiedzę i innowacje jako podstawowy zasób produkcyjny, podczas gdy kapitał ludzki staje się fundamentalnym kapitałem inwestycyjnym.

[2] W. Grudzewski, I.Hejduk, *E-learnig w systemie gospodarki opartej na wiedzy w Polsce,* www.e-edukacja.net/_referaty/4_e-edukacja.pdf, s. 5 (02. 12. 2013).
[3] M. Castells, *Społeczeństwo sieci,* Warszawa 2010, s. 150.

Jednak nie każdy zbiór danych jest informacją, a nie każdy zbiór informacji wiedzą. W sensie ekonomicznym wartość posiada jedynie wiedza, która ma zastosowanie praktyczne. W społeczeństwie informacyjnym na skalę masową wykorzystuje się zarządzanie wiedzą, innowacje i know-how[4]. Warto jednak nadmienić przy tej okazji, iż każdy podmiot gospodarczy akumuluje wiedzę posiadaną przez pracowników, ta zaś jest trudna do sformalizowania, gdyż opiera się na rutynie zawodowej. W teorii zarządzania wiedzą zwraca się więc uwagę na dwa fundamentalne wymiary wiedzy: wiedzę ukrytą i wiedzę jawną. Wiedza jawna istnieje w postaci dokumentów, aktów urzędowych, procedur postępowania przyjętych w przedsiębiorstwie czy organizacji. Jest ważna, gdyż uwspólnia sposób postrzegania zadań i celów firmy przez pracowników, klientów czy konkurencję. Jest wizytówką firmy i swoistym komunikatem adresowanym do otoczenia zewnętrznego. Z kolei wiedza ukryta stanowi niematerialny kapitał każdego przedsiębiorstwa. Składa się na nią katalog rzeczywistych umiejętności posiadanych przez kadry, nabytych w toku długotrwałego procesu pracy. O ile wiedza jawna poddaje się łatwo procesowi archiwizacji i jest w konsekwencji łatwa do odtworzenia, o tyle wiedza ukryta postaje niewymierna, ale stanowi o przewadze i konkurencyjności danego podmiotu gospodarczego poprzez specyficzność kompetencji jego kadr. Inicjując proces świadomego zarządzania wiedzą w przedsiębiorstwie, uwzględnić należy cztery rodzaje przeobrażeń, jakie zachodzą w obrębie obu rodzajów zasobów wiedzowych: socjalizację, czyli przekazywanie wiedzy ukrytej, transformację wiedzy ukrytej w wiedzę jawną, integrację, czyli łączenie ze sobą różnych form wiedzy jawnej, i internalizację, czyli indywidualne przyswajanie wiedzy jawnej przez każdego pracownika, a następnie jej przekształcanie w wiedzę ukrytą. Należy również upowszechniać i utrwalać przekonanie, że menadżering wiedzy w pojedynczej firmie – podobnie jak innowacje – spełnia funkcję ogólnospołeczną.

Istnieje bowiem silna korelacja pomiędzy poziomem i stopniem upowszechniania wiedzy w danym społeczeństwie a poziomem jego rozwoju i zamożności. Dlatego badacze zarządzania wiedzą podkreślają, że drogą do stabilnej i wydajnej ekonomiki każdego kraju jest inwestowanie w kompetencje informatyczne obywateli/pracowników. O sukcesie firmy decyduje coraz częściej skuteczna współpraca z nauką. Przechodzenie informacji w zasób produkcyjny prowadzi do nasilania się integracji badań naukowych i procesów produkcyjnych. Istotnym elementem staje się infrastruktura naukowa dzięki której rozwija się

[4] M. Fic, *Gospodarka oparta na wiedzy*, www.mikroekonomia.net/system/publication_files/1040/original/9.pdf?1315235637 (02. 12. 2013).

światowy rynek produktów nauki, co umożliwia swobodny przepływ wiedzy i technologii między poszczególnymi krajami. Tym samym zwiększa się udział państwa w produkcji wiedzy, zwłaszcza że badania podstawowe nie powinny pozostawać domeną organizacji prywatnych ze względu na: wysokie koszty z tym związane i bardzo długi ewentualny okres zwrotu; ograniczone możliwości zachowania tajemnicy naukowej pozwalającej uzyskać zwrot ponoszonych nakładów; konieczność wyrównania przez państwo luki informacyjnej jako warunku niedopuszczenia do monopolizacji rynku, w tym zwłaszcza w świetle polityki prowadzonej przez państwo w stosunku do małych i średnich przedsiębiorstw. Sukcesem wielostronnego dialogu między biznesem, sektorem nauki a państwem ma być docelowo utrwalenie modelu społeczeństwa informacyjnego, czyli społeczeństwa, w którym informacja staje się towarem, rozwijają się usługi związane z jej przechowywaniem, przesyłaniem i wytwarzaniem. Informacja staje się substytutem surowców, siły roboczej i innych zasobów”[5].

2. Społeczeństwo informacyjne – fenomen XXI wieku

„Pojęcie społeczeństwa informacyjnego oznacza formację społeczno-gospodarczą, w której produktywne wykorzystanie zasobu, jakim jest informacja, oraz intensywna pod względem wiedzy produkcja odgrywają dominującą rolę”[6]. Już w 1998 r. OECD uznała, iż gospodarka jutra będzie, w dużym stopniu, „gospodarką informacyjną”, a społeczeństwo będzie w rosnącym stopniu „społeczeństwem informacyjnym”. Oznaczało to, że informacja będzie stanowiła dużą część wartości dodanej większości dóbr i usług, a działalności informacyjnie intensywne będą, w rosnącym stopniu, charakteryzować gospodarstwa domowe i obywateli. Termin ten definiowano także jako „nowy system społeczeństwa kształtujący się w krajach o wysokim stopniu rozwoju technologicznego, gdzie zarządzanie informacją, jej jakość, szybkość przepływu są zasadniczymi czynnikami konkurencyjności zarówno w przemyśle, jak i w usługach, a stopień rozwoju wymaga stosowania nowych technik gromadzenia, przetwarzania, przekazywania i użytkowania informacji”[7]. Rozwój technologiczny, a przede wszystkim rozwój technologii informacyjnych i telekomunikacyjnych, odgrywa w tym procesie również ważną rolę. Występuje tutaj swoiste

[5] M. Fic, *Gospodarka oparta na wiedzy*, op.cit., s. 97.
[6] H. Kubicek, *Möglichkeiten und Gefahren der „Informationsgesellschaft*, www.fgtk.informatik.uni-bremen.de/ig/WS99-00/studienbrief/index.html (02. 12. 2013).
[7] Ministerstwo Łączności, *ePolska – Strategia rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006*, Warszawa 2001, s. 62.

sprzężenie, gdyż globalizacja prowadzi do rozwoju nowych środków technologicznych, a jednocześnie ich rozwój powoduje szybką ewolucje procesów globalizacyjnych.

Badacze społeczeństwa informacyjnego dostrzegają od lat 90. XX wieku pogłębiające się konsekwencje transformacji handlu i finansów pod wpływem rozwoju ICT. Do pozytywnych aspektów zaliczają: globalizację rynków, wzrost efektywności zarządzania strategicznego gospodarką w skali makro i wzrost efektywności procesów produkcji (skrócenie ich trwania i obniżenie kosztów). Ponadto wymienia się konsekwentnie postęp i optymalizację usług transportowych i bankowych, zmniejszenie luki cywilizacyjnej między regionami wiejskimi i zurbanizowanymi. Podkreśla się, że technologie dają również szanse szybkiego rozwoju krajom zacofanym gospodarczo. Wśród zagrożeń wymienia się natomiast: nadmierną wrażliwość i uzależnienie gospodarek od systemów informatycznych czy zwiększoną wrażliwość międzynarodowego systemu bankowego[8]. Wydaje się, że w kontekście ostatniego światowego kryzysu finansowego diagnoza ta okazała się niezwykle trafna.

3. Polska na drodze do społeczeństwa informacyjnego i gospodarki opartej na wiedzy – strategie rozwoju

Polska polityka informatyzacji i cyfryzacji zaczęła rozwijać się po przełomie ustrojowym 1989 r. W następstwie transformacji systemu społecznego i gospodarczego kolejne rządy podejmowały próby stworzenia fundamentów dla polskiego społeczeństwa informacyjnego i gospodarki opartej na wiedzy. Widać było jednak, że brak wiedzy eksperckiej ogranicza inicjatywy polityczne. W latach 90. zarysowała się współpraca władz ze środowiskiem informatyków. Pierwszy raport pt. „Propozycja strategii rozwoju informatyki i jej zastosowań w Rzeczpospolitej Polskiej" powstał w 1991 r. na zamówienie złożone przez ministra gospodarki Leszka Balcerowicza. Podkreślano w nim przewodnią rolę rządu w nadzorowaniu przeobrażeń, które powinny uwzględnić zauważalny w świecie, rosnący wpływ informatyki na gospodarkę. Zastosowanie informatyki w przemyśle i usługach Polski jako nowoczesnego państwa zostało określone jako kluczowe[9]. Uznano, że nadzór rządu nad tworzeniem polityki informatyzacji wynika z jego uprawnień konstytucyjnych tak

[8] Por.: L.W. Zacher, *Społeczeństwo informacyjne: aspekty techniczne, społeczne i polityczne*, Warszawa 1992.
[9] *Propozycja strategii rozwoju informatyki i jej zastosowań w Rzeczpospolitej Polskiej*, www.kbn.icm.edu.pl/pub/info/dep/pti.html; Raport został stworzony przez niemal dziesięciu ekspertów, o nazwiskach znanych Czytelnikowi badającemu problematykę ICT w Polsce. PTI wydało raport jako publikację zbiorową, odstępując do niej prawa autorskie podmiotowi zamawiającemu tj. Ministerstwu Gospodarki (02. 12. 2013).

w odniesieniu do sektora ekonomii, jak i bezpieczeństwa narodowego. Podkreślano, że prace nad całościową strategią informatyzacji państwa winny uwzględniać także zastosowania informatyki w sferze publicznej. Postulowano ponadto wprowadzenie koncesji na usługi informatyczne, by „współdziałanie różnych publicznych systemów informatycznych w Polsce nie było utrudnione, a inwestycje informatyczne okazały się efektywne”[10]. Aktywizacja lobbingu informatyków pogłębiła się w latach następnych, dlatego może być uznana za przejaw demokratyzacji życia branżowego, a także integracji wokół wspólnych celów zawodowych. W styczniu 1993 r. rozpoczęła działalność Polska Izba Informatyki i Telekomunikacji (PIIT) na podstawie ustawy o izbach gospodarczych z 30 maja 1989 r., gdzie zapisano, iż izba „jest uprawniona do wyrażania opinii i dokonywania ocen wdrażania i funkcjonowania przepisów prawnych dotyczących prowadzenia działalności gospodarczej”[11]. Środowisko to było już skupione w bardziej elitarnej skali w Polskim Towarzystwie Informatycznym, które prowadziło działalność ekspercką i naukowo-badawczą od 1981 r.[12], jednak nie działało dotąd jako lobby branżowe. W grudniu 1994 r. w Poznaniu rozpoczął się 1. Kongres Informatyki Polskiej. Postanowiono odnieść się do Raportu Bangemanna, a także zamanifestować wolę współtworzenia z rządem polityki informatyzacji Polski. Obrady odbywały się pod patronatem premiera Waldemara Pawlaka, co miało zachęcić do integracji środowisk zainteresowanych polityką ICT. Wzięli w nich udział liczni (350) parlamentarzyści i eksperci rządowi oraz przedstawiciele środowisk akademickich, użytkowników zastosowań informatyki, firmy szkoleniowe oraz firmy produkujące i sprzedające produkty informatyczne. Przesłanie płynące z powyższych, wczesnych wypowiedzi środowiska eksperckiego brzmiało wyraźnie: potrzebne jest partnerstwo prywatno-publiczne, rozwijane pod patronatem władz państwowych. W latach następnych inicjatywa związana z organizacją społeczeństwa informacyjnego skupiła się w rękach rządu i parlamentu RP. Już w lipcu 2000 r. Sejm podjął uchwałę, w której wzywał rząd do przedstawienia strategii rozwojowej na najbliższe lata. Owocem szybkich prac nad projektem był dokument pt. „Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce”. Jego rezultaty wykorzystano w opracowaniu strategii ePolska 2001-2006, przyjętej przez Radę

[10] Ibidem.

[11] Najwyższą władzą PIIT jest Walne Zgromadzenie Członków, zbierające się co najmniej raz w roku w pierwszym kwartale. Wybieralnymi organami Izby jest Rada Izby oraz Komisja Rewizyjna, Sąd Koleżeński i Komisja Arbitrażowa z Sądem Polubownym do spraw domen. Bieżącym zarządzaniem Izbą zajmuje się Zarząd Izby; za: www.piit.org.pl/piit/index.jsp?place=Menu01&news_cat_id=7&layout=3&reset_offset=1&lang=pl (02. 12. 2013).

[12] Por. Strona PTI, www.pti.org.pl/index.php (02. 12. 2013).

Ministrów 11 września 2001 r.[13] Wśród strategicznych celów na kolejne 10 lat wymieniano: umożliwienie osobom dorosłym zdobycia kwalifikacji niezbędnych do stosowania technik społeczeństwa informacyjnego; przygotowanie komputerowej bazy danych o modułowych programach szkolenia zawodowego i rynku usług szkoleniowych, zwiększenie udziału regionalnych i ogólnopolskich organizacji samorządowych w edukacji z zakresu ICT[14]. W dziale pt. „Praca zawodowa w gospodarce opartej na wiedzy" wskazywano na potrzeby: podniesienia poziomu informatyzacji firm małego i średniego biznesu; upowszechnienia telepracy jako sposobu walki z bezrobociem i wykluczeniem społecznym; zwiększenia liczby wykształconych informatyków i programistów jako bazowej kadry, niezbędnej w większości polskich firm[15]. Zapowiadano powszechny udział społeczny w gospodarce opartej na wiedzy, w tym walkę z wykluczeniem cyfrowym na rynku pracy mieszkańców regionów wiejskich oraz osób niepełnosprawnych. Pojawiła się pierwsza rządowa próba zdefiniowania „gospodarki elektronicznej" i sposobów jej upowszechniania[16]. Brakowało jednak odniesień do integracji Polski z UE, jak również do globalizacji gospodarki światowej.

Dalszy postęp w zakresie budowania strategii polskiego SI i KBE przyniosła w 2003 r. strategia „Strategia informatyzacji Rzeczpospolitej Polskiej. e-Polska 2004-2006"[17], gdzie znalazły się odwołania do strategii eEurope 2002 i eEurope 2005 w kontekście zbliżającej się akcesji Polski do UE. Wśród celów działania rządu znalazły się promocja handlu

[13] www.kbn.icm.edu.pl/cele/epolska.html; W dziale poświęconym inwestowaniu w wiedzę i umiejętności czytamy m.in.: „Doświadczenia krajów wysoko rozwiniętych pod względem ekonomicznym dowodzą, że sukcesy gospodarcze, wysoka pozycja tych krajów na rynku światowym i konkurencyjność gospodarek w coraz większym stopniu zależą od poziomu wiedzy społeczeństwa oraz umiejętności tworzenia i wykorzystywania wiedzy technicznej, ekonomicznej, informatycznej etc. w procesach gospodarczych. Gospodarki krajów wysoko rozwiniętych oparte są o rosnące zasoby ludzi dobrze wykształconych, posiadających umiejętności twórcze i innowacyjne, co jest niezbędnym warunkiem postępu technicznego, gospodarczego i społecznego", s. 21 (02. 12. 2013).

[14] www.kbn.icm.edu.pl/cele/epolska.html, s. 22 (02. 12. 2013).

[15] Por.: „Cele: Rozwój zawodów z zakresu zastosowań technologii informacyjnych i komunikacyjnych, Wykorzystanie technologii informacyjnych dla wzrostu poziomu zatrudnienia i ograniczenia bezrobocia.
Planowane działania: Identyfikacja oraz promocja zawodów i specjalności z zakresu zastosowań technologii informacyjnych i komunikacyjnych występujących na rynku pracy, Sporządzenie prognozy zapotrzebowania na zawody i specjalności z zakresu zastosowań technologii informacyjnych i komunikacyjnych do 2010 r.; Stworzenie formalno-prawnych podstaw rozwoju telepracy, Tworzenie nowych miejsc pracy w sektorze usług z zakresu zastosowań technologii informacyjnych i komunikacyjnych", ibidem, s. 26.

[16] W tym celu utworzono Międzyresortowy Zespół ds. Handlu Metodami Elektronicznymi, który przedstawił „Program prac legislacyjnych Rządu w zakresie handlu metodami elektronicznymi na lata 2000-2002". Program ten przyjęty został jako program rządowy na posiedzeniu Rady Ministrów w dniu 11 lipca 2000 r. Ponadto Prezes Rady Ministrów zarządzeniem nr 89 z dnia 30 listopada 2000 r., powołał Międzyresortowy Zespół ds. Gospodarki Elektronicznej, który zajął się koordynowaniem prac legislacyjnych dotyczących gospodarki elektronicznej (s. 34)

[17] Komitet Badań Naukowych, *Strategia informatyzacji Rzeczpospolitej Polskiej. e-Polska*, Warszawa 2003, www.archiwum-ukie.polskawue.gov.pl/HLP/files.nsf/0/79D0526B49538AE3C125721F00335DF3/$file/strategia_informatyzacji_polsk_-_epolska.pdf (02. 12. 2013).

elektronicznego i stworzenie bezpiecznej infrastruktury prawnej dla jego rozwoju. Pisano również o konieczności „zwiększenia informatycznego przygotowania zawodowego" i „zwiększeniu usług telekomunikacyjnych", wskazując, że większość z tych zadań ma być zrealizowana do 2004 r. włącznie.

W 2005 r., w kolejnym dokumencie rządowym pt. „Strategia kierunkowa rozwoju informatyzacji Polski do roku 2013 oraz perspektywiczna prognoza transformacji społeczeństwa informacyjnego do roku 2020", problemy inwestowania w wiedzę i technologie przez polski biznes były widoczne jeszcze wyraźniej[18]. Priorytetem określono rozwój gospodarki elektronicznej, zapewnienie dostępu do usług elektronicznych oraz uproszczenie procedur urzędowej obsługi obywateli i przedsiębiorców[19].

Z kolei w rządowym dokumencie pt. „Kierunki zwiększania innowacyjności gospodarki na lata 2007-2013" czytamy, iż „jedynie budowanie przewagi konkurencyjnej opartej na wiedzy i innowacjach może zagwarantować trwały rozwój w perspektywie krótko i średnioterminowej. Dlatego też należy skupić się na budowaniu w Polsce gospodarki opartej na wiedzy, będącej częścią globalnej gospodarki opartej na wiedzy w wymiarze Unii Europejskiej i świata"[20]. Podobnie myślą eksperci. A. Kukliński wymienia kilka warunków niezbędnego dostosowania Polski do KBE, wśród nich: dynamiczny wzrost firm wykorzystujących inwestycje w wiedzę, stworzenie warunków prawnych, propagandowych i społecznych, stanowiących podatny grunt dla zainteresowania się przedsiębiorców udziałem w tworzeniu KBE, dobrze zaprojektowany system edukacji, w tym kształcenia pracowników, rolę sektora nauki jako partnera dla biznesu[21]. Z kolei R. Żelazny dostrzega konieczność promocji wśród Polaków idei KBE jako podstawowy warunek jej rozwoju, uznając za wtórne takie działania jak przygotowanie strategii krajowej i regionalnej KBE czy dostosowanie infrastruktury prawnej[22]. Oceniając skutki integracji z UE, stwierdza się, że członkostwo

[18] Ministerstwo Informatyzacji, *Strategia kierunkowa rozwoju informatyzacji Polski do roku 2013 oraz perspektywiczna prognoza transformacji społeczeństwa informacyjnego do roku 2020*, Warszawa 2005, www.archiwum-ukie.polskawue.gov.pl/HLP/files.nsf/0/61B9E65B9496C453C125721F003DCC0E/$file/Strategia_kierunkowa_rozwoju_informatyzacji_Polski_do_roku_2013.pdf (02. 12. 2013).

[19] Ibidem, s. 15, 17 i nast.

[20] Ministerstwo Gospodarki, Departament Rozwoju Gospodarki, *Kierunki zwiększania innowacyjności gospodarki na lata 2007-2013*, Warszawa 19 sierpnia 2006, s.6.

[21] A. Kukliński, *Ku polskiej trajektorii rozwoju gospodarki opartej na wiedzy w kształtowaniu* [w:] *Gospodarka oparta na wiedzy. Wyzwanie dla Polski XXI wieku*, A. Kukliński (red.), Kancelaria Prezesa Rady Ministrów, Warszawa 2001, s. 267-268.

[22] R. Żelazny, *Gospodarka oparta na wiedzy w Polsce*, [w:] *Strategia lizbońska a możliwość budowania gospodarki opartej na wiedzy w Polsce*, E. Okoń-Horodyńska, K. Piech (red.), Wydawnictwo Polskiego Towarzystwa Ekonomicznego, Warszawa 2005, s. 117.

przyniosło Polsce szanse związane z koniecznością dostosowania ekonomiki narodowej do standardów unijnych, lecz skala wykorzystania programów pomocowych ukierunkowanych na KBE jest niezadowalająca.

W związku z praktyką dostosowawczą do nowelizowanej Strategii Lizbońskiej stworzono w Polsce trzy programy operacyjne: Sektorowego Programu Operacyjnego Wzrost Konkurencyjności i Przedsiębiorstw (SPO WKP), Sektorowego Programu Operacyjnego Rozwój Zasobów Ludzkich (SPO RZL) oraz Zintegrowanego Programu Operacyjnego Rozwoju Regionalnego (ZPORR). Głównym programem wspierającym rozwój innowacyjności, który powstał w ramach „Narodowego Planu Rozwoju 2007-2013", jest Program Operacyjny Innowacyjna Gospodarka. W okresie finansowania 2007-2013 zaplanowano na realizację celów Strategii Lizbońskiej w ramach tych właśnie programów operacyjnych ponad 35 mld euro[23].

Wiosną 2013 r. Ministerstwo Administracji i Cyfryzacji przedstawiło „Program zintegrowanej informatyzacji państwa"[24], wskazując na Deklarację z Malmo UE z 2009 r. jako na wytyczną „zapewnienia dostępności w Internecie szeregu kluczowych usług publicznych, umożliwiających przedsiębiorcom zakładanie i prowadzenie działalności gospodarczej z dowolnego miejsca w UE, niezależnie od ich pierwotnej lokalizacji, a obywatelom łatwiejsze podejmowanie nauki i pracy oraz zamieszkanie i przechodzenie na emeryturę w dowolnym miejscu w UE"[25]. Jak będzie realizowany ostatni z omówionych powyżej dokumentów, ocenić będziemy mogli w perspektywie najbliższych miesięcy.

Strategie rządowe są uważnie analizowane i komentowane przez ekspertów. Proponują oni rozwój krajowego sektora wiedzy i innowacji wg jednego z możliwych scenariuszy. W wariancie narodowym zakłada się, że zarówno tempo, jak i obszar inwestycji innowacyjnych nie zmienią się. Jest to scenariusz neutralny, ale nie zwiastujący szybkiego sukcesu. Tzw. droga grecka to z kolei scenariusz zakładający zwiększenie wydatków rządowych bez aktywizacji sektora prywatnego. Z uwagi na kryzys greckiej ekonomiki scenariusz ten wydaje się ryzykowny. W wariancie wzorowanym na Hiszpanii, przy zachowaniu na tym samym poziomie ogólnych wydatków w polityce innowacyjnej, należałoby pomyśleć o zwiększeniu udziału firm prywatnych w projektach badawczo-

[23] K. Żukrowska (red.), *Otwarta koordynacja w stosunkach międzynarodowych*, Wydawnictwo SGH, Warszawa 2006, s. 60.
[24]Ministerstwo Administracji i Cyfryzacji, *Program zintegrowanej informatyzacji państwa,* mac.gov.pl/wp-content/uploads/2013/03/PZIP-konsultacje-spoleczne-3.pdf (02. 12. 2013).
[25] Ibidem, s. 14.

rozwojowych. Na koniec – optymalnym scenariuszem wydaje się naśladownictwo Finlandii, gdzie przez najbliższe 30 lat planowana jest powolna zmiana proporcji w inwestycjach wiedzowych dla docelowego uzyskania w nich 25% udziału państwa i 75% udziału prywatnego kapitału[26].

Niestety jak dotąd Polska charakteryzuje się bardzo niskimi wskaźnikami wdrożenia innowacji w porównaniu z UE, przy czym głównym problemem polskiego systemu innowacji pozostaje małe zainteresowanie przedsiębiorstw inwestycjami w wiedzę. Wśród najczęstszych przyczyn takiego stanu rzeczy wymienia się słabą ochronę prawną partnerstwa prywatno-publicznego przy wysokim ryzyku niepowodzenia inwestycji z udziałem jednostek naukowo-badawczych.

4. ICT w służbie polskiego biznesu. Statystyki

Wyniki badań statystycznych w zakresie zastosowań ICT w polskich przedsiębiorstwach oraz kształcenie kadr w kierunku wykorzystania technologii budzą wiele obaw odnośnie do przyszłości polskiej gospodarki opartej na wiedzy. Główny Urząd Statystyczny prowadzi badania zmian w strukturze polskiego społeczeństwa informacyjnego od wielu lat w ramach seryjnej analizy zatytułowanej „Społeczeństwo informacyjne w Polsce"[27]. W 2004 r. powstał pierwszy kompleksowy raport, który uwzględniał poziom rozwoju technologicznego polskich firm. Wynikało z niego, że szerokopasmowy dostęp do Internetu posiadało 21% małych firm, 47% średnich i 79% dużych. Niecałe 36% firm wykorzystywało Internet w celach szkoleniowych, przy czym najwięcej (56%) takich szkoleń przeprowadzano w dużych przedsiębiorstwach. Wg kryterium branży najwięcej inwestował w umiejętności informatyczne pracowników sektor informatyki, lecz – co zdumiewa – na poziomie zaledwie 70%. W dalszej kolejności inwestowanie w kompetencje informatyczne pracowników wykazywała branża obrotu nieruchomościami (43%), transport i łączność (39%) oraz handel (34%). Stosunkowo słabo rozwijał się rynek B2B, gdyż zaledwie 3% firm potwierdzało dokonywanie zakupów i ich rozliczanie drogą elektroniczną, bez względu na wielkość firmy. Wśród państw członkowskich UE Polska zajmowała piąte od końca miejsce w zakresie wykorzystania ICT w biznesie, lecz nadzieje budziło trzecie miejsce w zakresie wykorzystania Internetu dla celów szkolenia kadr.

[26] W. Orłowski, *Scenariusze rozwoju sektora wiedzy w Polsce do roku 2040*, [w:] L. Zienkowski (red.), *Wiedza a wzrost gospodarczy*, Wydawnictwo Naukowe Scholar, Warszawa 2003, s.198-199.
[27] www.stat.gov.pl/gus/5840_4293_PLK_HTML.htm?action=show_archive (02. 12. 2013).

W kolejnej edycji raportu za lata 2004-2006 wykazano, że w Polsce 93% przedsiębiorstw wykorzystywało komputery, przy których pracowało 38% zatrudnionych. Analogiczne wskaźniki dla 25 krajów UE wyniosły 97% i 51%. Liczba przedsiębiorstw posiadających stronę www w latach 2004–2006 wzrosła o 30%, a liczba firm kupujących przez Internet (B2B) w latach 2003–2005 wzrosła 2,5-krotnie. Zaobserwowano ponadto powolną zmianę roli sektora ICT. W 2006 r. pod względem liczebności podmiotów firmy sektora ICT stanowiły 2,5% wszystkich przedsiębiorstw sektora produkcji i usług, a pod względem liczby pracujących 3,8%, przy czym w sektorze ICT 60% firm świadczyło usługi. Przychody ze sprzedaży sektora ICT wyniosły w 2006 r. 86,7 mld zł, co stanowiło 5,5% przychodów sektora produkcji i usług. Ponad 60% przychodów ze sprzedaży – usługi ICT, wśród których dominowała telekomunikacja, generując 70% przychodów. Wydajność pracy w sektorze ICT była o 44% wyższa niż w całym sektorze produkcji i usług. W 2005 r. nakłady na systemy komputerowe w Polsce wyniosły 4 mld zł, (3,8% nakładów inwestycyjnych). W związku z rozwojem bankowości elektronicznej najwięcej inwestował sektor finansowy – 25% całości nakładów na ten cel. W roku akademickim 2005/2006 liczba absolwentów specjalności informatycznych studiów magisterskich i zawodowych wyniosła ponad 17 tysięcy (wzrost o 32% w stosunku do roku akademickiego 2003/2004), w konsekwencji czego tylko 2% przedsiębiorstw deklarowało trudności z pozyskaniem pracowników z umiejętnościami w zakresie ICT.

Trzecia edycja raportu – opublikowana w 2008 r. – wskazywała dalszą ewolucję społeczeństwa i gospodarki w kierunku modeli opartych na wiedzy. 95% przedsiębiorstw korzystało z komputerów, a 93% miało dostęp do Internetu. Ponad połowa firm posiadała szerokopasmowy dostęp do sieci, 36% pracujących regularnie (co najmniej raz w tygodniu) korzystało z komputerów, a 28% z Internetu. 19% firm wyposażonych było w systemy do zarządzania informacjami o klientach (CRM), 12% firm posiadało systemy do kompleksowego planowania zasobów (ERP), 68% przedsiębiorstw kontaktowało się z administracją publiczną przez Internet. Wyraźnie zauważalne stało się naśladownictwo wzorców zachodnich w zakresie zarządzania wiedzą. 50% firm wyposażono w ERP (ang. *Enterprise Resorce Planning* – system informatyczny do planowania zasobów przedsiębiorstwa), w tym 25% średnich przedsiębiorstw i 12% małych. Upowszechniano również CRM (ang. *Customer Relatioship Management*) – systemy służące do zbierania, łączenia, przetwarzania i analizowania informacji o klientach. Ponadto 12% firm prowadziło

analizę danych o klientach w celu zdobycia wiedzy o sposobach zaspokojenia ich potrzeb, a 15% wysyłało lub otrzymywało faktury elektroniczne.

Kolejna edycja raportu z 2012 r.[28] wskazywała na znaczny postęp w zakresie wykorzystania ICT w biznesie. 95 % polskich firm posługiwało się komputerami z dostępem do Internetu, co sytuowało nas na 7 miejscu od końca w statystykach UE. Trzy branże – tj. finansowa, ubezpieczeniowa i rynek nieruchomości – wykazywały najwyższy współczynnik informatyzacji na poziomie 99% przy wysokim (ponad sześćdziesięcioprocentowym) wykorzystaniu szybkiego Internetu. Zmiana wywołana postępem technologicznym sprawiła, że ponad 40% firm wyposażało swoich pracowników w mobilne urządzenia z dostępem do Internetu, a prawie 15% firm zatrudniało specjalistów-informatyków. Szkolenie w zakresie ICT zapewniało swoim pracownikom 10% przedsiębiorstw, przy czym najwięcej w branży ubezpieczeniowej i bankowości. Własną stronę internetową posiadało ponad 67% firm. Odnotowano skokowy wzrost B2B z 3% do ponad 19%. Wobec nasycenia przedsiębiorstw produktami ICT zakupy urządzeń tego rodzaju stabilizowały się statystycznie na poziomie 35 % polskich firm.

W podsumowaniu można stwierdzić, że skala zmian związanych z inwestowaniem w narzędzia ICT i umiejętności informatyczne pracowników w ciągu dekady odmieniła zasadniczo oblicze polskich firm. Świadczą o tym również różnorodne formy integracji branżowej i regionalnej biznesu, które dowodzą, że Polska angażuje się aktywnie w globalny trend tworzenia struktur wiedzy, innowacji i technologii.

5. Inicjatywy regionalne, klastry i parki technologiczne z uwzględnieniem Polski Wschodniej

Jak wskazuje raport „Ośrodki innowacji i przedsiębiorczości w Polsce" od 1990 r. „liczba ośrodków innowacji i przedsiębiorczości systematycznie rosła (poza okresem 1998-2000), osiągając w połowie 2010 r. liczbę 735. W 2012 dokonano ponownej weryfikacji stanu instytucji wsparcia w oparciu o badania ankietowe i wywiad telefoniczny. W wyniku tych działań zdiagnozowano aktywne działanie 821 ośrodków"[29]. Znalazły się wśród nich: parki technologiczne, inkubatory technologiczne, centra transferu technologii[30].

[28] Wszystkie dane por.: Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2008-2012, www.stat.gov.pl/gus/5840_4293_PLK_HTML.htm (02. 12. 2013).
[29] A. Bąkowski, M. Mażewska (red.), *Ośrodki innowacji i przedsiębiorczości w Polsce*, Warszawa 2012, s. 13.

Pojęcie klastra wiedzy odwołuje się pośrednio do Strategii Lizbońskiej, gdzie główna uwaga UE skupiona została na odrabianiu przez Europę dystansu rozwojowego w dziedzinie nowoczesnych technologii. Strategia Lizbońska ogłoszona wiosną 2000 r. dotyczyła sfery ekonomicznej WE, zapowiadając przyspieszenie w promocji innowacyjnej gospodarki opartej na wiedzy, oznaczając nową postać gospodarki z relatywną przewagą usług (ponad 60%) przy wykorzystaniu technologii informatycznych (IT) bądź informacyjno-komunikacyjnych (ICT). Należy zaznaczyć, że koncepcja klastrów wiedzy nie jest jednak endemicznie europejska, ale pochodzi ze Stanów Zjednoczonych – jest zatem rodzajem zapożyczenia. Pierwsze klastry wiedzy pojawiły się w zachodnich stanach, przy czym najbardziej znana spośród pierwszych powstałych jest bez wątpienia Krzemowa Dolina. Różnica między klastrem a koncernem, syndykatem czy kartelem polega na celach, jakie są mu stawiane. Klastry nie łączą firm tej samej branży, nie integrują kapitału jednej firmy, nie służą też jego redystrybucji na spółki-córki. Klastry mają za zadanie wygenerowanie skoncentrowanego możliwie najtańszego kapitału wiedzy, przy okazji służąc powstaniu silnych nowych firm poprzez stymulację małej i średniej przedsiębiorczości. Rolą państwa pozostaje nieograniczanie aktywności gospodarczej prywatnego kapitału, a nawet wspomaganie go poprzez mechanizmy partnerstwa prywatno-publicznego.

Koncepcja klastrów wiedzy i innowacji mieści się w samym sercu wspólnotowych projektów budowania GOW. Jednym z podstawowych dokumentów przedstawiających założenia polityki klastrowej UE pozostaje Strategia Lizbońska, a działania władz polskich przybrały postać w dokumencie pt. „Kierunki i polityka rozwoju klastrów w Polsce" z 2009 r. W dokumencie tym czytamy: „Wyznacznikiem występowania realnego klastra jest przede wszystkim ponadprzeciętny stopień koncentracji przestrzennej podmiotów gospodarczych działających w danym sektorze i sektorach pokrewnych. Kluczowe dla zrozumienia istoty klastra jest uwzględnienie roli i interakcji pomiędzy takimi czynnikami jak: koncentracja przestrzenna, bliskość geograficzna, systemowy, sieciowy charakter społecznie zakorzenionych powiązań, kooperencja (*coopetition*) czyli jednoczesne konkurowanie i kooperacja podmiotów gospodarczych, wieloletnie tradycje danej działalności w danej lokalizacji (tzw. lokalne czy regionalne zagłębia tradycji), atrakcyjny rynek wyspecjalizowanej siły roboczej, efektywna dyfuzja tzw. wiedzy ukrytej (ang. *tacit knowledge*), której pozyskanie wymaga wchodzenia w bezpośrednie relacje międzyludzkie, znaczące zasoby kapitału społecznego (w tym kapitału relacyjnego) przejawiające się m.in. wzajemnym zaufaniem, patriotyzmem regionalnym, dostrzeganiem wspólnych celów

i przekładających się na efektywną współpracę w układzie potrójnej helisy (ang. *triple helix*) – tzn. między przedsiębiorcami, środowiskiem nauki oraz władzami publicznymi."[31]

Rozwój gospodarki opartej na wiedzy wymaga, aby jej filary – czyli kapitał ludzki, ICT oraz systemy innowacyjności – były ze sobą wzajemnie powiązane. Na podstawie Strategii Lizbońskiej zostały opracowane Regionalne Strategie Innowacji, które już od połowy lat dwutysięcznych przynosiły efekt w postaci bliższego i efektywniejszego kontaktu między sektorem nauki, biznesem i władzami lokalnymi. Z dokumentów PARP z 2012 r. wynika, że idea klastrów została dobrze zrozumiana i efektywnie wykorzystana w Polsce, zwłaszcza na wschodzie kraju. „Polscy przedsiębiorcy coraz lepiej rozumieją istotę klasteringu, widząc w nim szansę na dynamiczny rozwój przez lepsze wykorzystanie dostępnych zasobów i internacjonalizację działań. Wyrazem dużego zainteresowania klastrami jest ich rosnąca liczba, którą obecnie szacuje się na blisko 100. Najwięcej inicjatyw klastrowych powstało po 2007 r., czyli od momentu uruchomienia Funduszy Europejskich w ramach perspektywy finansowej na lata 2007-2013. Unia Europejska chętnie wspiera i promuje powiązania kooperacyjne, co znajduje swoje odzwierciedlenie na poziomie konkretnych programów operacyjnych. W Polsce jednym z programów operacyjnych wspierających inicjatywy klastrowe jest Rozwój Polski Wschodniej"[32], a liczba klastrów o stabilnej pozycji gospodarczej w województwach wschodnich wynosi po 36 i rośnie. Istotną korzyścią dla firm, które współtworzą klastry, jest efekt synergii branżowej, powodujący, że dawni konkurenci, stając się partnerami biznesowymi, pomnażają zyski i oszczędności. Ciekawymi przykładami integracji sektora informatycznego działającego w Polsce Wschodniej są: Wschodni Klaster Informatyczny, ICT Amber czy Północno-Wschodni Klaster Edukacji Cyfrowej. Ich pojawienie się stanowi dowód niespodziewanej nawet dla ekspertów dynamiki rozwoju regionów peryferyjnych, gdyż jeszcze przed kilkoma laty W. Sartorius pisał, iż „w Polsce Wschodniej nie należy oczekiwać w najbliższych latach rozwoju klastrów związanych z przemysłem informatycznym. We wszystkich 5 wschodnich województwach logicznym i korzystnym etapem rozwoju sektora technologii informatycznych i przemysłu treści cyfrowych będzie rozwój sieci współpracy firm prowadzącej do powstawania Wirtualnych Organizacji Sieciowych (*Network Virtual*

[31] Ministerstwo Gospodarki, *Kierunki i polityka rozwoju klastrów w Polsce*, Warszawa 2009, s. 5.
[32] Polska Agencja Rozwoju Przedsiębiorczości, *Rozwój klastrów w Polsce Wschodniej*, Warszawa 2012, s. 5-6.

Organizations – NVOs)"[33]. Jednak, jak uważa członek Wschodniego Klastra Informatycznego, najbardziej zachęcający do współpracy między firmami pozostaje efekt synergii, który sprawia, że klaster jako spójna całość, uzupełniona np. doradztwem biznesowym, staje się kompleksowym narzędziem do realizacji celów praktycznie każdego przedsiębiorstwa[34].

Wspomniany już Sartorius zwrócił także uwagę na potencjał rozwojowy regionów peryferyjnych Polski, widząc w nich nieodzowny komponent budowy krajowej gospodarki opartej na wiedzy. Wymienił przy tej okazji kilka endemicznych uwarunkowań, które w przypadku Polski Wschodniej przynieść mogą szybkie zmiany w kierunku KBE. Fundamentem ma być ukształtowanie postawy akceptacji i zainteresowania technologiami ze strony małego i średniego biznesu, zwracając także uwagę na konieczność ustawicznego szkolenia kadry zarządzającej pod względem przygotowania biznesplanów, współpracy z administracją oraz pozyskiwania kapitału[35]. Drugim czynnikiem powinien być rozwój infrastruktury teleinformatycznej, a trzecim – zwalczanie wykluczenia cyfrowego. Widzimy w ostatnich latach, jak procesy te przynoszą rezultaty, a firmy z województw wschodniej Polski wykazują rosnącą aktywność w tworzeniu już nie tylko klastrów, ale również platform i parków technologicznych.

Platforma Technologiczna to konsorcjum, które zrzesza przedsiębiorstwa, jednostki naukowe, ośrodki innowacji i przedsiębiorczości, instytucje finansowe i samorząd gospodarczy, mające na celu sformułowanie średnio i długookresowej wizji rozwoju technologicznego wybranego sektora gospodarki, wyznaczenie strategii zmierzającej do jej realizacji oraz przygotowanie spójnego planu działania[36]. Platformy technologiczne powstały w Polsce w latach 2004-2005, ale dopiero od 2011 r. znalazły partnera dla swej działalności w postaci Narodowego Centrum Badań i Rozwoju. Rozpoczęło ono negocjacje z Polskimi Platformami Technologicznymi w sprawie ustanowienia Sektorowych Programów Badawczych. Wśród podmiotów tworzących platformy technologiczne przeważają instytuty naukowe i uczelnie wyższe, mające za partnerów przedsiębiorstwa, fundacje i izby gospodarcze. Polska Platforma Technologiczna Bezpieczeństwa Wewnętrznego, kierowana

[33] W. Sartorius, *Społeczeństwo informacyjne i gospodarka oparta na wiedzy w Polsce Wschodniej,* www.mir.gov.pl/rozwoj_regionalny/poziom_regionalny/strategia_rozwoju_polski_wschodniej_do_2020/dokumenty/Documents/3c06195d761142c9b489f66512d7a63cSartorius.pdf, s. 429 (02. 12. 2013).
[34] Polska Agencja Rozwoju Przedsiębiorczości, *Rozwój klastrów w Polsce Wschodniej*, Warszawa 2012, s. 9-10.
[35] W. Sartorius, *Społeczeństwo informacyjne i gospodarka oparta na wiedzy w Polsce Wschodniej,* op. cit., s. 441-442 (02. 12. 2013).
[36] A. Bąkowski, M. Mażewska (red.), *Ośrodki innowacji i przedsiębiorczości w Polsce,* op. cit., s. 167.

przez Politechnikę Białostocką, obejmuje kilka jednostek naukowych i firm z obszaru całej Polski[37]. Kluczowymi partnerami są centralne organy państwowe odpowiedzialne za bezpieczeństwo państwa i obywateli. Platforma jest realizatorem strategicznych projektów z zakresu bezpieczeństwa wewnętrznego i sądownictwa. Innym przykładem jest Polska Platforma Technologiczna Żywności, koordynowana przez Uniwersytet Warmińsko-Mazurski w Olsztynie we współpracy ze Spółdzielnią Mleczarską MLEKPOL, czy Polska Platforma Technologiczna Lotnictwa, koordynowana przez WSK PZL-Rzeszów SA.

Z kolei parki technologiczne to rodzaj „zorganizowanych kompleksów gospodarczych, w ramach których realizowana jest polityka w zakresie: wspomagania młodych innowacyjnych przedsiębiorstw nastawionych na rozwój produktów i metod wytwarzania w technologicznie zaawansowanych branżach, optymalizacji warunków transferu technologii i komercjalizacji rezultatów badań z instytucji naukowych do praktyki gospodarczej"[38]. Skupionym w nich podmiotom naukowym i gospodarczym przynoszą ten sam efekt synergii, jaki obserwujemy w przypadku klastrów wiedzy. Wyróżniają się dużą elastycznością organizacyjną, stąd ich relatywnie duża liczba na terenie Polski, która łącznie z projektami w budowie wynosi 54. Jak zaznaczono powyżej, zauważalny jest udział podmiotów z województw Polski Wschodniej w tworzeniu infrastruktury parków technologicznych, a przykłady stanowią chociażby: Lubelski Park Naukowo-Technologiczny[39], Podkarpacki Park Naukowo-Technologiczny „AEROPOLIS" w Rzeszowie[40], Park Naukowo-Technologiczny Polska-Wschód w Suwałkach[41], Tarnowski Park Naukowo-Technologiczny[42]. W budowie znajdują się ponadto: Białostocki Park Naukowo-Technologiczny[43], Południowo-Wschodni Park Naukowo-Technologiczny w Zamościu[44] czy Olsztyński Park Naukowo-Technologiczny[45].

[37] www.ppbw.pl (02. 12. 2013).
[38] A. Bąkowski, M. Mażewska (red.), *Ośrodki innowacji i przedsiębiorczości w Polsce*, op. cit., s. 25.
[39] www.lpnt.pl (02. 12. 2013).
[40] www.aeropolis.com.pl (02. 12. 2013).
[41] www.park.suwalki.pl (02. 12. 2013).
[42] www.tarr.tarnow.pl (02. 12. 2013).
[43] www.bpnt.bialystok.pl (02. 12. 2013).
[44] www.parknaukowotechnologicznyzamosc.republika.pl (02. 12. 2013).
[45] www.parktechnologiczny.olsztyn.eu (02. 12. 2013).

Wnioski

1. W ciągu ostatnich dwudziestu lat ekonomiki krajów zachodnich uległy znaczącym strukturalnym zmianom. Państwa te ewaluowały z gospodarki opartej na pracy i kapitale do gospodarki opartej na wiedzy, gdzie wiedza jest kluczowym zasobem, a zasadniczą rolę odgrywają informacja oraz technologie. Wedle obowiązującego paradygmatu nowoczesnej ekonomii dzieje się tak, gdyż głównym czynnikiem konkurencyjności staje się właśnie wiedza, a tradycyjne czynniki produkcji ustępują jej miejsca.

2. Polska jako członek UE dokonuje od blisko dekady synchronizowanych ze Wspólnotami dostosowań prawnych i infrastrukturalnych do nowego wzorca rozwoju gospodarczego. Widać, że w ostatnich latach nastąpiło wyraźne przyspieszenie rozwoju polskiej KBE i proces ten pogłębia się dzięki dwóm trendom, tj. masowemu funkcjonowaniu małych i średnich firm w przestrzeni Internetu oraz kształceniu kadr z wykorzystaniem ICT.

3. Aktywizacja peryferyjnych regionów Polski poprzez udział przedsiębiorstw w różnorodnych centrach innowacji i przedsiębiorczości daje nadzieję, że w ciągu bieżącej dekady nasz kraj ukształtuje stabilny model społeczeństwa informacyjnego i gospodarki opartej na wiedzy.

Bibliografia:

1. Bąkowski A., Mażewska M. (red.), *Ośrodki innowacji i przedsiębiorczości w Polsce*, Warszawa 2012
2. ECCO. International Communications Network, *Polacy a nowe technologie, Czyli jak daleko nam do społeczeństwa informacyjnego? Raport z badań opinii z komentarzem*, w. m. w. 2011
3. Główny Urząd Statystyczny Urząd Statystyczny w Szczecinie, *Społeczeństwo informacyjne w Polsce*, Szczecin 2012
4. Główny Urząd Statystyczny Urząd Statystyczny w Szczecinie, *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych 2008-2012*, Szczecin 2012
5. Grudzewski W., Hejduk I., *E-learnig w systemie gospodarki opartej na wiedzy w Polsce*, http://www.e-edukacja.net/_referaty/4_e-edukacja.pdf
6. Jasiński A.H., *Innowacje i transfer techniki w procesie innowacji*, Warszawa 2006
7. Kasperkiewicz W., *Procesy innowacyjne w gospodarce rynkowej. Teoria i praktyka*, Piotrków Trybunalski 2008
8. Kozioł-Nadolna K., *Powiązania sieciowe przedsiębiorstw,* Finansowy Kwartalnik Internetowy „e-Finanse" 2011, vol. 7, nr 1, www.e-finanse.com/artykuly/175.pdf
9. Kozłowski J., *Statystyka nauki, techniki i innowacji w krajach UE i OECD. Stan i problemy rozwoju*, Departament Strategii MNiSW, 2011, www.nauka.gov.pl/g2/oryginal/2013_05/2a2fa1bfacf65d9ef5c7a3983c93e19f.pdf
10. Kukliński A., *Ku polskiej trajektorii rozwoju gospodarki opartej na wiedzy w kształtowaniu* [w:] *Gospodarka oparta na wiedzy. Wyzwanie dla Polski XXI wieku*, A. Kukliński (red.), Kancelaria Prezesa Rady Ministrów, Warszawa 2001.
11. Ministerstwo Informatyzacji, *Proponowane kierunki rozwoju nauki i technologii w Polsce do 2020 roku*, Warszawa 2004
12. Niklewicz-Pijaczyńska M., *Od koncepcji gospodarki opartej na wiedzy do nowej strategii rozwoju UE 2020*, www.bibliotekacyfrowa.pl/dlibra/docmetadata?id=35524&from=publication
13. Pawluczuk A., *Gospodarka oparta na wiedzy: edukacja i infrastruktura informatyczna w Polsce i w wybranych krajach OECD*, http://www.instytut.info/images/stories/ksiazki_polecane/15_przemiany_i_perspektywy_przedsiebiorstw_1/r27.pdf
14. Piech K., *Gospodarka oparta na wiedzy jako etap przemian społeczno-gospodarczych krajów transformacji systemowej*, [w:] J. Nowakowski, A. Skowronek-Mielczarek /red./, *Gospodarka, przedsiębiorstwo i konsument a wyzwania europejskie*, Warszawa 2004

15. Polska Agencja Rozwoju Przedsiębiorczości, *Rozwój klastrów w Polsce Wschodniej*, Warszawa 2012

16. Sartorius W., *Społeczeństwo informacyjne i gospodarka oparta na wiedzy w Polsce Wschodniej*, www.mir.gov.pl/rozwoj_regionalny/poziom_regionalny/strategia_rozwoju_polski_wschodniej_do_2020/dokumenty/Documents/3c06195d761142c9b489f66512d7a63cSartorius.pdf

17. Skrzypek E., *Gospodarka oparta na wiedzy i jej wyznaczniki*, www.ur.edu.pl/file/15853/022.pdf

18. Strzelecka A., Pytel M., *System zarządzania wiedzą jako czynnik wspomagania przedsiębiorstw w warunkach kryzysu*, www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2010/139_Strzelecka_A.pdf

19. Wydro K.B., Olender M., *Ekonomiczna wartość informacji*, Zakład Problemów Regulacyjnych i Ekonomicznych, Instytut Łączności, Warszawa 2006

Internet w pracy i rozwoju przedsiębiorstwa

Henryk Bednarczyk, Tomasz Frankowski, Ewa Serafin[1]

1. Wstęp

Internet w dobie XXI wieku to już nie „wirtualny świat", który jest novum przeznaczonym dla wybranych firm i instytucji. Dynamika wolnego rynku, szybki obieg informacji i pieniądza wymusza aktywne korzystanie z jego zasobów i możliwości. Dlatego każde przedsiębiorstwo musi aktywne korzystać z globalnej sieci, która umożliwia szybszą komunikację z partnerami biznesowymi i klientami, redukcję kosztów, reklamę oraz komunikację z urzędami. Skala wykorzystania Internetu w przedsiębiorstwie zależy od jego wielkości, struktury, branży i specyfiki działania.

2. Internet jako narzędzie pracy

Internet należy zdefiniować jako ogólnoświatową sieć komputerową, która łączy lokalne sieci korzystające z pakietowego protokołu komunikacyjnego **TCP/IP** oraz posiada jednolite zasady adresowania i nazywania węzłów (komputerów włączonych do sieci) i protokoły udostępniania informacji[2]. Internet składa się z 3 poziomów. Pierwszy z nich to sieć szkieletowa Internetu obejmująca zespół węzłów. Każdy z nich zawiera pełną informację o wszystkich sieciach, które są dołączone do Internetu i o trasach, którymi należy kierować

[1] Dr hab. prof. nadzw. Henryk Bednarczyk - specjalność naukowa – pedagogika pracy: teoretyczno-metodologiczne podstawy zintegrowanego wielopoziomowego systemu ustawicznej edukacji zawodowej (środowisko pracy, standardy kwalifikacji zawodowej, kształcenie modułowe, technologie, jakość kształcenia), członek Narodowej Akademii Nauk Pedagogicznych Ukrainy, Rosyjskiej Akademii Kształcenia Zawodowego, International Vocational Education and Training Association, Association for Career and Technical Education Research, autor i redaktor naukowy ponad 80 monografii oraz prac zbiorowych, ogółem ponad 500 publikacji w tym kilkadziesiąt w języku angielskim, rosyjskim, redaktor naukowy monograficznej serii wydawniczej Biblioteka Pedagogiki Pracy (261 tomów – 175150 egz.), kwartalnika Edukacja Ustawiczna Dorosłych Polish Journal of Continuing Education (83 tomów - 74200 egz.), Prezes Zarządu Stowarzyszenia Oświatowego Sycyna: Społeczna sieć eSycyna, 80 komputerów w 44 miejscowościach powiatu zwoleńskiego wzbogacona o 920 komputerów z projektu einclusion (2011–2015), Biblioteka Sycyńska: 40 + 23 monografii Małych Ojczyzn 60310 egz., Europejska sieć małych ojczyzn wielkich ludzi, dziedzictwo kulturowe szansą społeczeństwa lokalnego, stypendia oświatowe. Wiceprezes Stowarzyszenia Dziedzictwo i Rozwój – Leader+. Mgr Tomasz Frankowski - absolwent informatyki oraz ekonomii na Uniwersytecie Marii Curie-Skłodowskiej w Lublinie. W latach 1.09.2008 do 30.08.2012 pracownik Politechniki Radomskiej na Wydziale Nauczycielskim (Zakład Informatyki). Od 1.04.2009 właściciel firmy informatycznej DevilArt, później współwłaściciel DevilArt S.C. Autor publikacji z zakresu wykorzystania informatyki w ekonomii oraz edukacji. Redaktor statystyczny kwartalnika „EDUKACJA ustawiczna DOROSŁYCH" pod refakcją dr hab. Henryka Bednarczyka.

1 www.encyklopedia.pwn.pl (02. 12. 2013).

Dr inż. Ewa Serafin - Wydział Transportu i Elektrotechniki, UTH im. K. Pułaskiego w Radomiu (Zakład Elektrotechniki i Elektroenergetyki), Wydział Nauk Ekonomicznych i Technicznych, PSW im. Papieża Jana Pawła II w Białej Podlaskiej (Katedra Informatyki).

pakiety przeznaczone do tych węzłów. Drugi poziom to serwery i routery, które są przyłączone do sieci szkieletowej, tworzące podsieci. Przykładem takich podsieci są: wewnętrzne sieci na uniwersytetach, sieci operatorów telewizji kablowej, „Neostrada" itp. Ostatni (trzeci) poziom to użytkownicy, którzy są przyłączeni do Internetu za pośrednictwem poszczególnych dostawców. Informacje w Internecie są przesyłane w postaci pakietów (średnia wielkości to ~1500 bajtów). Komputery przyłączone do Internetu (węzły, ang. *host*) są oznaczone wieloczłonowymi identyfikatorami liczbowymi tzw. adresami **IP**. Wyróżniamy dwa rodzaje adresów IP: dynamiczne i statyczne. Dynamiczne adresy IP są przydzielane losowo przez dostawców Internetu. Natomiast statyczne adresy IP są przypisane na stałe do danego węzła sieci: komputera lub serwera. Statyczne adresy IP otrzymują zazwyczaj serwery. Natomiast użytkownicy końcowi korzystają z ich dynamicznych odpowiedników[3]. Adres IP danego węzła składa się z 12 cyfr (standard **IPv4**) pogrupowanych i oddzielonych znakiem kropki (przykład: 198.201.212.198). Stosowany jest również nowszy standard **IPv6**, który pozwala na zaadresowanie znacznie większej liczby węzłów (2^{128} w porównaniu do 2^{32} dla IPv4). Spojrzenie na Internet nie tylko z technicznego punktu widzenia lepiej oddaje jego specyfikę i wielopłaszczyznowość. E. Krol i E. Hoffman wskazują na złożoność Internetu, proponując, aby postrzegać go nie tylko z technicznego punktu widzenia, ale w trzech równoważnych aspektach:

- **technicznym** – jako połączone sieci komputerowe, oparte na wspólnym protokole przesyłania danych tj. TCP/IP,
- **społecznym** – jako zbiorowość ludzi, którzy wspólnie użytkują i rozwijają te sieci,
- **informacyjnym** – jako zbiór zasobów, które mogą być pozyskane za pomocą tych sieci[4].

Rozwinięcie powyższych punktów przedstawia W. Chmielarz. Jego definicja oddaje w sposób kompleksowy specyfikę i złożoność Internetu, który jest określony jako globalny, masowy system informatyczny, składający się z połączonych ze sobą wzajemnie sieci komputerowych opartych na protokołach TCP/IP. Na system ten składa się osprzęt komputerowy, telekomunikacyjny oraz oprogramowanie. Internet jest to również zbiór zasobów znajdujących się w sieci, zbiór reguł posługiwania się nimi oraz zbiór usług, jakie są dostępne: strony www, poczta elektroniczna, transfer plików, telepraca, listy dyskusyjne,

3 Kirch O., Dawson T., *Linux - podręcznik administratora sieci*, Warszawa 2000, s. 2-10
4 Bajdak A., *Internet w marketingu*, Warszawa 2003, s.14.

rozmowy w czasie rzeczywistym. Internet jest wykorzystywany i rozwijany przez jego użytkowników tworzących swoistą społeczność, świadomą jego możliwości i ograniczeń. W tak rozumianym kontekście używanie Internetu to działanie członków społeczności przy pomocy sieci telekomunikacyjnej, które ma na celu odnalezienie i wykorzystanie znajdujących się w niej zasobów informacyjnych oraz aktywne wzbogacanie jej zasobów[5].

Sieć internetowa udostępnia wiele usług, które umożliwiają szybsze pozyskanie informacji czy przekazanie danych adresatowi oddalonemu o tysiące kilometrów. Należą do nich między innymi:

- strony internetowe (strony WWW),
- poczta elektroniczna,
- grupy dyskusyjne – fora,
- chaty,
- komunikatory internetowe,
- platformy e-learningowe,
- usługi FTP,
- wirtualne dyski (chmura).

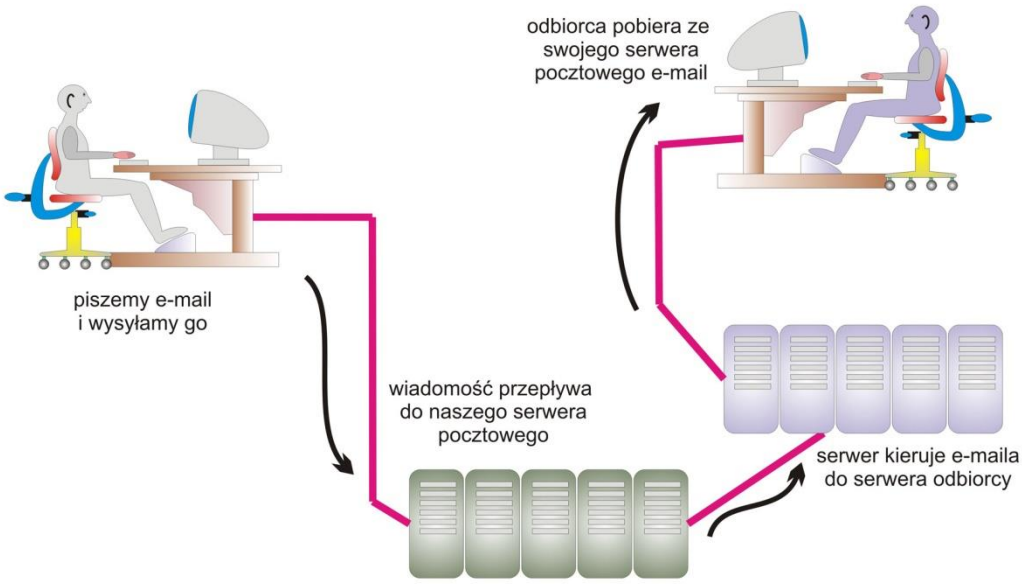
Najbardziej powszechną usługą Internetu są strony www oraz poczta elektroniczna. Strona internetowa, **strona WWW (ang. *web page***) jest to dokument HTML udostępniony w Internecie[6]. W skład strony wchodzi jej adres wpisywany w przeglądarce (domena internetowa) oraz serwer WWW, na którym fizycznie strona jest umieszczona. Domena i serwer nie muszą być zakupione u jednego dostawcy. Za połączenie domeny z serwerem odpowiadają adresy DNS, które wskazują miejsce do pobierania informacji – serwer WWW (zwany inaczej hostingiem). Po stronie użytkownika (hosta), strona WWW jest otwierana i wyświetlana za pomocą przeglądarki internetowej, co przedstawia rysunek 1.

5 Chmielarz W., *Systemy biznesu elektronicznego*, Warszawa 2007, s. 41.
6 Pytlak M., *Analiza wpływu nowych elementów formatowania zawartych w HTML5 i CSS3 na wygląd i zawartość treściową strony w przeglądarkach internetowych*, [w:] *Informatyka w dobie XXI wieku. Nauka, technika, edukacja a nowoczesne technologie informatyczne*, A. Jastriebow (red.), Radom 2011, s. 281-282

Rys. 1. Przykładowy wygląd firmowej strony internetowej

Źródło: http://www.devilart.pl

Strona internetowa może zawierać tekst, zdjęcia oraz animację. Rozbudowane strony www umożliwiają interakcję między użytkownikiem a zawartością strony internetowej. Druga najbardziej rozpowszechniona usługa to poczta elektroniczna i wiadomości e-mail. **Poczta elektroniczna** lub krótko e-poczta, (ang. *electronic mail* krótko *e-mail*) jest to usługa internetowa – w nomenklaturze prawnej określana zwrotem „świadczenie usług drogą elektroniczną" – służąca do przesyłania wiadomości tekstowych, tzw. listów elektronicznych – stąd zwyczajowa nazwa tej usługi. Schemat działania tej usługi przedstawia rysunek 2.



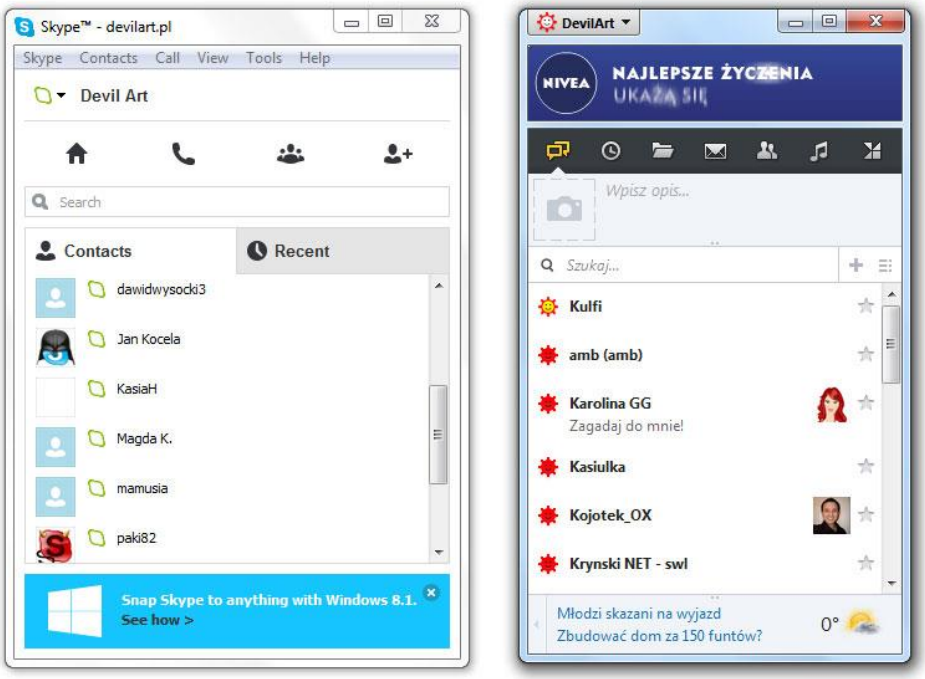
Rys. 2. Schemat działania poczty elektronicznej

Źródło: http://www.scholaris.pl

Do obsługi poczty elektronicznej wykorzystuje się wyspecjalizowane oprogramowanie uruchomione na stale działających serwerach. Znane i popularne programy tego typu to: Sendmail, Qmail. Po stronie użytkownika działa program klienta, który pozwala na redagowanie, wysyłanie i odbieranie wiadomości np. Outlook, Thunderbird. Wielu dostawców umożliwia obsługę poczty z poziomu przeglądarki internetowej. Przesyłane wiadomości mogą zawierać tekst, zdjęcia oraz dowolny rodzaj pliku stanowiący załącznik wiadomości. Mniej powszechną formą pozyskiwania informacji w Internecie są grupy dyskusyjne, potocznie zwane forami. **Forum dyskusyjne** jest to przeniesiona do struktury stron internetowych forma grup dyskusyjnych, która służy do wymiany informacji i poglądów między osobami o podobnych zainteresowaniach przy użyciu przeglądarki internetowej. Fora dyskusyjne były bardzo popularną formą grup dyskusyjnych w Internecie. Wraz z rozwojem wyszukiwarek internetowych – zwłaszcza Google – ich znaczenie zostało zmarginalizowane[7].

Coraz szybsze łącza internetowe umożliwiają płynne przesyłanie dźwięku i obrazu pomiędzy wieloma użytkownikami sieci. Dzięki temu obecne chaty i komunikatory umożliwiają prowadzenie rozbudowanych dyskusji i konferencji. Najbardziej znane to: GG oraz Skype, których interfejs przedstawia rysunek 3. Obydwa rozwiązania umożliwiają prowadzenie wideokonferencji między użytkownikami w czasie rzeczywistym.

7 Pronobis D., *Podstawy obsługi komputera i korzystania z Internetu. Podręcznik z ćwiczeniami dla ucznia*, Warszawa 2009, s. 63



Rys. 3. Interfejs popularnych komunikatorów Internetowych: Skype oraz GG

Źródło: opracowanie własne

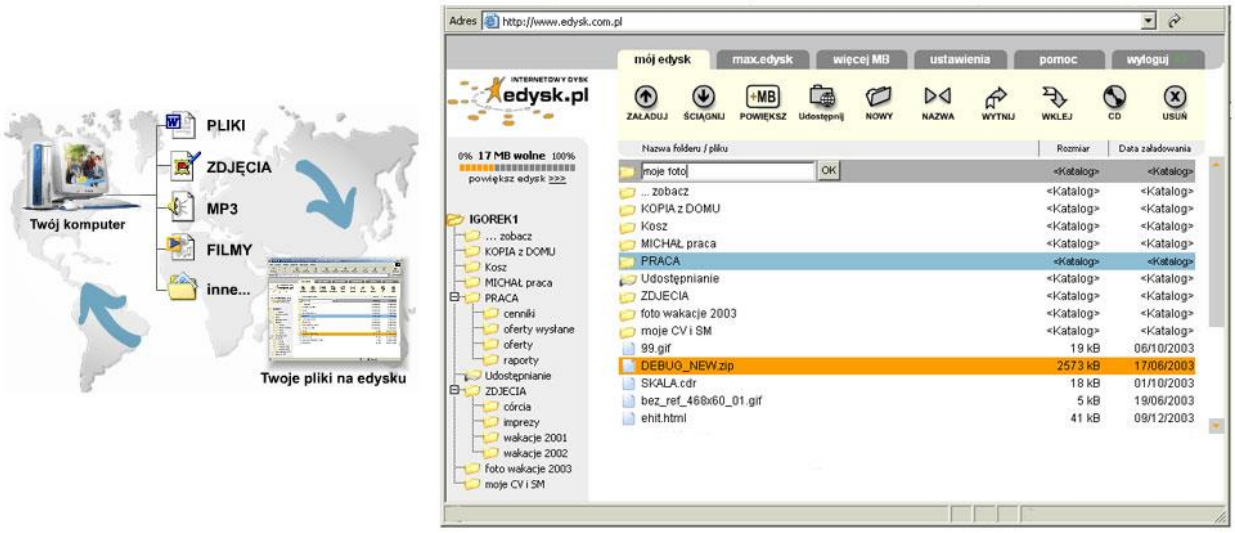
Grupę chatów i komunikatorów internetowych winno się rozszerzyć o **platformy e-learningowe**, które umożliwiają nauczanie z wykorzystaniem sieci komputerowych i Internetu. Wspomagają one proces dydaktyczny za pomocą komputerów osobistych i Internetu. Platforma e-learningowa pozwala na ukończenie kursu, szkolenia, a nawet studiów bez konieczności fizycznej obecności w sali wykładowej. Doskonale uzupełnia również tradycyjny proces nauczania[8]. Przykładem takich platform są:

- Uczelniana Platforma E-Learningowa AGH[9]
- Kurs e-learning – wortal „mikroprzedsiębiorczość”[10]

Ostatni rodzaj usług, które oferuje Internet, to przesyłanie i magazynowanie danych na serwerach zapoczątkowane przez protokół **FTP (ang. File Transfer Protocol)**, który umożliwia przesyłanie przez Internet wszelkiego rodzaju plików. Obecnie używany wyłącznie przez webmasterów i administratorów serwerów. **E-dyski** umożliwiają przechowywanie kopii

8 Zieliński Z., *E-learning w edukacji. Jak stworzyć multimedialną i w pełni interaktywną treść dydaktyczną*, Gliwice 2012, s. 5,15-23
9 www.upel.agh.edu.pl/kokpit/ (02. 12. 2013).
10 Bednarczyk H., Koprowska D., Kacak I., *Transfer wiedzy i usług wsparcia dla mikroprzedsiębiorstw – doświadczenia, refleksje*, Radom 2008, s. 139-154

zapasowej danych na zewnętrznym serwerze, który ma stałe podłączenie do Internetu. Dzięki temu dostęp do zgromadzonych danych jest możliwy z dowolnego miejsca na świecie. Wykorzystanie e-dysków nie ogranicza się do tworzenia kopii bezpieczeństwa. Platforma ta może być wykorzystywana w przedsiębiorstwie do wymiany danych między różnymi członkami zespołu. Rozmiar przesyłanych plików na dysk i z dysku nie ma limitu, w przeciwieństwie do poczty elektronicznej i dołączanych do niej załączników. Maksymalny (bezpieczny) rozmiar załącznika nie powinien przekraczać 10 Mb. Korespondencja z większymi załącznikami może być odrzucona przez serwery pocztowe i wrócić do nadawcy. Schemat działania e-dysku i jego interfejs przedstawia rysunek 4.



Rys. 4. Schemat działania oraz przykładowy interfejs e-dysku

Źródło: opracowanie własne na podstawie http://www.edysk.pl

Rozwój Internetu i jego usług determinuje coraz większe wymagania sprzętowe. **Minimalne wymagania**, które umożliwiające pracę w Internecie to:

Tabela 1. Minimalne wymagania sprzętowe potrzebne do pracy w Internecie

System operacyjny Windows	System operacyjny Linux
⅄ procesor minimum 800 MHz ⅄ pamięć RAM 512 MB ⅄ karta graficzna klasy DirectX 9 ⅄ 32 MB pamięci graficznej ⅄ dysk twardy o pojemności 20 GB	⅄ procesor Pentium II taktowany zegarem 233MHz ⅄ pamięć RAM 64 MB ⅄ karta graficzna 4MB ⅄ dysk twardy o pojemności 2GB

▲ karta sieciowa ▲ dostęp do sieci Internet, przepustowość minimum 512 kbps	▲ karta sieciowa ▲ dostęp do sieci Internet, przepustowość minimum 512 kbps

Źródło: opracowanie własne

Przedstawione zestawienie w tabeli nr 1 określa absolutne minimum, które jest potrzebne do pracy z podstawowymi usługami tj.: strony www oraz poczta elektroniczna. Do prowadzenia wideokonferencji lub korzystania z interaktywnych stron www wymagania sprzętowe znacznie wzrastają.

3. Wykorzystanie Internetu w przedsiębiorstwie

Dynamiczny rozwój technologii i wzrost znaczenia Internetu umożliwiają przedsiębiorstwom zmianę zasad działania w wielu płaszczyznach gospodarczych. Internet okazał się narzędziem podnoszącym stopień prawdopodobieństwa odniesienia sukcesu, ale jednocześnie stał się obszarem konkurowania. Cytując za U. Nalazkiem: „Internet zmienia gospodarkę jak burza, porównywalna tylko z rewolucją przemysłową. Ci, którzy jej zwiastuny dostrzegli odpowiednio wcześnie, już dzisiaj zbierają owoce wprowadzonych zmian. Ślepi na zmiany odpadną”[11]. Globalną sieć w przedsiębiorstwie można wykorzystać na różne sposoby. Przyjmuje się następującą, ogólną klasyfikację wymiany danych z wykorzystaniem Internetu:

- **B2B (Business-to-Business)** – obejmuje całokształt operacji związanych z realizacją wymiany handlowej między firmami (marketing, przygotowanie ofert, obsługa zamówień, płatności, raportowanie),
- **B2C (Business-to-Consumer)** – obejmuje obsługę relacji między firmą i klientem końcowym, a stroną inicjującą jest firma,
- **B2E (Business-to-Employee)** – najczęściej są to witryny firmowe dostępne tylko dla pracowników, obsługujące wewnętrzną komunikację. Często stosowany jest intranet lub ekstarnet. Platforma obsługuje również pracę zdalną,

11 Szczepańska K., *Zastosowanie Internetu w marketingu jako przykład wykorzystania zasobów sieci w zarządzaniu przedsiębiorstwem*, Zeszyty Naukowe Wyższej Szkoły Biznesu w Dąbrowie Górniczej, NR 1(7), Dąbrowa Górnicza 2000, s. 58, za: Nalazek U., Bonarowski M., *Dystans do sieci*, Businessman Magazine, nr 9 (102), 1999.

- **B2A (Business-to-Administration)**, łączona z **B2G (Business-to-Government)** – płaszczyzna wymiany informacji między firmami i urzędami administracji rządowej i samorządowej,
- **C2B (Consumer-to-Business)** – obejmuje obsługę relacji między klientem i firmą, a stroną inicjującą jest klient (np. zamieszczając ofertę zakupu określonych dóbr, firma decyduje natomiast o jej przyjęciu lub odrzuceniu),
- **C2C (Consumer-to-Consumer)** – obejmuje obsługę relacji handlowych między klientami, najczęściej za pośrednictwem aukcji internetowych.

Firmy mogą za pośrednictwem Internetu nawiązywać kontakt z klientami, przedstawiając swoje oferty. Inne podmioty gospodarcze na nowych zasadach organizują współpracę z partnerami i dostawcami. Są i takie przedsiębiorstwa, które swoje istnienie zawdzięczają upowszechnieniu się technologii Internetu. Jest to sektor e-commerce: sklepy internetowe, portale aukcyjne, firmy świadczące usługi internetowe (tworzenie stron www, pozycjonowanie w wyszukiwarkach internetowych oraz inne usługi e-marketingowe). Dzięki Internetowi dostawcy i odbiorcy lepiej poznają swoje potrzeby. Organizacja może w sposób istotny ograniczyć zapasy, organizując produkcję zgodnie z zasadą ***just in time***. Nie trzeba kupować towarów ani wytwarzać dużych gotowych partii na zapas. Obszerne hale magazynowe stają się zbędne, z wyjątkiem bardzo ograniczonych powierzchni, zapewniających ciągłość produkcji i dostaw. Łańcuch zmian i oszczędność zaczyna się wydłużać. W efekcie korzystanie z elektronicznych form płatności może dać firmom oszczędności sięgające 72% dotychczasowych kosztów. Z kolei obsługa transakcji za pomocą Internetu jest sto razy tańsza niż w oddziale banku i cztery razy tańsza niż w bankomacie[12].

Aspekt wykorzystania globalnej sieci Internet w przedsiębiorstwie należy rozpatrywać w dwóch płaszczyznach:

- wykorzystanie Internetu wewnątrz organizacji,
- wykorzystanie Internetu na zewnątrz organizacji.

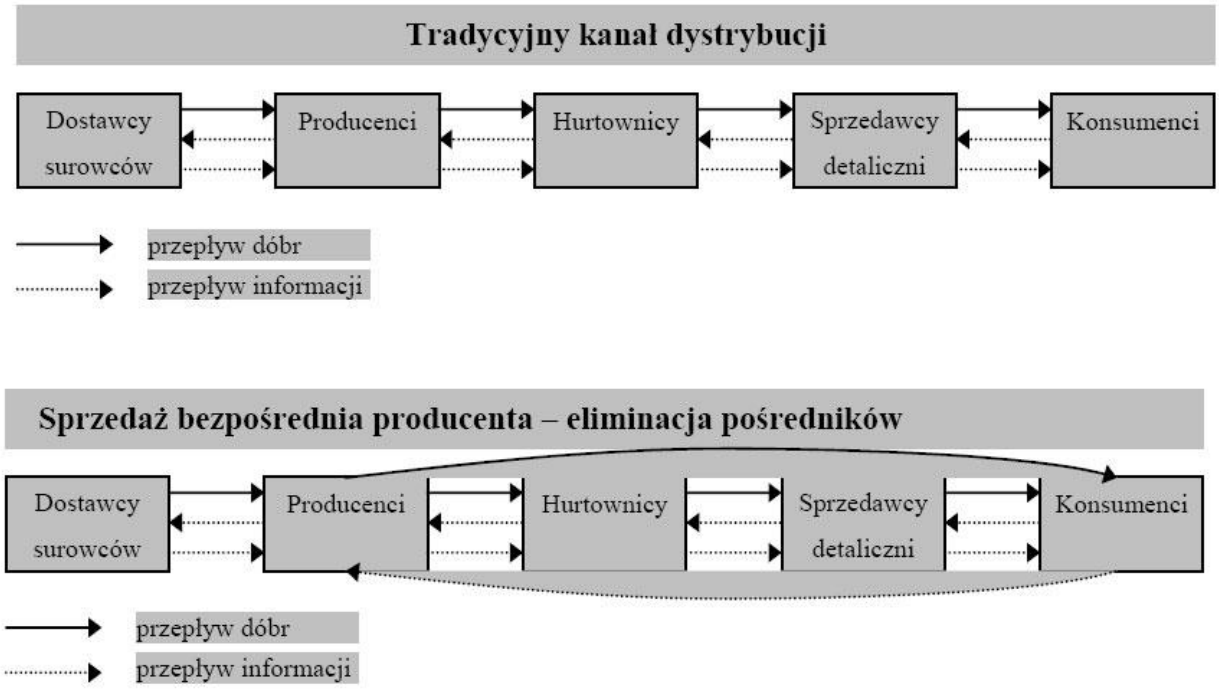
Pierwsza płaszczyzna umożliwia uzyskanie przedsiębiorstwu oszczędności, w postaci redukcji kosztów, poprawienia procesu zarządzania i logistyki oraz wewnętrznej komunikacji między pracownikami danej organizacji. Poprzez pozytywne wykorzystanie szans, jakie daje

12 Szczepańska K., *Zastosowanie Internetu w marketingu jako przykład wykorzystania zasobów sieci w zarządzaniu przedsiębiorstwem*, Śląska Biblioteka Cyfrowa2000, s.58-59, www.sbc.org.pl (02. 12. 2013).

Internet, przedsiębiorstwo może uzyskać przewagę nad innymi podmiotami gospodarczymi działającymi w danej branży. Poprzez uproszczony łańcuch logistyczny składający się z logistyki wejścia, procesu produkcji oraz logistyki wyjścia przedsiębiorstwo może znacznie zredukować koszty i pominąć niektóre jego aspekty.

Logistyka wejścia są to wszystkie działania związane z pozyskiwaniem, przechowywaniem oraz rozdysponowywaniem czynników produkcji. Wykorzystania Internetu daje przedsiębiorstwu możliwość zebrania szybko i po niskich kosztach aktualnych informacji o cenach oferowanych przez dostawców. Wykorzystując pocztę elektroniczną, przedsiębiorstwo może przesłać zapytanie ofertowe do wielu potencjalnych dostawców. W ten sposób redukowane są koszty dojazdów, koszt roboczogodzin związanych z czasem dojazdu pracowników do innych podmiotów gospodarczych.

Proces produkcji składa się z czynności związanych z transformacją czynników produkcji w produkt finalny. Szybki dostęp do informacji o działalności przedsiębiorstwa i przebiegu procesu produkcji, możliwy dzięki wykorzystaniu sieci Internet, pozwala na sprawniejszą kontrolę procesu produkcji. Dzięki Internetowi istnieje ponadto możliwość włączenia nabywcy do procesu kontroli wytwarzania danego produktu lub usługi. Rozwój aplikacji internetowych – zwłaszcza komunikatorów – pozwala natomiast na odbywanie wirtualnych spotkań (tj. wideokonferencji). Praca na odległość stała się także standardem prowadzenia wspólnych międzynarodowych przedsięwzięć naukowców. Brak konieczności spotykania się pracowników w siedzibie organizacji powoduje również, że przedsiębiorstwo może zatrudniać najlepszych specjalistów, redukując koszty związane z ich wynagrodzeniem. Rozproszenie pracowników przy wykorzystaniu Internetu umożliwia także pracę nad tym samym projektem bez przerw przy zmieniających się zespołach i dostępie do tej samej informacji i wyników pracy członków znajdujących się w innych miejscach.



Rys. 5. Porównanie kanałów dystrybucji produktów i usług

Źródło: Smit H. *Auswirkungen des e-Commerce auf den Postmarkt*, Wissenschaftliches Institut für Kommunikationsdienste nr. 237, Bad Honnef Juni 2002, s. 62

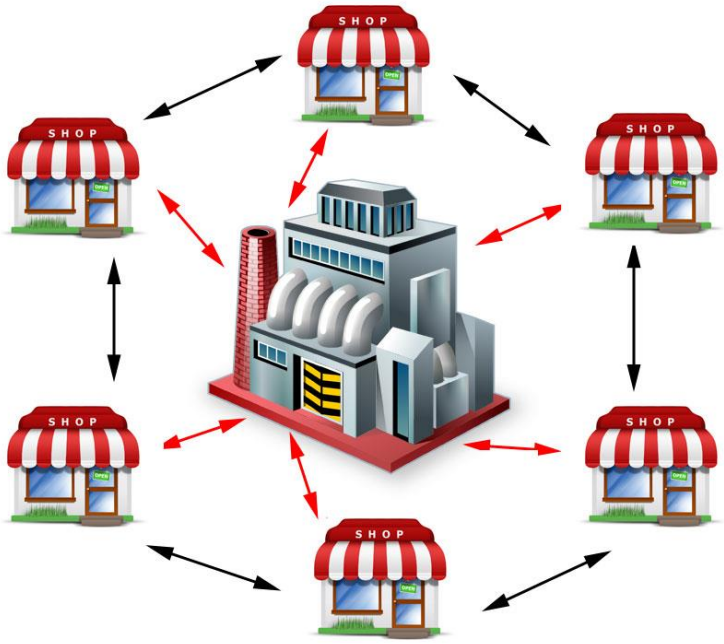
Logistyka wyjścia obejmuje czynności związane z dostarczaniem produktu finalnego klientowi końcowemu. Internet umożliwia przedsiębiorstwu bezpośredni dostęp do klienta. Ominiecie pośredników gwarantuje obniżenie ceny produktu poprzez redukcję kosztów dystrybucji[13]. Porównanie kanałów dystrybucji przedstawia rysunek 5.

Każde przedsiębiorstwo, wykorzystując Internet, może wypracować zwyczaje, symbole, sposoby komunikowania się oraz jej intensywność specyficzne dla swojej organizacji. Dostęp do globalnej sieci może przyczyniać się do większej integracji wokół celów i misji przedsiębiorstwa. Internet stwarza możliwość szybkiego oraz taniego komunikowania się między pracownikami, jak i organizacją bez względu na odległość geograficzną, co daje podstawy do jeszcze szybszego zarządzania przedsiębiorstwem.

Internet umożliwia prowadzenie rozproszonej sprzedaży, która oparta jest o centralny system magazynowy oraz punkty handlowe pobierające informacje o stanach magazynowych. Przykładem takiego rozwiązania jest Subiekt GT[14]. Schemat obiegu informacji między centralnym magazynem a poszczególnymi punktami sprzedaży został przedstawiony na

13 Szapiro T. , Ciemniak R., Internet – nowa strategia firmy, Warszawa 1999, s. 70
14 www.insert.com.pl/programy_dla_firm/sprzedaz/subiekt_gt/opis.html (02. 12. 2013)

rysunku 6.



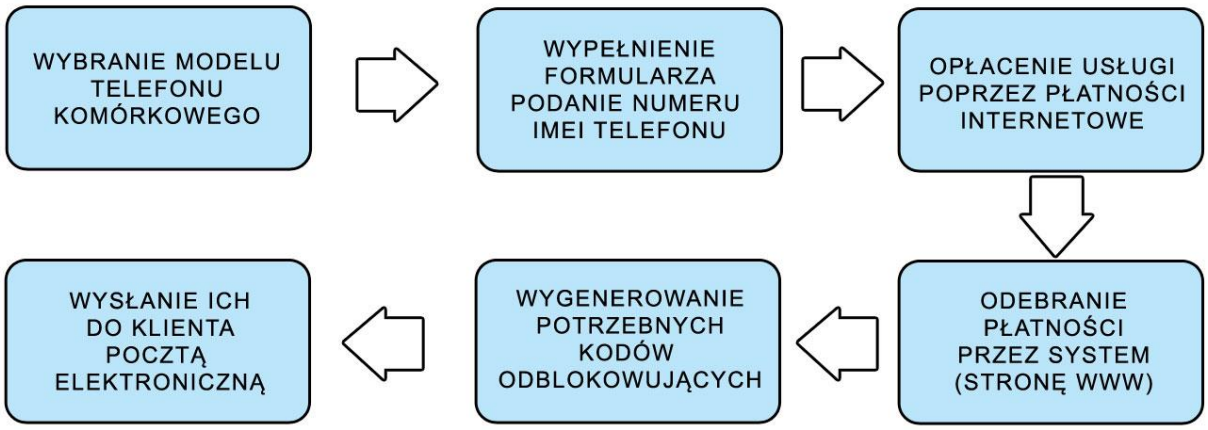
Rys. 6. Schemat obiegu informacji pomiędzy centralnym magazynem a punktami sprzedaży
Źródło: Opracowanie własne

Drugi aspekt to wykorzystanie Internetu na zewnątrz organizacji. Należy go rozważać w następujących płaszczyznach:

- komunikacja z klientami,
- prezentowanie oferty – strony internetowe,
- działania marketingowe,
- sprzedaż w Internecie,
- rozliczenia z dostawcami i klientami,
- rozliczenia z urzędami.

Dzięki nowoczesnym kanałom komunikacyjnym, jakie udostępnia Internet, model komunikacji z klientami uległ zmianie. Przedsiębiorstwo posiada szeroki wachlarz możliwych form porozumiewania się ze swoimi klientami i udzielenia im technicznego wsparcia. Należą do nich: chaty, video chaty, komunikatory internetowe, poczta elektroniczna. Dzięki nim pracownicy firmy mogą lepiej prezentować produkty i rozwiązywać problemy zgłaszane

przez klientów. Coraz częściej spotykany dwudziestoczterogodzinne wsparcie w postaci chatów, co pozwala efektywnie i na bieżąco rozwiązywać zgłaszane problemy. Przedsiębiorstwo skraca w ten sposób czas oczekiwania klientów na informacje o produkcie. Dzięki temu potencjalni klienci otrzymują potrzebne informacje w dogodnym dla nich czasie. Drugim kanałem, który umożliwia firmie lepsze zaprezentowanie swoich produktów, są strony internetowe. Informacje na nich zawarte są dostępne 24h na dobę. Jeśli strona posiada formularz kontaktowy lub zamówienia, przedsiębiorstwo może przyjmować zamówienia poza godzinami pracy. W połączeniu z płatnościami internetowymi transakcje mogą być przeprowadzone w pełni automatycznie. Przykładem takiego systemu jest platforma do zdejmowania blokady simlock z telefonów komórkowych odblokowania.pl. Schemat jej działania przedstawia rysunek 7.



Rys. 7. Schemat pełnej automatyzacji przyjęcia zamówienia, płatności za zamówioną usługę oraz jej dostarczenie klientowi

Źródło: Opracowanie własne

Automatyzacja procesu zamówienia, przyjmowania płatności oraz dostarczania usług umożliwia znaczą redukcję kosztów oraz zwiększenie mocy przerobowych danego przedsiębiorstwa.

Internet – oprócz możliwości prezentowania swojej oferty – umożliwił również sprzedawanie towarów i usług na globalną skalę. Sklep, który mieści się w województwie mazowieckim, z powodzeniem może sprzedawać swoje produkty w pozostałych. Czas dostawy towaru do klienta to przeważnie okres od 24 do 48 godzin. Dzięki temu firma dociera do nowych klientów, których nie pozyskałaby w tradycyjnym rejonie swojego działania. Sprzedaż w sieci umożliwia łatwe dotarcie do jednolitej docelowej grupy klientów, którzy są zdecydowani na zakup oferowanego produktu. Poprzez tworzenie własnych stron

przedsiębiorstwa zyskują także możliwość zaistnienia na ogólnoświatowym rynku. Koszt zbudowania takiej strony jest względnie niski w stosunku do liczby potencjalnych klientów, do których firma zyskuje dostęp. Dodatkowo istnieje możliwość organizowania społeczności wirtualnych wokół oferowanego rodzaju produktu bądź jednolitych zainteresowań czy innych cech konsumentów, m.in. dzięki takim portalom jak Facebook, Twitter czy Nasza Klasa[15]. Wykorzystując Internet, przedsiębiorstwo ma dostęp do ogromnej ilości informacji o klientach, które może zbierać poprzez swoje strony internetowe. Istnieją specjalne aplikacje internetowe, które pozwalają firmie sprawnie zbierać i sortować takie informacje. Zebrane i posortowane dane mogą następnie posłużyć jako bazy do rozsyłania spersonalizowanej oferty o produktach w postaci newslettera. Sprzedaż w Internecie jest możliwa dzięki szeroko rozumianym działaniom marketingowym:

- pozycjonowanie strony w wyszukiwarkach,
- reklamy Google AdWords,
- marketing szeptany,
- inne działania e-marketingowe mające na celu zwiększenie sprzedaży.

Reklama w Internecie posiada dużą przewagę nad pozostałymi kanałami promocji. To sami użytkownicy znajdują naszą ofertę. Dlatego osoby odwiedzające stronę firmy są zainteresowane jej produktami, gdyż same ją wyszukały lub otworzyły odnośnik do strony przedsiębiorstwa.

Przedsiębiorcy są aktywnie (za pośrednictwem tabeli opłat i prowizji) zachęcani do korzystania z Internetu przez bardzo istotnego uczestnika rynku, jakim są banki. Obecnie praktycznie każdy prowadzi obsługę rachunków w trybie online (przez Internet), a wiele umożliwia realizację przelewów w czasie rzeczywistym. W połączeniu z e-fakturami rozliczenia między podmiotami można skrócić do kilku godzin. Skrócenie czasu oczekiwania na zapłatę umożliwia szybszą dystrybucję towarów czy usług. Skraca się również okres oczekiwania na zamówiony towar, co wpływa bezpośrednio na brak konieczności utrzymywania wysokich stanów magazynowych.

Obowiązujące regulacje prawne wymuszają na przedsiębiorstwach korzystanie z Internetu. Podstawowe akty prawne takie jak Dziennik Ustaw czy Monitor Polski publikowane są **wyłącznie w postaci elektronicznej** i dostępne na stronach http://www.dziennikustaw.gov.pl/ i http://www.monitorpolski.gov.pl/.

15 Szapiro T. , op. cit., s. 74

Internet wykorzystywany jest przez przedsiębiorców głównie do komunikacji z:

- **ZUS** – korzystając z aplikacji PŁATNIK (przedsiębiorca) wysyła miesięczne raporty rozliczeniowe oraz deklaracje zgłoszeniowe. Uruchomiona przez ZUS Platforma Usług Elektronicznych (PUE) pozwala dodatkowo na sprawdzenie danych osób zgłoszonych do ubezpieczeń, złożenie wniosku i uzyskanie zaświadczenia o niezaleganiu, złożenie innych wniosków dotyczących rozliczeń, zobaczenie zestawienia deklaracji i wpłat,

- **urzędem skarbowym** – za pośrednictwem strony e-deklaracje można złożyć większość obowiązujących deklaracji podatkowych. Podatnik otrzymuje potwierdzenie złożenia deklaracji oraz jej poprawności formalnej i zgodności z obowiązującym wzorem,

- **ePUAP (Elektroniczna Platforma Usług Administracji Publicznej)** – portal obsługujący komunikację z urzędami administracji publicznej, pozwalający na zdalne załatwienie większości spraw,

- **PFRON**, który opracował system e-PFRON2 służący do składania deklaracji lub informacji przez teletransmisje danych w formie dokumentu elektronicznego przez pracodawców zobowiązanych do wpłat lub zwolnionych z wpłat na rzecz PFRON. Jest to jedyna forma składania deklaracji,

- **GUS** prowadzącym portal https://form.stat.gov.pl/edeklaracje, który służy do składania wszystkich deklaracji statystycznych,

- **NFZ**, który dopuszcza wyłącznie elektroniczne rozliczanie świadczeniodawców za pośrednictwem Internetu (SZOI lub Portal Świadczeniodawcy).

Wymiana dokumentów elektronicznych między podmiotami wymaga złożenia wiarygodnego podpisu cyfrowego, który zabezpieczy dokumenty i wiadomości elektroniczne przed nieuprawnioną modyfikacją i fałszerstwem oraz zapewni autentyczność pochodzenia (pewność co do autorstwa) i niezaprzeczalność. W zależności od skutków prawnych działania stosowane są różne formy podpisu cyfrowego:

- **kwalifikowany –** w ramach kontaktów między danymi kontrahentami, realizowany za pośrednictwem zabezpieczonego konta i haseł – stosowany jest w operacjach o niewielkiej wartości w relacjach między kontrahentami związanymi odrębnymi

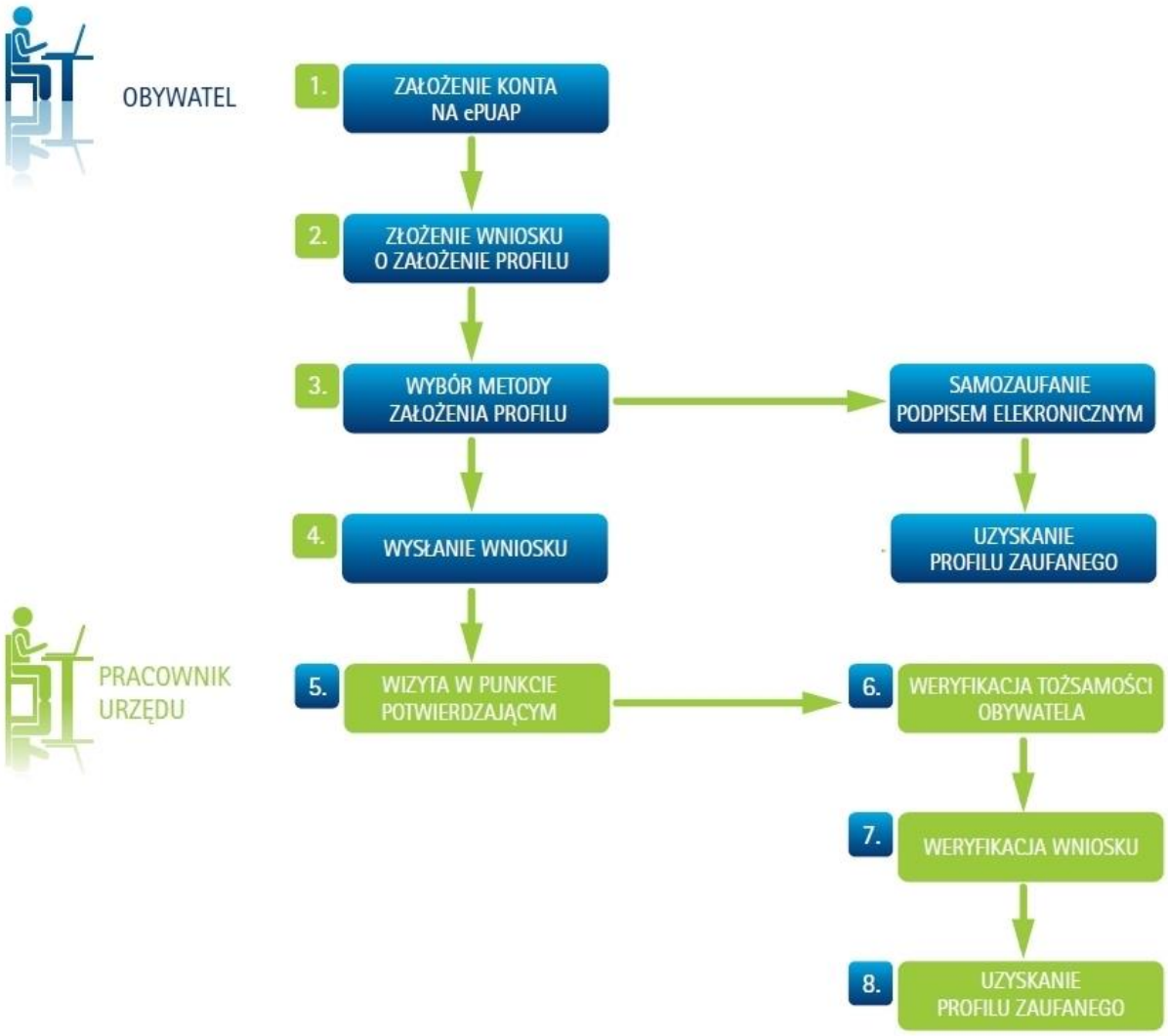
umowami, które sankcjonują taką autoryzację,

- **profil zaufany –** uzyskiwany np. za pośrednictwem ePUAP – wykorzystywany głównie do autoryzacji dokumentów w komunikacji z urzędami administracji państwowej i samorządowej. Profil zaufany jest bezpłatną metodą potwierdzania tożsamości obywatela w systemach elektronicznej administracji – to odpowiednik bezpiecznego podpisu elektronicznego, weryfikowanego certyfikatem kwalifikowanym,

- **podpis elektroniczny –** przypisany jest zawsze do osoby fizycznej, która może działać w imieniu podmiotu gospodarczego. Kwalifikowany podpis elektroniczny oznacza korzystanie z certyfikatu wystawionego przez kwalifikowany urząd certyfikacji. Podpis ten może być jeszcze opatrzony znacznikiem czasu gwarantującym autentyczność podpisu i czasu jego złożenia. Podpis elektroniczny wydawany jest na określony czas i jego posiadanie wiąże się z opłatami. Każdorazowe opatrzenie dokumentu znacznikiem czasu również wiąże się z opłatą (w praktyce kupuje się jednorazowo określoną liczbę znaczników czasu).

Profil zaufany ePUAP zawiera następujące dane użytkownika: imię i nazwisko, numer PESEL, identyfikator, identyfikator profilu zaufanego ePUAP, czas jego potwierdzenia, termin ważności, adres poczty elektronicznej, określenie sposobu autoryzacji. Termin ważności profilu zaufanego wynosi 3 lata i odnawiany jest na taki sam okres czasu.

Procedurę uzyskania profilu zaufanego ePUAP przedstawia rys.8.



Rys. 8. Schemat uzyskania profilu zaufanego

Źródło: http://epuap.gov.pl/wps/portal/E2_ZalozProfil

Procedura uzyskania kwalifikowanego podpisu elektronicznego jest bardzo podobna, jednak zamiast urzędu występuje w niej kwalifikowany urząd certyfikacji. Korzystanie z podpisu elektronicznego polega na stosowaniu bezpiecznych urządzeń do jego składania tzn. karty kryptograficznej z czytnikiem oraz zabezpieczonych haseł. Każda osoba składająca podpis elektroniczny powinna mieć świadomość, że jest on równoznaczny ze standardowym podpisem odręcznym.

4. Cyfrowe wykluczenie

Funkcjonowanie w ramach B2B, B2C czy B2E jest suwerenną decyzją przedsiębiorstwa opartą na kalkulacji, specyfice działalności, determinacji kierownictwa i pracowników. Znacznie poważniejszym problemem jest współpraca w ramach B2A – zależy

ona nie tylko od przedsiębiorców, ale w dużym stopniu od otoczenia gospodarczego i obowiązujących regulacji prawnych. Już teraz firmy zgłaszające do ubezpieczenia więcej niż 5 osób muszą składać deklaracje elektroniczne za pomocą Internetu. Składanie deklaracji podatkowych w postaci elektronicznej jest też obowiązkowe dla coraz większej liczby podmiotów gospodarczych. Odrębną grupą są firmy prowadzące działalność w zakresie ochrony zdrowia, które rozliczają się z NFZ. Dla nich jedyną formą rozliczeń jest postać elektroniczna z wykorzystaniem Internetu. Obowiązek prowadzenia elektronicznej dokumentacji medycznej wymusi aktywne korzystanie z Internetu przez wszystkich świadczących usługi medyczne, niezależnie od sposobu rozliczania działalności.

Zmiany przepisów i otoczenia gospodarczego narażają na cyfrowe wykluczenie dużą grupę przedsiębiorców – głównie tych, którzy nie chcą lub nie są w stanie wdrożyć technologii internetowych. Istotnym elementem, który zmniejsza wykluczenie cyfrowe, jest powszechna dostępność infrastruktury w postaci tanich łączy Internetu szerokopasmowego.

Ze względu na poziom informatyzacji i wykorzystania Internetu do prowadzenia działalności gospodarczej można wyróżnić:

- podmioty nieaktywne,
- podmioty bierne,
- podmioty aktywne.

Podmioty nieaktywne nie korzystają z dostępu do sieci. Nie dostrzegają korzyści i bagatelizują zagrożenia, które wynikają z nieprowadzenia działalności na wirtualnym rynku. Podmioty bierne to osoby fizyczne lub prawne, które korzystają z sieci Internet sporadycznie. Podmioty gospodarcze tej grupy w chwili obecnej nie wiążą swej strategii działania z aktywnością w Internecie. Najczęściej korzystają z poczty elektronicznej, przeglądają strony internetowe, nie dokonując transakcji internetowych. Do podmiotów aktywnych zaliczają się natomiast:

- przedsiębiorstwa pochodzące z tradycyjnych obszarów działalności,
- przedsiębiorstwa o mieszanych obszarach działalności: tradycyjny (stacjonarny) i internetowy,
- przedsiębiorstwa o wyłącznie internetowych formach aktywności.

Problem wykluczenia cyfrowego rozpatrywać można również w kontekście łatwości

dostępu oraz poziomu wykorzystania technik internetowych w podmiotach gospodarczych. Przeprowadzone w 2011 r. przez ONZ w 161 krajach badanie różnic w poziomie wykorzystania ICT przez przedsiębiorstwa o różnej skali działania pokazało, że w największym stopniu nowe technologie adaptowane i stosowane są w dużych firmach, zaś w najmniejszym stopniu w mikroprzedsiębiorstwach[16]. Różnice w tempie dyfuzji nowych technologii determinują szanse powodzenia podmiotu na rynku. Skuteczna walka o konsumenta wymaga aktywnych narzędzi komunikacji marketingowej. Zjawisko przenoszenia się wielu dziedzin życia gospodarczego i społecznego do Internetu wymaga od firm podążania za zmianami, jakie niesie za sobą wirtualny świat. Sieć udostępnia wiele aktywnych form przekazu, za pomocą których można dotrzeć do klienta ze skutecznością, której pozazdrościć mogą wszystkie tradycyjne media. Co więcej, dzięki technologiom interaktywnym istniejące formy komunikacji marketingowej zwiększyły swoją skuteczność. Obecność firmy w sieci stała się koniecznością. Internet stał się źródłem niezwykle cennych informacji o klientach, a jego umiejętne wykorzystanie przez podmioty gospodarcze pozwala na zaplanowanie skutecznej strategii działania. Bierność w podążaniu za zmianami oraz niezauważanie konieczności uwzględnienia Internetu w strategii funkcjonowania przedsiębiorstwa w krótkim okresie przyczyni się do zmniejszenia udziału w rynku – spadku liczby zamówień. W długim czasie może natomiast doprowadzić do całkowitej marginalizacji przedsiębiorstwa i jego likwidacji.

5. Wsparcie informatyzacji przedsiębiorstw w nowych projektach europejskich. Podsumowanie

Przedsiębiorstwa, które chcą zwiększać stopień informatyzacji swojej organizacji, mogą liczyć na wsparcie Unii Europejskiej dostępne w ramach Regionalnych Programów Operacyjnych czy też w ramach Programu Operacyjnego Innowacyjna Gospodarka. Dzięki temu firmy mogą uzyskać fundusze przeznaczone właśnie na wdrożenie systemów informatycznych. W 2013 r. przewidziano dofinansowanie wdrażania elektronicznego biznesu typu B2B z przeznaczeniem na realizację projektów o charakterze technicznym, informatycznym i organizacyjnym, które prowadzą do realizacji procesów biznesowych w formie elektronicznej obejmujących trzech lub więcej współpracujących przedsiębiorców. Wsparcie może być udzielone przedsiębiorcy, który planuje rozpoczęcie lub rozwój współpracy w oparciu o rozwiązanie elektroniczne, w szczególności przez dostosowanie

16 UNCTAD, Information Economy Report, 2011, s. 25

własnych systemów informatycznych do systemów informatycznych przedsiębiorców, z którymi kooperuje. Typowy projekt obejmuje integrację systemów informatycznych przedsiębiorstw lub wdrażanie nowych systemów, które mają na celu umożliwienie automatyzacji wymiany informacji między systemami informatycznymi współpracujących przedsiębiorstw. Projekty mogą być objęte wsparciem przez okres nie dłuższy niż 24 miesiące.

Jednym z głównych priorytetów programów regionalnych jest „Społeczeństwo informacyjne", w ramach którego można uzyskać dofinansowanie np. rozbudowy infrastruktury informatycznej.

Program Innowacyjna Gospodarka obejmuje między innymi działania „Przeciwdziałanie wykluczeniu cyfrowemu – eInclusion".

Informatyzacja przedsiębiorstw jest uwzględniania również w projektach europejskich na lata 2014-2020. W załącznikach przedstawiono:

- zestawienie adresów centralnych ewidencji i baz danych wykorzystywanych w działalności gospodarczej,
- wykaz dotychczasowych projektów oraz tych na lata 2014-2020,
- adresy wybranych stron internetowych zawierających informacje ułatwiające implementację rozwiązań informatycznych w przedsiębiorstwie.

6. Załączniki

Internet jest zasobem bardzo wielu informacji niezbędnych do prowadzenia działalności gospodarczej. Podstawowe dane można pozyskać ze stron:

- https://ems.ms.gov.pl/krs/wyszukiwaniepodmiotu?t:lb=t – dane podmiotów wpisanych do KRS,
- https://prod.ceidg.gov.pl/ceidg.cms.engine/ - dane podmiotów wpisanych do Centralnej Ewidencji i Informacji o Działalności Gospodarczej,
- http://www.stat.gov.pl/regon/ - rejestr REGON,
- https://ems.ms.gov.pl/msig/przegladaniemonitorow - opublikowane przez Ministerstwo Sprawiedliwości Monitory Sądowe i Gospodarcze,
- http://ekw.ms.gov.pl – centralna ewidencja ksiąg wieczystych,
- http://dokumenty.rcl.gov.pl – Rządowe Centrum legislacji publikujące obowiązujące teksty Dziennika Ustaw, Monitora Polskiego, Dzienniki Urzędowe,
- http://www.nbp.pl/home.aspx?f=/Kursy/kursy_archiwum.html - kursy walut publikowane przez NBP,
- http://bazy.uprp.pl/patentwebaccess/databasechoose.aspx?language=polski – baza Urzędu Patentowego RP.

Internet w pracy i rozwoju przedsiębiorstw, upowszechnienie technologii cyfrowych jest jednym z priorytetów Unii Europejskiej i wszystkich krajów członkowskich. W celu jego realizacji uruchomiono wiele przedsięwzięć finansowanych ze środków publicznych, np.:

- Portal Funduszy Europejskich (http://www.funduszeeuropejskie.gov.pl) prowadzony przez Ministerstwo Infrastruktury i Rozwoju obejmujący podstrony dla poszczególnych programów:
  - realizowanych w latach 2014-2020:
    - Infrastruktura i Środowisko (http://www.pois.gov.pl/2014_2020/Strony/glowna.aspx),
    - Inteligentny Rozwój (http://www.poig.gov.pl/2014_2020/Strony/glowna.aspx),
    - Wiedza Edukacja Rozwój (http://www.efs.gov.pl/2014_2020/Strony/glowna.aspx),
    - Polska Cyfrowa (http://www.funduszeeuropejskie.gov.pl/polska_cyfrowa/Strony/glowna.aspx),

- Polska Wschodnia (http://www.polskawschodnia.gov.pl/2014_2020/Strony/glowna.aspx),
- Pomoc Techniczna (http://www.popt.gov.pl/2014_2020/Strony/glowna.aspx),
- Europejska Współpraca Terytorialna i Europejski Instrument Sąsiedztwa (http://www.ewt.gov.pl/2014_2020/Strony/glowna.aspx),
- Programy Regionalne (http://www.funduszeeuropejskie.gov.pl/RPO/Aktualnosci/Strony/default.aspx#zakladka=4&strona=1)

○ realizowanych w latach 2007-2013:

- Program Kapitał Ludzki EFS (http://www.efs.gov.pl)
- Program Innowacyjna Gospodarka (http://www.poig.gov.pl)
- Program Infrastruktura i Środowisko (http://www.pois.gov.pl)
- Programy Europejskiej Współpracy Terytorialnej (http://www.ewt.gov.pl)
- Program Rozwoju Polski Wschodniej (http://www.polskawschodnia.gov.pl)
- Program Pomoc Techniczna (http://www.popt.gov.pl)
- Programy Regionalne (http://www.funduszeeuropejskie.gov.pl/RPO)

- PARP (http://www.parp.gov.pl) – Polska Agencja Rozwoju Przedsiębiorczości
- KSU (http://ksu.parp.gov.pl) – Krajowy System Usług

W celu opracowania strategii rozwoju ważnych dla Europy sektorów gospodarki i przyszłościowych technologii Komisja Europejska tworzy Platformy Technologiczne (więcej informacji na stronach http://www.kpk.gov.pl). Jednym z głównych zadań Platform ma być ustanowienie efektywnego partnerstwa publiczno-prywatnego dla wdrożenia przygotowanych strategii. Funkcjonują już między innymi:

- Polska Platforma Technologii Informatycznych (http://www.kpk.gov.pl/ppt/ppt.html?id=939)
- Polska Platforma Technologii Mobilnych i Komunikacji Bezprzewodowej (http://www.kpk.gov.pl/ppt/ppt.html?id=818)
- Polska Platforma Technologiczna Inteligentnych Systemów Transportowych (http://www.kpk.gov.pl/ppt/ppt.html?id=998)
- Polska Platforma Technologiczna Procesów Produkcji (http://www.kpk.gov.pl/ppt/ppt.html?id=824)
- Platforma informatyczna wspomagająca transfer wyników badań do praktyki

gospodarczej (http://platforma-inf.itee.radom.pl/)

- Zintegrowane Laboratoria Zrównoważonych Technologii Eksploatacji (http://www.programinwestycyjny-poig.itee.radom.pl/index.php)
- Innowacyjne systemy wspomagania technicznego zrównoważonego rozwoju gospodarki (http://www.programstrategiczny-poig.itee.radom.pl/index.php)
- Portal Innowacji (http://www.pi.gov.pl/parp/chapter_86000.asp)

Wiele firm stara się stymulować rozwój przedsiębiorstw organizując Internetowe platformy edukacyjne pozwalające na łatwe pozyskiwanie wiedzy i niezbędnych umiejętności. Jedną z nich jest Akademia PARP (http://www.akademiaparp.gov.pl), która posiada w swoich zasobach między innymi szkolenia:

- Biznesplan
- Marketing internetowy i e-commerce w MŚP
- Badanie rynku
- E-biznes
- Jak założyć własną firmę?
- Zarządzanie kryzysowe
- Plan marketingowy w MMŚP
- Negocjacje handlowe w MŚP
- Komunikacja marketingowa i public relations
- Jak rozwijać firmę
- Zarządzanie sprzedażą i relacjami z klientem
- Zabezpieczanie transakcji handlowych
- Zamówienia publiczne
- Techniki sprzedaży
- Pozyskiwanie funduszy UE na projekty w MŚP
- Telesprzedaż

7. Literatura

1. Bajdak A., *Internet w marketingu*, Warszawa 2003
2. Bednarczyk H., Koprowska D., Kacak I., *Transfer wiedzy i usług wsparcia dla mikroprzedsiębiorstw – doświadczenia, refleksje*, Radom 2008
3. Chmielarz W., *Systemy biznesu elektronicznego*, Warszawa 2007
4. Kirch O., Dawson T., *Linux - podręcznik administratora sieci*, Warszawa 2000
5. Pytlak M., *Analiza wpływu nowych elementów formatowania zawartych w HTML5 i CSS3 na wygląd i zawartość treściową strony w przeglądarkach internetowych*, [w:] *Informatyka w dobie XXI wieku. Nauka, technika, edukacja a nowoczesne technologie informatyczne*, A. Jastriebow (red.), Radom 2011, s. 281-282
6. Pronobis D., *Podstawy obsługi komputera i korzystania z Internetu. Podręcznik z ćwiczeniami dla ucznia*, Warszawa 2009
7. Zieliński Z., *E-learning w edukacji. Jak stworzyć multimedialną i w pełni interaktywną treść dydaktyczną*, Gliwice 2012
8. Szapiro T., Ciemniak R., *Internet – nowa strategia firmy*, Warszawa 1999
9. Szczepańska K., *Zastosowanie Internetu w marketingu jako przykład wykorzystania zasobów sieci w zarządzaniu przedsiębiorstwem*, Zeszyty Naukowe Wyższej Szkoły Biznesu w Dąbrowie Górniczej, NR 1(7), Dąbrowa Górnicza 2000
10. UNCTAD, *Information Economy Report*, 2011
11. Strona Insert S.A. - http://www.insert.com.pl
12. Encyklopedia PWN - http://encyklopedia.pwn.pl
13. Uczelniana Platforma E-LERNINGOWA AGH - http://upel.agh.edu.pl/kokpit
14. Platforma usług elektronicznych ZUS - https://pue.zus.pl
15. Ministerstwo Finansów, Systemy Informatyczne, Deklaracje Elektroniczne - http://www.finanse.mf.gov.pl/systemy-informatyczne/e-deklaracje
16. Portal Elektronicznych Usług Administracji Publicznej - http://epuap.gov.pl
17. Portal Państwowego Funduszu Osób Niepełnosprawnych - http://www.e-pfron.pl/
18. Portal Krajowego Systemu Usług dla Małych i Średnich Przedsiębiorstw - http://ksu.parp.gov.pl
19. Portal Funduszy Europejskich, Program Kapitał Ludzki - http://www.efs.gov.pl

Znaczenie partnerstwa publiczno-prywatnego w nowej perspektywie finansowej 2014-2020 (kontekst cyfryzacji)

Maciej Perkowski, Wojciech Zoń[1]

Okres transformacji w Polsce wymusił na administracji publicznej duże zmiany. Należało porzucić okowy poprzedniego systemu i wprowadzić bardziej demokratyczne, europejskie standardy. Nie robiono tego jednak obok obywatela – te zmiany musiały być widoczne przede wszystkim dla niego. Administracja musiała porzucić traktowanie obywatela przedmiotowo, wypracowując podejście partnerskie. Odnosiło się to również do osób prowadzących działalność gospodarczą, która zaczęła się kształtować od zera. Jednak standardy partnerstwa instytucji publicznych i podmiotów prywatnych systematyzowano niezwykle powoli. Stąd też późne ukształtowanie się formuły partnerstwa publiczno-prywatnego – istotnej, choć ciągle zbyt mało popularnej formy współpracy na rzecz realizacji interesu publicznego. Jednak w nowej perspektywie finansowej 2014-2020 warto zacząć korzystać powszechniej z tej formuły – będzie to przede wszystkim szansa na rozwój cyfryzacji i walkę z wykluczeniem cyfrowym. Są to sprawy szczególnie ważne dla północno-wschodniej Polski – to ostatnia szansa na nadrobienie braków i budowanie stabilnego rozwoju infrastruktury, przedsiębiorstw i społeczeństwa.

Partnerstwo publiczno-prywatne

Partnerstwo publiczno-prywatne (PPP), jak wskazują badania i praktyka – „nie tylko w wymiarze genealogicznym, ale i perspektywicznym – stanowi międzynarodowy kompromis koncepcyjny. To spostrzeżenie skłania zaś do wniosku, że PPP jest „międzynarodowe z natury”[2]. Wielu badaczy twierdzi, że ta idea w Polsce, podobnie jak w Holandii, Japonii i Republice Południowej Afryki, wywodzi się z modelu brytyjskiego. Jest to jednak błędne założenie, bowiem instytucja ta była wcześniej stosowana w naszym kraju i to w sposób odmienny niż w Wielkiej Brytanii. Niektóre z projektów zrealizowanych na przełomie lat osiemdziesiątych i dziewięćdziesiątych można zakwalifikować jako projekty partnerstwa publiczno-prywatnego, realizowane w oparciu o przepisy prawne i zasadę

[1] Autorem opracowania jest M. Perkowski, jednak współpraca w zakresie wstępnej selekcji materiałów i przygotowania fragmentów roboczych uzasadnia rozciągnięcie współautorstwa tekstu na W. Zonia.
[2] M. Perkowski, *Partnerstwo publiczno-prywatne w ujęciu międzynarodowym. Natura koncepcji*, w: *Partnerstwo publiczno-prywatne. Zagadnienia teorii i praktyki*, pod. red. M. Perkowskiego, Białystok 2007, s. 50.

wolności gospodarczej, która została sformułowana w Ustawie z dnia 23 grudnia 1988 r. o działalności gospodarczej. Partnerstwo publiczno-prywatne w Polsce nie jest wzorowane na żadnym znanym modelu – z tego też powodu budzi kontrowersje i problemy praktycznego jego wykorzystania (tym bardziej, że nie istnieje jednolita definicja PPP). Pierwszą ustawą, która regulowała *de facto* jeden z modeli PPP, była Ustawa z dnia 27 października 1994 r. o autostradach płatnych[3]. Regulacje w niej zawarte przewidywały wprowadzenie systemu koncesyjnego w odniesieniu do budowy autostrad płatnych w Polsce. Jednak była to regulacja o tyle nietrafiona, że udało się dzięki niej zrealizować zaledwie jeden projekt: odcinek A2 Nowy Tomyśl – Konin, który realizowała Autostrada Wielkopolska SA. Udział finansowy Skarbu Państwa ograniczył się jedynie do gwarancji Skarbu Państwa w stosunku do kredytu, jakiego udzielił wykonawcy Europejski Bank Inwestycyjny.

Formalnie koncepcja partnerstwa publiczno-prywatnego pojawiła się w Polsce w 2005 r. poprzez Ustawę z dnia 28 lipca 2005 r. o partnerstwie publiczno-prywatnym[4], która jednak nie działała w praktyce (pomimo istnienia przepisów wykonawczych do tej ustawy). W 2009 r. po raz kolejny podjęto próbę uregulowania tej kwestii – tym razem z lepszym skutkiem. Zgodnie z artykułem 1.2. nowej Ustawy z dnia 19 grudnia 2009 r. o partnerstwie publiczno-prywatnym[5] „przedmiotem partnerstwa publiczno-prywatnego jest wspólna realizacja przedsięwzięcia oparta na podziale zadań i ryzyk pomiędzy podmiotem publicznym i partnerem prywatnym”[6] w ramach współpracy między tymi podmiotami na podstawie odpowiedniej umowy. Chodzi tu zatem nie tylko o realizację przedsięwzięć infrastrukturalnych, lecz także o usługi publiczne z obszaru dotychczas zmonopolizowanego przez administrację, które w ramach PPP miałby świadczyć partner prywatny (choć formalnie byłoby to świadczenie wspólne – publiczne i prywatne jednocześnie). Do zaistnienia partnerstwa publiczno-prywatnego potrzebna jest umowa regulująca zasady realizacji partnerskiego przedsięwzięcia wypracowana w ramach ustawowych procedur[7]. Te ostatnie muszą zweryfikować zasadność powierzenia zadania publicznego partnerowi prywatnemu. Należy podkreślić, że nie wszystkie zadania mogą być wykonane przez podmioty publiczne w sposób efektywny, biorąc pod uwagę przede wszystkim stan finansowy i ograniczone możliwości sfery publicznej – szczególnie na poziomie samorządowym. W tym kontekście

[3] Ustawa z dnia 27 października 1994 r. o autostradach płatnych, Dz. U. 1994 nr 127 poz. 627 z późn. zm.
[4] Ustawa z dnia 28 lipca 2005 r. o partnerstwie publiczno-prywatnym, Dz. U. 2005 nr 169 poz. 1420 z późn. zm.
[5] Ustawa z dnia 19 grudnia 2008 r. o partnerstwie publiczno-prywatnym, Dz. U. z 2009 r., nr 19, poz. 100 z późn. zm.
[6] Art. 1.2. Ustawy z dnia 19 grudnia 2008 r. o partnerstwie publiczno-prywatnym… op. cit.
[7] *Partnerstwo publiczno-prywatne jako metoda realizacji zadań publicznych*, Departament Polityki Regionalnej, Ministerstwo Gospodarki i Pracy, Warszawa 2005, s. 14.

ważny jest cel współpracy publiczno-prywatnej, a mianowicie wspólne działanie na rzecz „interesu publicznego". To ostatnie pojęcie jest kształtowane na bieżąco w praktyce. Obecnie można je określić jako zbiór dóbr, wartości przypisanych do sektora publicznego, ale również wspólnoty (obywateli, lokalnej społeczności). Zadaniem administracji publicznej jest poszanowanie tych wartości poprzez prowadzenie działań sprzyjających ich zachowaniu i umożliwiających rozwój. Nie mogąc w pełni zaspokoić oczekiwań społeczeństwa w tym względzie, administracja publiczna może zwrócić się do partnera zewnętrznego, który udzieliłby jej wsparcia. Tu właśnie użyteczna staje się formuła PPP, w ramach której realizowane będą zadania finansowania, budowy (jak też odbudowy), zarządzania, a także utrzymania infrastruktury lub dostarczania usług publicznych, jakie zobowiązuje się wykonać partner prywatny na podstawie odpowiedniej umowy na rzecz administracji publicznej. Partner prywatny jest wynagradzany za realizację zadań w sposób zapewniający mu zysk, a dla administracji oznacza to oszczędność lub lepsze wykonanie danego zadania. Oczywiście „wynagrodzenie partnera prywatnego zależy przede wszystkim od rzeczywistego wykorzystania lub faktycznej dostępności przedmiotu partnerstwa publiczno-prywatnego"[8]. Współpraca w ramach partnerstwa publiczno-prywatnego jest na ogół długoterminowa, łącząc w sobie zróżnicowane wymiary danego projektu, a w jej ramach zazwyczaj wymagany jest wysoki kapitał początkowy. Jej konstrukcja opiera się o „produkt końcowy" oraz montaż finansowy kapitału prywatnego ze środkami innych uczestników tego procesu, np. pozyskanymi od instytucji finansujących, a czasem od podmiotu publicznego. Jednak to partner prywatny ponosi najczęściej ryzyko kapitałowe podczas realizacji danego projektu. Partner prywatny zapewnia wykonywanie poszczególnych elementów określonego projektu, natomiast podmiot publiczny skupia się na identyfikacji interesu publicznego. Koncentruje się on również na poziomie jakości, jak też mechanizmie cenowym rządzącym projektem. Podmiot publiczny odpowiada również za monitoring i kontrolę zrealizowanego przedsięwzięcia. Oba podmioty (prywatny i publiczny) łączy optymalny podział ryzyk, zgodnie z zasadą, że określonym ryzykiem obciąża się ten podmiot, który potrafi nim najsprawniej zarządzać[9].

PPP – w swym założeniu – przynosi różnorodne korzyści, w tym zwłaszcza:

- „zwiększenie strumienia kapitału, który zostanie przeznaczony na inwestycje w sferze usług publicznych poprzez pozyskanie kapitału prywatnego,

[8] Art. 7.2. Ustawy z dnia 19 grudnia 2008 r. o partnerstwie publiczno-prywatnym… op. cit.
[9] *Partnerstwo publiczno-prywatne jako metoda realizacji zadań publicznych*, op. cit., s. 4.

- pozyskanie wiedzy i doświadczenia sektora prywatnego i tym samym zwiększenie wydajności i jakości na polu wykonywania zadań publicznych,
- lepszy podział ryzyka w ramach realizowanego przedsięwzięcia,
- większą efektywność w wykorzystaniu zasobów i lepszą jakość usług,
- zwiększenie roli zarządczej sektora publicznego,
- zapewnienie optymalnego zarządzania przedsięwzięciem przy jednoczesnym ograniczaniu jego kosztów całkowitych,
- możliwość generowania dodatkowych przychodów od osób trzecich w ramach przedsięwzięcia, co ogranicza potrzebę angażowania środków publicznych”[10].

Jednak pomimo wielu korzyści wynikających z PPP, nie jest to formuła zbyt popularna. Dzieje się tak głównie z powodu negatywnego nastawienia społeczeństwa do kontaktów instytucji publicznych z podmiotami prywatnymi. W opinii publicznej dominuje przeświadczenie o kryminogennym charakterze takich kontaktów, szczególnie w kontekście korupcji. W istocie „istnienie szerokich swobód charakterystycznych dla państw demokratycznych o gospodarce rynkowej stanowi często trudną do odparcia pokusę dla potencjalnych przestępców. Osoby te starają się maksymalnie wykorzystać przysługujące im prawa i wolności, a najczęściej swoim zachowaniem doprowadzają do ich nadużycia oraz złamania”[11]. Do obiegu potocznego przenikła deskrypcja skrótu „PPP”, jako „pewnie przyjdzie prokurator”. Mając na względzie rzeczywiste i wyimaginowane słabości tytułowej formuły, ze zdwojoną determinacją należy promować dobre praktyki i przystępnie podaną wiedzę o PPP, a zwłaszcza o możliwościach jego dofinansowania.

Projekty hybrydowe

Środki na realizację zadania publicznego w formule projektu PPP nie muszą pochodzić w całości od partnerów, gdyż istnieje możliwość dofinansowania tak zaplanowanego przedsięwzięcia z funduszy Unii Europejskiej. Mowa tu o tzw. projektach hybrydowych. Dotacja rozwojowa z funduszy europejskich w projektach PPP pozwala na realizację przedsięwzięć publicznych, które bez dotacji byłyby nierentowne. Ogranicza przy tym obciążenie partnera prywatnego, zmniejszając jego zapotrzebowanie na kredyt inwestycyjny, a gdyby ten okazał się jednak potrzebny – udział UE uwiarygodnia projekt

[10] Ibidem, s. 17.
[11] W. Filipkowski, *Wokół partnerstwa publiczno-prywatnego. Aspekty kryminologiczne i prawne*, w: *Partnerstwo publiczno-prywatne. Zagadnienia teorii i praktyki*, pod. red. M. Perkowskiego, Białystok 2007, s. 76-77.

wobec instytucji finansujących. Mimo tych zalet niewiele państw członkowskich (jak dotąd 7) opracowuje programy operacyjne, w których projekty PPP byłyby współfinansowane ze środków UE. Monitoring Komisji Europejskiej wskazuje, że sceptycyzm opiera się na obawie o skutek łączenia różnych unijnych i krajowych zasad i praktyk oraz harmonogramów w jednym projekcie (co dla beneficjentów może być skomplikowane i zniechęcające). Nie dziwi więc fakt, że w obecnym okresie budżetowym w Polsce zostało opracowanych niewiele projektów partnerstwa publiczno-prywatnego z udziałem wsparcia finansowego Unii Europejskiej. Jednak z drugiej strony wartość tych projektów przekracza aż 5 mld zł. Duży wpływ na to mają cztery projekty spalarniowe – łączny koszt ich realizacji wynosi ponad 4,4 mld zł, a wnioskodawcy starają się o dofinansowanie UE w wysokości ponad 1,5 mld zł. Warto dodać, że projekty te znajdują się na liście projektów kluczowych Programu Operacyjnego Infrastruktura i Środowisko. Może się więc wydawać, że najbardziej istotnym argumentem za hybrydowym projektowaniem spalarni stał się poziom długu publicznego poszczególnych samorządów. Samorządy założyły, że projekt nie może zwiększać długu publicznego, własność obiektu ma być dalej publiczna, a samorząd musi posiadać strategiczną kontrolę nad jakością, jak też cenami świadczonych usług. Formułę projektu hybrydowego zastosowano również w partnerstwach dotyczących rekreacji, jak na przykład termy i parki wodne (projekt Term Gostynińskich) oraz w PPP sportowo-rekreacyjnych – tutaj zainteresowaniem cieszy się w największym stopniu budowa i rozwój infrastruktury sportowej w modelu PPP/koncesji, co stanowi ok. 45% wszystkich postępowań. Dofinansowania UE mają znaczenie dla idei PPP nie tylko przez projekty hybrydalne. Od niedawna prowadzone są pierwsze przedsięwzięcia PPP na majątku wytworzonym dzięki projektom unijnym (jako przykład można tu podać koncesję na usługi wodno-kanalizacyjne w Będzinie). Można więc prognozować, że takich projektów będzie przybywało[12]. Na tę chwilę nie ma zbyt wielu projektów hybrydowych w Polsce. Wszystkie zostały przedstawione w tabeli poniżej (patrz Tabela nr 1.):

[12] M. Perkowski, *Wykonywanie zadań j.s.t. w trybie partnerstwa publiczno-prywatnego*, w: *Finanse samorządowe. 580 pytań i odpowiedzi. Wzory uchwał, deklaracji, decyzji, umów*, pod red. C. Kosikowskiego i J. M. Salachny, Warszawa 2012, s. 175-189.

Tabela nr 1. Projekty hybrydowe w Polsce – październik 2013

L. p.	1.	2.	3.	4.
Nazwa projektu	Kompleks mineralnych basenów w Solcu – Zdroju	Rewitalizacja dworca PKP oraz terenów przydworcowych w Sopocie	Budowa Wielkopolskiej Sieci Szerokopasmowej	System Gospodarki Odpadami dla Miasta Poznania
Nazwa beneficjenta	Gmina Solec Zdrój	Urząd Miasta Sopot	Wielkopolska Sieć Szerokopasmowa S.A. (WSS S.A.)	Urząd Miasta Poznań
Województwo	świętokrzyskie	pomorskie	wielkopolskie	wielkopolskie
Data zawarcia umowy PPP	09.01.200	23.01.2012	2010	8.04.2013
Data podpisania umowy o dofinansowanie/na pożyczkę	13.10.2011	7.01.2013	23.12.2010	5.10.2011
Wartość projektu (mln PLN)	19,83	95,78	407,11	757,83
Wartość Dofinansowania przez UE (mln PLN)	6,80	41,91	283,64	352,00
Program z jakiego pochodzą Środki UE	RPO Świętokrzyskie 2007-2013	RPO Pomorskie 2007-2013	RPO Wielkopolskie 2007-2013	POIiŚ 2007-2013
Sektor	sport i rekreacja	rewitalizacja	telekomunikacja	gospodarka odpadami

5.	6.	7.	8.	9.
Zarządzanie Sosnowieckim Parkiem Naukowo-Technologicznym (SPNT)	Zarządzanie infrastrukturą sportową stoku Dębowiec w Bielsku-Białej	Sieć szerokopasmowa Polski Wschodniej - województwo warmińsko-mazurskie	Małopolska Sieć Szerokopasmowa	Sieć szerokopasmowa Polski Wschodniej - województwo podkarpackie
Urząd Miasta Sosnowiec	Urząd Miasta Bielsko-Biała	Urząd Marszałkowski Województwa Warmińsko – Mazurskiego	Małopolska Sieć Szerokopasmowa sp. z o.o.	Urząd Marszałkowski Województwa Podkarpackiego
śląskie	śląskie	warmińsko-mazurskie	małopolskie	podkarpackie
25.07.2012	12.2012	19.04.2013	23.08.2013	26.09.2013
06.2010 08.2010	2010	16.11.2010	27.06.2013	11.03.2011
38,75	61,32	327,04	192,33	321,85
29,54	44,96	226,34	54,38	222,85
RPO Śląskie 2007-2013	RPO Śląskie 2007-2013	PO RPW 2007 - 2013	RPO Małopolskie 2007-2013	PO RPW 2007 - 2013
innowacje	sport i rekreacja	telekomunikacja	telekomunikacja	telekomunikacja

10.	11.	12.	13.	14.
Sieć szerokopasmowa Polski Wschodniej - województwo świętokrzyskie	Sieć szerokopasmowa Polski Wschodniej - województwo podlaskie	Sieć szerokopasmowa Polski Wschodniej - województwo lubelskie	Likwidacja obszarów wykluczenia informacyjnego i budowa dolnośląskiej sieci szkieletowej	Internet dla Mazowsza
Urząd Marszałkowski Województwa Świętokrzyskiego	Urząd Marszałkowski Województwa Podlaskiego	Urząd Marszałkowski Województwa Lubelskiego	Urząd Marszałkowski Województwa Dolnośląskiego	Samorząd województwa Mazowieckiego - Agencja Rozwoju Mazowsza S.A.
świętokrzyskie	podlaskie	lubelskie	dolnośląskie	mazowieckie
brak	brak	brak	brak	brak
27.01.2011	15.04.2011	21.01.2011	29.01.2013	28.09.2011
200,73	250,75	385,08	215,00	493,34
139,42	174,10	266,97	149,70	340,94
PO RPW 2007 - 2013	PO RPW 2007 - 2013	PO RPW 2007 - 2013	RPO Dolnośląskie 2007-2013	RPO Mazowieckie 2007 - 2013
telekomunikacja	telekomunikacja	telekomunikacja	telekomunikacja	telekomunikacja

15.	16.	17.
Budowa stacji gazowej wysokiego ciśnienia, sieci gazowej średniego ciśnienia relacja Dębowa Łąka - Książki - Jabłonowo Pomorskie wraz z siecią rozdzielczą średniego ciśnienia na terenie gminy Książki i gminy Jabłonowo Pomorskie - Etap I	Budowa stacji gazowej wysokiego ciśnienia, sieci gazowej średniego ciśnienia relacja Dębowa Łąka - Książki - Jabłonowo Pomorskie wraz z siecią rozdzielczą średniego ciśnienia na terenie gminy Książki i gminy Jabłonowo Pomorskie - Etap II	Rozbudowa Szpital Św. Wincentego a' Paulo Sp. z o.o. w Gdyni w celu rozszerzenia usług medycznych z uwzględnieniem udziału partnera prywatnego w ramach PPP
Gmina Książki	Gmina Książki	Miasto Gdynia Szpital Św. Wincentego A Paulo Sp. z o.o. Gdynia
kujawsko-pomorskie	kujawsko-pomorskie	pomorskie
brak	brak	brak
20.03.2013	20.03.2013	brak
7,72	8,14	70,00
2,63	2,78	52,50
RPO Kujawsko-Pomorskie 2007-2013	RPO Kujawsko-Pomorskie 2007-2013	RPO Pomorskie 2007-2013 instrument zwrotny JESSICA
efektywność energetyczna	efektywność energetyczna	ochrona zdrowia

Czy inwestować w umiejętności informatyczne pracowników?

18.	Budowa Centrum Przesiadkowego w Zabrzu	Miasto Zabrze	śląskie	brak	brak	214,32	160,74	RPO Śląskie 2007-2013 lub 2014-2020	rewitalizacja
19.	Kompleksowa termomodernizacja budynków oświatowych Gminy Świdnica w formule partnerstwa publiczno-prywatnego	Gmina Świdnica	lubuskie	brak	brak	1,31	1,29	RPO Lubuskie 2007-2013	efektywność energetyczna

Źródło: Zestawienie na podstawie opracowania Departamentu Wsparcia Projektów Partnerstwa Publiczno-Prywatnego w Ministerstwie Rozwoju Regionalnego, na podstawie danych wygenerowanych z Krajowego Systemu Informatycznego SIMIK 2007-2013, Instytucji Zarządzających oraz analiz własnych.

Na podstawie powyższego zestawienia można stwierdzić, że choć projektów hybrydowych jest niewiele, to jednak ich wartość jest wysoka. Szczególnym optymizmem napawa fakt realizacji wielu projektów z sektora telekomunikacyjnego. Dzięki temu widać, jak wielką rolę PPP odgrywa w znoszeniu barier cywilizacyjnych na gruncie cyfryzacji i walką z cyfrowym wykluczeniem. Na osobne podkreślenie zasługuje kwestia PPP w obszarze rozwoju sieci szerokopasmowego dostępu do Internetu, który jest intensywnie wspierany przez Unię Europejską. Według Strategii Europa 2020 i Europejskiej Agendy Cyfrowej do 2020 r. każdy Europejczyk będzie posiadał dostęp do szybkiego Internetu o przepustowości przekraczającej 30-40 Mb/s, a co najmniej połowa wszystkich europejskich gospodarstw domowych będzie miała dostęp do Internetu i to o przepustowości przekraczającej aż 100 Mb/s.).

Przyspieszeniu procesu budowy szybkich sieci światłowodowych w Polsce sprzyja obowiązująca Ustawa z 7 maja 2010 r. o wspieraniu rozwoju sieci i usług telekomunikacyjnych[13], znana inaczej jako „Megaustawa". Zgodnie z jej treścią tym, co ma napędzać rozwój sieci szerokopasmowych, ma być powierzenie samorządom terytorialnym roli inwestora na rynku telekomunikacyjnym. Ma być tak zarówno na etapie budowania tych

[13] Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju sieci i usług telekomunikacyjnych, Dz. U. z 2010 r., nr 106, poz. 675.

sieci, jak **i** świadczenia usług telekomunikacyjnych. Jeżeli chodzi o szeroko pojętą telekomunikację, należy zauważyć, że od niedawna należy ona w Polsce do zadań własnych o charakterze użyteczności publicznej jednostek samorządu terytorialnego. Natomiast te ostatnie, będące składnikami gospodarki komunalnej, mogą być powierzone innym podmiotom w celu ich realizacji. Jest to możliwe szczególnie na podstawie umowy o PPP.

Ten scenariusz jawi się jako optymistyczny, zwłaszcza biorąc pod uwagę niedorozwój polskiej infrastruktury telekomunikacyjnej, powszechnego występowania „białych plam" oraz przeznaczenia na realizację tych celów środków UE o wartości przekraczającej 1 mld euro, zapotrzebowaniu na profesjonalne know-how i kapitał na wkład własny. W sposób oczywisty partnerstwo publiczno-prywatne tworzy doskonałe warunki do budowy internetowych sieci szerokopasmowych. Partner prywatny ma prawo wybudować oraz eksploatować sieć telekomunikacyjną, jak również zarządzać i utrzymywać infrastrukturę już istniejącą. Wynagrodzenie partnera prywatnego będzie pochodziło ze świadczenia usług na rzecz operatorów dostępowych. Będzie ono również efektem udostępniania sieci telekomunikacyjnej innym przedsiębiorcom telekomunikacyjnym. Jeżeli zaś chodzi o wybór partnera prywatnego, będzie on dokonywany w trybie ustawy o koncesjach (na roboty budowlane i usługi), albo też PZP (prawa zamówień publicznych)[14].

Perspektywa finansowa UE 2007-2013

W perspektywie finansowej 2007-2013 Polska była największym beneficjentem funduszy strukturalnych Unii Europejskiej. Brakowało jednak jasnych wytycznych co do możliwości łączenia PPP z funduszami europejskimi. Tutaj szansą okazały się inicjatywy unijne:

1. JASPERS (wspólna inicjatywa wsparcia projektów w regionach europejskich) – cel: pomoc na każdym etapie cyklu PPP lub projektu w obszarze infrastruktury;

2. JESSICA (wspólne europejskie wsparcie na rzecz trwałych inwestycji w obszarach miejskich) – cel: wspieranie trwałych inwestycji PPP w obszarach miejskich lub projektów w obszarach miejskich stanowiących część zintegrowanego planu rozwoju obszarów miejskich;

[14] M. Perkowski, *Wykonywanie zadań j.s.t. w trybie partnerstwa publiczno-prywatnego*, w: *Finanse samorządowe. 580 pytań i odpowiedzi. Wzory uchwał, deklaracji, decyzji, umów*, pod red. C. Kosikowskiego i J. M. Salachny, Warszawa 2012, s. 175-189.

3. JEREMIE (wspólne europejskie zasoby dla mikro-, małych i średnich przedsiębiorstw) – cel: wspieranie tworzenia nowych przedsiębiorstw i poprawy dostępu przedsiębiorstw do finansowania.

Komisja Europejska podkreśliła, że na poziomie unijnym formuła PPP może pomóc realizować projekty, które mają na celu między innymi: „zapobieganie zmianom klimatu, wspieranie alternatywnych źródeł energii oraz efektywności energetycznej i surowcowej, wspieranie transportu zorganizowanego z poszanowaniem zasady zrównoważonego rozwoju, zapewnianie niedrogiej opieki zdrowotnej na wysokim poziomie oraz realizację dużych projektów badawczych, takich jak wspólne inicjatywy technologiczne, mających na celu zapewnienie Europie pozycji lidera w obszarze technologii strategicznych”[15].

W nowej perspektywie finansowej na lata 2007 - 2013 – w projektach realizowanych w ramach regionalnych programów operacyjnych (RPO) oraz Programu Operacyjnego Rozwój Polski Wschodniej (PO RPW) – zaplanowano budowę sieci światłowodowych. Chodzi tu przede wszystkim o sieci szkieletowo-dystrybucyjne, dzięki którym będzie można uzupełnić braki w zakresie nowoczesnej infrastruktury telekomunikacyjnej w regionach, a także zwiększyć konkurencję przez zagwarantowanie operatorom ostatniej mili dostępu do infrastruktury na jednakowych warunkach. Podstawowym założeniem wszystkich projektów było objęcie jak największym zasięgiem sieci dystrybucyjnych ponad połowy obywateli i instytucji. Ze względu na skalę, wartość i prognozowane wskaźniki spośród wszystkich inwestycji, które będą realizowane w regionach, wyróżnić należy dziewięć (łączna wartość dofinansowania z EFRR wynosi ok. 1 mld zł)[16]. Zakładają utworzenie „15,8 tys. km sieci szkieletowo-dystrybucyjnych, co stanowi ponad 3/4 całości sieci szkieletowej i dystrybucyjnej zakładanej do realizacji w ramach 16 RPO. Natomiast w ramach projektów sieci szerokopasmowych PO RPW przewidziano infrastrukturę sieciową o łącznej długości 10,4 tys. km, za kwotę blisko 1,459 mld zł”[17]. Wsparcie dostarczania usługi szerokopasmowego dostępu do Internetu bezpośrednio do użytkownika (etap tzw. ostatniej mili) proponowane jest głównie w ramach działania 8.4 Programu Operacyjnego Innowacyjna

[15] *Wspieranie inwestycji publiczno-prywatnych krokiem w kierunku naprawy gospodarki i długoterminowej zmiany strukturalnej: zwiększanie znaczenia partnerstw publiczno-prywatnych*, Komunikat Komisji Wspólnot Europejskich do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, Bruksela, dnia 19.11.2009, KOM (2009) 615 wersja ostateczna, s. 8.
[16] *Diagnoza dla Programu Operacyjnego Polska Cyfrowa 2014-2020*, Warszawa 2013, www.funduszeeuropejskie.gov.pl/2014_2020/konsultacje/Documents/Zal_1_POPC%20ver30_Diagnoza_21013.pdf, s. 10 (02. 12. 2013).
[17] Ibidem, s.10.

Gospodarka (PO IG), II osi priorytetowej PO RPW, a także w niektórych RPO i w ramach Programu Rozwój Obszarów Wiejskich (PROW)[18].

W praktyce natrafiono na szereg problemów związanych z realizacją sieci dystrybucyjno-szkieletowych, takich jak: rozbudowany system pozyskiwania dofinansowania (w tym opracowywania dokumentacji aplikacyjnej), brak doświadczenia i kompetencji sektora publicznego (głównie w początkowej fazie uruchamiania projektów szerokopasmowych), stosunkowo długi czas procedur notyfikacyjnych (spowodowany indywidualną notyfikacją planowanej pomocy publicznej dla poszczególnych projektów), brak inwentaryzacji stanu infrastruktury szerokopasmowej w momencie przygotowania projektów. Nie obeszło się też bez trudności z realizacją sieci dostępowych, w tym zwłaszcza braku inwentaryzacji stanu infrastruktury szerokopasmowej (co faktycznie uniemożliwiało przeprowadzenie konkursów), negatywnego zjawiska tzw. blokowania miejscowości, wynikającego z zastosowania definicji „białej plamy" (zawartej w Wytycznych wspólnotowych w sprawie stosowania przepisów dotyczących pomocy państwa w odniesieniu do szybkiego wdrażania sieci szerokopasmowych[19]), a także problemów operatorów telekomunikacyjnych natury administracyjnej oraz finansowej (związanych głównie z uzyskaniem kredytów i gwarancji bankowych na etapie planowania i realizacji inwestycji)[20]. Problemy towarzyszyły też wdrażaniu w latach 2007-2013 interwencji w zakresie e-administracji[21]. Odnotowano brak kompleksowego i strategicznego podejścia do rozwoju elektronicznej administracji (co stwarzało ryzyko budowy silosowych, nie współpracujących ze sobą systemów, realizujących wąskie, wyspecjalizowane potrzeby poszczególnych instytucji i dublowania podejmowanych działań w ramach różnych projektów) i niewystarczającą koordynację między różnymi źródłami finansowania projektów e-administracji (m.in. PO Innowacyjna Gospodarka, PO Kapitał Ludzki oraz RPO) w połączeniu z brakiem szczegółowej analizy projektów pod względem komplementarności

[18] Ibidem, s. 10.

[19] Wytyczne wspólnotowe w sprawie stosowania przepisów dotyczących pomocy państwa w odniesieniu do szybkiego wdrażania sieci szerokopasmowych, Dz. Urz. UE C 235/7 z 30.09.2009. Wnioskodawcy deklarowali doprowadzenie Internetu do miejscowości, która przestawała być dostępna dla innych podmiotów, chcących złożyć wnioski na ten obszar. Realizowany projekt nie zapewniał jednak powszechnego dostępu do Internetu na tym terenie. Dopiero wprowadzenie definicji „białej plamy" jako obszaru, na którym poziom nasycenia usługami szerokopasmowego dostępu do Internetu o przepustowości min. 2 Mb/s w każdej miejscowości objętej projektem wynosi nie więcej niż 30%, rozwiązało ten problem i pobudziło konkurencję pomiędzy operatorami telekomunikacyjnymi działającymi na tym samym terenie oraz spowodowało ich zainteresowanie coraz bardziej zaawansowanymi technologiami (wyżej oceniany jest projekt gwarantujący lepsze parametry i szerszy dostęp). *Diagnoza dla Programu Operacyjnego Polska Cyfrowa 2014-2020…* op. cit.

[20] *Diagnoza dla Programu Operacyjnego Polska Cyfrowa 2014-2020…* op. cit.

[21] Zostały one zidentyfikowane i zaadresowane m.in. w ramach realizacji planu naprawczego dla osi 7 POIG (Remedial Action Plan), uzgodnionego między Polską a Komisją Europejską.

z innymi projektami informatycznymi wdrażanymi lub zrealizowanymi na poziomie centralnym i regionalnym. Zabrakło też właściwej koordynacji realizacji projektów (w oparciu o jasno zdefiniowane etapy – kamienie milowe, co częściowo przyczyniło się do opóźnień we wdrażaniu poszczególnych usług), monitorowania postępów w systemie wdrażaniu projektów (w tym niewystarczający nadzór nad zmianami w harmonogramach, brak prowadzonej analizy ryzyka, co stwarzało trudności w oszacowaniu poziomu zaawansowania wykonanych prac i ich rozliczeniu) oraz problemy: z zapewnieniem finansowej trwałości projektu lub jego efektów, z opóźnieniami prac legislacyjnych (powodującymi opóźnienia w realizacji projektów oraz brak możliwości wykorzystywania wdrożonych rozwiązań w praktyce), ze stosowaniem prawa zamówień publicznych (nie tylko wynikającym z niewystarczającej znajomości przepisów po stronie zamawiających, ale również z niewątpliwych wad tych przepisów, które realnie wpływały na trudności w ich stosowaniu). Ponadto zidentyfikowano ograniczoną zdolność instytucjonalną beneficjentów. Objawiała się ona między innymi brakiem zintegrowanego podejścia do realizacji danego projektu, bardzo rozciągniętymi w czasie pracami przygotowawczymi podczas tworzenia, ale też niedostatecznym doświadczeniem w procedurach dotyczących zamówień publicznych oraz błędną identyfikacją potrzeb interesariuszy i właściciela określonego procesu. Dalsze kwestie problematyczne dotyczyły m.in. kwestii kadrowych beneficjentów (fluktuacja, trudność w pozyskaniu i/lub finansowaniu odpowiednich kadr), niewystarczającej weryfikacji merytorycznej składanych przezeń wniosków o płatność i niedostatecznego wsparcia procesu prawidłowej realizacji projektów poprzez kontrole *ex-ante* udzielanych zamówień, a nawet braku spójnego systemu kontrolnego obowiązującego wszystkie instytucje, które posiadały stosowne uprawnienie wobec realizowanych projektów, i niejednolitych procedur antykorupcyjnych obowiązujących u beneficjentów projektów, co w konsekwencji oznaczało większe ryzyko zachowań korupcyjnych. Na tym tle problem kumulacji efektów rzeczowych oraz płatności w końcowych okresach realizacji projektów jawi się już „całkiem niewinnie”[22].

Nowa perspektywa finansowa UE 2014-2020

Nowy okres programowania różni się od poprzedniego – i to znacznie. Zmiany dotyczą przygotowywania dokumentów programowych i ich wdrażania oraz współfinansowania z budżetu UE najważniejszych polityk jak: Wspólnej Polityki Rolnej (WPR), Wspólnej Polityki Rybołówstwa (WPRyb) i Polityki Spójności (PS). Do

[22] *Diagnoza dla Programu Operacyjnego Polska Cyfrowa 2014-2020*… op. cit.

głównych kierunków tych zmian należy zaliczyć: realizację celów wynikających ze strategii Europa 2020, koncentrację tematyczną i koncentrację wsparcia, osiąganie konkretnych rezultatów, mierzonych konkretnymi wskaźnikami, wsparcie terytorialne[23]. Oprócz tego w nowej perspektywie wprowadza się:

- warunkowość *ex ante*;
- makrowarunkowść;
- warunkowość *ex post* (rezerwę wykonania);
- wielopoziomowe zarządzanie;
- współpracę partnerów, ich sieciowanie;
- decentralizację środków;
- umowę partnerską;
- kontrakt terytorialny;
- *ring fencing* – limit środków na poszczególne obszary tematyczne np. na gospodarkę niskoemisyjną[24].

Gwarantuje się także wsparcie dla trzech priorytetów Strategii „Europa 2020" – rozwoju inteligentnego (nacisk na rozwój wiedzy i innowacji tudzież kształcenia i technologii cyfrowych), rozwoju zrównoważonego (lepsze, bardziej efektywne wykorzystanie zasobów idące w parze ze zwiększaniem konkurencyjności) oraz rozwoju sprzyjającemu włączeniu społecznemu (podnoszenie kwalifikacji zawodowych społeczeństwa UE, zwiększanie aktywności zawodowej i walka z ubóstwem). Mają w tym pomóc fundusze trzech polityk unijnych: Polityki Spójności, Wspólnej Polityki Rolnej i Wspólnej Polityki Rybackiej[25].

W odpowiedzi na wskazane wyżej problemy sektora teleinformatycznego podjęto szereg działań zarówno strategicznych (powołanie 25 listopada 2011 r. Ministerstwa Administracji i Cyfryzacji; powołanie 5 stycznia 2012 r. Komitetu Rady Ministrów

[23] *Nowa perspektywa programowo – finansowa UE 2014 – 2020 – najważniejsze zmiany*, Centrum Doradztwa Rolniczego w Brwionowie, Oddział w Krakowie, Kraków 2013, www. cdrkursy.edu.pl/cdr/wydawnictwa/perspektywa2020.pdf, s. 2 (02. 12. 2013).
[24] Ibidem, s. 4. Por.: M. Perkowski, *Dalsze możliwości korzystania przez państwa członkowskie UE ze środków funduszy europejskich oraz środków wynikających z inicjatyw unijnych oraz stosowania instrumentów i mechanizmów finansowych UE*, w: *Przyszłość Unii Europejskiej w świetle jej ustroju walutowego i finansowego*, pod red. C. Kosikowskiego, Białystok 2013, s. 214-223.
[25] Ibidem, s. 5. Por.: M. Perkowski, *Dalsze możliwości korzystania przez państwa członkowskie UE ze środków funduszy europejskich…* op. cit.

ds. Cyfryzacji[26]; opublikowanie w kwietniu 2012 r. raportu „Polska 2.0. Nowy start dla administracji"), jak i wdrożeniowych, związanych z funkcjonowaniem instytucji systemu realizacji osi 7 POIG. Wszystkie te działania zostały wzięte pod uwagę przy planowaniu interwencji Programu Operacyjnego Polska Cyfrowa (POPC) na lata 2014-2020. W szczególności zaplanowano koncentrację interwencji w zakresie krajowych e-usług publicznych w jednym krajowym programie, z zapewnieniem mechanizmów współpracy w wyborze projektów między jego systemem realizacji a instytucjami zarządzającymi RPO oraz zasad współdziałania między interwencją POPC a interwencją w ramach celu tematycznego 11 realizowaną w Programie Operacyjnym Wiedza, Edukacja, Rozwój (POWER)[27]. Założono też odpowiednio wczesne zdefiniowanie projektów o priorytetowym charakterze, wyznaczenie właściwego porządku realizowanych projektów oraz rozpoczęcie prac przygotowawczych, a następnie koordynację i regularny nadzór nad realizacją projektów w ramach KRMC. Dla wszystkich przedsięwzięć informatyzacyjnych w administracji publicznej określono wymóg zalecanych uznanych metodyk zarządzania programami/projektami. Podjęto tez próbę udoskonalenia procesu oceny projektów, w szczególności poprzez zapewnienie odpowiednich kryteriów ich wyboru (odnoszących się m.in. do dokonania *ex-ante* analizy niezbędnych zmian prawnych oraz wykazania przez beneficjenta powiązań miedzy wdrażanymi „rozwiązaniami IT" a usprawnieniem realizowanych procesów administracyjnych w celu uniknięcia „digitalizacji chaosu") i zwiększony nacisk na jakość dokonanej analizy kosztów i korzyści. Projekty – począwszy od prac koncepcyjnych – powinny być realizowane przez zespoły odpowiedzialne za utrzymanie uzyskanych produktów projektu, czemu sprzyjać powinien system motywacyjny, powiązany z osiąganymi przezeń wynikami. Owe zespoły mają mieć zapewnione skoordynowane i kompleksowe wsparcie doradcze w zakresie zarządzania, działań doradczych, analizy zagadnień wykraczających zakresem poza poszczególne projekty oraz możliwości współpracy poszczególnych zespołów projektowych. W powiązaniu z tym przewidziano wprowadzenie spójnego systemu kontroli *ex-ante* planowanych do udzielenia zamówień publicznych i wprowadzenie zaleceń dotyczących realizacji projektów w podziale na etapy z wyznaczeniem kamieni milowych, które pozwolą na stopniową realizację projektu.

[26] Komitet Rady Ministrów ds. Cyfryzacji (KRMC) dokonuje przeglądu realizowanych i planowanych projektów informatycznych pod kątem ich wzajemnej koordynacji, interoperacyjności stosowanych rozwiązań oraz efektywności wydatkowanych środków publicznych. Przewodniczącym KRMC jest minister właściwy ds. informatyzacji, a zastępcą spodsekretarz stanu w Ministerstwie Rozwoju Regionalnego. W skład KRMC wchodzą sekretarze lub podsekretarze stanu.

[27] Chodzi o *Program Operacyjny Polska Cyfrowa na lata 2014-2020*, wersja 4.0, Warszawa 5 grudnia 2013 r.

Takie podejście sprawi, że będzie możliwe odbieranie poszczególnych usług/funkcjonalności już podczas realizacji projektu. To znacząco zmniejszy ryzyko niezrealizowania danych projektów w pełni oraz w określonym terminie. Powiązane z tym jest wdrożenie już od początku realizacji danego programu monitoringu projektów. Powinien on w szczególności obejmować nadzór nad realizacją kamieni milowych projektu, zmianami w harmonogramach, jak też zarządzaniem ryzykiem[28]. Osobnego zaakcentowania wymaga ambitne założenie wprowadzenia zaleceń, które pozwalają na elastyczne i efektywne wprowadzenie mechanizmów legislacyjnych umożliwiających efektywne wdrażanie projektów oraz ich produktów, aby proces legislacyjny był prowadzony równolegle z realizacją projektu (tak, aby po wdrożeniu projektu nie było ograniczeń prawnych, które uniemożliwiałyby korzystanie z poszczególnych rozwiązań projektowych). Dopełnieniem planowanych rozwiązań jest wprowadzenie spójnych procedur kontrolnych obowiązujących wszystkie instytucje, które posiadają uprawnienia kontrolne wobec realizowanych projektów, ze ściśle określonym zakresem przedmiotowym kontroli[29].

W okresie programowania 2014 - 2020 kwestia połączenia finansowania projektów PPP ze środkami europejskimi ma duże znaczenie, tym bardziej że z nowego budżetu polityki spójności Polska otrzyma 72,9 mld euro. Jeżeli chodzi o konkretne zmiany w nowej perspektywie 2014 - 2020 widoczne szczególnie w kontekście PPP, to jest ich kilka. Dnia 26 czerwca 2012 r. odbyło się posiedzenie Rady do Spraw Ogólnych, podczas którego przyjęto kompromis prezydencji duńskiej dla czterech bloków negocjacyjnych pakietu legislacyjnego polityki spójności. Były to: koncentracja tematyczna, instrumenty finansowe, ramy i ocena wykonania oraz projekty generujące dochód i partnerstwo publiczno-prywatne (PPP)[30]. Warto dodać, że w kwietniu 2012 r. Polska przygotowała własną koncepcję odnośnie do przepisów szczególnych dotyczących PPP, którą poddano dyskusji i osiągnięto kompromis. Do najważniejszych jej założeń zaliczyć należy: „uznanie szczególnej specyfiki PPP poprzez zapewnienie prymatu przepisów dla tego trybu nad przepisami o charakterze ogólnym, wprowadzenie do rozporządzenia ogólnego definicji PPP, zapewnienie, że beneficjentem projektu może być podmiot publiczny lub podmiot prywatny, zapewnienie możliwości zmiany beneficjenta w trakcie realizacji projektu, bez uszczerbku dla przepisów

[28] Ibidem, s. 32.
[29] *Diagnoza dla Programu Operacyjnego Polska Cyfrowa 2014-2020...* op. cit.
[30] *Przebieg negocjacji nad kształtem polityki spójności po 2013 roku w poszczególnych blokach tematycznych, czerwiec 2012 r. - Rada do Spraw Ogólnych*, www.mrr.gov.pl/fundusze/Fundusze_Europejskie_2014_2020/Negocjacje_2014_2020/Negocjacje/Strony/Przebieg_negocjacji_nad_ksztaltem_polityki_spojnosci_po_2013_czerwiec_2012.aspx (02. 12. 2013).

dot. trwałości, uznanie kwalifikowalności wydatków w przypadku wpłaty refundacji UE na rachunek powierniczy, jeśli kontrakt PPP przewiduje ponoszenie przez podmiot publicznych opłat za dostępność rozłożonych w fazie operacyjnej projektu, tj. po zakończeniu okresu kwalifikowalności wydatków"[31]. Są to ważne ustalenia, które sprzyjają korzystaniu z PPP.

Z punktu widzenia podmiotów prywatnych i instytucji publicznych korzystne jest również nowe podejście w stosunku do realizacji dużych projektów. Lista tych projektów nie będzie musiała być poddawana zatwierdzeniu przez Komisję Europejską, jak również postanowiono o zniesieniu ograniczeń co do jej aktualizacji. Próg dla nich oparto o koszty kwalifikowane – 50 mln euro. Zmieniono także maksymalny okres na podpisanie pierwszego kontraktu na roboty budowlane – czas wydłużono do 3 lat, a przypadku PPP warunek ten zostanie spełniony po zawarciu właściwej umowy[32].

W ramach zwiększenia dostępności, stopnia wykorzystania i jakości technologii informacyjno-komunikacyjnych w nowej perspektywie finansowej wsparte zostaną inwestycje w sieć następnej generacji (NGN), poszerzenie dostępu i zarządzanie informacją, digitalizacja i otwarcie zasobów publicznych (w obszarze edukacji, kultury, sądownictwa i innych obszarach), i szeroko pojęta cyfryzacja – odnośnie do informowania i usług publicznych i niepublicznych. Istotne będą tutaj również kwestie dotyczące rozwoju kompetencji cyfrowych skierowane do dwóch grup: osób nauczających (powinni oni nauczyć się wykorzystywać zasoby sieci Internet do szeroko pojętego kształcenia innych i siebie) oraz osób starszych (w celu pokazania korzyści wynikających z użytkowania Internetu)[33].

Jeżeli chodzi o najważniejsze elementy istotne dla zaprogramowania zintegrowanego wsparcia wybranych obszarów strategicznej interwencji, to w miastach wojewódzkich i ich obszarach funkcjonalnych wspierane będzie „promowanie instrumentów zwrotnych (Jessica), PPP i większego angażowania środków krajowych i prywatnych", natomiast w miastach średniej wielkości (nie będących miastami wojewódzkimi) wymagających rewitalizacji będzie promowane angażowanie partnerów prywatnych nie tylko w formule PPP, ale też w innych formułach[34].

[31] Ibidem.
[32] *Programowanie perspektywy finansowej na lata 2014-2020*, Ministerstwo Rozwoju Regionalnego, Departament Koordynacji Polityki Strukturalnej, www.mrr.gov.pl/fundusze/Fundusze_Europejskie_2014_2020/Programowanie_2014_2020/Documents/uwarunkowania_strategiczne.pdf, s. 9 (02. 12. 2013).
[33] Ibidem, s. 12.
[34] Ibidem, s. 24.

Na koniec warto wyszczególnić kluczowe instrumentarium, które umożliwia zastosowanie PPP we wdrażaniu funduszy europejskich w obszarze szeroko pojętej cyfryzacji[35]. Opracowany w ostatnim czasie dokument „Program Operacyjny Polska Cyfrowa na lata 2014-2020"[36] w swoim celu szczegółowym 1 (Ograniczenie terytorialnych różnic w możliwości dostępu do szerokopasmowego Internetu o wysokich przepustowościach) zakłada, że „interwencja będzie polegać na wsparciu projektów w zakresie budowy, rozbudowy lub przebudowy sieci dostępowej o parametrach co najmniej 30 Mb/s oraz na wsparciu projektów z zakresu budowy, rozbudowy i przebudowy sieci szkieletowej i dystrybucyjnej zapewniającej szerokopasmowy dostęp do Internetu jako uzupełnienie istniejącej infrastruktury telekomunikacyjnej, w tym powstałej w ramach perspektywy finansowej 2007-2013"[37]. Jedynie w uzasadnionych przypadkach możliwe będzie wsparcie finansowe projektów zakładających dostarczanie usług telekomunikacyjnych o parametrach niższych niż 30 Mb/s. Ma to mieć miejsce „na obszarach szczególnie zagrożonych trwałym wykluczeniem cyfrowym ze względu na bardzo niskie nasycenie usługami szerokopasmowego dostępu do Internetu lub ich brak, gdzie budowa sieci zgodnie z wymaganiami EAC nie jest uzasadniona ekonomicznie"[38]. „Wdrożenie tak ściśle ukierunkowanej interwencji obejmie niewielki odsetek gospodarstw domowych i będzie rozpatrywane tam, gdzie inny sposób interwencji publicznej będzie nieskuteczny lub nieefektywny. Udzielane wsparcie w ramach celu szczegółowego będzie odbywać się przy zachowaniu neutralności technologicznej. Wsparcie w tym zakresie przyczyni się do ograniczenia terytorialnych różnic w możliwości dostępu do szerokopasmowego Internetu poprzez dalszy rozwój i uzupełnienie istniejącej sieci dostępowej oraz szkieletowej i dystrybucyjnej"[39]. Jako grupy beneficjentów przewidziano tu: przedsiębiorców telekomunikacyjnych oraz jednostki samorządu terytorialnego lub ich związki i stowarzyszenia (ale jedynie w uzasadnionych przypadkach, np. w sytuacji, gdy przedsiębiorcy telekomunikacyjni nie będą chcieli realizować inwestycji na danym obszarze). Wyraźnie podkreślono, że przewiduje się możliwość realizacji projektów z wykorzystaniem partnerstwa publiczno-prywatnego. Ukierunkowaniem terytorialnym objęto obszary, na

[35] W tym celu (poniżej) wskazano wprost konkretne fragmenty POPC, istotne w zakresie problematyki tytułowej niniejszego opracowania.
[36] *Program Operacyjny Polska Cyfrowa na lata 2014-2020…* op. cit.
[37] Ibidem, s. 16.
[38] Ibidem.
[39] Ibidem.

których nie można zapewnić szerokopasmowego dostępu do Internetu w oparciu i warunki rynkowe, z uwzględnieniem właściwych przepisów o pomocy publicznej[40].

Kolejny cel szczegółowy 5 (E-integracja i e-aktywizacja na rzecz zwiększenia aktywności oraz jakości korzystania z Internetu) zakłada:

1) Wykorzystanie lokalnych centrów aktywności do działań w zakresie cyfrowej integracji i aktywizacji lokalnych społeczności. „Służyć temu będą lokalne centra aktywności, które oferując dostęp do szybkiego Internetu, odpowiedni sprzęt, a przede wszystkim szeroką ofertę usług szkoleniowo-doradczych, przyciągać będą obecnych oraz przyszłych użytkowników Internetu i nowoczesnych technologii. Wsparcie będzie kierowane do istniejących punktów oferujących publiczny dostęp do Internetu poprzez rozszerzenie ich dotychczasowej oferty o działalność w zakresie cyfrowej integracji i aktywizacji. Oferta będzie skoncentrowana na grupie zagrożonej wykluczeniem cyfrowym – osobach starszych (50+), niepełnosprawnych, rencistach oraz emerytach – zamieszkałych zwłaszcza na terenach wiejskich (wsparcie obejmie także rolników i domowników) i małych miast. Centrum będzie służyło aktywizacji społeczności lokalnych dzięki zastosowaniu technologii informacyjno-komunikacyjnej (TIK) oraz upowszechnianiu korzystania z Internetu i nowych technologii poprzez naukę ich zastosowania, tj.: naukę korzystania z powszechnych e-usług prywatnych i publicznych (np. e-bankowość, e-deklaracje, e-handel, e–konsultacje społeczne, kontakty międzyludzkie, pomoc w uzyskaniu profilu zaufanego, e-zdrowie itp.), udostępnianie cyfrowych zasobów kultury, pomoc szkoleniową i doradczą dostosowaną do zgłaszanych potrzeb. Trenerzy pracujący w centrach, odpowiadają za przygotowanie kilkuletnich planów działań jako podstaw do animowania lokalnych partnerstw na rzecz aktywności cyfrowej, ze szczególnym uwzględnieniem innych lokalnych zasobów i trenerów deklarujących współpracę z centrum, lokalnych władz samorządowych oraz innych partnerów społeczno-gospodarczych. Działanie to przyczyni się do aktywniejszego korzystania z Internetu oraz cyfrowej integracji grup zagrożonych cyfrowym wykluczeniem, a co za tym idzie – do zwiększenia popytu na usługi szerokopasmowe i publiczne usługi i treści dostępne w formie cyfrowej. Ponadto w wyniku działania powstanie trwały mechanizm podnoszenia kompetencji cyfrowych przez całe życie, poprzez rozszerzenie funkcji wielu instytucji samorządowych w taki sposób, aby mogły one działać jako wielofunkcyjne ośrodki dostępu do informacji, wiedzy i kultury z wykorzystaniem technologii informacyjno-komunikacyjnej,

[40] Ibidem, s. 15.

nie tracąc całkiem swoich tradycyjnych atrybutów. Zakłada się tu możliwość realizacji projektów parasolowych, tj. projektów, na których realizację została przyznana dotacja i które są wdrażane poprzez mikroprojekty (określone części projektu parasolowego). W projekcie parasolowym występuje jeden partner wiodący (wnioskodawca), partnerzy mikroprojektów oraz partnerzy uczestniczący. Wszystkie działania mikroprojektów w ramach projektu parasolowego mają łącznie tworzyć jeden spójny projekt i służyć osiągnięciu wspólnego celu"[41]. Jako grupy beneficjentów przewidziano jednostki samorządu terytorialnego oraz ich związki i stowarzyszenia, organizacje pozarządowe i ich partnerstwa (w tym partnerstwa organizacji pozarządowych z jednostkami samorządu terytorialnego). Ukierunkowanie terytorialne wskazuje na cały kraj, jednak z preferencjami na rzecz obszarów wiejskich i terenów de faworyzowanych, w szczególności o najniższym poziomie dostępu mieszkańców do dóbr i usług[42].

2) Wsparcie inicjatyw społecznych na rzecz aktywizacji cyfrowej oraz e-integracji, a w szczególności nowatorskich inicjatyw na rzecz e-integracji i budowania kapitału społecznego z wykorzystaniem technologii cyfrowych, skierowanych do różnych grup społecznych z uwzględnieniem ich specyficznych potrzeb. Wsparcie otrzymają podmioty realizujące inicjatywy o charakterze prospołecznym i ponadregionalnym skierowane na:

- podnoszenie kompetencji cyfrowych z nastawieniem na praktyczne ich wykorzystanie, w tym głównie grup wymagających szczególnego rodzaju wsparcia (m.in. osoby niepełnosprawne, osoby w wieku 50+) oraz niemobilne;
- animowanie innowacyjnych działań budujących kapitał społeczny (w tym postawy partycypacyjne) z wykorzystaniem technologii cyfrowych;
- stworzenie innowacyjnych narzędzi podnoszenia umiejętności cyfrowych wśród osób o średnim poziomie kompetencji.

„Działania takie mogą przyjmować formę stacjonarnej działalności szkoleniowo-doradczej, różnych form samokształcenia na odległość (np. e-learning, masowe otwarte kursy on-line) lub formę mieszaną. Realizacja działania przyczyni się do zwiększenia aktywności cyfrowej grup o najniższych kompetencjach wymagających szczególnego rodzaju wsparcia, głównie przez eliminowanie dotyczących ich barier kompetencyjnych i mentalnych oraz do rozwoju kapitału społecznego i twórczego w oparciu o technologie cyfrowe. Interwencje

[41] Ibidem, s. 32.
[42] Ibidem.

realizowane w ramach niniejszego działania przyczynią się również do poprawy kompetencji obywateli z zakresu korzystania z technologii informacyjno-komunikacyjnej. Ponadto działanie przyczyni się do e-aktywizacji społeczeństwa poprzez rozwijanie średnich kompetencji cyfrowych"[43]. Jako grupy beneficjentów przewidziano: jednostki samorządu terytorialnego oraz ich związki i stowarzyszenia, organizacje pozarządowe, konsorcja powyższych z jednostkami samorządu terytorialnego, instytucje prowadzące działalność w zakresie uniwersytetów trzeciego wieku. Nie przewidziano tu ukierunkowań terytorialnych.

3) Kampanie edukacyjno-informacyjne na rzecz zwiększania znaczenia e-umiejętności oraz upowszechniania korzyści z wykorzystywania technologii cyfrowych, których celem jest eliminowanie barier mentalnych przez podniesienie świadomości publicznej na temat korzyści płynących ze stosowania technologii cyfrowych. Prowadzone działania będą dotyczyły technologii informacyjno-komunikacyjnej w szerszym zakresie niż sama interwencja POPC. „Kampanie edukacyjno-informacyjne prowadzone będą w oparciu o przygotowaną strategię komunikacji, która określi obszary tematyczne, grupy docelowe i narzędzia przekazu skierowanego do ww. grup docelowych. Działanie to przyczyni się do podniesienia świadomości oraz umiejętnego wykorzystywania technologii informacyjno-komunikacyjnej, co będzie skutkowało: wzrostem popytu na usługi cyfrowe, wzrostem aktywności społecznej i lepszym wykorzystania kapitału intelektualnego. Działanie wpłynie również na eliminowanie barier mentalnych w wykorzystaniu nowych technologii, co potencjalnie zwiększy skalę uczestnictwa społeczeństwa w cyfrowym świecie"[44]. Jako grupy beneficjentów wskazano beneficjenta pozakonkursowego. Nie przewidziano tu ukierunkowań terytorialnych[45].

Jeszcze jednym instrumentarium zorientowanym na formułę PPP, jest cel szczegółowy 6 (Pobudzanie potencjału uzdolnionych programistów dla zwiększenia zastosowania rozwiązań cyfrowych w gospodarce i administracji), a zwłaszcza działanie „E-pionier – opracowywanie nowych rozwiązań na potrzeby społeczne i gospodarcze bazujących na technologii informacyjno-komunikacyjnej poprzez akceleracje pomysłów zdolnych programistów", którego celem jest „wykorzystanie potencjału uzdolnionych studentów kierunków z zakresu technologii informacyjno-komunikacyjnej do rozwiązywania istotnych problemów społecznych i gospodarczych. Ma ono również na celu podniesienie świadomości

[43] Ibidem. s. 33-34.
[44] Ibidem s. 33.
[45] Ibidem.

społecznej, że zaawansowane kompetencje cyfrowe mogą służyć do rozwiązywania ww. problemów oraz podnoszenia konkurencyjności przedsiębiorstw. W ramach działania przewiduje się realizację przedsięwzięć, których przedmiotem będzie wsparcie pomysłów na rozwiązywanie problemów istotnych społecznie lub gospodarczo i bazujących na narzędziach oferowanych przez technologie informacyjno-komunikacyjne. W ramach wsparcia prowadzona będzie weryfikacja technologiczna i biznesowa proponowanych rozwiązań. Studentom kierunków technologii informacyjno-komunikacyjnej oraz interdyscyplinarnym zespołom studentów zostanie jednocześnie zapewniony coaching, mentoring (z udziałem doświadczonych praktyków), doradztwo, a także pogłębianie wiedzy i rozwój kompetencji poprzez możliwość np. udziału w warsztatach, seminariach, stażach, czy też wizytach studyjnych. Zakłada się, że część wsparcia może być ukierunkowana na projekty studentów/interdyscyplinarnych zespołów studentów rozwijające innowacyjne produkty/usługi do wykorzystania w działalności społecznej, biznesowej lub administracji publicznej, przy czym ważny problem społeczny lub gospodarczy do rozwiązania będzie określony przez operatora konkursu z udziałem uznanych ekspertów i praktyków życia społecznego i gospodarczego. Możliwe będzie uzyskanie wsparcia finansowego na pokrycie początkowych etapów rozwoju produktu (*proof of principle* i/lub *proof of concept*)"[46]. Wyraźnie przewiduje się tu możliwość zastosowania partnerstwa publiczno-prywatnego. Działanie to przyczyni się do promowania zaawansowanych kompetencji cyfrowych w społeczeństwie przy wykorzystaniu potencjału osób z wykształceniem informatycznym. Jako grupy beneficjentów przewidziano beneficjenta systemowego. Nie sprecyzowano tu ukierunkowań terytorialnych[47].

[46] Ibidem, s. 34-35.
[47] Ibidem, s. 35.

Wnioski

Aktualnie Unia Europejska (choć nie wypracowała w tym względzie specjalnego oprzyrządowania prawnego) sprzyja idei partnerstwa publiczno-prywatnego. Kluczowe znaczenie ma jednak praktyczne podejście państw, regionów i poszczególnych beneficjentów do tej sytuacji. Bezspornie istotne wydaje się zastosowanie PPP jako panaceum na wyczerpanie zdolności kredytowych samorządów (co w niedalekiej przyszłości spowoduje brak innych źródeł finansowania niż środki podmiotów prywatnych). Trudno wymagać od administracji publicznej rynkowej konkurencyjności w podejściu do klienta (o oczekiwaniach konsumenta). Potrzeby i wymagania rynku usług rosną, a sektor publiczny za nimi nie nadążą. Pożądana wysoka jakość realizowanych przedsięwzięć wymusza profesjonalizację poprzez powierzanie realizacji przedsięwzięć podmiotom prywatnym. Konieczna jest przy tym odpowiednio zdecydowana i merytorycznie kompetentna postawa sektora publicznego, aby nie tylko odeprzeć rozmaite imaginacje krytyczne, ale wręcz dowieść przewagi konkurencyjnej PPP nad doraźnym zlecaniem zadań publicznych podmiotom prywatnym. Konieczne wydaje się usprawnienie systemu zamówień publicznych i odstąpienie od schematyzmu projektowego (preferującego projekty poprawnie napisane, choć niekoniecznie dobre). Należy starać się zniwelować istotne rozwarstwienie przedmiotowych umiejętności wśród urzędników administracji publicznej i pracowników podmiotów prywatnych (część osób doświadczona w pozyskiwaniu środków zewnętrznych w ramach PPP, uwzględniając również projekty hybrydowe, a część nie). Warto rozważyć specjalne konkursy dla PPP. Można fakultatywnie modelować formułę PPP (przewidzieć schematy i dzięki temu je podpowiedzieć zainteresowanym stronom, wybrać rozwiązania całościowe, nie zwiększające długu publicznego). Zasadne wydaje się też „zejście” PPP na niższy poziom związany z realizacją podstawowych zadań przez administrację lokalną, np. budowa przedszkoli, szkół, obiektów kulturalnych. Tylko w ten sposób idea partnerstwa publiczno-prywatnego będzie powszechnie i dobrze działała, służąc społeczeństwu i odciążając sektor publiczny.

Bibliografia:

Druki zwarte:

1. Korbus B., J. Trzaskowska, E. Malak, M. Jasińska, *Partnerstwo publiczno-prywatne w Polsce*, Warszawa 2006
2. Korbus B., *Partnerstwo publiczno-prywatne*¸ Warszawa 2003
3. *Nowa perspektywa programowo-finansowa UE 2014 –2020 – najważniejsze zmiany*, Centrum Doradztwa Rolniczego w Brwionowie, Oddział w Krakowie, Kraków 2013, www. cdrkursy.edu.pl/cdr/wydawnictwa/perspektywa2020.pdf, Kraków 2013
4. Panasiuk A., *Koncesja na roboty budowlane lub usługi. Partnerstwo publiczno-prywatne – komentarz, Warszawa 2009*
5. *Partnerstwo publiczno-prywatne jako metoda realizacji zadań publicznych*, , Departament Polityki Regionalnej, Ministerstwo Gospodarki i Pracy Warszawa 2005
6. *Partnerstwo publiczno-prywatne. Zagadnienia teorii i praktyki*, pod. red. M. Perkowskiego, Białystok 2007
7. Perkowski M., *Wykonywanie zadań j.s.t. w trybie partnerstwa publiczno-prywatnego*, w: *Finanse samorządowe. 580 pytań i odpowiedzi. Wzory uchwał, deklaracji, decyzji, umów*, pod red. C. Kosikowskiego i J.M. Salachny, Warszawa 2012
8. *Programowanie perspektywy finansowej na lata 2014-2020*, Ministerstwo Rozwoju Regionalnego, Departament Koordynacji Polityki Strukturalnej, www.mrr.gov.pl/fundusze/Fundusze_Europejskie_2014_2020/Programowanie_2014_2020/Documents/uwarunkowania_strategiczne.pdf.

Dokumenty:

1. *Diagnoza dla Programu Operacyjnego Polska Cyfrowa 2014-2020*, Warszawa 2013, www.funduszeeuropejskie.gov.pl/2014_2020/konsultacje/Documents/Zal_1_POPC%20ver30_Diagnoza_21013.pdf, dzień dostępu 24.11.2013 r.
2. Komunikat Komisji Wspólnot Europejskich do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-społecznego oraz Komitetu Regionów, *Wspieranie inwestycji publiczno-prywatnych krokiem w kierunku naprawy gospodarki i długoterminowej zmiany strukturalnej: zwiększanie znaczenia partnerstw publiczno-prywatnych*, Bruksela, dnia 19.11.2009, KOM(2009) 615 wersja ostateczna
3. Ustawa z dnia 27 października 1994 r. o autostradach płatnych, Dz. U. 1994 nr 127 poz. 627, z późn. zm.
4. Ustawa z dnia 28 lipca 2005 r. o partnerstwie publiczno-prywatnym, Dz. U. 2005 nr 169, poz. 1420, z późn. zm.
5. Ustawa z dnia 19 grudnia 2008 r. o partnerstwie publiczno-prywatnym, Dz. U. 2009, nr 19, poz. 100, z późn. zm.
6. Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju sieci i usług telekomunikacyjnych, Dz. U. 2010, nr 106, poz. 675.

Strony internetowe:

1. Oficjalna strona internetowa Ministerstwa Rozwoju Regionalnego, www.mrr.gov.pl/fundusze/Fundusze_Europejskie_2014_2020/Negocjacje_2014_2020/Negocjacje/Strony/Przebieg_negocjacji_nad_ksztaltem_polityki_spojnosci_po_2013_czerwiec_2012.aspx

Kompetencje pracowników ośrodków innowacji i przedsiębiorczości w kontekście wykorzystania nowych technologii informacyjnych

Marzena Mażewska[1]

W ostatnich latach zagadnienie braku wykwalifikowanych kadr dla gospodarki zaczyna istotnie przybierać na sile. Pomimo rosnącej w Polsce liczby osób uzyskujących wyższe wykształcenie pracodawcom coraz trudniej jest znaleźć odpowiednich do ich potrzeb pracowników. Należy zwrócić uwagę, że rozwiązaniem problemu niedoboru pewnych grup pracowników nie jest wzrost liczby ludzi dostępnych na rynku pracy, ale dostępność odpowiednich ludzi o pożądanych kompetencjach i umiejętnościach[2]. Podmioty rynku pracy (instytucje, urzędy, przedsiębiorstwa) coraz częściej stają przed arcytrudnym pytaniem w postaci: jak – we właściwym czasie i we właściwym miejscu – znaleźć odpowiednich ludzi. Problem ten również dotyczy ośrodków innowacji i przedsiębiorczości (OIiP), które ze względu na szczególną rolę w gospodarce mają równie trudne zadanie w tym obszarze jak wysoko technologiczne przedsiębiorstwa – ich klienci. Pomimo szerokiej rzeszy absolwentów szkół wyższych o kierunku ekonomia i zarządzanie, marketing czy finanse, ale również kierunków technicznych tylko jednostki są w stanie spełniać wymogi, jakie stawiają przed nimi ośrodki innowacji.

Dotychczasowa praktyka zatrudnienia w ośrodkach innowacji pokazuje, że profilowe wykształcenie pracowników nie odgrywa wiodącej roli w procesie realizacji zadań ośrodka.

[1] Konsultant, trener, specjalistka z zakresu organizacji i zarządzania przedsiębiorczością, instrumentów wsparcia dla innowacji. Absolwentka Uniwersytetu Gdańskiego i Wyższej Szkoły Biznesu i Administracji w Warszawie. Posiada dwudziestoletnie doświadczenie w doradztwie dla MSP oraz instytucji otoczenia biznesu w dziedzinie inkubacji przedsiębiorczości i innowacji, transferu technologii oraz rozwoju regionalnego. W latach 1996-1998 ekspert Projektu Banku Światowego w zakresie rozwoju przedsiębiorczości w Polsce, a w latach 2000-2007, 2012-2013 ekspert Programu Rozwoju Ekonomiki i Przedsiębiorczości Fundacji *Open Society Institute w* Nowym Jorku. Koordynatorka i współrealizatorka kilkudziesięciu krajowych i międzynarodowych projektów związanych z rozwojem sektora MSP i instytucji otoczenia biznesu. Posiada 20 lat doświadczeń w realizacji projektów badawczych oraz aplikacyjnych w dziedzinie inkubacji przedsiębiorczości i innowacji, transferu technologii oraz rozwoju regionalnego w Polsce i Europie Środkowo-Wschodniej, Azji Centralnej. Autorka i realizatorka kilkudziesięciu programów edukacyjnych dla przedsiębiorców i kadry ośrodków innowacji i przedsiębiorczości. Autorka i współautorka ponad 70 publikacji, analiz, ekspertyz i opracowań na temat przedsiębiorczości, tworzenia i zarządzania ośrodkami innowacji i przedsiębiorczości, ich strategii rozwoju, oraz rozwoju regionalnego. Wieloletni członek władz Stowarzyszenia Ośrodków Innowacji i Przedsiębiorczości w Polsce, od 2012 Prezes Zarządu SOOIPP. Członek Rady Ogólnopolskiego Klastra Innowacyjnych Przedsiębiorstw.

[2] Por. *Niedobór talentów na rynku pracy 2008 r*., Raport ekspercki Manpower.

Szacunkowo można przyjąć, że ok 60% pracowników ośrodków ma wykształcenie nieodpowiadające zajmowanym stanowiskom pracy. W tej grupie można wymienić między innymi filologów, dziennikarzy, archeologów, psychologów czy politologów. A jednak ludzie ci sprawdzają się w swoich funkcjach, ponieważ posiadają kilka podstawowych cech i umiejętności, które pozwalają im szybko uzupełniać wiedzę i rozwijać kompetencje pracownicze.

Rozwijająca się gospodarka, postępujący proces cyfryzacji administracji publicznej i bardzo szybki rozwój nowych technologii to czynniki wpływające istotnie na oczekiwany poziom kompetencji pracowników ośrodków innowacji i przedsiębiorczości – instytucji postrzeganych jako podmioty kreatywne i sprawne na równi z innowacyjnymi przedsiębiorstwami.

Również rozwój samych OIiP zarówno w aspekcie infrastrukturalnym, jak i funkcjonalnym już obecnie pociąga za sobą konieczność budowy wielofunkcyjnych zespołów ludzkich o szerokich i zróżnicowanych kompetencjach, które będą w stanie w najbliższej przyszłości sprostać oczekiwaniom przedsiębiorców. Wraz z postępującymi w ośrodkach zmianami, funkcjonujące w nich zespoły ludzkie będą podejmować nowe zadania wymagające wiedzy i umiejętności, które dotąd nie były pierwszoplanowymi przy rozpatrywaniu decyzji o zatrudnieniu pracowników.

Wobec istotnych zmian w sposobie i zakresie świadczenia usług przez ośrodki innowacji i przedsiębiorczości – wykorzystanie nowych technologii komunikacyjnych i informatycznych, a w odniesieniu do parków i inkubatorów technologicznych wyposażenie ich w wysoko wyspecjalizowaną nowoczesną aparaturę badawczą – konieczne będzie ich wejście na wyższy poziom organizacji. Tak więc predyspozycje i kompetencje kadry w tych ośrodkach powinny odpowiadać nie tylko potrzebom samej instytucji w zakresie wypełniania obowiązków, ale przede wszystkim potrzebom ich klientów.

Rozbudowa potencjału ludzkiego ośrodków będzie bezwzględną koniecznością dla tych z nich, które znacząco zwiększą swój potencjał techniczny do świadczenia usług. Dla zapewnienia bezawaryjnego ich funkcjonowania ważne jest, aby doprecyzować poziom wiedzy i kwalifikacji pracowników na poszczególnych stanowiskach, stosując przy tym sprawny system uzupełniania i zastępowania kompetencji. Ma to szczególnie ważne

znaczenie wobec konieczności utrzymania praktycznie nieprzerwanego systemu świadczenia usług (linie technologiczne lub aparatura laboratoryjna pracująca cała dobę).

Każda instytucja, w zależności od skali i zasięgu działania, w inny sposób tworzy zespoły pracownicze, uwzględniając przy tym niezbędne w swojej działalności potrzeby w zakresie potencjału, doświadczenia, wiedzy i umiejętności, jakimi powinni dysponować pracownicy do efektywnej realizacji powierzonych im zadań. Praktyka funkcjonowania instytucji otoczenia biznesu wskazuje na specyficzne cechy organizacji i kształtowania zespołów. Przede wszystkim wobec stosunkowo skomplikowanych systemów zależności i współpracy z otoczeniem w ośrodkach innowacji i przedsiębiorczości najwięcej uwagi należy poświecić zazwyczaj dość małym zespołom pracowniczym, stanowiącym podstawowe komórki organizacyjne struktury, takim jak: zespół zarządczy, zespół administracyjno-informacyjny, zespół doradczo-konsultingowy czy zespół techniczny.

Należy zwrócić uwagę, że każdy klient ośrodka, korzystając z jego usług, jest bezpośrednio lub pośrednio jednocześnie klientem wszystkich zespołów pracowniczych danej instytucji. Dotyczą go bowiem działania zespołu zarządczego, który na podstawie zgłaszanych przez klientów potrzeb buduje ofertę usługową ośrodka. Zespół merytoryczny ma bezpośredni kontakt z klientami w zakresie świadczenia usług, natomiast zespoły administracyjno-informacyjny i techniczny poprzez swoje działania bezpośrednio wzmacniają aktywność dwóch pierwszych, zabezpieczając warunki do świadczenia usług.

Wobec przedstawionego powyżej systemu powiązań między poszczególnymi zespołami a klientami ośrodka do głównych zmian, które nadchodzą, należy zaliczyć:

- nieuniknioną formalizację powiązań między grupami pracowników wewnątrz ośrodków – szczególnie wielofunkcyjnych – wymuszoną nowymi warunkami specjalizacji;
- w wielu przypadkach zastąpienie wielofunkcyjności pracowników wąską specjalizacją;
- systemowe i bardziej efektywne wykorzystanie potencjału zewnętrznego do realizacji zadań parku (ekspertów, innych instytucji otoczenia biznesu).

Wyzwania, stojące w najbliższym czasie przed ośrodkami innowacji i przedsiębiorczości, spowodują, że ważnym elementem kształtowania ich potencjału usługowego będzie dobór odpowiednich ludzi do realizacji określonych zadań. Nie wnikając

w szczegółowe zakresy obowiązków pracowników, można powiedzieć, że do cech, które będą nabierać coraz większego znaczenia wśród personelu ośrodków, będą należeć przede wszystkim:

–komunikatywność;
–odpowiedzialność;
–bardzo dobra organizacja pracy;
–umiejętność pracy w zespole.

W zależności od typu zespołu układ cech pracowników będzie zróżnicowany. Będzie to powiązane przede wszystkim z zakresem ich działania, poziomem odpowiedzialności i zadaniami które stawiać będą przed nimi interesariusze.

Tabela 1. Wybrane kompetencje zespołów pracowniczych w OIiP

Zespół zarządczy	Zespół merytoryczny	Zespół administracyjno - informacyjny	Zespół techniczny
– kreatywność, decyzyjność – umiejętność podejmowania skalkulowanego ryzyka – umiejętność strategicznego myślenia – zdolność i gotowość do ciągłego uczenia się – umiejętność działania sieciowego – znajomość	– postawienia się w sytuacji klienta – komunikowania się – używania języka zrozumiałego dla klienta – przekazywania wiedzy – wzbudzania zaufania, – przejawianie zainteresowania i pozytywnego nastawienia do klienta – zachęcenia do	– dysponowanie aktualną informacją gospodarczą i wiedzą, skąd można ją pozyskać – zdolność ciągłego uczenia się – komunikatywność – sprawna obsługa urządzeń biurowych – biegłość w wykorzystywaniu najnowszych technologii komunikacyjnych	– znajomość infrastruktury technicznej ośrodka – wysoki poziom kompetencji w ramach wybranej specjalizacji – komunikatywność – odpowiedzialność – dokładność – sumienność

języków obcych	działania – znajomość języków obcych	– znajomość języków obcych	

Źródło: Opracowanie własne

Przedstawione powyżej cechy i umiejętności w odniesieniu do poszczególnych zespołów niezbędne będą dla zabezpieczenia możliwości efektywnej i sprawnej obsługi klientów oraz ułatwienia przepływu informacji pomiędzy zespołami, których funkcje i zadania w procesie świadczenia usług przenikają się w sposób wymagający jednoczesnego zaangażowania członków różnych komórek organizacyjnych.

W zespole merytorycznym na szczególną uwagę będą zasługiwać predyspozycje interpersonalne oraz wysoki poziom empatii w odniesieniu do świadczenia usług konsultingowo-doradczych. Coraz większa rola sposobu obsługi klientów – w niektórych wypadkach ważniejsza niż jej merytoryczna wartość – wymagać będzie od pracowników mających bezpośredni kontakt z klientem wiedzy i umiejętności, nie tylko przedstawienia oferty i zastosowania procedury realizacji usługi, ale również wykazania zainteresowania jego sprawami i organizacji odpowiedniego sposobu jej materializacji. Ponadto szczególnie w tej grupie pracowników należy zwrócić uwagę na predyspozycje do tworzenia i wykorzystywania sieci powiązań zewnętrznych na rzecz klientów ośrodka oraz umiejętność kojarzenia pozornie niezwiązanych ze sobą informacji w logicznie uporządkowany zasób wiedzy, który może być wykorzystany w procesie wsparcia klientów zarówno w obszarze stricte informacyjnym, jak i w różnych formach wsparcia merytorycznego.

Istotnym, choć dość często bagatelizowanym, zagadnieniem szczególnie w organizacji usług parkowych związanych z korzystaniem przez klientów z powierzchni użytkowych i usług badawczych jest obsługa administracyjno-techniczna, w odniesieniu do której zazwyczaj podstawowym kryterium doboru pracowników są kompetencje fachowe. Większość zarządzających wychodzi z założenia, że osoby zatrudnione na tych stanowiskach nie muszą wykazywać się cechami i umiejętnościami właściwymi dla pionu merytorycznego. Jednak, biorąc pod uwagę fakt, że kontakt osób pracujących w zespołach administracyjnym i technicznym z klientami ośrodków jest równie codzienny jak pionu merytorycznego, należy zadbać o ich odpowiednie przygotowanie do obsługi klientów.

W zakresie kompetencyjnym pracownicy zespołu zarządczego i merytorycznego powinni dysponować umiejętnością swobodnego posługiwania się językami obcymi (w tym nie tylko językiem angielskim). Ten rodzaj kwalifikacji związany będzie przede wszystkim z procesem umiędzynaradawiania ośrodków, ale również polskich przedsiębiorstw. To zaś pociągnie za sobą konieczność posługiwania się językami, które dla klientów ośrodków staną się sposobem bieżącej komunikacji z ich partnerami biznesowymi. Ponadto szczególnie w parkach i inkubatorach technologicznych pojawią się popularne już w Europie usługi *soft landing* dla firm zagranicznych, które będą chciały wejść na nasz rynek. Będzie się to wiązało z koniecznością nabycia przez personel tych ośrodków wiedzy na temat zasad funkcjonowania podmiotów zagranicznych w Polsce oraz przygotowania specjalnych pakietów usług dla tego szczególnego rodzaju lokatorów.

Wdrażanie nowych technologii zarówno przez lokatorów, jak i ośrodki powoduje, że rosną wymagania w zakresie wykorzystania technologii informacyjnych przez pracowników merytorycznych, jak i obsługę administracyjno-techniczną. Szczególnie ważna będzie znajomość i umiejętność tworzenia oraz wykorzystania własnych systemów bazodanowych na potrzeby ośrodków zarówno w odniesieniu do klientów, poziomu ich rozwoju oraz potencjału, jak i systemów zarządzania relacjami z klientami. Własne zasoby bazodanowe stanowią ogromny potencjał wiedzy i informacji statystycznej, bardzo przydatnej w zarządzaniu ośrodkami, budowie ich strategii, ale również podejmowaniu krótkoterminowych decyzji zarządczych. Stanowić one będą również bazę do stosowania systemów CRM, pozwalających na lepsze zarządzanie kontaktami i zwiększanie ich efektywności oraz dostosowanie oferty usług do potrzeb klientów. Rozwój nowych technologii sprawi, że pracownikom ośrodków innowacji i przedsiębiorczości potrzebne będą kwalifikacje zarówno z zakresu informatyki, jak i psychologii, pozwalające uczynić kontakty z klientami i lokatorami możliwie najbardziej efektywnymi.

W obszarze obsługi administracyjnej działalności ośrodków oraz tworzenia zasobów informacyjnych kwalifikacje pracowników powinny obejmować przede wszystkim wykorzystanie technologii biurowych związanych z:

1. Elektroniczną archiwizacją dokumentacji;
2. Tworzeniem, aktualizacją i zarządzaniem bazami danych klientów;
3. Wykorzystaniem CRM do tworzenia więzi i komunikowania się z klientami;

4. Sprawnym opracowywaniem i tworzeniem dokumentów niezbędnych do prawidłowej działalności ośrodka i obsługi jego klientów;
5. Wykorzystaniem tzw. chmur internetowych w zakresie użytkowania profesjonalnego oprogramowania czy przechowywania danych zbieranych w bazach danych;
6. Wykorzystywaniem najnowszych narzędzi do tworzenia prezentacji i materiałów informacyjnych.

Ad 1) Elektroniczna archiwizacja dokumentacji – ośrodki wraz z rozwojem swojej aktywności gromadzą coraz większa ilość dokumentów, danych statystycznych, materiałów szkoleniowych i informacyjnych. Dokumenty te w większości wymagają archiwizacji w formie papierowej. ale również coraz częściej elektronicznej. Umiejętności wykorzystania programów i oprzyrządowania oraz odpowiedniego ich porządkowania i archiwizacji, z uwzględnieniem obowiązujących przepisów będzie nabierać znaczenia.

Ad 2) Tworzenie, aktualizacja i zarządzanie bazami danych klientów – tworzenie własnych baz danych jest niezwykle pożądane i przydatne zarówno dla szczebli zarządczych, jak i zespołów merytorycznych, Na poziomie zarządczym korzystanie z danych statystycznych dotyczących rodzaju klientów ośrodka oraz zapotrzebowaniu na jego usługi jest jednym z podstawowych źródeł budowy strategii rozwoju, z kolei dla pracowników merytorycznych szybki dostęp do wiedzy o dotychczasowych usługach świadczonych danej osobie czy firmie pozwala w sposób bardziej efektywny realizować kolejne usługi i rozwijać obszary współpracy z klientami.

Ad 3) Zarządzanie relacjami z klientami – CRM (Customer Relationship Management). „Zgromadzone dzięki CRM informacje umożliwiają również identyfikację i zarządzanie wąskimi gardłami w funkcjonowaniu ośrodka i co za tym idzie ich poprawę. Ponadto kompleksowo administrowane kontakty z klientami pokazują, jakie są oczekiwania klientów wobec organizacji, jej produktów czy usług, co z kolei pozwala na ich ciągłe udoskonalenie i dopasowanie do potrzeb odbiorców”[3]. Wykorzystanie CRM w tworzeniu więzi i komunikowaniu się z klientami to przede wszystkim większa elastyczność działania, lepsza obsługa klienta, lepszy marketing docelowy. Takie są podstawowe zalety korzystania z nowoczesnych programów pozwalających na zwiększanie sprzedaży i upowszechnianie informacji o działaniach ośrodka.

[3] I. Kowalczyk,J. Pawłowska,F. Sarti, I. Z. Biasetti, *Metody inkubacji projektów biznesowych*, PARP, Warszawa 2011 s. 26

Ad 4) Sprawne opracowywanie i tworzenie dokumentów niezbędnych do prawidłowej działalności ośrodka i obsługi jego klientów – „standaryzacja w zakresie dokumentacji wprowadza pewną strukturę funkcjonowania instytucji i reguluje procesy zachodzące wewnątrz niej. Dodatkowo dokumentacja stanowi pewne ramy merytoryczne i formalne, w których pracownicy mogą się poruszać, oraz buduje system wartości, który instytucja chce prezentować na zewnątrz. Warto pamiętać, że system dokumentacji może, i de facto powinien, być regularnie sprawdzany pod kątem efektywności działania i w razie potrzeby aktualizowany. Wprowadzenie standardów działania do procesów zachodzących wewnątrz instytucji przyczyni się znacznie do zwiększenia jej konkurencyjności. Korzyści z tego płynące mogą obejmować swoim zakresem obszary takie jak stworzenie bardziej efektywnych procesów biznesowych, ulepszenie technik marketingowych, zwiększenie świadomości pracowników o wartościach instytucji i ich motywacji do lepszej pracy oraz zwiększenie poziomu zadowolenia klientów” [4].

Ad 5) Wykorzystanie tzw. chmur internetowych w zakresie korzystania z profesjonalnego oprogramowania, przechowywania danych zbieranych w bazach danych – dla ośrodków istotnym elementem korzystania z chmur internetowych może być możliwość sięgania po oprogramowanie, które może być potrzebne zarówno samemu ośrodkowi, jak i jego klientom. Jest to rozwiązanie dużo mniej kosztowne aniżeli zakup profesjonalnego oprogramowania, a potem jego aktualizacji, szczególnie w przypadkach gdy zachodzi potrzeba tylko okazjonalnego korzystania z danego typu oprogramowania.

Ad 6) Wykorzystywanie najnowszych narzędzi do tworzenia materiałów informacyjnych i prezentacji – coraz bardziej dostępne są programy graficzne wykorzystujące techniki video, dzięki czemu możliwe jest włączanie do materiałów informacyjnych i szkoleniowych elementów graficznych, fotografii i animacji, które sprzyjają łatwiejszej absorbcji przekazywanych informacji i uatrakcyjniają zajęcia dla przedsiębiorców. Konkurencja na rynku usług szkoleniowych i informacyjnych w najbliższych latach będzie stale rosła. Umiejętność wykorzystania nowinek technologicznych w tym zakresie będzie istotnym elementem przewagi konkurencyjnej.

[4] Tamże, s. 109

Natomiast w obszarze komunikacji z klientami i bezpośrednim świadczeniu usług szczególne znaczenie będzie odgrywać wykorzystanie nowych technologii komunikacyjnych i informacyjnych, między innymi takich jak:

1. Wykorzystanie nowych technologii informacyjnych w doradztwie;
2. Organizacja wideokonferencji;
3. Korzystanie z obcojęzycznych stron internetowych i baz danych;
4. Komunikacja międzynarodowa.

Ad 1) Już obecnie na porządku dziennym w pracy ośrodków można spotkać doradztwo świadczone telefonicznie, mailowo lub przy użyciu internetowych komunikatorów (np. skype). Taka forma świadczenia usług stawia nowe wyzwania w postaci umiejętności sprawnego posługiwania się elektronicznymi źródłami informacji w procesie świadczenia tego typu usług, kompletowania elektronicznych źródeł informacji na potrzeby klientów i sprawnego ich przesyłania w uzupełnieniu do świadczonych usług. To jednak tylko mały element potencjału technologii informacyjnych. Wśród już działających można wymienić platformy e-learningowe, platformy branżowe, różnego rodzaju ogólnodostępne bazy danych zarówno w obszarze biznesu, jak i administracji publicznej, bazy informacyjne z zakresu prawa, biznesu, nowych technologii. Coraz większego znaczenia nabiera funkcja brokera informacji, który swobodnie porusza się w internecie i jest w stanie wyszukać na zlecenie firmy informacje w danym obszarze.

Ad 2) W połączeniu z doradztwem indywidualnym coraz częściej będzie się pojawiać zapotrzebowanie na organizację wideokonferencji nawet w dość licznym gronie, a w ślad za nimi umiejętność planowania i moderowania dyskusji z osobami będącymi niejednokrotnie na różnych krańcach świata i posługującymi się obcymi językami. Już obecnie niektóre wyspecjalizowane ośrodki (głownie parki technologiczne) dysponują profesjonalną aparaturą do prowadzenia profesjonalnych wideokonferencji. Również najprostsze narzędzia umożliwiają prowadzenie takich działań, a zapotrzebowanie będzie rosło wraz z udoskonalaniem technologii komunikacyjnych.

Ad 3) Umiejętność korzystania z obcojęzycznych stron internetowych i baz danych jest szczególnie ważna w odniesieniu do doradców i konsultantów pracujących na potrzeby ośrodków. Wiedza dotycząca kontaktów komercyjnych oraz o stanie techniki coraz częściej wymaga przeszukiwania licznych źródeł informacji w obcych językach, co wymusza na pracownikach ośrodków znajomość fachowej nomenklatury i wiedzę o źródłach tych

informacji. Jest to prawdziwe wyzwanie szczególnie dla mniejszych ośrodków, które nie dysponują zasobami ludzkimi o tak unikalnych kwalifikacjach.

Ad 4) Komunikacja międzynarodowa zarówno na potrzeby własne ośrodków jak i ich klientów również będzie nabierała coraz większego znaczenia. Mimo tego, ze znajomość języka angielskiego jest coraz bardziej powszechna, to specjalistyczne usługi dla firm w zakresie zarówno tłumaczeń informacji technicznych, jak i dokumentów formalno-prawnych będą cieszyły się coraz większym zainteresowaniem. Dotyczyć to będzie nie tylko języka angielskiego, ale również hiszpańskiego i rosyjskiego jako najbardziej popularnych. Ośrodki dla zapewnienia potrzeb swoich klientów będą musiały rozwijać własne kontakty międzynarodowe, uczestniczyć w działaniach sieci współpracy krajowych i zagranicznych. Tu też pojawia się zapotrzebowanie na nowy obszar kompetencyjny pracowników ośrodków w postaci umiejętności prowadzenia efektywnych działań networkingowych z innymi instytucjami działającymi w ich otoczeniu i mającymi bezpośredni wpływ na działania ośrodków [5]. Drugim obszarem działań networkingowych jest tworzenie i działanie w sieciach kooperacyjnych z innymi ośrodkami innowacji i przedsiębiorczości. To obszar wymagający dobrej orientacji w zakresie działania poszczególnych ośrodków, ale również predyspozycji do nawiązywania i utrzymywania kontaktów pozwalających na realizację wspólnie zaplanowanych działań.

Przygotowanie do świadczenia usług proinnowacyjnych

Zawrotne tempo rozwoju nauki i nowych technologii powoduje, że pracownicy będą musieli stale poszerzać spektrum swojej wiedzy i łączyć nauki ścisłe z humanistycznymi czy ekonomicznymi, co będzie możliwe jedynie wtedy, gdy zostaną wyposażeni w odpowiednie umiejętności i wiedzę z zakresu metodyki pozyskiwania wiedzy. W świetle wielu badań i dyskusji prowadzonych w grupach eksperckich dotyczących kompetencji, które stanowić będą w przyszłości o jakości kadr zarówno na poziomie zarządczym, jak i wykonawczym, wynika[6], że dominować wśród nich będą:

- kreatywność i przedsiębiorczość;
- „przekwalifikowalność" i mobilność;

[5] Por. J. Adamska, J. Kotra, *Kreowanie Środowiska Innowacyjnego w parkach technologicznych*, PARP, Poznań/Gliwice 2011 oraz S. Mazurkiewicz, M. Mażewska, M. Nowak, *Współpraca ośrodków innowacji z administracją publiczną*, PARP, Warszawa 2011

[6] Por. Krzysztof B. Matusiak, J. Kuciński, A. Gryzik (red.), *Foresight kadr nowoczesnej gospodarki*, PARP, Warszawa 2009

- komunikacja interpersonalna;
- praca w zespole, zarządzanie zespołami;
- umiejętność funkcjonowania w otoczeniu międzynarodowym;
- ugruntowane podstawy matematyki;
- zarządzanie wiedzą i infobrokerstwo;
- znajomość technologii informatycznych;
- wykorzystanie technologii mobilnych;
- ochrona własności intelektualnej;
- znajomość języków obcych.

Przedstawiona powyżej lista kompetencji powinna być jeszcze uzupełniona o kształtowanie postawy odpowiedzialnego i rzetelnego pracownika bez względu na funkcję i zadania, jakie wykonuje. Przeprowadzone badania i dyskusje panelowe wskazują jednoznacznie na konieczność zwiększenia liczby studentów na kierunkach ścisłych, ale również podnoszą ważny problem kształcenia na wszystkich kierunkach studiów w zakresie efektywnego wykorzystania technologii informacyjnych ze szczególnym naciskiem na umiejętność obsługi programów użytkowych. Stały rozwój informatyzacji procesów gospodarczych będzie w perspektywie najbliższych lat wymagał od pracowników dużo większych umiejętności posługiwania się nie tylko podstawowymi programami Pakietu Office. Z przedstawionych opinii wynika, iż przygotowanie personelu merytorycznego do profesjonalnego świadczenia usług proinnowacyjnych z uwzględnieniem krajowych i międzynarodowych standardów będzie kolejnym zadaniem, przed jakimi staną ośrodki innowacji i przedsiębiorczości.

Usługi o charakterze proinnowacyjnym, to usługi służące rozwojowi przedsiębiorcy przez poprawę istniejącego lub wdrożenie nowego procesu, produktu lub rozwiązania, dotyczące w szczególności:

- oceny zgłoszonych przez przedsiębiorcę potrzeb w zakresie dotychczas wytwarzanych/stosowanych lub nowych produktów, procesów, rozwiązań organizacyjnych i marketingu;
- zaproponowania przedsiębiorcy optymalnego rozwiązania prowadzącego do wzrostu jego konkurencyjności;

— wdrożenia innowacyjnych rozwiązań;
— innych działań, w wyniku których następuje transfer wiedzy lub innowacyjnej technologii;

Wśród dotychczas oferowanych przez ośrodki innowacji i przedsiębiorczości usług zwanych proinnowacyjnymi najczęściej wymieniane są:

- audyty technologiczne;
- usługi w zakresie transferu technologii;
- badanie potencjału rynkowego pomysłu na innowację;
- usługi w zakresie badania nowych trendów i rozwiązań technologicznych;
- budowa gotowości inwestycyjnej przedsiębiorstw;
- badanie zdolności patentowej i stanu techniki;
- szacowanie ekonomicznej opłacalności innowacyjnych rozwiązań;
- diagnozowanie możliwości wdrożenia innowacyjnych rozwiązań.

Do nowych kierunków rozwoju usług proinnowacyjnych należy zaliczyć:

- *proof of concept* – ocena wykonalności przedsięwzięcia gospodarczego;
- audyt eksportowy;
- poszukiwanie partnerów zagranicznych dla przedsiębiorstw;
- poszukiwanie rynków zbytu dla produktów innowacyjnych;

Jednak zadanie związane z odpowiednim przygotowaniem kadr ośrodków będzie wymagało sporego wysiłku i uzyskania względnej stabilizacji strukturalnej i finansowej dla prowadzenia przemyślanej i sensownie ukierunkowanej polityki w zakresie doboru i kształcenia kadr w ośrodkach. Chodzi tu przede wszystkim o tworzenie stabilnych i dobrze opłacanych stanowisk pracy, dających pracownikom poczucie stabilizacji.

Zagadnienie to jest bezpośrednio związane również z wyposażeniem ośrodków w najnowsze rozwiązania w zakresie technologii informatycznych i komunikacyjnych. Szczególnie ostatni okres finansowania ze środków europejskich obfitował w inwestycje w tym zakresie w parkach i inkubatorach technologicznych, centrach transferu technologii oraz innych ośrodkach innowacji realizujących projekty w ramach Programu Operacyjnego Innowacyjna Gospodarka. Posiadanie wyspecjalizowanego wyposażenia może jednak obok ewidentnych korzyści przynieść sporo negatywnych konsekwencji wynikających z braku profesjonalnej kadry niezbędnej do jego obsługi.

Według R. Kozłowskiego i M. Matejuna „pracownicy zajmujący się obsługą zaawansowanych technologii zaliczani są do kategorii pracowników wiedzy, profesjonalistów, »białych kołnierzyków« oraz inżynierów i charakteryzują się specyficznymi rolami zawodowymi. Ich wiedza ma charakter ezoteryczny, oparty na teorii naukowej, wynikający nie tylko z formalnego wykształcenia, ale również z ciągłego doskonalenia, dokształcania w trakcie wykonywania zawodu oraz udziału w nieformalnych grupach wymiany i upowszechniania wiedzy oraz umiejętności. Jednocześnie pracownicy ci powinni cechować się ponadprzeciętną kreatywnością, samodzielnością działania oraz odwagą w rozwijaniu i wdrażaniu do praktyki innowacyjnych rozwiązań wynikających z posiadanej i rozwijanej wiedzy fachowej.

Wykorzystanie nowych technologii w przedsiębiorstwie prowadzi do konieczności posiadania pracowników, którzy są w stanie ją we właściwy sposób obsługiwać. W przeciwnym razie dochodzi do poważnych zaburzeń. Przedsiębiorstwa już istniejące zatrudniają pracowników o predyspozycjach i wykształceniu wystarczającym do realizowania powierzonych im zadań w aktualnej sytuacji firmy. Po zmianie technologii ta sytuacja ulega zachwianiu. W zależności od wielkości zaburzeń powodowanych przez nowe, wdrażane technologie występują różne problemy związane z zasobami ludzkimi organizacji. Najczęstszymi, pojawiającymi się w takiej sytuacji konsekwencjami są:

- problemy z naborem nowej kadry o odpowiednich kwalifikacjach;
- konieczność przeprowadzenia szkoleń wybranych pracowników;
- przymus zwolnienia niektórych pracowników;
- wzrost niektórych kosztów stałych np. płac i kosztów zmiennych np. szkoleń, zwiększonej liczby braków, itp.;
- okresowe zmniejszenie wydajności."[7]

W zakresie podnoszenia i rozwijania kwalifikacji pracowników ośrodków związanych z innowacjami i nowymi technologiami należy zatem zwrócić szczególną uwagę na następujące obszary:

- prawa autorskiego i prawa własności przemysłowej;
- implementacji nowych rozwiązań technologicznych i organizacyjnych w gospodarce;

[7] Kozłowski R., Matejun M., *Problemy obsługi zaawansowanych technologii w przedsiębiorstwie informatycznym - studium przypadku*, [w:] Lachiewicz S., Matejun M. (red.), *Współczesne koncepcje zarządzania produkcją, jakością i logistyką*, Wydawnictwo Politechniki Łódzkiej, Łódź 2010, s. 213-237

- wykorzystania technologii informacyjnych w zarządzaniu firmą;
- metod oceny potencjału rynkowego technologii;
- umiejętności językowe – profil biznesowy;
- szkoleń branżowych – prezentacja najnowszych rozwiązań, wąsko specjalizowane dla różnych dziedzin gospodarki;
- szkoleń w zakresie zmian regulacji prawnych w poszczególnych branżach – aktualizacyjne.

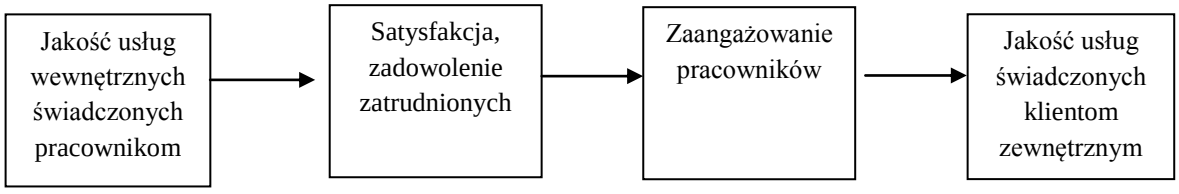
Niewątpliwie pracownicy wysoko wykwalifikowani w zakresie realizacji usług proinnowacyjnych będą oczekiwali wynagrodzeń adekwatnych do ich kompetencji i umiejętności oraz stworzenia im odpowiednich warunków do dalszego rozwoju. Oznacza to, że ośrodki będą musiały bardziej profesjonalnie aniżeli do tej pory podejść do zagadnienia budowy systemu motywacji pracowników, planów rozwoju ich kompetencji, jak również wdrożenia systemu marketingu wewnętrznego.

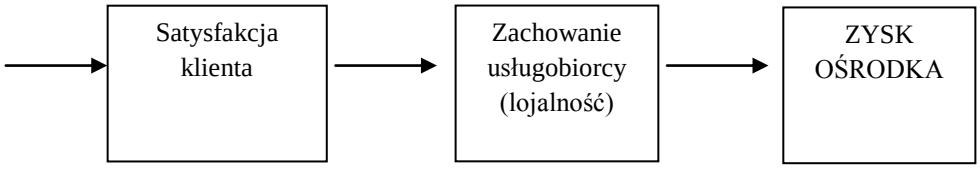
To ostatnie działanie, stosunkowo rzadko spotykane w polskich ośrodkach innowacji, opiera się na podejściu do pracowników w sposób podobny jak do klientów ośrodka. Tak więc zarządzający powinni badać potrzeby i aspiracje swoich pracowników pod względem:

- wyposażenia technicznego stanowisk pracy;
- warunków pracy;
- możliwości rozwoju i awansu;
- kształtowania atmosfery w zespole;
- możliwość wprowadzenia elastycznego czasu pracy;
- zachowania balansu miedzy życiem zawodowym i prywatnym.

Działania te zwane są usługami wewnętrznymi świadczonymi pracownikom i w polskich przedsiębiorstwach powoli zaczynają nabierać coraz większego znaczenia.

Schemat 1. Wpływ zadowolenia pracowników na poziom satysfakcji klientów





Źródło: opracowanie własne

Jak wynika z powyższego schematu, pomiędzy utrzymaniem lojalności klientów i dochodowością ośrodka a oddziaływaniem na zespół pracowników jest bezpośrednia zależność. Biorąc pod uwagę chęć utrzymania wysokokwalifikowanej kadry zapewniającej wysoką jakość usług w ośrodku, działania w zakresie marketingu wewnętrznego będą musiały stać się nieodłączną praktyką w organizacji funkcjonowania ośrodków innowacji i przedsiębiorczości.

Outsourcing w działalności ośrodków innowacji i przedsiębiorczości

Jest zupełnie zrozumiałe, że w większości ośrodków nie ma możliwości zatrudnienia wielu wysoko wyspecjalizowanych pracowników, ale też często nie ma po temu potrzeby, aby utrzymywać taką funkcję w pełnym wymiarze czasu pracy. W ostatnich latach coraz częściej korzysta się z podwykonawców w miejsce stałego personelu również w ośrodkach innowacji i przedsiębiorczości.

Biorąc pod uwagę specyfikę działania ośrodków, powinny one jednak uwzględniać potencjalne negatywne konsekwencje przekazywania poszczególnych obszarów działania firmom lub osobom z zewnątrz. Chociaż wydaje się to z różnych względów korzystne, to jednak każdą taką decyzję należy szczegółowo rozważyć z kilku powodów:

- realizacji celów strategicznych ośrodka;
- skutków organizacyjnych;
- skutków finansowych.

Realizacja celów strategicznych przez ośrodki może odbywać się zarówno przy wykorzystaniu własnego potencjału pracowniczego, jak i podmiotów zewnętrznych. Należy jednak zbudować efektywny system zarówno kontroli nad podwykonawcami, jak i włączenia ich w bieżącą działalność ośrodka, tak aby wiedza pozyskiwana przez nich w trakcie zlecanych im usług nie pozostawała poza zasięgiem OIiP. Podobnie organizacja takiej współpracy wymaga zwiększonego wysiłku i kontroli ze strony podstawowego zespołu ośrodka. Każda źle zrealizowana przez podwykonawcę usługa jest odbierana jako

nierzetelność samego ośrodka, a to wpływa niekorzystnie na jego wizerunek. W odniesieniu do nowych technologii ważne jest, aby ośrodki dysponowały w ramach swoich podstawowych zespołów pracownikami o kompetencjach pozwalających zweryfikować oferowane przez podwykonawców usługi i zabezpieczyć ośrodek przed ewentualnymi stratami finansowymi wynikłymi ze źle wykonanych usług.

Podsumowanie

Gospodarka oparta na wiedzy to gospodarka ludzi kreatywnych, z inicjatywą, posiadających rozwinięte umiejętności i kompetencje w określonych dziedzinach. Tylko wtedy możemy liczyć na jej intensywny, a przede wszystkim prawidłowy rozwój. Ośrodki innowacji i przedsiębiorczości na swój sposób stanowią forpocztę innowacyjnych postaw, które kreują i rozwijają w polskich małych i średnich przedsiębiorstwach. Należy podkreślić, że bez strategicznego planowania rozwoju ośrodków, a co za tym idzie – planowania rozwoju i organizacji zespołów ludzkich w tych ośrodkach, innowacyjność polskich przedsiębiorstw nie będzie mogła rozwijać się w tempie założonym w najnowszej Strategii Rozwoju Kraju do 2020 roku.

Bibliografia:

1. Adamska J., Kotra J., *Kreowanie Środowiska Innowacyjnego w parkach technologicznych*, PARP, Poznań/Gliwice 2011
2. Kozłowski R., Matejun M., *Problemy obsługi zaawansowanych technologii w przedsiębiorstwie informatycznym - studium przypadku*, [w:] Lachiewicz S., Matejun M. (red.), *Współczesne koncepcje zarządzania produkcją, jakością i logistyką*, Wydawnictwo Politechniki Łódzkiej, Łódź 2010,
3. Kowalczyk I., Pawłowska J., Sarti F., I.Z. Biasetti, *Metody inkubacji projektów biznesowych*, PARP, Warszawa 2011 s. 26
4. Matusiak K. B., Kuciński J., Gryzik A. (red.), *Foresight kadr nowoczesnej gospodarki*, PARP, Warszawa 2009
5. Mazurkiewicz S., Mażewska M., Nowak M., *Współpraca ośrodków innowacji z administracją publiczną*, PARP, Warszawa 2011
6. *Niedobór talentów na rynku pracy 2008 r.*, Raport ekspercki Manpower

Realne zagrożenia wirtualnego świata – cyberprzestrzeń a przedsiębiorcy

Karol Wasilewski[1]

Wstęp

Wirtualna rzeczywistość rodzi coraz więcej realnych zagrożeń, które dotykają przedsiębiorców. Jak wskazują badania, które zostały wykonane przez Ponemon Institute we współpracy z HP Enterprise Security Products, koszty związane z cyberprzestępczością wzrosły czwarty rok z rzędu[2]. Eksperci z amerykańskiej firmy McAfee, która zajmuje się m.in. bezpieczeństwem w sieci, szacują je na kwotę od 300 miliardów do nawet biliona dolarów rocznie w wymiarze globalnym[3]. Co więcej, badania wykazują także wzrost częstotliwości ataków w sieci, jak i wydłużenie się czasu, który jest potrzebny na ich odparcie[4].

Przytoczone wyżej statystyki pozwalają na wyciągnięcie dwóch istotnych wniosków. Po pierwsze, pokazują, że dysproporcje między tymi, którzy wykorzystują cyberprzestrzeń do działalności przestępczej, a tymi, którzy powinni się przed ich atakami bronić, są w dalszym ciągu znaczące, a nawet pogłębiają się. Obserwacja ta pozwala na sformułowanie drugiego, równie mało optymistycznego wniosku – potencjał rozwoju cyberprzestępczości wciąż jest znaczny.

---

[1] Doktorant na Wydziale Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego, autor artykułów na temat cyberbezpieczeństwa w kontekście stosunków międzynarodowych, były redaktor naczelny Przeglądu Spraw Międzynarodowych Notabene. Zainteresowania naukowe: stosunki międzynarodowe w regionie Bliskiego Wschodu, polityka zagraniczna Republiki Turcji, historia Imperium Osmańskiego, cyberbezpieczeństwo.

[2] *Cost of Cybercrime Increases 78 Percent,* www.securitymagazine.com/articles/84817-cost-of-cybercrime-increases-78-percent (02. 12. 2013).

[3] *The Economic Impact of Cybercrime and Cyber Espionage,* Center for Strategic and International Studies, lipiec 2013, www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf, s. 5. Przyczyna ogromnych rozbieżności w szacunkach zostanie wyjaśniona na dalszym etapie niniejszego artykułu. Na tym etapie warto jednak zauważyć, że kwota prezentuje się jeszcze bardziej imponująco, gdy porówna się ją do innych źródeł wpływów przestępców. Cała międzynarodowa przestępczość zorganizowana szacowana jest przez Biuro Narodów Zjednoczonych ds. narkotyków i przestępczości (UNODC) na 870 miliardów dolarów, zob. *Proceeds of transnational crime in billions, number of victims in millions, says UNODC chief,* www.unodc.org/unodc/en/frontpage/2012/October/transnational-crime-proceeds-in-billions-victims-in-millions-says-unodc-chief.html (02.12.2013).

[4] *Cost of Cybercrime Increases 78 Percent,* op. cit.

Taki stan rzeczy powoduje konieczność dokładnego przyjrzenia się problemowi. Wiele wskazuje bowiem na to, że przestępczość w sieci może wkrótce stać się – o ile już nim nie jest – znaczącym kłopotem również polskich przedsiębiorców. Autor niniejszego artykułu postawił sobie zatem dwa cele. Przede wszystkim chciałby zwrócić uwagę przedsiębiorców na problem cyberprzestępczości. W realizacji tego zamierzenia ma pomóc omówienie w tekście podstawowych zagadnień związanych z przestępczością w sieci, z uwzględnieniem najnowszych trendów, jakie zachodzą w tym obszarze. Autor wierzy bowiem, że pomoże to w zwiększeniu świadomości problemu wśród przedsiębiorców, co konieczne jest do skutecznego stawiania czoła zagrożeniom. Po wtóre, w artykule przedstawione zostaną wskazówki odnośnie do walki z cyberprzestępczością i bronienia się przed jej skutkami. Kwestia ta również zostanie omówiona w szerszym kontekście – i z uwzględnieniem zmian zachodzących w cyberprzestrzeni – aby czytelnicy mogli dokładniej zrozumieć skalę problemu.

1. Podmiotowy katalog zagrożeń

Wyczerpujące wyliczenie podmiotów, które mogą zagrażać przedsiębiorcom w cyberprzestrzeni, jest niezwykle trudne. Sytuacja taka powodowana jest kilkoma względami. Przede wszystkim należy zauważyć, że granice między definicjami niektórych podmiotów są niekiedy niezwykle cienkie, co wywołuje trudności w przyporządkowaniu poszczególnych osób lub ich grup do określonych kategorii. Kłopotliwe w tym zakresie jest także tempo zmian zachodzących w cyberprzestrzeni, które powoduje, że katalog zagrożeń również podlega dynamicznym zmianom.

Amerykański ICS-CERT (The Industrial Control Systems Cyber Emergency Response Team) zdefiniował podmiotowy katalog zagrożeń w oparciu o określenie „cyberzagrożenia dla systemu sterowania", które opisał w odniesieniu do „osób, które próbują w sposób nieautoryzowany uzyskać dostęp do urządzenia systemu sterowania i/lub sieci za pomocą ścieżki transmisji danych. Próba dostępu może zostać podjęta zarówno wewnątrz organizacji – przez zaufanego użytkownika – jak i przez nieznaną osobę, która korzysta z Internetu"[5]. W oparciu o tę definicję jako podstawowe źródła zagrożeń zostały wymienione następujące osoby lub grupy osób: terroryści, szpiedzy przemysłowi, zorganizowane grupy przestępcze, haktywiści i hakerzy. Co ciekawe, w tym samym tekście instytucja wyraźnie zaznacza jednak,

[5] *Cyber Threat Source Descriptions*, www.ics-cert.us-cert.gov/content/cyber-threat-source-descriptions (02.12.2013).

że nie jest to katalog wyczerpujący[6]. Pozwala to uzmysłowić sobie, jak wielkie trudności wiążą się z próbą jednoznacznego i pełnego określenia źródeł zagrożeń w sieci[7].

Wydaje się, że na potrzeby niniejszego artykułu nadużyciem nie będzie przedstawienie i bardziej wnikliwe opisanie trzech głównych źródeł zagrożeń w cyberprzestrzeni, nie zagłębiając się zbytnio w próby dokładnej ich klasyfikacji. Przede wszystkim należy zwrócić uwagę na dwa tradycyjne podmioty – o ile można tu mówić o jakiejkolwiek tradycji – jakimi są hakerzy i cyberprzestępcy. Choć terminy te często używane są synonimicznie – a w artykule autor opisze je w ramach jednego podpunktu – należy odnotować, że w rzeczywistości nie są jednoznaczne[8]. Jako trzecie, równie istotne źródło zagrożenia zostanie opisane państwo, któremu autor poświęci szczególną uwagę. Taki stan rzeczy wynika z dwóch przyczyn. Po pierwsze, aktualności problemu – państwa stanowią bowiem relatywnie nowy rodzaj zagrożenia dla przedsiębiorców. Po wtóre, ich aktywności w tej materii warto przyjrzeć się również ze względu na spory wśród samych specjalistów odnośnie do tego, czy rzeczywiście stanowią poważne zagrożenie. Na końcu niniejszej części artykułu zostaną pokrótce opisane pozostałe podmioty wraz z pewnym wyjaśnieniem odnośnie do kryteriów ich wyodrębniania.

a) Hakerzy i cyberprzestępcy

Subtelną różnicę, jaka istnieje między hakerami a cyberprzestępcami, pozwala wyczuć już sama lektura definicji obu terminów w Słowniku Języka Polskiego[9]. Różnicę tę doskonale opisał także V. Hargrave, który zauważył, że „w biznesie bezpieczeństwa powinno się rozróżniać hakerów, których określa się mianem białych kapeluszy i czarnych kapeluszy. Organizacje zatrudniają białe kapelusze – czasem określane jako »etyczni hakerzy« – aby wypróbowywały ich systemy komputerowe i włamywały się do nich w celu ustalenia, do jakiego stopnia są one bezpieczne, i przedstawienia odpowiednich rekomendacji, które mogą przyczynić się do zwiększenia ich bezpieczeństwa. Tacy hakerzy bardzo często w pełni

[6] „Zagrożenia dla systemu sterowania mogą pochodzić z rozmaitych źródeł, włączając w to wrogie rządy, grupy terrorystyczne, niezadowolonych pracowników i złośliwych intruzów", zob. ibidem. Wrażenie takie można odnieść już po samej lekturze definicji, jak i zestawieniu jej z wymienionym później katalogiem zagrożeń.

[7] Dla uzyskania pełni obrazu por. katalog zagrożeń przedstawiony przez również amerykańskie Government Accountability Office w raporcie dla kongresu, zob. *CYBERSECURITY. National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, Government Accountability Office, www.gao.gov/assets/660/652170.pdf, s. 5 (02. 12. 2013).

[8] Przyczyny takiego stanu rzeczy, a zarazem różnice między hakerami a cyberprzestępcami zostaną omówione na dalszym etapie tekstu. W tym miejscu warto jedynie zauważyć, że hakerzy stanowią katalog szerszy, ponieważ nie wszyscy są cyberprzestępcami.

[9] Zob. www.sjp.pl/haker; www.sjp.pl/cyberprzest%EApca (02. 12. 2013).

upubliczniają swoje odkrycia, aby szersza społeczność mogła czerpać korzyści z zaprezentowanych przez nich informacji. Działalność białych kapeluszy jest legalna, gdyż została wcześniej usankcjonowana przez ich klientów. Czarne kapelusze zaś to cyberprzestępcy, których cel jest całkowicie szkodliwy. Bez zaproszenia plądrują systemy komputerowe dla osiągnięcia własnych celów przy jednoczesnym ponoszeniu znacznych kosztów przez ich ofiary"[10].

Zaprezentowane wyżej wyjaśnienie dowodzi, że słowo „haker" jest terminem szerszym. Oznacza osobę, która może korzystać ze swych wyjątkowych umiejętności w różny sposób, podczas gdy cyberprzestępcy mają jednoznacznie określony cel, który najprościej można ująć jako chęć dokonania przestępstwa w sieci. Należy jednak zauważyć, że granica ta jest w rzeczywistości niezwykle cienka, w związku z czym bardzo szybko może zostać przekroczona. Wynika to z faktu, że każdy haker ma techniczne możliwości zostania cyberprzestępcą[11]. Nie oznacza to oczywiście, że musi z nich korzystać[12]. Być może pewnego rodzaju problem w tym zakresie stanowi również specyfika kultury hakerskiej, która w odpowiednich uwarunkowaniach – i ze względu na dużą rolę, jaką w motywowaniu hakerów odgrywa czynnik prestiżu – może skłaniać do podjęcia działań przestępczych[13].

Definicja cyberprzestępcy jako osoby, która dąży do osiągnięcia określonego zysku – najczęściej ekonomicznego – powoduje, że do kategorii tej można zaliczyć różne podmioty. W jednym z raportów firma PwC sugeruje na przykład, żeby umieścić w jej obrębie międzynarodowe grupy przestępcze, zdeprawowaną konkurencję, która dokonuje cyberszpiegostwa, aby osiągnąć przewagę ekonomiczną, tzw. samotnych wilków – jak wskazuje nazwa, osoby, które działają na własną rękę – a nawet zagraniczne wywiady[14]. Należy przyznać, że zwłaszcza ostatni podmiot może budzić pewne wątpliwości. Zdaniem

[10] V. Hargrave, *Hacker, Hacktivist, or Cybercriminal?,* www.fearlessweb.trendmicro.com/2012/hackers-and-phishing/whats-the-difference-between-a-hacker-and-a-cybercriminal/. Więcej na temat różnic między tzw. białymi a czarnymi kapeluszami, zob. także L. G. Crovitz, www.online.wsj.com/news/articles/SB10001424127887324635904578643943968885044 (02. 12. 2013).

[11] Jak słusznie zauważył T. Jordan: „We wszystkich przypadkach [cyberprzestępczości - przyp. aut.] spotykamy techniki znane z hakerstwa", zob. T. Jordan, *Hakerstwo,* Wydawnictwo Naukowe PWN, Warszawa 2011, s. 113.

[12] Jak zostało to już wspomniane, część hakerów korzysta ze swych umiejętności w szczytnych celach. Kolejnym, niezwykle ciekawym przykładem tego typu inicjatywy może być organizacja Hackers For Charity. Więcej na jej temat zob. www.hackersforcharity.org/ (02. 12. 2013).

[13] Pomocne w zrozumieniu zagadnień związanych z kulturą hakerską mogą być szczególnie dwie dostępne w Polsce książki: T. Jordan, *Hakerstwo,* op. cit. oraz M. Glenny, *Mroczny rynek. Hakerzy i nowa mafia,* Wydawnictwo W. A. B., Warszawa 2013. Należy zauważyć, że druga publikacja, choć ma charakter publicystyczny, jest szczególnie wartościowa ze względu na znaczący poziom infiltracji środowiska hakerów i cyberprzestępców przez autora.

[14] *Getting real about cyber threats: where are you headed,* www.pwc.com/en_US/us/industry/utilities/assets/getting-real-about-utilities-infrastructure-cyber-threats.pdf (02. 12. 2013).

autora niniejszego artykułu pokazuje to jednak ponownie, jak duże trudności wiążą się z próbą definiowania zjawisk, które zachodzą w obrębie cyberprzestrzeni, a także obrazuje, jak szeroki może być katalog osób lub grup, które mogą zakwalifikować się do zbioru cyberprzestępców.

Na tym etapie warto odnotować również pewne relatywnie nowe trendy, które zachodzą w obrębie zjawiska hakerstwa. Już teraz mają one bowiem poważne konsekwencje dla całej cyberprzestrzeni, a niewykluczone, że w niedalekiej przyszłości będą stanowiły również istotne źródło zagrożenia dla przedsiębiorców. Ostatnimi czasy mamy do czynienia z nasileniem się tzw. haktywizmu. Mianem tym określa się podejmowanie nielegalnych działań, które motywowane są jednak względami, „które w określonych przypadkach mogą być uważane za słuszne”[15]. Wydaje się, że do najbardziej znanych haktywistów można zaliczyć grupę Anonymous, choć stwierdzenie to z pewnością wywołałoby wątpliwości niektórych ekspertów, którzy jej działalność rozpatrywaliby raczej w kategorii cyberprzestępczości[16]. Zjawisko haktywizmu nie jest obce również polskiej przestrzeni publicznej. Jak twierdzą eksperci, doskonale zostaliśmy zapoznani z nim w trakcie protestów przeciw podpisaniu ACTA[17].

Haktywizm łączy się poniekąd z niezwykle ciekawym trendem, jakim jest zwiększanie się znaczenia czynnika politycznego w motywacji niektórych hakerów[18]. Dotychczas, co można było wywnioskować z poprzednich fragmentów tekstu, na ich działania największy wpływ wywierały czynniki psychologiczne i ekonomiczne. Obecnie ulega to zmianie. Coraz częściej do głosu dochodzą hakerzy, którzy grożą podjęciem akcji z pobudek politycznych. Prym w tym zakresie wiodą zwłaszcza Syryjczycy i Irańczycy[19]. Szczególnie warte odnotowania są deklaracje syryjskich hakerów, którzy najpierw zaatakowali m.in. stronę wiodącej amerykańskiej gazety „New York Times”, a później oznajmili gotowość do dokonania ataku odwetowego, jeśli Stany Zjednoczone zdecydują się na interwencję militarną

[15] V. Hargrave, *Hacker, Hacktivist, or Cybercriminal?,* op. cit.
[16] Należy przyznać, że haktywiści działają na pograniczu tego, co legalne i nielegalne, w związku z czym niektórzy zaliczają ich do kategorii tzw. szarych kapeluszy, zob. ibidem.
[17] M. Płociński, *To nie był cyberterroryzm*, www.rp.pl/artykul/799250.html (02. 12. 2013).
[18] Wydaje się, że sam ICS-CERT zalicza hakerów motywowanych politycznie po prostu do grupy haktywistów, zob. *Cyber Threat Source Descriptions*, op. cit.
[19] L. Franceschi-Bicchierai, *Syrian Electronic Army: If U.S. Attacks 'We Will Target All of It'*, www.mashable.com/people/lorenzo-franceschi-bicchierai/; J. Barnes, S. Gorman, *Iran Blamed for Cyberattacks*, www.online.wsj.com/news/articles/SB10000872396390444657804578052931555576700 (02. 12. 2013).

w ich kraju[20]. Co ciekawe, ich działania miały dotknąć nie tylko instytucje rządowe, ale również prywatne[21]. Należy zauważyć, że jeśli trend okazałby się trwały, mógłby stanowić rewolucyjną zmianę, której skutki w tej chwili pozostają nieodgadnione. Zawiłości związane z tą kwestią można prześledzić właśnie na przykładzie gróźb syryjskich hakerów. Zakładając, że rzeczywiście doszłoby do takiej sytuacji, należałoby znaleźć odpowiedzi na kilka pytań. Przede wszystkim, jakie straty mogłaby spowodować ich akcja? Czy ograniczyłaby się wyłącznie do Amerykanów, czy może dotknęłaby również inne państwa zachodnie? Jeśli atak okazałby się skuteczny i dotkliwy oraz, co gorsza, jeśli mógłby zostać powtórzony przez każde państwo, które dysponuje odpowiednim oddziałem hakerów, jak wpłynęłoby to na procesy decyzyjne poszczególnych państw w przyszłości? O ile w chwili obecnej trudno udzielić odpowiedzi na wymienione wyżej pytania, o tyle z pewnością można stwierdzić, że trend ten w konsekwencji wywarłby również wpływ na działalność przedsiębiorców.

Najważniejsze wykorzystywane przez cyberprzestępców metody, które zagrażają biznesowi, zostaną omówione w innym miejscu artykułu. W ramach podsumowania tej części warto jednak wyciągnąć jeszcze jeden niezbyt optymistyczny wniosek. Jak zostało to zaznaczone we wstępie, rozmiary przestępczości w sieci stale wzrastają. Biorąc pod uwagę fakt, że „koszt cyberbroni jest znacznie niższy niż broni tradycyjnej", w najbliższej przyszłości należy spodziewać się zarówno utrzymania tego trendu, jak i wzrostu liczby osób, które będą kwalifikowały się do katalogu cyberprzestępców[22].

b) Państwa

Jak zostało już wspomniane, państwa stanowią relatywnie nowe źródło zagrożenia w cyberprzestrzeni. Za pierwszy przypadek ataku w sieci, który był sterowany przez państwo, uważa się wydarzenia z Estonii z 2007 r. Choć oficjalnie nigdy tego nie udowodniono, sądzi się, że zostały zainicjowane przez Rosję[23]. Podejrzenia wzmacnia fakt, że cyberataki na

[20] C. Haughney, N. Perlroth, *Times Site Is Disrupted in Attack by Hackers*, www.nytimes.com/2013/08/28/business/media/hacking-attack-is-suspected-on-times-web-site.html?_r=0 (02. 12. 2013).
[21] S. Waterman, *Syrian hackers threaten retaliation for any U.S. strike*, www.washingtontimes.com/news/2013/aug/30/syrian-hackers-threaten-retaliation-any-us-strike/?page=all (02. 12. 2013).
[22] C. Thompson, *Businesses Facing Increasing Cyber Threats: Security Experts*, www.cnbc.com/id/100421313 (02. 12. 2013).
[23] Zob. np. I. Traynor, *Russia accused of unleashing cyberwar to disable Estonia*, www.theguardian.com/world/2007/may/17/topstories3.russia (02. 12. 2013).

estoński rząd zbiegły się w czasie ze sporem politycznym między oboma państwami[24]. Wprawdzie nadbałtycki kraj – głównie dzięki wysokiemu stopniowi zaawansowania technologicznego – poradził sobie z nimi relatywnie dobrze, jednak wydarzenia z 2007 r. były pierwszym poważnym sygnałem, że cyberprzestrzeń może wkrótce stać się również polem konfrontacji państw[25]. Co więcej, ataki na rząd Estonii potwierdziły, że jednoznaczne wskazanie sprawcy tego typu działań jest niemal niemożliwe[26]. Pozwalało to na wyciągnięcie wniosku, że aktorzy państwowi mogą w przyszłości tym chętniej korzystać z tak efektywnego, a zarazem w pewnym sensie dyskretnego instrumentu do realizacji swoich celów.

Rzeczywiście, już nieodległe wydarzenia dostarczały dowodów na to, że państwa coraz bardziej interesują się cyberprzestrzenią, a być może prowadzą w niej nawet całkiem zaawansowane operacje. W trakcie drugiej połowy 2007 r. zarówno Stany Zjednoczone, jak i Chiny miały przesłanki ku temu, by sądzić, że padają ofiarą ataków sterowanych przez inne państwa[27]. Nie były to jednak na tyle istotne działania, żeby wywołać poważniejsze zainteresowanie opinii publicznej. Na kolejny przełom w tej materii trzeba było czekać do lata 2008 r., gdy wybuchła wojna rosyjsko-gruzińska, w trakcie której cyberprzestrzeń odegrała niezwykle ważną rolę[28]. Choć ponownie nie udało się jednoznacznie udowodnić, że ataki na gruzińskie instytucje były kierowane przez Kreml, wiele wskazywało na to, że

[24] Spór wynikał z decyzji władz estońskich o przeniesieniu z centrum Tallinna pomnika sowieckiego żołnierza, zob. ibidem.

[25] Amerykański major W.C. Ashmore oceniał ich znaczenie w następujący sposób: „Niezależnie od tego, czy rząd Federacji Rosyjskiej był zamieszany w jakikolwiek cyberatak – lub będzie w takowy zaangażowany w przyszłości – rzeczywistością pozostaje fakt, że narody, grupy czy jednostki, które znajdują się w opozycji do Rosji, mogą stać się celem cyberataków. Będą one wykorzystywane do tego, aby wpłynąć na opinię publiczną lub liderów rządu przez wywieranie cyberpresji", zob. W. C. Ashmore, *Impact of Alleged Russian Cyber Attacks*, Baltic Security & Defence Review, Tom 11, 2009, www.bdcol.ee/files/files/documents/Research/BSDR2009/1_%20Ashmore%20-%20Impact%20of%20Alleged%20Russian%20Cyber%20Attacks%20.pdf (02. 12. 2013).

[26] „Z ataków na Estonię wynika wniosek, że o ile można z dużą dozą prawdopodobieństwa odgadnąć, kto jest inicjatorem tego rodzaju wydarzeń, o tyle rzadko można być tego całkowicie pewnym", zob. M. Glenny, *Mroczny rynek. Hakerzy i nowa mafia*, op. cit., s. 201.

[27] Stany Zjednoczone doświadczały prób ataków na Pentagon, podczas gdy Chiny twierdziły, że zagraniczni hakerzy wykradają istotne z ich punktu widzenia informacje, zob. www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm (02. 12. 2013). Należy jednak zauważyć, że stwierdzenie z całą pewnością, że w obu przypadkach mieliśmy do czynienia z operacjami sterowanymi przez państwo, byłoby sporym nadużyciem.

[28] J. Markoff, *Georgia Takes a Beating in the Cyberwar With Russia*, bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia/?_r=0; R. Haddick, *This Week at War: Lessons from Cyberwar I*, www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i#sthash.RAISroHV.dpbs; D. Danchev, *Coordinated Russia vs Georgia cyber attack in progress*, www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670; J. Markoff, *Before the Gunfire, Cyberattacks*, www.nytimes.com/2008/08/13/technology/13cyber.html (02. 12. 2013).

w rzeczywistości działania ofensywne w sieci stały się istotną częścią rosyjskiej strategii[29]. W ten sposób został uczyniony kolejny krok w kierunku wykorzystania przez państwa cyberprzestrzeni do prowadzenia operacji wymierzonych w inne państwa.

Domniemane użycie przez Rosję cyberbroni w trakcie wojny z Gruzją z pewnością było najbardziej zaawansowaną operacją, jaka została przeprowadzona przez państwo w cyberprzestrzeni. Jak się wkrótce okazało, nie wyczerpało jednak wszystkich możliwości aktorów państwowych. Prawdziwe poruszenie w tej materii wywołało odkrycie w 2010 r. superwirusa „Stuxnet". O ile bowiem w wyżej opisanych przypadkach można było przedstawić argumenty na rzecz tezy, że cyberataki w Estonii i Gruzji były tylko pośrednio wspierane przez państwo – a nawet, że były efektem czegoś w rodzaju omawianego już w niniejszym artykule haktywizmu lub patriotycznego zrywu rosyjskich hakerów – o tyle odkrycie nowego wirusa nie pozostawiło już żadnych wątpliwości odnośnie do tego, że państwa są bezpośrednio zaangażowane w prowadzenie działań o charakterze ofensywnym w cyberprzestrzeni[30]. Z punktu widzenia niniejszego artykułu nie jest ważne dokładne opisanie mechanizmu działania „Stuxneta"[31]. Wystarczy jedynie wspomnieć, że superwirus poważnie spowolnił irański program nuklearny – przez zadawanie mu fizycznych zniszczeń, na co szczególnie warto zwrócić uwagę – a jego powstanie miało być według prasy częścią amerykańskiej operacji „Igrzyska Olimpijskie", w ramach której cyberprzestrzeń została wykorzystana do powstrzymania nuklearnych ambicji Irańczyków[32]. O wiele ważniejsze są konsekwencje, jakie wiązały się z jego odkryciem. Po pierwsze, co zostało już wspomniane,

[29] Więcej na ten temat zob. D. Hollis, *Cyberwar Case Study: Georgia 2008,* www.smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 (02. 12. 2013).

[30] Cytowany wielokrotnie w tym artykule M. Glenny pisał o tym w następujący sposób: „Stuxnet jest przejawem wyraźnego narastania trzeciego z najistotniejszych zagrożeń: chodzi o wojnę cybernetyczną. Jest to oprogramowanie tak skomplikowane, że zdaniem badaczy stworzenie go musiało wymagać wieloletniej pracy inżynierów programistów. Przestępczość zorganizowana nie funkcjonuje w taki sposób. Jedyną strukturą zdolną do stworzenia czegoś takiego jak Stuxnet jest państwo dysponujące środkami pozwalającymi na zaprojektowanie i wyprodukowanie zarówno obronnych, jak i zaczepnych typów broni cybernetycznej", zob. M. Glenny, *Mroczny rynek. Hakerzy i nowa mafia,* op. cit., s. 210.

[31] Więcej na ten temat zob. *Stuxnet evolution: NSA input turned stealth weapon into internet-roaming spyware,* www.rt.com/news/stuxnet-pressure-uranium-nsa-080/, E. Kaspersky, *The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight,* wwww.eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/; R. Langner, *Stuxnet's Secret Twin,* www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack (02. 12. 2013).

[32] Więcej na ten temat zob. D. E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran,* www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html; K. Wasilewski, *Wirusy naszych czasów,* Tak Po Prostu. Należy zauważyć, że choć autorstwo „Stuxneta" zarzuca się Stanom Zjednoczonym i Izraelowi, w rzeczywistości trudno stwierdzić z całą pewnością, kto jest za to odpowiedzialny, a oba państwa oczywiście nie przyznają się w sposób jednoznaczny do winy. Warto jednak wspomnieć, że również Edward Snowden twierdził, że „Stuxnet" był efektem współpracy amerykańsko-izraelskiej, zob. *Leaker Snowden says Israel, US created Stuxnet virus,* www.timesofisrael.com/leaker-snowden-says-israel-us-created-stuxnet-virus/ (02. 12. 2013).

dobitnie uświadomiło ono, że państwa są bezpośrednio zaangażowane w prowadzenie ofensywnych działań w cyberprzestrzeni. W powiązaniu z wcześniejszymi doniesieniami o aktywności Rosjan w tej materii mogło to natomiast wskazywać, że trend ten będzie odnotowywał tendencję wzrostową. Po drugie, specyficzne właściwości „Stuxneta" uświadomiły ekspertom, że tak potężne narzędzia, jakimi bez wątpienia są superwirusy komputerowe tworzone przez państwa, mogą być wykorzystywane nie tylko do wywoływania szkód w rzeczywistości wirtualnej, ale również do zadawania poważnych strat materialnych.

„Stuxnet" nie był ostatnim tego rodzaju instrumentem[33]. Z czasem pojawiało się coraz więcej oznak ofensywnej obecności państw w cyberprzestrzeni. Ponieważ nie wnosiły one aż tak dużo do debaty na temat zagrożeń wynikających z działalności aktorów państwowych w tym obszarze dla przedsiębiorców, ich dokładne omówienie nie stanowi punktu zainteresowania niniejszego artykułu. Warto jednak odnotować, że nie tylko potwierdzały omówiony wcześniej trend, ale pokazywały również, że działalność państw w cyberprzestrzeni podlega ciekawej ewolucji. Już po omówionych w tekście przykładach widać bowiem, że kolejne ataki miały coraz bardziej precyzyjny charakter. O ile w przypadku Estonii i Gruzji ich zamierzeniem było doprowadzenie do ogólnego paraliżu państwa, o tyle „Stuxnet" był już narzędziem zaprojektowanym do osiągnięcia konkretnego celu. Wnikliwa obserwacja tego zjawiska pozwalała na wyciągnięcie niezbyt optymistycznych wniosków również w kontekście biznesu już na tym etapie.

Rzeczywistość wkrótce potwierdziła obawy, że działalność państw w cyberprzestrzeni może dotknąć również przedsiębiorców. Przełom w tej kwestii związany był z działaniami Chin, które stworzyły specjalny oddział hakerów odpowiedzialnych m.in. za wykradanie cennych informacji i know-how zachodnim firmom[34]. Wprawdzie podejmowane przez nich akcje były przedmiotem zainteresowania prasy już od jakiegoś czasu – a niektórzy już dawno podejrzewali, że koordynowane są przez państwo – jednak istnienie tzw. oddziału 61398 zostało ostatecznie udowodnione dopiero w lutym 2013 r., gdy firma Mandiant opublikowała

[33] Więcej na ten temat zob. np. K. Wasilewski, *Ciekawski robak*, www.notabene.org.pl/index.php/ciekawski-robak/ (02. 12. 2013).

[34] Sztandarowy przykład może stanowić przypadek amerykańskiej firmy Solid Oak Software Inc., od której Chińczycy postanowili „pożyczyć" technologię wykorzystaną później w rodzimym programie cenzury Internetu, zob. M. Riley, *China Mafia-Style Hack Attack Drives California Firm to Brink*, www.bloomberg.com/news/2012-11-27/china-mafia-style-hack-attack-drives-california-firm-to-brink.html (02. 12. 2013).

obszerny raport, który był efektem trwającego od kilku lat śledztwa[35]. Władze Chińskiej Republiki Ludowej oczywiście nie przyznały się do zarzucanych im czynów[36].

Działania chińskich hakerów – a zwłaszcza fakt, że dotyczyły amerykańskich przedsiębiorców – radykalnie zmieniły sposób patrzenia na kwestie związane z cyberbezpieczeństwem. Upublicznienie informacji, a także kolejne wiadomości o chińsko-amerykańskiej konfrontacji w sieci sprzyjały zwiększeniu świadomości istnienia problemu[37]. Wkrótce w Internecie zaczęły pojawiać się wyliczenia strat, jakie ponosi biznes w związku z różnego rodzaju cyberprzestępczością. Jedne z pierwszych danych w tym obszarze ukazały się dzięki brytyjskiej Federacji Małego Biznesu (Federation of Small Businesses), która informowała, że jej członkowie tracą wskutek przestępczej działalności w sieci około 800 milionów funtów rocznie[38]. W przeliczeniu na jednego członka federacji koszt wynosił blisko 4 tysiące funtów. Jednocześnie zauważono, że ofiarą cyberprzestępstw padło 41% firm zrzeszonych w organizacji. Część z nich – ze względu na obawy odnośnie do bezpieczeństwa – powstrzymywało się od prowadzenia działalności w Internecie, co hamowało ich dalszy rozwój.

Należy również odnotować, że zaangażowanie się państwa w kradzież technologii za pomocą Internetu przeniosło problem cyberprzestępczości na zupełnie nowy poziom. O ile dotychczas bardziej świadome przedsiębiorstwa mogły zabezpieczyć się na ewentualność kradzieży relatywnie łatwo, o tyle obecnie ich sytuacja jest bardziej skomplikowana. Trudno bowiem spodziewać się, że jakakolwiek firma – o ile nie będzie to jedna z wiodących korporacji teleinformatycznych – będzie posiadać zasoby (kapitał, wiedzę, kadry), które umożliwią jej skuteczną obronę przed nieporównywalnie większymi zasobami, którymi

[35] *APT 1. Exposing One of China's Cyber Espionage Units,* Mandiant, www.intelreport.mandiant.com/Mandiant_APT1_Report.pdf. Więcej materiałów na temat działań Chińczyków, zob. np. S. Gorman, D. Barrett, D. Yadron, *Chinese Hackers Hit U.S. Media,* www.online.wsj.com/news/articles/SB10001424127887323926104578276202952260718; N. Perlroth, *Hackers in China Attacked The Times for Last 4 Months*, www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?_r=0; *China's cyber-hacking. Getting Ugly,* www.economist.com/news/leaders/21572200-if-china-wants-respect-abroad-it-must-rein-its-hackers-getting-ugly; P. Harris, *Chinese army hackers are the tip of the cyberwarfare iceberg,* www.theguardian.com/technology/2013/feb/23/mandiant-unit-61398-china-hacking (02. 12. 2013).

[36] *Beijing denies existence of PLA hacking unit,* www.wantchinatimes.com/news-subclass-cnt.aspx?id=20130221000009&cid=1101; M. Xuequan, *China opposes U.S. report on Chinese military,* wwww.news.xinhuanet.com/english/china/2013-05/07/c_124677298.htm (02. 12. 2013).

[37] Więcej na temat chińsko-amerykańskich nieporozumień w kwestiach związanych z cyberbezpieczeństwem, zob. K. Wasilewski, *Jak rozpętałem cyberwojnę?,* www.notabene.org.pl/index.php/jak-rozpetalem-cyberwojne/ (02. 12. 2013).

[38] J. Hurley, *Cyber crime 'costs small companies £800m a year'*, www.telegraph.co.uk/finance/yourbusiness/10069374/Cyber-crime-costs-small-companies-800m-a-year.html (02. 12. 2013).

dysponuje państwo. W tej chwili nie sposób jednoznacznie powiedzieć, jak zostanie rozwiązany ten dylemat, wiadomo jednak, że w niedalekiej przyszłości będzie miał prawdopodobnie istotny wpływ na środowisko funkcjonowania przedsiębiorstw. Wiele wskazuje na to, że skuteczna obrona przed tego typu zagrożeniami będzie wymagała jakiejś formy partnerstwa publiczno-prywatnego, w ramach którego będzie funkcjonował szybki przepływ informacji między przedsiębiorcami a odpowiednią jednostką administracji rządowej[39]. W tym miejscu należy jednak wspomnieć o kolejnym problemie, który został obnażony przy okazji upublicznienia informacji o działalności chińskich hakerów. W trakcie licznych dyskusji, które odbyły się w tym okresie, dostrzeżono, że w rzeczywistości trudno ustalić precyzyjnie skalę zjawiska. Wynika to z faktu, że nie wszystkie firmy pragną podzielić się informacją, że zostały zaatakowane, co jest oczywiście wynikiem obawy o utratę zaufania klientów[40]. Pozwala to uzmysłowić sobie, jak trudnym i odpowiedzialnym zadaniem może być budowa platformy współpracy między rządem a przedsiębiorcami w zakresie cyberbezpieczeństwa.

Wśród ekspertów i dziennikarzy zajmujących się tematyką bezpieczeństwa w sieci nadal trwają spory, czy działalność aktorów państwowych w cyberprzestrzeni powinna być postrzegana jako zagrożenie przez wszystkich przedsiębiorców. Niektórzy podkreślają, że zaniepokojenie mogą odczuwać co najwyżej firmy, które działają w obrębie sektora obronnego, co wynika z faktu, że to właśnie tego rodzaju technologia może stanowić przedmiot zainteresowania innych państw[41]. Z drugiej jednak strony nie brakuje również takich ekspertów, którzy podkreślają, że przedsiębiorcy powinni być świadomi zagrożeń, jakie wynikają z wykorzystywania przez państwa cyberprzestrzeni, i odpowiednio się na nie przygotować[42]. Wydaje się, że dotychczasowe przykłady i trendy w zakresie działalności aktorów państwowych w sieci skłaniają raczej do uwzględnienia mniej optymistycznej wersji przyszłości. Wzrost liczby hakerów motywowanych czynnikami politycznymi w połączeniu z relatywną atrakcyjnością cyberprzestrzeni dla realizacji celów państw – a więc pewnego rodzaju splot haktywizmu i polityki – a także ewolucja instrumentów, z których korzystają

[39] Zagadnienia te zostaną poruszone w dalszej części artykułu.
[40] M.in. ta kwestia jest przyczyną trudności w dokładnym oszacowaniu kosztów związanych z cyberprzestępczością.
[41] Zob. np. A. Scott, *Defend yourself against the cyber threats ready to attack your business*, www.theguardian.com/media-network/media-network-blog/2013/oct/30/cyber-threats-business-botnets-protect (02. 12. 2013).
[42] R. Lemos, *World's Trouble Spots Escalating Into Cyberthreats For Businesses*, www.darkreading.com/advanced-threats/worlds-trouble-spots-escalating-into-cyb/240160851 (02. 12. 2013).

aktorzy państwowi, i charakteru ich działalności ofensywnej powodują, że przedsiębiorcy mogą spodziewać się większego zagrożenia ze strony państw.

Problem ten dotyczy zwłaszcza rozwiniętych firm zachodnich, których atutem jest dysponowanie zaawansowaną technologią lub odpowiednim know-how. Należy również zauważyć, że kwestię tę powinno się interpretować w kontekście modelu gospodarki opartej na wiedzy (GOW), do przyjęcia którego dążymy również w Polsce[43]. Jeśli uznamy, że podstawowymi czynnikami wzrostu są – lub mają być w przyszłości – wiedza i technologia, tym bardziej powinniśmy troszczyć się o odpowiednie zabezpieczenie kapitału w postaci szeroko rozumianej własności intelektualnej. Z pewnością innowacyjność, a co za tym idzie atrakcyjność większości polskich firm jest niższa niż przedsiębiorstw amerykańskich czy brytyjskich, wydaje się jednak, że wyciągnięcie na tej postawie wniosku, że z całą pewnością nie muszą obawiać się zagrożenia ze strony państw, które z różnych względów byłyby zainteresowane kradzieżą ich technologii, byłoby błędem[44]. Rzecz jasna – co wymaga szczególnego pokreślenia – analiza bezpieczeństwa przedsiębiorstwa w tym kontekście wymaga każdorazowo indywidualnego i rozsądnego podejścia oraz uwzględnienia odpowiedniej skali, z pewnością jednak świadomość zagrożenia będzie istotną wartością dodaną zarówno w trakcie bieżącego funkcjonowania firmy, jak i przy podejmowaniu decyzji odnośnie do ewentualnej ekspansji w przyszłości.

c) Pozostałe podmioty

Istnieją różne klasyfikacje szczegółowe, które zawierają szerszy katalog podmiotów stanowiących zagrożenie w cyberprzestrzeni. Wspomniane już w tym artykule GAO wymienia wśród nich np.: operatorów botnetów, grupy przestępcze, hakerów, tzw. insiderów, narody, phisherów, spamerów, autorów złośliwych programów i oprogramowania szpiegowskiego oraz terrorystów[45]. Należy jednak wskazać na dwie właściwości tego typu klasyfikacji. Po pierwsze – ich szczegółowy charakter. Wydaje się bowiem, że niemal każdy

[43] Organizacja Współpracy Gospodarczej i Rozwoju (OECD) opisuje GOW w następujący sposób: „Kraje OECD są w coraz większym stopniu zorganizowane w oparciu o wiedzę i informację. Wiedza jest obecnie uważana za katalizator produktywności i ekonomicznego wzrostu. W konsekwencji kładzie się nowy nacisk na rolę informacji, technologii i nauczania w osiągnięciach gospodarczych. Termin »gospodarka oparta na wiedzy« wynika z tego szerszego uznania roli wiedzy i technologii w gospodarkach państw OECD", zob. www.oecd.org/sti/sci-tech/theknowledge-basedeconomy.htm (02. 12. 2013).

[44] Więcej na temat innowacyjności polskich przedsiębiorstw, zob. *Obecny stan aktywności innowacyjnej polskich przedsiębiorstw,* www.inwestor.msp.gov.pl/si/polska-gospodarka/wiadomosci-gospodarcze/25869,Obecny-stan-aktywnosci-innowacyjnej-polskich-przedsiebiorstw.html (02. 12. 2013).

[45] *CYBERSECURITY. National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, op. cit., s. 5.

z wymienionych tutaj podmiotów z powodzeniem zmieściłby się również w szerszym zbiorze cyberprzestępców. Po drugie, nazwy niektórych z nich (np. phisherzy, spamerzy) biorą się od narzędzi, którymi posługują się w swojej działalności przestępczej. Nie dotyczy to oczywiście tzw. insiderów – osoby, które działają wewnątrz organizacji – i terrorystów, którzy najprawdopodobniej również coraz chętniej będą wykorzystywać możliwości, jakie daje cyberprzestrzeń, do prowadzenia swoich działań[46]. Oba argumenty, jak również charakter niniejszego artykułu, skłoniły zatem autora do pominięcia dokładniejszego ich opisu i jedynie wymienienia tych podmiotów, aby czytelnicy mieli pełniejszy obraz sytuacji[47].

2. Przedmiotowy katalog zagrożeń i narzędzia cyberprzestępców

Przedstawienie wyczerpującego katalogu zagrożeń przedmiotowych jest równie trudne jak wyliczenie podmiotów, których działalności mogą obawiać się przedsiębiorcy. Sytuacja taka wynika zarówno z tempa zmian, jakie zachodzą w obrębie cyberprzestrzeni, jak i ze ścisłych powiązań między poszczególnymi zagrożeniami. Jest również podyktowana faktem, że cyberprzestępcy dość szybko dostosowują swoje metody do „warunków rynkowych"[48]. Biorąc pod uwagę cele, jakie postawił sobie autor artykułu, rozsądne wydaje się opisanie podstawowych, a zarazem najistotniejszych narzędzi, którymi posługują się przestępcy w sieci do przeprowadzania ataków na przedsiębiorców, wraz z zaznaczeniem aktualnych trendów w tym zakresie. Jednocześnie należy zauważyć, że zdecydowano się na pominięcie dokładnego opisu złośliwego oprogramowania (ang. *malware*) i przedstawienia jego klasyfikacji. Podyktowane jest to również celem, jaki przyświeca niniejszemu tekstowi. Złośliwe oprogramowanie jest bowiem w pewnym sensie terminem generalnym – to ono jest źródłem lub nieodłącznym elementem większości problemów, jakie zachodzą w cyberprzestrzeni, również tych, które zostaną omówione poniżej. Stanowi zarazem zagrożenie dla wszystkich użytkowników komputerów, pełne jego omówienie mogłoby więc

[46] Możliwości, jakie daje cyberprzestrzeń, dla prowadzenia działalności terrorystycznej mogłyby być przedmiotem odrębnego artykułu. Ciekawy raport na temat wykorzystania Internetu przez terrorystów, zob. *CRS Report for Congress Prepared for Members and Committees of Congress. Terrorist Use of the Internet:Information Operations in Cyberspace*, Congressional Research Service, Marzec 2011, www.fas.org/sgp/crs/terror/R41674.pdf (02. 12. 2013).

[47] Sytuacja taka podyktowana jest również faktem, że część narzędzi, które wykorzystywane są przez wymienione wyżej podmioty, zostanie opisana w następnym podpunkcie.

[48] A. Scott, *Defend yourself against the cyber threats ready to attack your business*, op. cit. Dobrym przykładem, który pozwala zobrazować innowacyjność cyberprzestępców, jest fakt, że próbują dostosować swoje metody do urządzeń mobilnych, zob. np. *Emerging Cyber Threats Report 2014*, Georgia Tech Information Security Center, Georgia Tech Research Institute, wwww.gtsecuritysummit.com/2014Report.pdf, s. 6 - 8 (02. 12. 2013).

stanowić przedmiot zainteresowania innego, równie generalnego artykułu[49]. Autor postanowił zatem zwrócić uwagę tylko na te jego aspekty, które są szczególnie istotne z punktu widzenia grupy docelowej niniejszego artykułu, czyli przedsiębiorców.

a) Botnet

Terminem „botnet" określa się „zbiór zainfekowanych komputerów kontrolowanych zdalnie przez atakującego"[50]. Maszyny mogą być następnie wykorzystywane m.in. do rozsyłania spamu, złośliwego oprogramowania lub dokonywania tzw. ataków DDoS (ang. *Distributed Denial of Service*)[51]. Należy zauważyć, że narzędzie to jest szczególnie atrakcyjne z punktu widzenia cyberprzestępców. Sytuacja taka wynika z faktu, że zainfekowany komputer pracuje w miarę normalnie, a co za tym idzie – wykrycie ataku jest niemal niemożliwe dla niezaawansowanego użytkownika[52].

Szczególnie wart podkreślenia jest w pewnym sensie zbiorowy charakter przedsięwzięcia. Przestępcy zainteresowani są zainfekowaniem jak największej liczby maszyn, które mogą służyć im do realizacji ich celów. Czyni to przedsiębiorstwa naturalnym celem ataków[53].

Należy również zauważyć, że twórcy botnetów często nie są ich użytkownikami. Źródłem ich zarobku jest zatem wygenerowanie odpowiedniego systemu i sprzedanie go zleceniodawcom[54]. Warte odnotowania jest również zjawisko powstawania tzw. mobilnych

[49] Więcej na temat szkodliwości m.in. złośliwego oprogramowania dla biznesu, zob. *Security threats: A guide for SMEs,* GFI White Paper, www.gfi.com/whitepapers/Security_threats_SMEs.pdf, s. 3 - 4 (02. 12. 2013).
[50] *What is a Botnet?,* www.blog.kaspersky.com/botnet/ (02. 12. 2013).
[51] „Ataki DDoS to najpowszechniejsza broń w cyberprzestrzeni. Dokonują ich tak zwane botnety, czyli cybernetyczne odpowiedniki ożywionych umarlaków z nakręconego w latach pięćdziesiątych hollywoodzkiego klasyka pod tytułem *Inwazja porywaczy ciał.* Wirus »przechwytuje« komputer, który znajduje się pod wpływem tak zwanego Command and Control Server (serwer dowodzenia i kontroli). Wirus zakaża tysiące komputerów, które zyskują następnie miano »zombie«, aby służyć jako niewolnicy potężnego serwera dowodzenia. Na co dzień pracują normalnie, jak zwykłe komputery. Zwyczajny użytkownik nie zdaje sobie sprawy, że jego komputer został teraz żołnierzem potężnej armii cyfrowej śmierci. Nieszczęsna ofiara może co najwyżej spostrzec, że komputer chodził jakby wolniej… I nic dziwnego, skoro ze wszystkich sił, choć po kryjomu, wysyła gigabajty spamu z reklamą Vicodinu (…)"; „Jednak często zamiast tego botnety otrzymują polecenie przeprowadzenia ataku DDoS. Wszystkim zombi każe się wtedy wejść w tym samym czasie na tę samą stronę. Każdy portal czy serwer padnie, jeżeli będzie miał do czynienia z takim natężeniem ruchu. Strona przestaje działać. Jeśli atak jest odpowiednio silny, zawieszają się całe systemy", zob. M. Glenny, *Mroczny rynek. Hakerzy i nowa mafia,* op. cit., s. 131. Więcej na temat ataków DDoS zob. także ibidem.
[52] *What is a botnet?,* www.microsoft.com/security/resources/botnet-whatis.aspx (02. 12. 2013).
[53] „Małe i średnie przedsiębiorstwa są idealnym środowiskiem dla użycia botnetów: dysponują sporą liczbą maszyn powiązanych między sobą, a pracownicy biurowi zazwyczaj ich nie wyłączają, gdy wychodzą, tworząc tym samym dostęp do wirtualnie nieskończonych zasobów dla atakujących", zob. A. Scott, *Defend yourself against the cyber threats ready to attack your business,* op. cit.
[54] Zob. ibidem; *What is a Botnet?,* op. cit.

botnetów, które działają – jak wskazuje nazwa – w oparciu o urządzenia mobilne, np. smartfony[55].

O ile niezwykle trudna jest obrona przed atakami DDoS, które dokonywane są za pomocą botnetów, o tyle relatywnie łatwo uchronić się przed staniem się częścią mechanizmu. Aby zachować bezpieczeństwo, użytkownicy powinni na bieżąco aktualizować oprogramowanie, które zainstalowane jest na ich komputerach, oraz powstrzymywać się przed klikaniem w nieznane linki, które często wysyłane są za pośrednictwem botnetów na pocztę e-mail[56].

b) Phishing i tzw. inżynieria społeczna

Phising definiuje się jako „oszustwo komputerowe bazujące na zasadach socjotechniki i charakteryzujące się próbą uzyskania poufnych informacji, takich jak hasła czy informacje dotyczące kart kredytowych, przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikatory internetowe”[57]. Wejście w posiadanie ważnych informacji – w zależności od ich rangi – otwiera przestępcom drogę do podejmowania szeregu rozmaitych działań[58]. Atak phisingowy często odbywa się przez stworzenie kopii strony odpowiedniej instytucji (np. banku), co pozwala na wyłudzenie od mniej zorientowanych użytkowników istotnych danych, jak również – jak wskazuje przytoczona wyżej definicja – wskutek podszycia się przez cyberprzestępcę pod konkretną osobę (np. administratora danych czy firmowego specjalistę od urządzeń teleinformatycznych), która może mieć specjalne – nadane jej na przykład przez firmę lub po prostu związane ze sprawowaną funkcją – kompetencje w zakresie dostępu do danych użytkowników[59].

Przeprowadzenie ataku phisingowego często wiąże się z tzw. inżynierią społeczną, która polega na „manipulowaniu ludźmi tak, aby podjęli odpowiednie działania lub dostarczyli informacje, np. sprawienie, że ściągną określony plik lub zdradzą swoje hasło albo

[55] *Internet Security Threat Report 2013,* Tom 18, kwiecień 2013, Symantec, www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf, s. 37 (02. 12. 2013).
[56] *What is a Botnet?,* op. cit.
[57] *Co to jest Phishing?,* www.support.kaspersky.com/pl/viruses/general/2313 (02. 12. 2013).
[58] Wystarczy wspomnieć, że przestępcy, którzy wejdą w posiadanie tak ważnych informacji, mogą zarówno okraść przedsiębiorstwo, jak i sprzedać zdobyte dane innym podmiotom. Poznanie np. haseł dostępu może również otworzyć im drogę do podejmowania innych przestępczych działań.
[59] *Na czym polega atak phishingowy?,* www.kaspersky.pl/cyberthreats.html?s=threats_phishing; *Top 5 Cyber Threats to Businesses,* www.checkmarx.com/2012/03/28/top-5-cyber-threats-to-businesses/ (02. 12. 2013).

szczegóły dotyczące karty kredytowej”[60]. Przestępcy umiejętnie wykorzystują w ten sposób największą słabość wszelkich systemów bezpieczeństwa, jaką stanowi człowiek.

Jak pokazują aktualne dane, phising jest istotnym problemem użytkowników Internetu[61]. Należy jednak przyznać, że sprzyja temu ewolucja, jaka zachodzi w sposobach korzystania z dostępu do niego, zwłaszcza w obrębie tzw. portali społecznościowych. Jak bowiem słusznie zauważył J. Henderson, zastosowanie skomplikowanych technik socjotechnicznych nie jest obecnie tak bardzo potrzebne, gdy „szczegóły, których poszukuje przestępca, są już umieszczone na portalach społecznościowych”[62]. Warto zauważyć, że źródłem potencjalnego zagrożenia w tej materii mogą stać się zarówno nieuważnie opublikowane przez użytkowników dane, jak i zbyt duża ilość publikowanych w sieci materiałów[63]. Odrębny problem stanowią fikcyjne profile różnych organizacji, które również mogą pomóc cyberprzestępcom w zbieraniu danych[64].

Choć skuteczna obrona przed atakami phishingowymi jest relatywnie łatwa, ogromna ich liczba – dane firmy Kasperky pokazują, że ich ofiarą pada dziennie około 100 tysięcy osób – może sugerować, że w rzeczywistości jest inaczej[65]. Przyczyną takiego stanu rzeczy jest – wspomniane już w tym artykule – umiejętne korzystanie przez cyberprzestępców z największej luki systemów bezpieczeństwa, jaką stanowi człowiek. Pozwala to uzmysłowić sobie, że wszelkie rozwiązania w zakresie walki z atakami phishingowymi będą nieskuteczne, jeśli pracownicy firmy nie będą odpowiednio uświadomieni odnośnie do istnienia zagrożenia. Kierownictwo przedsiębiorstwa powinno zatem organizować szkolenia, w ramach których

[60] A. Scott, *Defend yourself against the cyber threats ready to attack your business*, op. cit. Inżynieria społeczna nazywana jest również socjotechniką, którą definiuje się w następujący sposób: „Socjotechnika to wywieranie wpływu na ludzi i stosowanie perswazji w celu oszukania ich tak, aby uwierzyli, że socjotechnik jest osobą o sugerowanej przez siebie, a stworzonej na potrzeby manipulacji tożsamości. Dzięki temu socjotechnik jest w stanie wykorzystać swoich rozmówców, przy dodatkowym (lub nie) użyciu środków technologicznych, do zdobycia poszukiwanych informacji”, zob. K. Mitnick, *Sztuka podstępu,* Helion, Gliwice 2003, s. 4.

[61] D. Real, *Cyber threats: trends in phishing and spear phishing – infographic*, www.theguardian.com/media-network/media-network-blog/2013/jul/12/cyber-threats-trends-spear-phishing; *Kaspersky Lab report: 37.3 million users experienced phishing attacks in the last year*, www.kaspersky.com/about/news/press/2013/kaspersky_lab_report_37_3_million_users_experienced_phishing_attacks_in_the_last_year (02. 12. 2013).

[62] J. Henderson, *Check Point: Biggest cyber security threats to businesses*, www.techday.com/it-brief/news/check-point-biggest-cyber-security-threats-to-businesses/173034/. Więcej na temat roli porali społecznościowych w procedurze phishingu, zob. *Internet Security Threat Report 2013*, op. cit., s. 35 - 37. (02. 12. 2013).

[63] Pozwala to bowiem na dość dokładne sprofilowanie użytkownika, co może zostać wykorzystane do ataku phisingowego, jak również ułatwić kradzież tożsamości, zob. *Top 5 Cyber Threats to Businesses*, op. cit.

[64] J. Henderson, *Check Point: Biggest cyber security threats to businesses*, op. cit. Więcej na temat zastosowania fikcyjnych kont przez cyberprzestępców, zob. także B. Jackson, *8 cyber-security threats to prepare for in 2014*, www.itbusiness.ca/news/8-cyber-security-threats-to-prepare-for-in-2014/44815 (02. 12. 2013).

[65] Dane za: *Kaspersky Lab report: 37.3 million users experienced phishing attacks in the last year*, op. cit.

poruszane będą zagadnienia związane z cyberbezpieczeństwem. Wszyscy pracownicy powinni również zostać uczuleni na kwestię zasadniczych reguł postępowania, które mogą ograniczyć ryzyko stania się ofiarą phishingu. Już przestrzeganie podstawowych zasad – takich jak nieotwieranie załączników umieszczonych w mailach od nieznanych lub podejrzanych nadawców, niewypełnianie formularzy, które wymagają podania danych osobowych, uważne korzystanie ze stron internetowych banków i innych instytucji, informowanie odpowiednich organów o wszystkich niepokojących ruchach w sieci, posiadanie aktualnego oprogramowania – może bowiem znacznie przyczynić się do zwiększenia poziomu bezpieczeństwa przedsiębiorstwa[66].

c) BYOD

Powstanie anglojęzycznego terminu „BYOD" (*bring your own device*) związane jest ze zmianami technologicznymi, jakie miały miejsce w ciągu ostatnich kilku lat, a zwłaszcza z pojawieniem się w obiegu smartfonów i innych urządzeń mobilnych, które zrewolucjonizowały rynek telekomunikacji. BYOD pierwotnie oznaczał politykę firm, w ramach której pozwalano pracownikom na przynoszenie do pracy i korzystanie w jej trakcie z prywatnych urządzeń mobilnych[67]. Gwałtowny rozwój cyberprzestępczości szybko spowodował jednak, że termin ten zaczął być kojarzony również z nowym – istotnym z punktu widzenia przedsiębiorców – źródłem zagrożenia bezpieczeństwa w sieci.

Należy zauważyć, że urządzenia mobilne stały się niezwykle cennym dla cyberprzestępców narzędziem. Wpływ na taki stan rzeczy miało kilka ściśle ze sobą powiązanych czynników. Przede wszystkim fakt, że za ich pośrednictwem można było nie tylko połączyć się z Internetem, ale – co wymaga szczególnego podkreślenia – mieć do niego stały dostęp[68]. Po drugie, użytkownicy urządzeń mobilnych, choć korzystają z nich równie często jak z komputerów, nie dbają w wystarczającym stopniu o odpowiednie ich zabezpieczenie przed złośliwym oprogramowaniem[69]. Po trzecie, popularności tego typu urządzeń wśród cyberprzstępców sprzyjał rzecz jasna omówiony wyżej trend BYOD, dzięki

[66] Więcej na temat zabezpieczeń przed atakiem phishingowym, zob. *Na czym polega atak phishingowy?*, op. cit.
[67] *Internet Security Threat Report 2013*, op. cit., s. 37.
[68] Znaczenie tego argumentu dla przestępców, którzy prowadzą swoją działalność w sieci, zostało omówione przy okazji opisu botnetów.
[69] *Top 5 Cyber Threats to Businesses*, op. cit.; E. Blair, *More than 80% of Mobile Devices Will Remain Unprotected in 2013, Juniper Research Reports*, www.reviewstudio.net/789-more-than-80-of-mobile-devices-will-remain-unprotected-in-2013-juniper-research-reports; *Number of the Week: 55% of Mobile Devices Using Unprotected Wi-Fi Networks*, www.kaspersky.com/about/news/virus/2012/Number_of_the_Week_55_of_Mobile_Devices_Using_Unprotected_Wi_Fi_Networks (02. 12. 2013).

któremu zyskali kolejne źródło dostępu do zazwyczaj lepiej zabezpieczonych sieci firmowych[70]. Warto podkreślić, że działanie w tej materii ułatwia przestępcom fakt, że część pracowników wykorzystuje swoje prywatne urządzenia mobilne w celach służbowych[71].

Wydaje się, że wzrost popularności smartfonów pozwala na wyciągnięcie niezbyt optymistycznego wniosku, że rosła będzie także skala zagrożeń, które związane są z ich użytkowaniem. Sytuacja taka prawdopodobnie wymusi na przedsiębiorcach konieczność opracowania i przyjęcia odpowiedniej polityki w zakresie wykorzystania urządzeń mobilnych w miejscu pracy w niedalekiej przyszłości. Na tę chwilę skuteczna ochrona przed omawianymi zagrożeniami wymaga jednak zarówno wzrostu świadomości problemu, jak i instalacji podstawowych zabezpieczeń (np. programów antywirusowych), które utrudnią cyberprzestępcom dostęp do smartfonów i innych tego typu narzędzi[72].

d) Zagrożenia wewnętrzne

Działalność tzw. insiderów – osób, które funkcjonują w obrębie różnego rodzaju instytucji i posiadają „informacje niedostępne dla innych" – stanowi tradycyjne źródło zagrożenia dla biznesu[73]. Cyberprzestrzeń otworzyła jednak przed nimi inne możliwości i nadała ich przedsięwzięciom nowy wymiar. Dzięki funkcjonowaniu w sieci mogą bowiem działać niepostrzeżenie, a co za tym idzie – przynosić przedsiębiorstwu szkody w dłuższym okresie[74].

[70] „Pomyśl o tym – Twój smartfon ma kamerę. Ma także mikrofon. Może nagrywać rozmowy. Dodaj te cechy do możliwości dostępu do twojej sieci firmowej, a otrzymasz idealną drabinę do wspięcia się po ścianach, o których mówimy", zob. J. Henderson, *Check Point: Biggest cyber security threats to businesses,* op. cit.; : „Jeżeli firma nie reguluje wykorzystywania prywatnych smartfonów i tabletów mających dostęp do korporacyjnej infrastruktury IT, poufne informacje zaczną wyciekać z systemu - jest to tylko kwestia czasu. Wyciek może zostać spowodowany infekcją szkodliwego oprogramowania lub zgubieniem urządzenia przez pracownika; w obu przypadkach rezultat jest taki sam – dane zostają utracone lub wpadają w niepowołane ręce", zob. *34% firm ryzykuje wyciekiem danych, nie kontrolując prywatnych urządzeń w miejscu pracy,* www.kaspersky.pl/about.html?s=news&newsid=2027 (02. 12. 2013).

[71] Chodzi tu głównie o dostęp do służbowej poczty, zob. *34% firm ryzykuje wyciekiem danych, nie kontrolując prywatnych urządzeń w miejscu pracy,* op. cit.

[72] Warto zauważyć, że wbrew obiegowej opinii nie ma całkowicie bezpiecznych urządzeń mobilnych. Problem złośliwego oprogramowania dotyczy – choć należy przyznać, że w różnej skali – zarówno narzędzi opartych na systemie iOS, jak i na Androidzie. Więcej na ten temat zob. *Internet Security Threat Report 2013,* op. cit., s. 37.

[73] Definicja za Słownikiem Języka Polskiego, zob. www.sjp.pl/insider (02. 12. 2013).

[74] Trudno o odpowiednie dane, które obrazowałyby skalę zjawiska w Polsce, jednak amerykańskie statystyki pokazują, że insiderzy, którzy działają w obrębie tamtejszego sektora finansowego, są w stanie kontynuować swój proceder nieprzerwanie przez 32 miesiące, zob. J. Henderson, *Check Point: Biggest cyber security threats to businesses,* op. cit.; C. M. Matthews, *Insider Theft: the Real Cyber Threat?, www.blogs.wsj.com/riskandcompliance/2013/03/27/insider-theft-the-real-cyber-threat/* (02. 12. 2013).

Kaspersky Lab proponuje wyróżnić sześć typów insiderów[75]. Pierwszy – a zarazem najczęściej występujący – to tzw. insider nieostrożny. Są to osoby zazwyczaj nieświadome zagrożenia, które nieumyślnie mogą spowodować straty dla przedsiębiorstwa, np. przez wynoszenie związanych z pracą materiałów poza obręb biura lub utratę nośnika danych, na którym gromadziły służbowe informacje. Kolejny typ – tzw. naiwny insider – jest ściśle powiązany z procederem wspomnianego wyżej pishingu. To osoby, które ulegają manipulacji i wskutek niej przekazują informacje przestępcom. Warto zauważyć, że te dwa rodzaje insiderów łączy jedno – zarówno nieostrożni, jak i naiwni przyczyniają się do wycieku cennych danych w sposób nieświadomy, co oznacza, że nie zdają sobie sprawy ze szkód, jakie wyrządzają własnej firmie.

Inaczej sytuacja ma się z pozostałymi czterema typami insiderów, których Kaspersky Lab określa mianem złośliwych. Pierwsi to sabotażyści, którzy szkodzą przedsiębiorstwu z różnego rodzaju pobudek osobistych[76]. Niezwykle ciekawa jest ich cecha charakterystyczna, która sprawia, że powodowane przez nich zagrożenie może być różnej rangi. Sabotażyści nie zamierzają bowiem opuszczać swojego miejsca pracy, a ich celem jest najczęściej po prostu szkodzenie przedsiębiorstwu. Taki stan rzeczy powoduje, że ich działalność może dotyczyć zarówno mało istotnych kwestii, które jednak utrudniają pracę przedsiębiorstwa, jak i spraw dużo poważniejszych[77]. Kolejna grupa insiderów, która zagraża firmie w sposób świadomy, to nielojalni pracownicy. Od sabotażystów różni ich fakt, że zamierzają opuścić przedsiębiorstwo, ale jeszcze nie poinformowali o tym władz zwierzchnich. Wykradają zatem informacje, co do których mają przekonanie, że przydarzą im się w przyszłości dla osiągnięcia korzyści osobistych, np. w celu ich sprzedaży konkurencji[78].

Działalność dwóch ostatnich typów insiderów – tzw. moonlighterów i kretów – jest szczególnie niebezpieczna dla przedsiębiorców. Wynika to z faktu, że ich przedsięwzięcia są wysoce ukierunkowane, co oznacza, że doskonale zdają sobie sprawę z tego, jakie informacje chcą wyprowadzić. Tzw. moonlighterzy wykradają dane z różnych przyczyn – może

[75] Więcej zob. *Rozpoznawanie różnych typów insiderów - osób atakujących z wewnątrz*, www.securelist.pl/analysis/7061,rozpoznawanie_roznych_typow_insiderow_osob_atakujacych_z_wewnatrz.html (02. 12. 2013).

[76] „Często są niezadowoleni i czują się tak, jakby byli traktowani jak zło konieczne: ich wynagrodzenie jest niskie, są zbyt nisko w hierarchii korporacyjnej drabiny, nie są uprawnieni do pewnych wygód, takich jak laptop, samochód służbowy, sekretarka itd.", zob. ibidem.

[77] Sabotażyści lubią szkodzić zwłaszcza wizerunkowi firmy.

[78] Przykład działania nielojalnego pracownika, zob. A. Sachdev, *Former Motorola engineer sentenced to 4 years in trade-secret case*, www.articles.chicagotribune.com/2012-08-31/business/ct-biz-0830-moto-theft--20120831_1_trade-secret-case-hanjuan-jin-trade-secrets (02. 12. 2013).

powodować nimi zarówno chęć powiększenia własnego dochodu, jak i groźba ze strony nieuczciwej konkurencji, której ulegli. Jak zauważyła firma Kaspersky Lab, do ich grona mogą zaliczać się pracownicy różnego szczebla[79]. Inaczej jest w przypadku tzw. kretów. Ten rodzaj insiderów charakteryzuje się odpowiednimi umiejętnościami – często hakerskimi – które pozwalają na zdobycie dokładnie tych informacji, w posiadanie których chce wejść ich zleceniodawca. Cecha ta – w połączeniu z determinacją – powoduje, że tzw. krety stanowią bardzo poważne źródło niebezpieczeństwa.

Zagrożenia wewnętrzne – ze względu na ścisłe powiązania z czynnikiem ludzkim – są poważnym, a zarazem dość trudnym do zneutralizowania problemem przedsiębiorstw[80]. O ile skutki działalności dwóch pierwszych typów insiderów – nieostrożny i naiwny – można ograniczyć przez zwiększanie świadomości pracowników (np. przez organizację odpowiednich szkoleń), o tyle znacznie trudniej walczyć z insiderami złośliwymi. W tym celu przedsiębiorstwa powinny stworzyć przejrzystą politykę i system dostępu do szczególnie cennych informacji, a także ustanowić odpowiedni system monitoringu w celu weryfikacji, czy pracownicy – zwłaszcza ci, którzy mają dostęp do cennych informacji – stosują się do zaleceń w wystarczającym stopniu[81]. Część ekspertów – odwołując się tym samym do istotnej roli, jaką odgrywa czynnik ludzki w zagrożeniach wewnętrznych – proponuje jednak spojrzeć na sprawę szerzej i wymienione już rozwiązania uzupełnić o tzw. miękkie środki, które poprawią atmosferę w pracy[82]. Jakkolwiek idealistycznie i generalnie to brzmi, należy przyznać, że może przyczynić się do ograniczenia działalności przynajmniej tych insiderów, którzy motywowani są swoim złym samopoczuciem w miejscu pracy.

e) Zagrożenia typu APT

Termin „APT" (ang. *Advanced Persistent Threat*) można rozpatrywać zarówno na płaszczyźnie przedmiotowej, jak i podmiotowej[83]. W rozumieniu, jakie proponuje się

[79] *Rozpoznawanie różnych typów insiderów - osób atakujących z wewnątrz,* op. cit.
[80] Jak twierdzą eksperci firmy Symantec: „Większość małych i średnich przedsiębiorstw powinna przejmować się kimś, kto jest wewnątrz, tak bardzo jak powinna przejmować się anonimowym hakerem", zob. *Internet Security Threat Report 2013,* op. cit., s. 18.
[81] C. M. Matthews, *Insider Theft: the Real Cyber Threat?,* op. cit. Więcej na temat roli monitoringu (zwłaszcza działu telekomunikacyjnego firmy), zob. *Countering the cyber threat to business,* Big Picture, Institute of Directors, wiosna 2013, s. 17.
[82] „Ponadto jest ważne, aby pamiętać, że pozytywne środowisko pracy, w którym ludzie są szczęśliwi, jest mniej podatne na ataki insiderów niż środowisko, które jest opresyjne", zob. *Security threats: A guide for SMEs,* GFI White Paper, op. cit., s. 8.
[83] „Z jednej strony APT odnosi się do wysoce precyzyjnego rodzaju cyberataku. Z drugiej może się także odnosić do grup, często wspieranych przez państwo lub dobrze finansowanych przez inne źródło, które są

w niniejszej części artykułu, oznacza on „zaawansowane trwałe zagrożenia", czyli działania przestępcze, które opierają się na „zaawansowanej technologii, jak również na wielu metodach i różnych wektorach ataku. Wszystko po to, by dotrzeć do konkretnych organizacji w celu pozyskania określonych, niejawnych informacji"[84].

Ataki APT to jedno z najpotężniejszych narzędzi w rękach cyberprzestępców. Dzieje się tak co najmniej z kilku względów. Przede wszystkim należy zauważyć, że za ich dokonywanie odpowiedzialna jest zazwyczaj grupa specjalistów, którzy dysponują zaawansowanymi umiejętnościami hakerskimi i socjotechnicznymi[85]. Problematyczny jest również fakt, że przyświeca im – co wymaga szczególnego pokreślenia – konkretny cel, który są w stanie osiągnąć za pomocą wszelkich środków. Co więcej, zazwyczaj nie dokonują tego przez agresywny, a co za tym idzie – łatwy do zauważenia atak, lecz starają się „zyskać dostęp do sieci i wykraść informację po cichu. Przyjmują powolne nastawienie, które często czyni ich działania trudnymi do wykrycia, co z kolei zapewnia im wysokie prawdopodobieństwo sukcesu"[86].

Zaawansowane trwałe zagrożenia były przedmiotem poważnych wątpliwości wśród ekspertów[87]. Przyczyna takiego stanu rzeczy leży w samej naturze zagrożenia. Można się bowiem zastanawiać, czy zastosowanie tak skomplikowanych narzędzi – do czego wymagane są zarówno odpowiednie umiejętności, jak i środki – jest możliwe i opłacalne wobec innych podmiotów niż państwa i wiodące w skali świata korporacje. Należy przyznać, że wątpliwości te przez długi czas wzmacniały także znane przypadki posłużenia się APT[88]. Sytuacja taka

odpowiedzialne za dokonywanie takich precyzyjnych ataków". zob. B. Donohue, *What is APT?,* www.blog.kaspersky.com/apt/ (02. 12. 2013).

[84] *Zaawansowane trwałe zagrożenia: to nie jest przeciętne szkodliwe oprogramowanie*, www.vs.kaspersky.pl/download/beready/zawansowane_dlugotrwale_zagrozenia.pdf, s. 3 (02. 12. 2013).

[85] „(…) mózgi operacji APT wydają się być wysoce zorganizowanymi syndykatami cyberprzestępczymi, dysponującymi zespołami ekspertów i posiadającymi na wyciągnięcie ręki cały wachlarz technik wywiadowczych i szpiegowskich", zob. ibidem.

[86] J. Henderson, *Check Point: Biggest cyber security threats to businesses*, op. cit.

[87] Zob. A. Shimel, *APT: The security attack everyone loves to hate*, www.networkworld.com/community/blog/apt-security-attack-everyone-loves-hate (02. 12. 2013).

[88] Uważa się, że wspomniany w niniejszym artykule Stuxnet, a także jego „następca" (Flame) były przykładem APT, zob. A. Z. Tabana, *Advanced Persistent Threat (APT) – A Hyped up Marketing Term or a Security Concern?*, www.gfi.com/blog/advanced-persistent-threat-apt-a-hyped-up-marketing-term-or-a-security-concern/; *Zaawansowane trwałe zagrożenia: to nie jest przeciętne szkodliwe oprogramowanie*, op. cit., s. 2. Wskutek ataku APT ucierpiało także m.in. Googgle, zob. M. J. Schwartz, *Google Aurora Hack Was Chinese Counterespionage Operation*, www.informationweek.com/attacks/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060?; W. Ashford, *How to combat advanced persistent threats: APT strategies to protect your organization*, www.computerweekly.com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation (02. 12. 2013).

powodowała zatem, że niektórzy bagatelizowali ten rodzaj zagrożenia[89]. Z drugiej jednak strony zastanowienie mogła wzbudzić inna charakterystyczna cecha zaawansowanych trwałych zagrożeń – zasięg ataku. Jak bowiem słusznie zauważył B. Donohue z Kaspersky Lab, dążenie do osiągnięcia celu za wszelką cenę, a zarazem relatywnie cierpliwie powoduje, że niebezpieczeństwo dotyczy wszystkich, którzy w jakikolwiek sposób mogą być powiązani z informacją, do której dostęp chcą zyskać cyberprzestępcy[90].

Przekonanie o realności zagrożenia – a raczej o jego aktualności w stosunku do szerszego grona podmiotów – potwierdza standardowy model ataku typu APT[91]. Zazwyczaj rozpoczyna się on od rozpoznania[92]. Na tym etapie cyberprzestępcy starają się zdobyć wszelkie informacje, które otworzą im drogę dostępu do systemu[93]. Warto zauważyć, że już pierwsze zebrane przez nich dane mogą być istotne także z punktu widzenia celu końcowego, co pozwala lepiej zrozumieć skalę operacji. Szczególnie wart podkreślenia jest również fakt, że ofiarą wstępnych działań cyberprzestępców mogą paść zwłaszcza szeregowi pracownicy przedsiębiorstwa – idealni do tego są wspomniani wyżej nieostrożni lub naiwni insiderzy – którzy zapewniają relatywnie łatwy dostęp do systemu[94]. Gdy uda im się to osiągnąć, poszerzają skalę swojej działalności. Dokonują wnikliwej infiltracji podmiotu atakowanego, która polega na zbieraniu wszystkich istotnych z punktu widzenia celu końcowego informacji[95]. Używają do tego zestawu rozmaitych narzędzi, które mają im zapewnić odpowiednie – czyli nieprzerwane i dyskretne – warunki pracy[96]. W tym miejscu

[89] „Wielu myślało, że przesadziliśmy, że nie było to tak duże zagrożenie lub nie różniło się od innych zagrożeń dla bezpieczeństwa. Wielu myślało, że APT zostało wyolbrzymione przez speców od bezpieczeństwa szukających sławy i fortuny oraz media, które zajmują się bezpieczeństwem, żeby miały o czym pisać", zob. A. Shimel, *APT: The security attack everyone loves to hate*, op. cit.

[90] „Chodzi o to, że nie musisz należeć do kadry zarządzającej, żeby być celem potencjalnego atak APT. Niemal każdy, kto posiada połączenie do Internetu, jest potencjalnym celem", zob. B. Donohue, *What is APT?*, op. cit.

[91] Należy podkreślić, że jak przystało na tak zaawansowane zagrożenie, ataki typu APT mogą przebiegać w rozmaity sposób. Opisany w tekście model jest wyliczeniem cech, które zazwyczaj towarzyszą tego typu atakom, nie oznacza jednak, że może mieć zastosowanie w każdym przypadku.

[92] A. Z. Tabana, *Advanced Persistent Threat (APT) – A Hyped up Marketing Term or a Security Concern?*, op. cit.

[93] Cyberprzestępcy starają się poznać zasady funkcjonowania atakowanego podmiotu, jak i systemów, na którym opiera swoją działalność, zob. ibidem.

[94] „Hakerzy, którzy dokonują ataku typu APT, uciekają się do wyboru coraz bardziej skromnych celów, aby doprowadzić do zbudowania skomplikowanego łańcucha infekcji, który ostatecznie będzie przynosił plony w postaci cennych danych", zob. B. Donohue, *What is APT?*, op. cit. Jak zauważono w raporcie Kaspersky Lab: „Od tego momentu APT polega na starannie przygotowanej socjotechnice i rozpoczyna próby infiltracji organizacji, poczynając od jej najsłabszego ogniwa – użytkownika końcowego", zob. *Zaawansowane trwałe zagrożenia: to nie jest przeciętne szkodliwe oprogramowanie*, op. cit., s. 4.

[95] „Kiedy są już w środku, zbierają informacje o infrastrukturze, hierarchii, zaufanych związkach, strukturze bezpieczeństwa itd., co pozwoli na nawet dalej posuniętą eksploatację systemu", zob. A. Z. Tabana, *Advanced Persistent Threat (APT) – A Hyped up Marketing Term or a Security Concern?*, op. cit.

[96] „W głównej fazie ataku APT do infekcji sieci wykorzystywana jest dowolna liczba wyrafinowanych trojanów, robaków i innych wyspecjalizowanych szkodników, do systemów wprowadza się wiele backdoorów, które

warto również zwrócić uwagę na kolejne cechy charakterystyczne ataków typu APT, które powodują, że są niezwykle groźne. Po pierwsze, cyberprzestępcy zazwyczaj starają się zapewnić sobie stały dostęp do danego komputera, nawet jeśli maszyna na daną chwilę nie jest przedmiotem ich zainteresowania. Po wtóre, nie rezygnują z działań nawet w przypadku ich wykrycia[97]. Oznacza to także, że po osiągnięciu celu zazwyczaj nie wycofują się z systemu całkowicie – wprawdzie zacierają ślady swojej obecności, ale wciąż utrzymują w nim obecność, która cechuje się mniejszą intensywnością działań[98].

Aktualność problemów, jakie wiążą się z atakami typu APT dla przedsiębiorców, potwierdzają również najnowsze trendy. Z raportu firmy Symantec wynika, że ofiarą tego typu zagrożenia pada coraz więcej małych i średnich przedsiębiorstw (MSP)[99]. Sytuacja taka może być powodowana kilkoma faktami. Na wstępie należy zauważyć, że zmiany w tej materii powinny być prawdopodobnie rozpatrywane w szerszym kontekście, a więc przez pryzmat innych trendów, które zachodzą w obrębie całej cyberprzestrzeni. Szczególnie niebezpieczne w tym zakresie może być przede wszystkim pojawienie się aktorów państwowych jako źródeł zagrożeń dla firm. To państwa dysponują bowiem znacznymi zasobami i środkami, które umożliwiają przeprowadzenie ataku przy wykorzystaniu tzw. zaawansowanych trwałych zagrożeń, a ponadto – co zostało wspomniane wyżej – z różnych względów wydają się coraz bardziej zainteresowane kradzieżą technologii firm. To one mogą również wspierać inne grupy, które kierują się rozmaitymi celami[100]. Nie bez znaczenia jest też z pewnością generalny trend rozwoju cyberprestępczości. Wydaje się, że błędem nie byłoby wysunięcie założenia, że jeśli coraz więcej dobrze zorganizowanych grup przestępczych decyduje się na prowadzenie działalności w sieci, to przynajmniej część z nich może dysponować zasobami, które umożliwiają dokonywanie tego typu ataków[101]. Należy też zauważyć, że cyberprzestrzeń otworzyła nowe możliwości przed nieuczciwymi przedsiębiorstwami, które decydują się na wykradanie informacji konkurencji.

---

prawdopodobnie pozostaną na komputerach użytkowników i serwerach na zawsze. W tym czasie zagrożenie przenosi się niepostrzeżenie z jednego hosta na drugi - pozostaje cały czas w ukryciu, co pozwala mu wytropić sprecyzowany wcześniej cel", zob. *Zaawansowane trwałe zagrożenia: to nie jest przeciętne szkodliwe oprogramowanie*, op. cit., s. 4.

[97] R. Grimes, *5 signs you've been hit with an advanced persistent threat*, www.infoworld.com/d/security/5-signs-youve-been-hit-advanced-persistent-threat-204941?page=0,0 (02. 12. 2013).

[98] A. Z. Tabana, *Advanced Persistent Threat (APT) – A Hyped up Marketing Term or a Security Concern?*, op. cit.

[99] W 2011 r. firmy, które liczą poniżej 250 pracowników, były celem 18% ataków. Przed końcem 2012 r. stanowiły już 31% ofiar, zob. *Internet Security Threat Report 2013*, op. cit., s. 20.

[100] M.in. haktywistów.

[101] Należy zauważyć, że zagadnienie to jest niezwykle ciekawe i wymagałoby odrębnej analizy – przyjęcie takiego założenia oznaczałoby bowiem, że grupy przestępcze, które posługują się APT, nastawione są na zyski w dłuższym okresie.

Zaawansowane trwałe zagrożenia – ze względu na możliwość długiego ich stosowania w sposób niepostrzeżony i związane z tym wysokie prawdopodobieństwo sukcesu – wydają się natomiast idealnym narzędziem do tego procederu.

Opisane wyżej zmiany wywołały jednak jeszcze jeden, istotny zwłaszcza z punktu widzenia małych i średnich przedsiębiorstw skutek – wzrost świadomości wśród większych podmiotów. To z kolei spowodowało, że ciężar ataków zaczął przesuwać się w kierunku znacznie mniej zabezpieczonych, świadomych, zasobnych – zarówno w odpowiedni kapitał ludzki, jak i niezbędne środki pieniężne – a co za tym idzie – nieprzygotowanych do konfrontacji z tak poważnym zagrożeniem organizacji, jakie wchodzą w skład sektora MSP[102]. Gdy uwzględni się, że ataki typu APT były dotychczas wykorzystywane przeważnie do wykradania informacji od tak potężnych aktorów jak państwa czy wiodące w skali światowej korporacje (m.in. Google czy Lockheed Martin), można zrozumieć, przed jak istotnym – a zarazem trudnym do pokonania – wyzwaniem stają obecnie przedsiębiorstwa.

Nawet tak poważne zagrożenie nie stawia jednak firm na jednoznacznie straconej pozycji. Choć odparcie ataku, w którym wykorzystywane są zaawansowane trwałe zagrożenia, rzeczywiście może przerastać możliwości większości małych i średnich przedsiębiorstw, spełnienie pewnych warunków może znacznie pomóc w ograniczeniu prawdopodobieństwa padnięcia ofiarą ataku. Podstawowym instrumentem w tym zakresie pozostają oczywiście szkolenia, które zarówno zwiększą świadomość istnienia zagrożenia wśród wszystkich pracowników, jak i zapoznają ich z podstawowymi narzędziami wykorzystywanymi przez przestępców[103]. Jak bowiem słusznie zwracają uwagę eksperci, to ludzie stanowią podstawę dobrego systemu bezpieczeństwa[104]. Należy zauważyć, że argument ten nabiera znacznie większej wagi, gdy uwzględni się, że w początkowych etapach nawet tak szkodliwych ataków istotną rolę odgrywają umiejętności socjotechniczne cyberprzestępców. W walce z zagrożeniami typu APT szczególnie duże znaczenie mają regularne aktualizacje

[102] Jak słusznie zauważyli autorzy raportu Kaspersky Lab: „Ponieważ wielu dostawców wojskowych i coraz większa liczba głównych graczy na rynku dużych przedsiębiorstw zyskuje świadomość niebezpieczeństwa i wzmacnia obronę, logicznym krokiem jest przeniesienie koncentracji ataku na mniejsze organizacje", zob. *Zaawansowane trwałe zagrożenia: to nie jest przeciętne szkodliwe oprogramowanie*, op. cit., s. 6.
[103] W. Ashford, *How to combat advanced persistent threats: APT strategies to protect your organization*, op. cit.
[104] W. Ashford, *Infosec 2011: APT attacks a real threat to business, says security panel*, www.computerweekly.com/news/1280095750/Infosec-2011-APT-attacks-a-real-threat-to-business-says-security-panel (02. 12. 2013).

oprogramowania – ataki często opierają się bowiem na lukach, które znajdują w nim napastnicy[105].

Przedsiębiorstwo, które chce zabezpieczyć się przed atakami przy wykorzystaniu zaawansowanych trwałych zagrożeń, powinno także opracować odpowiednią politykę w zakresie cyberbezpieczeństwa, która obejmowałaby zarówno kwestie związane z wykrywaniem zagrożenia, jak i odpowiedzią na jego pojawienie się, oraz dbać o regularne monitorowanie szeroko rozumianej infrastruktury bezpieczeństwa[106]. Niektórzy eksperci nazywają takie podejście „głęboką obroną" i wskazują, że jej elementami powinny być m.in.: weryfikacja pracowników i kontrahentów, system zarządzania dostępem, dbanie o odpowiednie zarządzanie informacją – zarówno w kwestii dostępu do niej, jak i jej przechowywania – i system monitorujący[107].

Przedstawione wyżej rozwiązania są oczywiście dość ogólnymi propozycjami, które nie wyczerpują szczegółowych środków walki z zagrożeniem[108]. Ważne jest jednak odnotowanie, że ataki typu APT, które stanowią niezwykle groźny instrument w rękach przestępców, wymagają poważnego i całościowego podejścia do kwestii związanych z cyberbezpieczeństwem. Choć dla niektórych przedsiębiorców przyjęcie środków takiej rangi może wydawać się przesadzone, należy zauważyć, że niepokojący trend, który wskazuje, że tego typu zagrożenia dotykają coraz częściej również sektor MSP, sugeruje jednak, że niedaleka przyszłość może wymusić na firmach przyjęcie strategii bezpieczeństwa skrojonej na miarę nawet tak poważnych zagrożeń.

f) Chmury internetowe

Warto zwrócić uwagę na jeszcze jeden aktualny trend, z którym w niedalekiej przyszłości mogą wiązać się kolejne zagrożenia dla przedsiębiorców. Coraz więcej firm decyduje się bowiem na przechowywanie swoich informacji w tzw. chmurach internetowych[109]. Choć może się to wydawać korzystne z punktu widzenia niektórych

[105] *Zaawansowane trwałe zagrożenia: to nie jest przeciętne szkodliwe oprogramowanie*, op. cit., s. 7.
[106] A. Z. Tabana, *Advanced Persistent Threat (APT) – A Hyped up Marketing Term or a Security Concern?*, op. cit.; W. Ashford, *How to combat advanced persistent threats: APT strategies to protect your organization*, op. cit. Więcej na temat oznak ataku APT, zob. R. Grimes, *5 signs you've been hit with an advanced persistent threat*, op. cit.
[107] W. Ashford, *How to combat advanced persistent threats: APT strategies to protect your organization*, op. cit.
[108] Więcej na ten temat, zob. ibidem; A. Z. Tabana, *Advanced Persistent Threat (APT) – A Hyped up Marketing Term or a Security Concern?*, op. cit.
[109] Na temat ekspansji biznesu chmur internetowych, zob. *Internet Security Threat Report 2013*, op. cit., s. 38. W uproszczonym znaczeniu, którego używa się w niniejszym artykule, chmura internetowa to specyficzny

przedsiębiorstw – i często rzeczywiście takie jest, zwłaszcza dla małych firm, których nie stać na utrzymanie wykwalifikowanych kadr informatycznych lub odpowiednie zabezpieczenia – należy zauważyć, że zjawisko to przyciąga również uwagę cyberprzestępców[110].

Przedsiębiorcy, którzy chcą skorzystać z chmury internetowej, powinni zatem najpierw dobrze zorientować się odnośnie do polityki dostawcy usługi w kwestii bezpieczeństwa danych, a następnie zadbać, by była ona odpowiednio uregulowana w stosownej umowie[111]. Z pewnością warto byłoby, gdyby decyzję podjęli w oparciu o dokładną analizę co najmniej kilku ofert, podchodząc do kwestii w sposób indywidualny[112]. Ważne jest także, aby zadbali o takie szyfrowanie danych, które z jednej strony zapewniłoby im bezpieczeństwo, a z drugiej nie utrudniało nadmiernie korzystania z usługi[113].

Na koniec należy wspomnieć także o poruszanym już wielokrotnie w niniejszym artykule czynniku ludzkim. Warto bowiem zauważyć, że zagrożenie może stanowić nie tylko atak cyberprzestępców na chmurę internetową, w której firma zdecydowała się ulokować swoje zasoby, ale także nieroztropne umieszczanie danych służbowych przez pracowników przedsiębiorstwa w ich prywatnych chmurach. Zjawisko to jawi się jako tym bardziej niebezpieczne, gdy uwzględni się poruszane wyżej wątpliwości zarówno odnośnie do urządzeń mobilnych, jak i innych rodzajów zagrożeń. W świetle rozwoju tego typu narzędzi wydaje się, że w przyszłości konieczne będzie zapewne także wypracowanie odpowiedniej polityki w zakresie korzystania z chmur internetowych wewnątrz przedsiębiorstw.

3. Cyberprzestępczość a sektor MSP

Choć w poprzedniej części artykułu opisano najważniejsze zagrożenia, które wynikają z działalności cyberprzestępców dla wszystkich przedsiębiorców, warto poświęcić odrębne miejsce dla zwięzłego omówienia sytuacji sektora MSP. Podyktowane jest to kilkoma

rodzaj dysku zewnętrznego. Więcej na ten temat, zob. A. Huth, J. Cebula, *The Basics of Cloud Computing*, www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf (02. 12. 2013).

[110] „Hakerzy po prostu śledzą, gdzie przechowywane są krytyczne informacje, i w pewnych przypadkach mogą dojść do wniosku, że dostawcy chmur są łatwiejsi do wykorzystania niż przedsiębiorstwa, które z nich korzystają", zob. B. Jackson, *8 cyber-security threats to prepare for in 2014*, op. cit.

[111] J. Henderson, *Check Point: Biggest cyber security threats to businesses*, op. cit.

[112] Należy bowiem zauważyć pewien paradoks, który może dotyczyć dostawców chmur internetowych. Z jednej strony można założyć, że wiodące firmy mają odpowiednio restrykcyjną politykę prywatności. Z drugiej jednak powstaje wątpliwość, czy tego rodzaju dostawcy – zwłaszcza jeśli uwzględni się fakt, że ze względu na renomę, jaką się cieszą, mogą przyciągać wielu klientów – nie są bardziej narażeni na zagrożenie ze strony cyberprzestępców. W takiej sytuacji firma musi odpowiednio oszacować ryzyko związane z miejscem przechowywania danych. Więcej na ten temat zob. *Internet Security Threat Report 2013*, op. cit., s. 38.

[113] Więcej na ten temat, zob. *Emerging Cyber Threats Report 2014*, s. 1 - 3.

powiązanymi ze sobą przyczynami. Przede wszystkim istnieniem przesłanek, które pozwalają sądzić, że kwestie związane z cyberbezpieczeństwem są zaniedbywane przez małe i średnie przedsiębiorstwa[114]. Należy zauważyć, że zjawisko to jest szczególnie niebezpieczne w kontekście Polski, co wynika z ogromnego znaczenia sektora MSP dla gospodarki kraju[115]. Zrozumiałe wydaje się zatem, że w świetle celów, jakie postawił sobie autor niniejszego artykułu – i ze względu na fakt, że odbiorcami tekstu będą przedstawiciele polskiego biznesu – położenie nacisku na sytuację małych i średnich przedsiębiorców jest konieczne, aby nie mieli oni żadnych wątpliwości odnośnie do aktualności problemu wobec ich firm.

Potrzebę krótkiego omówienia sytuacji sektora MSP w kontekście cyberprzestępczości potwierdzają również statystyki, które wskazują na wysoki stopień komputeryzacji i informatyzacji polskich firm. Z danych, które zostały przedstawione w raporcie Ministerstwa Administracji i Cyfryzacji, wynika, że 95% polskich przedsiębiorstw wykorzystuje w swojej pracy komputery, a 93% firm posiada dostęp do Internetu. Co ciekawe, statystyki pokazują także, że jedynie około 40% pracowników małych i średnich przedsiębiorstw korzysta z komputerów w pracy[116]. Wynika z nich również, że 41% przedsiębiorców wyposaża swoich podwładnych w urządzenia mobilne z dostępem do Internetu[117]. Choć liczby te nieznacznie odbiegają od średnich dla europejskich odpowiedników, obrazują, że cyberprzestępcy mają znaczne możliwości rozwoju swojej działalności również w Polsce[118]. W takiej sytuacji wyraźne zaznaczenie, że problem cyberprzestępczości może dotykać również sektor MSP, wydaje się tym bardziej niezbędne.

Podstawowym problemem małych i średnich przedsiębiorców jest przekonanie, że ich firmy są za małe, aby wzbudzić zainteresowanie przestępców[119]. Już część omówionych

[114] G. Westerman, *Your Business Is Never Too Small For A Cyber Attack, Here's How To Protect Yourself*, www.forbes.com/sites/forbesleadershipforum/2013/05/13/your-business-is-never-too-small-for-a-cyber-attack-heres-how-to-protect-yourself/ (02. 12. 2013).

[115] Jak twierdzi Portal Polskich Przedsiębiorców MSP-24.pl, „sektor MSP w Polsce wytwarza 67% PKB i tworzy miejsca pracy dla ok. 70% wszystkich zatrudnionych", zob. www.msp-24.pl/Sektor-MSP-w-Polsce-i-UE,8,78.html (02. 12. 2013). Więcej na ten temat zob. także *Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce w latach 2011 - 2012*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2013, www.parp.gov.pl/files/74/81/626/18355.pdf (02. 12. 2013).

[116] *Społeczeństwo informacyjne w liczbach 2013*, Departament Społeczeństwa Informacyjnego, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013, www.mac.gov.pl/wp-content/uploads/2013/09/Spoleczenstwo-informacyjne-w-liczbach-2013.pdf, s. 123 - 125 (02. 12. 2013).

[117] Wśród celów, do których realizacji wykorzystuje się urządzenia mobilne w polskich firmach, wymienia się: pozyskiwanie informacji z Internetu (39%), dostęp do poczty elektronicznej przedsiębiorstwa (37%), dostęp i modyfikacja dokumentów przedsiębiorstwa (27%), wykorzystanie dedykowanych aplikacji biznesowych (13%), zob. ibidem, s. 130.

[118] Stosowne porównania można odnaleźć również w raporcie Ministerstwa Administracji i Cyfryzacji.

[119] „Niektórzy właściciele małych firm mogą odczuwać komfort, który spowodowany jest iluzją, że ich operacje są zbyt mało istotne, aby przyciągnąć uwagę międzynarodowych cyberprzestępców, którzy atakują globalne

w niniejszym artykule zagadnień i źródeł zagrożeń pozwala na obalenie tego założenia. Najbardziej niepokojące w tym zakresie są oczywiście trendy, które wskazują na upowszechnienie się zjawiska cyberprzestępczości, jak i sygnały oraz statystyki, które pokazują, że przestępcy dokonują redefinicji celów i zwracają się w kierunku gorzej chronionych podmiotów[120].

Szczególnego podkreślenia wymaga fakt, że nawet jeśli dysponowanie skromniejszymi zasobami czy mniej innowacyjnymi technologiami powoduje, że małe i średnie przedsiębiorstwa jawią się dla cyberprzestępców jako mniej atrakcyjne niż duże korporacje, nie oznacza to, że sektor MSP może czuć się bezpieczny. Choć rzeczywiście perspektywa mniejszych zysków może zniechęcać przestępców do podejmowania działań wymierzonych w małych i średnich przedsiębiorców, za dokonaniem takiego ataku przemawiają inne czynniki, które mogą okazać się równie korzystne[121]. Sprzyja im m.in. wspomniany wyżej fakt, że tego typu podmioty są zazwyczaj mniej zabezpieczone na wypadek ewentualnego cyberataku. Sytuacja taka jest oczywiście wynikiem zarówno błędnego poczucia bezpieczeństwa – często wywołanego brakiem świadomości istnienia problemu – jak i niedysponowania odpowiednimi zasobami[122]. Jak nietrudno wywnioskować, redukuje to ryzyko wykrycia ataku, a co za tym idzie – gwarantuje cyberprzestępcom większe prawdopodobieństwo sukcesu.

Ostatnim, istotnym argumentem, który powinien przekonać małych i średnich przedsiębiorców, że przestępczość w sieci stanowi poważne zagrożenie również dla nich, może być analiza kosztów, jakie ponoszą wskutek cyberataków. Z wspomnianych już na początku artykułu badań wynika, że choć podmioty, które wchodzą w skład sektora MSP, mogą ponosić mniejsze straty nominalne niż duże korporacje, to jednak ich koszt relatywny

banki, sprzedawców internetowych lub jednostki rządowe, aby zebrać bazy danych z numerami kart kredytowych, hasłami klientów i informacjami o kontach", zob. *Combating Small Business Security Threats: How SMBs Can Fight Cybercrime,* White Paper, McAfee Endpoint Protection Suite Security, www.mcafee.com/us/resources/white-papers/wp-combating-smb-threats.pdf, s. 1 (02. 12. 2013).

[120] Jak zostało już wspomniane, przed końcem 2012 r. małe i średnie przedsiębiorstwa stanowiły 31% ofiar cyberataków dokonywanych przy pomocy APT, zob. *Internet Security Threat Report 2013,* op. cit., s. 20. W kwestii statystyk wystarczy przypomnieć wyliczenia brytyjskiej Federacji Małego Biznesu, jak i wskazać na dane ze Stanów Zjednoczonych, z których wynika, że małe i średnie przedsiębiorstwa są celem blisko 20% cyberataków, zob. G. Westerman, *Your Business Is Never Too Small For A Cyber Attack, Here's How To Protect Yourself,* op. cit.

[121] „Chociaż można stwierdzić, że korzyści z atakowania małych firm są mniejsze od tych, które można zyskać od dużego przedsiębiorstwa, jest to więcej niż kompensowane przez fakt, że wiele małych firm jest zazwyczaj mniej ostrożnych w swojej cyberobronie", zob. *Internet Security Threat Report 2013,* op. cit., s. 4.

[122] Zarówno w formie kapitału, który można byłoby przeznaczyć na szeroko rozumiane cyberbezpieczeństwo, jak i wykwalifikowanego personelu. Więcej na ten temat zob. J. Peabody, *Q&A with cyber crime expert Tim Francis,* www.blogs.reuters.com/small-business/2013/05/03/qa-with-cyber-crime-expert-tim-francis/ (02. 12. 2013).

jest większy[123]. Małe i średnie przedsiębiorstwa, które padną ofiarą cyberprzestępców, muszą zatem zmierzyć się ze stosunkowo dużym wyzwaniem, które może nie tylko poważnie zakłócić funkcjonowanie firmy, ale nawet przyczynić się do jej upadku[124]. Zwłaszcza ten argument powinien skłonić małych i średnich przedsiębiorców do zastanowienia się nad bezpieczeństwem własnej firmy w kontekście cyberprzestrzeni.

4. Cyberprzestępcy a przedsiębiorcy – nierówna walka w niepewnym środowisku. Wnioski

Niniejszy artykuł miał zobrazować, że zmiany, które zachodzą w cyberprzestrzeni, są źródłem rozmaitych zagrożeń dla przedsiębiorców. Co gorsza, trudno rozpatrywać je w oderwaniu od innych trendów, jakie można zaobserwować w sieci. Paradoksalnie jednak sytuacja taka ma również swoją pozytywną stronę, przynajmniej dla części polskich firm. Pewnego rodzaju ujednolicenie warunków – a co za tym idzie także omówionych wyżej zagrożeń – które dokonało się dzięki rozwojowi Internetu, pozwala bowiem na dokładniejszą obserwację zjawisk, jakie zachodzą w obrębie cyberprzestrzeni. Tak więc choć podmioty, które działają w jej ramach, mają różne struktury, prowadzą inny rodzaj działalności gospodarczej czy dostarczają towary lub usługi w odmiennych lokalizacjach geograficznych, często muszą stawiać czoła jednakowym wyzwaniom[125]. Dzięki temu przedsiębiorcy mają unikalną możliwość wyciągania przydatnych wniosków z doświadczeń różnych firm – zarówno takich, które prowadzą podobny rodzaj działalności gospodarczej w innym miejscu świata, jak i innych, które z rozmaitych przyczyn mogą paść ofiarą tego samego zagrożenia – i lepszego przystosowania się do dynamicznie zmieniających się warunków funkcjonowania w cyberprzestrzeni. Zrozumiałe jest, że polscy przedsiębiorcy powinni podpatrywać rozwiązania, które stosowane są w tym zakresie, zwłaszcza na bardziej innowacyjnych rynkach.

Tezę o ujednoliceniu warunków potwierdza po części katalog podstawowych narzędzi, które mogą być wykorzystywane do walki z zagrożeniami w sieci. Należy zauważyć, że fundamentem dobrego funkcjonowania wszystkich systemów bezpieczeństwa jest odpowiednia świadomość istnienia problemu, która może pomóc w zneutralizowaniu

[123] *Cost of Cybercrime Increases 78 Percent,* op. cit.

[124] Badania przeprowadzone w Stanach Zjednoczonych pokazują, że blisko 60% małych firm, które doświadczyły działalności cyberprzestępców, zmuszonych jest do zakończenia prowadzenia działalności gospodarczej w ciągu pół roku od ataku, zob. G. Westerman, *Your Business Is Never Too Small For A Cyber Attack, Here's How To Protect Yourself*, op. cit.

[125] Jak słusznie zauważono w raporcie GFI: „Każda organizacja jest inna, jednak w wielu przypadkach zagrożenia są wspólne dla wszystkich", zob. *Security threats: A guide for SMEs,* GFI White Paper, op. cit., s. 10.

największej ich wady, jaką stanowi czynnik ludzki. Gdy jej zabraknie, skuteczne zastosowanie nawet najprostszych narzędzi może okazać się bezowocne.

Jeśli pracownicy przedsiębiorstwa będą uświadomieni odnośnie do zagrożeń, które wiążą się z użytkowaniem Internetu, obrona przed mniej zaawansowanymi atakami cyberprzestępców może stać się relatywnie łatwa. Efektywność większości zagrożeń może być bowiem ograniczona m.in. przez tak podstawowe działanie, jakim jest kontrolowanie aktualności zainstalowanego na firmowym sprzęcie oprogramowania, czy po prostu ostrożne (czyt. świadome) korzystanie z zasobów sieci i urządzeń. Niezwykle pomocne w tej kwestii mogłoby być także opracowanie przez każdą firmę dostosowanej do własnych potrzeb polityki, która regulowałaby kwestie związane z funkcjonowaniem w cyberprzestrzeni, jak również zatrudnienie wykwalifikowanego personelu, który czuwałby nad bezpieczeństwem przedsiębiorstwa.

Z drugiej jednak strony nowe trendy – a zwłaszcza dołączenie aktorów państwowych do katalogu zagrożeń dla przedsiębiorców – sugerują, że obrona przed niektórymi atakami może wymagać zasobów, które są nieosiągalne dla większości firm. Sytuacja taka powoduje, że w niedalekiej przyszłości skuteczna walka z zagrożeniami w cyberprzestrzeni będzie najprawdopodobniej wymagać jakiejś formy partnerstwa publiczno-prywatnego. Warto odnotować, że takie rozwiązania są już stosowane w niektórych krajach[126]. Co zrozumiałe, tego typu współpraca między sektorem państwowym a prywatnym może rodzić obawy o różne nieprawidłowości. Jej ramy muszą zatem zostać ściśle doprecyzowane, a przedsiębiorstwa, które zdecydują się w nią zaangażować, powinny otrzymać od państwa gwarancję dyskrecji i niezależności.

Argument o konieczności równoprawnego ułożenia relacji w ramach ewentualnego partnerstwa publiczno-prywatnego jest również podnoszony przez ekspertów do spraw bezpieczeństwa. Ich zdaniem zapewnienie niezależności – zwłaszcza firmom, które zajmują się cyberbezpieczeństwem, a miałyby być częścią tego rodzaju współpracy – jest niezbędnym warunkiem skutecznego reagowania[127]. Sektor prywatny jest bowiem bardziej elastyczny, co

[126] Zob. np. *Government launches information sharing partnership on cyber security*, www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security. Co ciekawe, Wielka Brytania była pierwszym krajem na świecie, który oficjalnie przyznał się do posiadania ofensywnych zdolności w zakresie walki w cyberprzestrzeni, zob. J. Blitz, *UK becomes first state to admit to offensive cyber attack capability*, www.ft.com/intl/cms/s/0/9ac6ede6-28fd-11e3-ab62-00144feab7de.html#axzz2oyAL31HA (02. 12. 2013).

[127] C. Thompson, *Businesses Facing Increasing Cyber Threats: Security Experts*, www.cnbc.com/id/100421313 (02. 12. 2013).

miałoby odpowiadać dynamice zmian, które zachodzą w cyberprzestrzeni. Gdy weźmie się pod uwagę biurokratyczne procedury, według których funkcjonuje większość jednostek rządowych, można zrozumieć słuszność tego założenia.

Należy również zauważyć, że wykorzystanie przez aktorów państwowych cyberprzestrzeni w sposób ofensywny przyniosło jeszcze jeden skutek. Jak się wydaje, doniesienia medialne o kolejnych przypadkach działalności państw, zwróciły uwagę na problem cyberprzestępczości i przyczyniły się do zwiększenia świadomości istnienia problemu. Badania pokazują, że trend ten odczuwalny był również w Polsce[128]. Na optymistyczne spojrzenie na kwestie związane ze świadomością w skali naszego kraju pozwala również fakt, że problem cyberbezpieczeństwa został dostrzeżony przez autorów Białej Księgi Bezpieczeństwa Narodowego RP[129]. Warto również wspomnieć, że jeden z wiodących dokumentów w tym zakresie, jakim jest Polityka Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej, traktuje kwestię bezpieczeństwa w sieci w szerszej perspektywie, czego może dowodzić zarówno ujęcie w nim spraw dotyczących współpracy z przedsiębiorcami, jak i podkreślenie szczególnej roli edukacji w walce z problemem[130]. Pozostaje mieć nadzieję, że deklaracje zawarte w rządowych dokumentach będą znajdowały odzwierciedlenie w rzeczywistości.

Rzetelność nakazuje, aby w ramach podsumowania wspomnieć również o głosach sceptyków. Niektórzy eksperci sugerują bowiem, że kwestie związane z cyberprzestępczością są celowo wyolbrzymiane przez firmy, które zajmują się bezpieczeństwem w sieci[131]. Rzeczywiście, należy przyznać, że cyberbezpieczeństwo staje się ostatnimi czasy niezwykle dochodowym biznesem[132]. Autor niniejszego artykułu radziłby jednak zachować sceptycyzm

[128] Badania Eurobarometru w zakresie bezpieczeństwa cybernetycznego z 2013 r. pokazują, że 70% Polaków sądzi, że w ciągu ostatniego roku wzrosło ryzyko padnięcia ofiarą przestępstwa w sieci, zob. *Bezpieczeństwo Cybernetyczne*, Eurobarometr, Komisja Europejska, www.ec.europa.eu/public_opinion/archives/ebs/ebs_404_fact_pl_pl.pdf, s. 3. Warto zauważyć, że statystyki pokazują, że polscy internauci tracą wskutek cyberprzestępczości ok. 5 miliardów złotych, zob. *Wyniki Norton Cybercrime Report 2012 ujawniają, że cyberprzestępstwa kosztują polskich użytkowników indywidualnych nawet 4,8 mld zł*, www.symantec.com/pl/pl/about/news/release/article.jsp?prid=20120925_01 (02. 12. 2013).

[129] Zob. Biała Księga Bezpieczeństwa Narodowego RP, Biuro Bezpieczeństwa Narodowego, www.spbn.gov.pl/sbn/biala-ksiega/4630,Biala-Ksiega.html, s. 62 - 64 (02. 12. 2013). Należy zauważyć, że kwestie cyberbezpieczeństwa pojawiają się w wielu miejscach niniejszej publikacji.

[130] Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013, www.mac.gov.pl/wp-content/uploads/2013/06/Polityka-Ochrony-Cyberprzestrzeni-RP_wersja-pl.pdf (02. 12. 2013).

[131] Zob. np. M. Egan, *As Cyber Threats Mount, Business is Booming in the Security World*, www.foxbusiness.com/technology/2013/03/12/as-cyber-threats-mount-business-is-booming-in-security-world/ (02. 12. 2013).

[132] Eksperci szacują, że jego wartość może w 2013 r. sięgnąć blisko 70 miliardów dolarów, zob. *Global 20 Leading Cyber Security Companies 2013: Competitive Landscape Analysis,*

zarówno wobec takich opinii, jak i głosów skrajnych, które przekonują wszystkich do traktowania cyberbezpieczeństwa w sposób zero-jedynkowy, niemal w kategoriach życia lub śmierci[133]. Należy podkreślić, że analiza bezpieczeństwa danego przedsiębiorstwa – a co za tym idzie dobór odpowiednich do walki z problemem środków – powinna być każdorazowo dokonywana w sposób rozsądny, z uwzględnieniem indywidualnej sytuacji firmy. Zrozumiałe jest, że nie wszystkie zagrożenia będą dotyczyć przedsiębiorców w ten sam sposób i w takiej samej skali. Ryzyko, jakie wiąże się z funkcjonowaniem w cyberprzestrzeni, jest różne dla firmy, która dysponuje istotnymi informacjami klientów, i dla takiej, która prowadzi działalność gospodarczą w mniej newralgicznym obszarze oraz na mniejszą skalę. Kluczem do zapewnienia bezpieczeństwa jest jednak zarówno świadomość istnienia problemu, jak i zagrożeń, które się z nim wiążą. Ten fundamentalny element może nie tylko pomóc przedsiębiorcom skutecznie stawić czoła wyzwaniom, jakie stawia przed nimi cyberprzestrzeń, ale także odpowiednio zaprojektować swoje działania w przyszłości.

www.marketwatch.com/story/global-20-leading-cyber-security-companies-2013-competitive-landscape-analysis-2013-05-08 (02. 12. 2013).

[133] Debaty takie są zresztą nie do rozstrzygnięcia, te same argumenty mogą być bowiem wykorzystywane przez obie strony. Doskonałym przykładem mogą być dane, które wskazują na występowanie różnicy w umiejętnościach między osobami, które zajmują się cyberbezpieczeństwem, a cyberprzestępcami. Jedni z pewnością będą to interpretować jako dowód na konieczność zwiększenia inwestycji w zakresie bezpieczeństwa w sieci, podczas gdy inni będą twierdzić, że brak odpowiedniego kapitału ludzkiego jest w jakiś sposób wynikiem zamierzonej polityki tego typu firm, nawet jeśli argument ten wydawałby się mało rozsądny. Więcej na temat wspomnianych różnic w umiejętnościach, zob. *Cybersecurity Skills Gap Beginning to Have Real Effects on Business,* www.infosecurity-magazine.com/view/35373/cybersecurity-skills-gap-beginning-to-have-real-effects-on-business/ (02. 12. 2013).

Bibliografia:

1. *34% firm ryzykuje wyciekiem danych, nie kontrolując prywatnych urządzeń w miejscu pracy*, www.kaspersky.pl/about.html?s=news&newsid=2027
2. *APT 1. Exposing One of China's Cyber Espionage Units*, Mandiant, www.intelreport.mandiant.com/Mandiant_APT1_Report.pdf
3. Ashford W., *How to combat advanced persistent threats: APT strategies to protect your organization*, www.computerweekly.com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation
4. Ashford W., *Infosec 2011: APT attacks a real threat to business, says security panel*, www.computerweekly.com/news/1280095750/Infosec-2011-APT-attacks-a-real-threat-to-business-says-security-panel
5. Ashmore W. C., *Impact of Alleged Russian Cyber Attacks*, Baltic Security & Defence Review, Tom 11, 2009, www.bdcol.ee/files/files/documents/Research/BSDR2009/1_%20Ashmore%20-%20Impact%20of%20Alleged%20Russian%20Cyber%20Attacks%20.pdf
6. Barnes J., Gorman S., *Iran Blamed for Cyberattacks*, www.online.wsj.com/news/articles/SB10008723963904446578045780529315555767700
7. *Beijing denies existence of PLA hacking unit*, www.wantchinatimes.com/news-subclass-cnt.aspx?id=20130221000009&cid=1101
8. *Bezpieczeństwo Cybernetyczne*, Eurobarometr, Komisja Europejska, www.ec.europa.eu/public_opinion/archives/ebs/ebs_404_fact_pl_pl.pdf
9. Biała Księga Bezpieczeństwa Narodowego RP, Biuro Bezpieczeństwa Narodowego, www.spbn.gov.pl/sbn/biala-ksiega/4630,Biala-Ksiega.html
10. Blair E., *More than 80% of Mobile Devices Will Remain Unprotected in 2013, Juniper Research Reports*, www.reviewstudio.net/789-more-than-80-of-mobile-devices-will-remain-unprotected-in-2013-juniper-research-reports
11. Blitz J., *UK becomes first state to admit to offensive cyber attack capability*, www.ft.com/intl/cms/s/0/9ac6ede6-28fd-11e3-ab62-00144feab7de.html#axzz2oyAL31HA
12. *China's cyber-hacking. Getting Ugly*, www.economist.com/news/leaders/21572200-if-china-wants-respect-abroad-it-must-rein-its-hackers-getting-ugly
13. *Co to jest Phishing?*, www.support.kaspersky.com/pl/viruses/general/2313
14. *Combating Small Business Security Threats: How SMBs Can Fight Cybercrime*, White Paper, McAfee Endpoint Protection Suite Security, www.mcafee.com/us/resources/white-papers/wp-combating-smb-threats.pdf
15. *Cost of Cybercrime Increases 78 Percent*, www.securitymagazine.com/articles/84817-cost-of-cybercrime-increases-78-percent
16. *Countering the cyber threat to business*, Big Picture, Institute of Directors, wiosna 2013
17. Crovitz L. G., www.online.wsj.com/news/articles/SB10001424127887324635904578643943968885044
18. *CRS Report for Congress Prepared for Members and Committees of Congress. Terrorist Use of the Internet:Information Operations in Cyberspace*, Congressional Research Service, Marzec 2011, www.fas.org/sgp/crs/terror/R41674.pdf
19. *Cyber Threat Source Descriptions*, www.ics-cert.us-cert.gov/content/cyber-threat-source-descriptions
20. *Cybersecurity Skills Gap Beginning to Have Real Effects on Business*, www.infosecurity-magazine.com/view/35373/cybersecurity-skills-gap-beginning-to-have-real-effects-on-business/
21. *CYBERSECURITY. National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, Government Accountability Office, www.gao.gov/assets/660/652170.pdf

22. Danchev D., *Coordinated Russia vs Georgia cyber attack in progress*, www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670
23. Donohue B., *What is APT?*, www.blog.kaspersky.com/apt/
24. Egan M., *As Cyber Threats Mount, Business is Booming in the Security World*, www.foxbusiness.com/technology/2013/03/12/as-cyber-threats-mount-business-is-booming-in-security-world/
25. *Emerging Cyber Threats Report 2014*, Georgia Tech Information Security Center, Georgia Tech Research Institute, wwww.gtsecuritysummit.com/2014Report.pdf
26. Franceschi-Bicchierai L., *Syrian Electronic Army: If U.S. Attacks 'We Will Target All of It'*, www.mashable.com/people/lorenzo-franceschi-bicchierai/
27. *Getting real about cyber threats: where are you headed*, www.pwc.com/en_US/us/industry/utilities/assets/getting-real-about-utilities-infrastructure-cyber-threats.pdf
28. Glenny M., *Mroczny rynek. Hakerzy i nowa mafia*, Wydawnictwo W. A. B., Warszawa 2013
29. *Global 20 Leading Cyber Security Companies 2013: Competitive Landscape Analysis*, www.marketwatch.com/story/global-20-leading-cyber-security-companies-2013-competitive-landscape-analysis-2013-05-08
30. Gorman S., Barrett D., Yadron D., *Chinese Hackers Hit U.S. Media*, www.online.wsj.com/news/articles/SB10001424127887323926104578276202952260718
31. *Government launches information sharing partnership on cyber security*, www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security
32. Grimes R., *5 signs you've been hit with an advanced persistent threat*, www.infoworld.com/d/security/5-signs-youve-been-hit-advanced-persistent-threat-204941?page=0,0
33. Haddick R., This *Week at War: Lessons from Cyberwar I*, www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyber war_i#sthash.RAISroHV.dpbs
34. Hargrave V., *Hacker, Hacktivist, or Cybercriminal?*, www.fearlessweb.trendmicro.com/2012/hackers-and-phishing/whats-the-difference-between-a-hacker-and-a-cybercriminal/
35. Harris P., *Chinese army hackers are the tip of the cyberwarfare iceberg*, www.theguardian.com/technology/2013/feb/23/mandiant-unit-61398-china-hacking
36. Haughney C., Perlroth N., *Times Site Is Disrupted in Attack by Hackers*, www.nytimes.com/2013/08/28/business/media/hacking-attack-is-suspected-on-times-web-site.html?_r=0
37. Henderson J., *Check Point: Biggest cyber security threats to businesses*, www.techday.com/it-brief/news/check-point-biggest-cyber-security-threats-to-businesses/173034/
38. Hollis D., *Cyberwar Case Study: Georgia 2008*, www.smallwarsjournal.com/jrnl/art/cyber war-case-study-georgia-2008
39. Hurley J., *Cyber crime 'costs small companies £800m a year'*, www.telegraph.co.uk/finance/yourbusiness/10069374/Cyber-crime-costs-small-companies-800m-a-year.html
40. Huth A., Cebula J., *The Basics of Cloud Computing*, www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf
41. *Internet Security Threat Report 2013*, Tom 18, kwiecień 2013, Symantec, www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf
42. Jackson B., *8 cyber-security threats to prepare for in 2014*, www.itbusiness.ca/news/8-cyber-security-threats-to-prepare-for-in-2014/44815
43. Jordan T., *Hakerstwo*, Wydawnictwo Naukowe PWN, Warszawa 2011
44. Kaspersky E., *The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight*, wwww.eugene.kaspersky.com/2011/11/02/

the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/
45. *Kaspersky Lab report: 37.3 million users experienced phishing attacks in the last year*, www.kaspersky.com/about/news/press/2013/kaspersky_lab_report_37_3_million_users_experienced_phishing_attacks_in_the_last_year
46. Langner R., *Stuxnet's Secret Twin*, www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack
47. *Leaker Snowden says Israel, US created Stuxnet virus*, www.timesofisrael.com/leaker-snowden-says-israel-us-created-stuxnet-virus/
48. Lemos R., *World's Trouble Spots Escalating Into Cyberthreats For Businesses*, www.darkreading.com/advanced-threats/worlds-trouble-spots-escalating-into-cyb/240160851
49. Markoff J., Before the Gunfire, Cyberattacks, www.nytimes.com/2008/08/13/technology/13cyber.html
50. Markoff J., *Georgia Takes a Beating in the Cyberwar With Russia*, bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia/?_r=0
51. Matthews C.M., *Insider Theft: the Real Cyber Threat?*, *www.blogs.wsj.com/riskandcompliance/2013/03/27/insider-theft-the-real-cyber-threat/*
52. Mitnick K., *Sztuka podstępu,* Helion, Gliwice 2003
53. *Na czym polega atak phishingowy?*, www.kaspersky.pl/cyberthreats.html?s=threats_phishing
54. *Number of the Week: 55% of Mobile Devices Using Unprotected Wi-Fi Networks*, www.kaspersky.com/about/news/virus/2012/Number_of_the_Week_55_of_Mobile_Devices_Using_Unprotected_Wi_Fi_Networks
55. *Obecny stan aktywności innowacyjnej polskich przedsiębiorstw,* www.inwestor.msp.gov.pl/si/polska-gospodarka/wiadomosci-gospodarcze/25869,Obecny-stan-aktywnosci-innowacyjnej-polskich-przedsiebiorstw.html
56. Peabody J., *Q&A with cyber crime expert Tim Francis*, www.blogs.reuters.com/small-business/2013/05/03/qa-with-cyber-crime-expert-tim-francis
57. Perlroth N., Hackers in China Attacked The Times for Last 4 Months, www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?_r=0
58. Płociński M., *To nie był cyberterroryzm,* www.rp.pl/artykul/799250.html
59. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013, www.mac.gov.pl/wp-content/uploads/2013/06/Polityka-Ochrony-Cyberprzestrzeni-RP_wersja-pl.pdf
60. *Proceeds of transnational crime in billions, number of victims in millions, says UNODC chief*, www.unodc.org/unodc/en/frontpage/2012/October/transnational-crime-proceeds-in-billions-victims-in-millions-says-unodc-chief.html
61. *Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce w latach 2011 - 2012*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2013, www.parp.gov.pl/files/74/81/626/18355.pdf
62. Real D., *Cyber threats: trends in phishing and spear phishing – infographic*, www.theguardian.com/media-network/media-network-blog/2013/jul/12/cyber-threats-trends-spear-phishing
63. Riley M., *China Mafia-Style Hack Attack Drives California Firm to Brink*, www.bloomberg.com/news/2012-11-27/china-mafia-style-hack-attack-drives-california-firm-to-brink.html
64. *Rozpoznawanie różnych typów insiderów - osób atakujących z wewnątrz,* www.securelist.pl/analysis/7061,rozpoznawanie_roznych_typow_insiderow_osob_atakujacych_z_wewnatrz.html
65. Sachdev A., *Former Motorola engineer sentenced to 4 years in trade-secret case,*

www.articles.chicagotribune.com/2012-08-31/business/ct-biz-0830-moto-theft--20120831_1_trade-secret-case-hanjuan-jin-trade-secrets

66. Sanger D.E., *Obama Order Sped Up Wave of Cyberattacks Against Iran*, www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
67. Schwartz M. J., *Google Aurora Hack Was Chinese Counterespionage Operation*, www.informationweek.com/attacks/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060?
68. Scott A., *Defend yourself against the cyber threats ready to attack your business*, www.theguardian.com/media-network/media-network-blog/2013/oct/30/cyber-threats-business-botnets-protect
69. *Security threats: A guide for SMEs*, GFI White Paper, www.gfi.com/whitepapers/Security_threats_SMEs.pdf
70. Shimel A., *APT: The security attack everyone loves to hate*, www.networkworld.com/community/blog/apt-security-attack-everyone-loves-hate
71. *Społeczeństwo informacyjne w liczbach 2013*, Departament Społeczeństwa Informacyjnego, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013, www.mac.gov.pl/wp-content/uploads/2013/09/Spoleczenstwo-informacyjne-w-liczbach-2013.pdf
72. *Stuxnet evolution: NSA input turned stealth weapon into internet-roaming spyware*, www.rt.com/news/stuxnet-pressure-uranium-nsa-080/
73. Tabana A.Z., *Advanced Persistent Threat (APT) – A Hyped up Marketing Term or a Security Concern?*, www.gfi.com/blog/advanced-persistent-threat-apt-a-hyped-up-marketing-term-or-a-security-concern/
74. *The Economic Impact of Cybercrime and Cyber Espionage*, Center for Strategic and International Studies, lipiec 2013, www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf
75. Thompson C., *Businesses Facing Increasing Cyber Threats: Security Experts*, www.cnbc.com/id/100421313
76. Thompson C., *Businesses Facing Increasing Cyber Threats: Security Experts*, www.cnbc.com/id/100421313
77. *Top 5 Cyber Threats to Businesses*, www.checkmarx.com/2012/03/28/top-5-cyber-threats-to-businesses/
78. Traynor I., *Russia accused of unleashing cyberwar to disable Estonia*, www.theguardian.com/world/2007/may/17/topstories3.russia
79. Wasilewski K., *Ciekawski robak*, www.notabene.org.pl/index.php/ciekawski-robak/
80. Wasilewski K., *Jak rozpętałem cyberwojnę?*, www.notabene.org.pl/index.php/jak-rozpetalem-cyberwojne/
81. Wasilewski K., *Wirusy naszych czasów*, Tak Po Prostu
82. Waterman S., *Syrian hackers threaten retaliation for any U.S. strike*, www.washingtontimes.com/news/2013/aug/30/syrian-hackers-threaten-retaliation-any-us-strike/?page=all
83. Westerman G., *Your Business Is Never Too Small For A Cyber Attack, Here's How To Protect Yourself*, www.forbes.com/sites/forbesleadershipforum/2013/05/13/your-business-is-never-too-small-for-a-cyber-attack-heres-how-to-protect-yourself/
84. *What is a Botnet?*, www.blog.kaspersky.com/botnet/
85. *What is a botnet?*, www.microsoft.com/security/resources/botnet-whatis.aspx
86. www.hackersforcharity.org/
87. www.msp-24.pl/Sektor-MSP-w-Polsce-i-UE,8,78.html
88. www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm
89. www.oecd.org/sti/sci-tech/theknowledge-basedeconomy.htm
90. www.sjp.pl/haker; www.sjp.pl/cyberprzest%EApca
91. *Wyniki Norton Cybercrime Report 2012 ujawniają, że cyberprzestępstwa kosztują polskich użytkowników indywidualnych nawet 4,8 mld zł,*

www.symantec.com/pl/pl/about/news/release/article.jsp?prid=20120925_01
92. Xuequan M., *China opposes U.S. report on Chinese military*, wwww.news.xinhuanet.com/english/china/2013-05/07/c_124677298.htm
93. *Zaawansowane trwałe zagrożenia: to nie jest przeciętne szkodliwe oprogramowanie,* www.vs.kaspersky.pl/download/beready/zawansowane_dlugotrwale_zagrozenia.pdf