Janusz Wielki

Analiza wyzwań związanych z zarządzaniem przestrzenią elektroniczną przez współczesne organizacje gospodarcze

Problemy Zarządzania 10/3, 54-66

2012

Problemy Zarządzania, vol. 10, nr 3 (38): 54–66
ISSN 1644-9584, © Wydział Zarządzania UW
DOI 10.7172.1644-9584.38.4

Analiza wyzwań związanych z zarządzaniem przestrzenią elektroniczną przez współczesne organizacje gospodarcze

Janusz Wielki

Niniejszy artykuł dotyczy kwestii zarządzania przestrzenią elektroniczną w kontekście rosnącego wykorzystywania Internetu przez współczesne organizacje gospodarcze. Składa się on z czterech części. W pierwszej z nich przedstawiony został krótki zarys podstawowych aspektów związanych z przestrzenią elektroniczną i zarządzaniem nią. Dwie następne części są kluczowe z punktu widzenia niniejszego artykułu. W pierwszej z nich przeprowadzono analizę działań związanych z zabezpieczeniem i ochroną aktywności organizacji on-line, jako kluczowego elementu zarządzania przestrzenią elektroniczną. Następnie zaprezentowano możliwości aktywnego oddziaływania przedsiębiorstw na e-przestrzeń, jako elementu dopełniającego zarządzaniem nią. Końcowa, czwarta cześć artykułu zawiera najważniejsze wnioski, konkluzje i zalecenia.

1. Wprowadzenie

Problem wpływu Internetu na funkcjonowanie organizacji gospodarczych jest zagadnieniem coraz bardziej istotnym zarówno z punktu widzenia każdej z nich, jak i z perspektywy całej współczesnej gospodarki. Niezwykle szybko rosnąca rola i oddziaływanie Internetu na praktycznie każdy sektor gospodarki powoduje konieczność jak najlepszego rozumienia przez podmioty w niej funkcjonujące istoty zagadnienia i całej jego złożoności. Aby skutecznie rywalizować w nowej, postindustrialnej rzeczywistości gospodarczej, w której coraz większą rolę odgrywa globalna infrastruktura sieciowa, jaką jest Internet, organizacje muszą umieć się w niej poruszać tak, aby z jednej strony wykorzystywać wyłaniające się szanse i często niedostępne wcześniej możliwości, a z drugiej minimalizować lub też całkowicie eliminować nowe i nieznane im wcześniej zagrożenia.

W tej sytuacji coraz bardziej istotnym elementem aktywności każdego przedsiębiorstwa staje się umiejętność zarządzania przestrzenią elektroniczną, w której odbywa się funkcjonowanie wszelkich podmiotów korzystających z Internetu i do której przenosi się w szybkim tempie coraz większa cześć współczesnej działalności gospodarczej, oraz włączanie tego typu działań do zakresu rutynowych aktywności każdej firmy. Dlatego też każda organizacja powinna

podejmować odpowiednie całościowe działania związane z szeroko pojętym zarządzaniem nią, tj. planowaniem i organizowaniem działalności on-line, kierowaniem ludźmi w niej działającymi oraz kontrolowaniem zarówno poszczególnych elementów, jak i całości swej aktywności w środowisku elektronicznym.

W tym kontekście wskazać można dwa zasadnicze aspekty, które powinny być brane pod uwagę:

- zabezpieczenie i szeroko pojęta ochrona działalności on-line (działania prewencyjno-zabezpieczające),
- wykorzystanie możliwości aktywnego oddziaływania na nią (działania proaktywne).

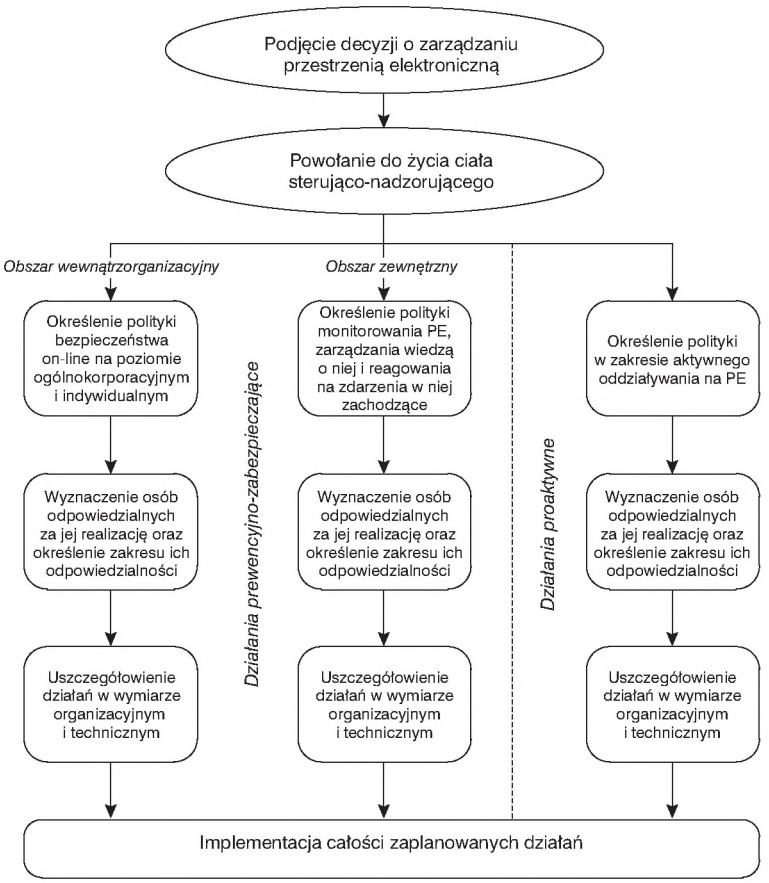
2. Działania związane z zabezpieczeniem i ochroną aktywności organizacji on-line

Niewątpliwie pierwszym krokiem, jaki powinien być podjęty w kontekście działań związanych z obydwoma powyższymi obszarami, jest powołanie ciała sterującego-nadzorująco (np. komitetu sterującego), którego zadaniem będzie czuwanie nad całością zagadnień związanych z zarządzaniem przestrzenią elektroniczną w kontekście realizacji celów organizacyjnych. Ze względu na specyfikę jej ewolucji i oddziaływania na organizację jego skład powinien obejmować przedstawiciela kierownictwa przedsiębiorstwa oraz kierownictw działów IT i marketingu. Wynika to z faktu, iż aspekty te nie mogą być w dzisiejszych warunkach traktowane (jak to się wciąż często zdarza) jako zagadnienie czysto techniczne. Stąd wynika z jednej strony konieczność zaangażowania kierownictw działów, które kwestie te w największym stopniu dotykają. Z drugiej natomiast strony szeroko pojęte zagadnienia związane z zarządzaniem przestrzenią elektroniczną, w tym bezpieczeństwem on-line, są na tyle w dzisiejszych warunkach gospodarczych istotne, iż decyzje z nimi związane nie mogą być pozostawione wyłącznie w zakresie odpowiedzialności osób znajdujących się na średnich czy też niskich szczeblach hierarchii organizacyjnej. Toteż coraz częstsze są przypadki firm, w których aspekty związane z cyberbezpieczeństwem (*cybersecurity*) traktowane są jako element strategii biznesowej, w które bezpośrednio zaangażowana jest najwyższa kadra zarządzająca (Kaplan i in. 2011).

Jeśli chodzi o pierwszy z wymienionych wcześniej aspektów związanych z zarządzaniem przestrzenią elektroniczną, tj. działania odnoszące się do zabezpieczenia i szeroko pojętej ochrony działalności on-line, to wyodrębnić należy dwa zasadnicze ich obszary, których aktywność ciała nadzorująco-sterującego powinna dotyczyć, tj. *wewnątrzkorporacyjny* oraz *zewnętrzny* (rysunek 1).

W pierwszym przypadku niewątpliwie kluczowym aspektem jest zdefiniowanie polityki bezpieczeństwa on-line na poziomie zarówno ogólnokorporacyjnym, jak i indywidualnym. Wiąże się to z takimi działaniami jak precyzyjne określenie zasad korzystania przez pracowników z przestrzeni elektronicz-

nej, łącznie z wykorzystywanymi przez nich tam narzędziami, oraz zakresu monitorowania ich aktywności on-line. Ze względu na dużą dynamikę zmian zachodzących w środowisku pracy organizacji i w ich otoczeniu konieczne jest stałe dostosowywanie istniejących rozwiązań do zmieniającej się sytuacji. W tym kontekście należy zauważyć dwa narastające wyzwania, jakie stają przed organizacjami. Z jednej strony są to media społecznościowe (*social media*) i korzystanie z nich przez pracowników (Deloitte 2011). Z drugiej strony jest to natomiast zjawisko „konsumeryzmu IT" (*consumerization-of-IT*), którego przejawem jest nasilający się trend – określanym mianem *bring-your-own-device* (BYOD) (Faas 2012) – do wykorzystywania w środowisku pracy własnych narzędzi mobilnych takich jak smartfony czy tablety (Stackpole 2011; Marciniak 2011).



Rys. 1. Całościowe spojrzenie na zarządzanie przestrzenią elektroniczną przez organizacje. Źródło: opracowanie własne.

Powyższe kwestie dotyczą pracowników funkcjonujących w obszarze „fizycznej" infrastruktury organizacji, ale również realizujących swe zadania w ramach telepracy czy też jako tzw. wolni strzelcy (*freelancers*). Zauważyć należy, iż ta druga grupa staje się coraz bardziej istotna ze względu na coraz powszechniejsze wykorzystanie tego typu pracowników przez przedsiębiorstwa (Raszkowska 2011). Jednocześnie istotnym elementem tych działań są kwestie związane z nadzorowaniem właściwego funkcjonowania i zabezpieczenia infrastruktury IT organizacji w kontekście bezpieczeństwa ogólnokorporacyjnego w przestrzeni elektronicznej. Jak istotne są to kwestie, przekonało się już wiele firm, łącznie z największymi, takimi jak Sony, w przypadku której z pozoru banalne zaniedbania w tym obszarze doprowadziły do znaczących strat finansowych (Urbanowicz 2011; Williams 2011).

Stąd też kolejnym elementem działań powinno być wyznaczenie osób odpowiedzialnych za realizację zadań w wyżej wymienionych obszarach i określenie zakresów ich odpowiedzialności, jak również ustalenie sposobów oraz częstotliwości przekazywania informacji zwrotnych dotyczących podejmowanych przez nie działań i ewentualnie występujących problemów. Trzeci poziom aktywności w tym obszarze to ich uszczegółowienie w wymiarze organizacyjnym, jak również w odniesieniu do wykorzystywanych narzędzi i technologii (rysunek 1).

Drugi, zewnętrzny obszar działań, jeśli chodzi o zabezpieczenie i ochronę działalności on-line, związany jest bezpośrednio z przestrzenią elektroniczną i jej oddziaływaniem. Podobnie jak w poprzednim przypadku, podstawowym zadaniem komitetu sterującego jest określenie polityki organizacji związanej z jej monitorowaniem, zarządzaniem wiedzą o niej oraz sposobami reagowania na określone wydarzenia w niej zachodzące. W tym kontekście kolejnym elementem działań jest również ustalenie osób odpowiedzialnych za realizację poszczególnych zadań i zakresu ich odpowiedzialności, ale też, jeśli to konieczne, powołanie do życia międzydziałowych zespołów eksperckich i ustalenie zakresu ich odpowiedzialności, jak również zdefiniowanie sposobów oraz częstotliwości przekazywania informacji zwrotnych w kontekście podejmowanych działań oraz występujących problemów. Podobnie jak w poprzednim przypadku, trzeci poziom działań w tym obszarze związany jest z ich uszczegółowieniem w wymiarze organizacyjnym i technicznym.

W tym kontekście istotna jest odpowiedź na takie kluczowe pytania jak:

1. Które podmioty (i ich aktywność) powinny być monitorowane?
2. Jak mogą one oddziaływać na organizację i jej funkcjonowanie?
3. Jakie obszary przestrzeni elektronicznej powinny być monitorowane?
4. Jakie środki techniczne powinny być do tego celu wykorzystywane?
5. Kto powinien być odpowiedzialny za proces monitorowania przestrzeni elektronicznej, podejmowanie decyzji w kwestii reagowania na zachodzące tam zdarzenia oraz samą reakcję i wykorzystywane do tego celu środki techniczne?

6. Jakie działania w stosunku do podmiotów działających w przestrzeni elektronicznej będących interesariuszami organizacji, lub też uważającymi się za nich, mogą być podejmowane i są akceptowane przez organizację w ramach zarządzania nimi?

Jeśli chodzi o pierwsze pytanie, to niewątpliwie kluczowym elementem działań jest z tej perspektywy przeprowadzenie przez organizację segmentacji podmiotów funkcjonujących w przestrzeni elektronicznej z punktu widzenia ich potencjalnego oddziaływania na nią. Pozwoli to na wyodrębnienie tych firm, grup, osób prywatnych czy też określonych miejsc on-line, których aktywność powinna być monitorowana z punktu widzenia zapobiegania występowaniu niekorzystnych dla niej zdarzeń lub też, jeśli jest to niemożliwe, odpowiednio szybkiego reagowania na nie. Dotyczy to tak kwestii różnego typu potencjalnego oddziaływania fizycznego na infrastrukturę organizacji, jak również wpływu na jej szeroko pojęte aspekty wizerunkowe (Garnajewa i Namiestnikow 2012).

W tym kontekście wskazać można trzy podstawowe segmenty podmiotów operujących on-line (Wileki 2007: 324). Jeśli chodzi o pierwszy z nich, tj. znane i identyfikowalne podmioty funkcjonujące w przestrzeni elektronicznej i oddziaływujące na organizację, to kwestia ich wyodrębnienia powinna być relatywnie prosta, z uwagi na fakt, iż dotyczy ona generalnie rzecz biorąc „klasycznych" interesariuszy organizacji zarówno zewnętrznych, jak i wewnętrznych. Jednak w nowych warunkach dynamicznie rozwijającej się gospodarki postindustrialnej wraz z jej coraz istotniejszą częścią osadzoną i rozwijającą się on-line, nie jest to już tak oczywiste jak wcześniej, a wynika to z kilku istotnych kwestii.

Po pierwsze podmioty typowo należące do tej grupy, takie jak dostawcy, partnerzy biznesowi czy też konkurenci, a nawet klienci, w rosnącym stopniu funkcjonują w coraz bardziej skomplikowanych i różnorodnych powiązaniach sieciowych, stąd też coraz trudniej jest jednoznacznie określić, do jakich konkretnych grup należy ich zaliczyć, aby następnie monitorować ich aktywność i gromadzić wiedzę o nich, a tym samym odpowiednio szybko i skutecznie ją wykorzystywać.

Po drugie do omawianej tu grupy należy zaliczyć podmioty, które dopiero wraz z rozwojem gospodarki elektronicznej ujawniły się jako interesariusze organizacji. Dotyczy to z jednej strony np. wpływowych lokalnych i globalnych blogerów, ale przede wszystkim największych wyszukiwarek internetowych, których skala oddziaływania na gospodarkę i pojedynczą organizację jest coraz bardziej znacząca i wielowymiarowa (Wielki 2008). Jednocześnie z punktu widzenia coraz większej części przedsiębiorstw podmiotami, które w ich kontekście powinny być zaliczone do tej grupy, są takie globalane serwisy jak Wikipedia czy WikiLeaks.

Jeśli chodzi o drugą grupę to jest ona najtrudniejsza z punktu widzenia jej identyfikacji przez organizacje oraz zarządzania wiedzą o nich w kontekście funkcjonowania w przestrzeni elektronicznej. Obejmuje ona wszelkie te pod-

mioty – zarówno nieznane, jak i trudno identyfikowalne – które wywierają na nią realny i odczuwalny wpływ. W jej ramach wyróżnić można dwa zbiory podmiotów, których aktywność powinna być monitorowana, a zgromadzona wiedza odpowiednio wykorzystywana.

Pierwszy z nich jest związany z kwestiami fizycznego bezpieczeństwa infrastruktury IT organizacji, a co za tym idzie jej samej, ale również jej klientów oraz partnerów biznesowych. Zagadnienia te nabierają coraz większego znaczenia w kontekście dynamicznego rozwoju gospodarki elektronicznej, a jednocześnie stają się coraz bardziej skomplikowane i trudne z uwagi na fakt stosowania przez podmioty należące do tej grupy coraz bardziej wyrafinowanych technologii i metod działania (Ponemon Institute 2012).

Drugi zbiór podmiotów należących do analizowanej grupy to osoby fizyczne lub firmy wykorzystujące narzędzia internetowe do oddziaływania na wiarygodność czy też reputację organizacji. Sięgając po wszelkie dostępne w danym momencie, a nieustannie rozwijające się narzędzia oparte na technologiach internetowych i mobilnych, potrafią one niezwykle skutecznie wpływać na samą organizację, jak również jej bezpośrednich interesariuszy.

Ostatnia, trzecia grupa obejmuje podmioty co prawda funkcjonujące w przestrzeni elektronicznej i realizujące tam swoje cele, jednak uznawane za neutralne z punktu widzenia danej organizacji i podejmowanych przez nią działań. Mogą to być takie, których istnienia jest ona świadoma, jak również te całkowicie jej nieznane. Warto jednocześnie w tym kontekście zauważyć, iż ze względu na dużą dynamikę zmian zachodzących w przestrzeni elektronicznej, podmioty należące do tej grupy mogą praktycznie z dnia na dzień stać się interesariuszami organizacji. Dotyczy to tak firm działających wcześniej w zupełnie innym obszarze gospodarki, ale również osób fizycznych organizujących się *ad hoc* w określone grupy interesów (np. motywowanych politycznie różnego typu haktywistów – *hacktivists*) (Symantec 2012).

W kontekście przeprowadzonej segmentacji podmiotów funkcjonujących w przestrzeni elektronicznej, ze względu na kwestie ich potencjalnego oddziaływania na organizację, kolejnym elementem działań powinna być ich analiza z punktu widzenia różnych typów możliwych ich wpływów na nią (fizyczny/niefizyczny, bezpośredni/pośredni, ukierunkowany na zasoby materialne/niematerialne) (Wielki 2007: 325–326). Wiąże się to z odpowiedzią na drugie z powyżej sformułowanych pytań.

Kolejny element aktywności związanej z działaniami prewencyjno-zabezpieczającymi w obszarze zewnętrznym wiąże się z możliwościami zarządzania zidentyfikowanymi grupami interesariuszy organizacji funkcjonującymi w przestrzeni elektronicznej w kontekście realizacji przez nią swych celów. W odniesieniu do tego poziomu niezbędne jest uszczegółowienie kwestii organizacyjno-technicznych związanych z zagadnieniami zawartymi w trzech kolejnych pytaniach, tj. 3, 4 oraz 5.

Z jednej strony jest to kwestia doprecyzowania, jakie obszary przestrzeni elektronicznej i aktywność jakich podmiotów w nich operujących powinny

być szczególnie monitorowane. Chociaż z punktu widzenia organizacji wykorzystujących Internet w swej działalności potencjalnie wszystko, co się w niej dzieje, jest dla firmy istotne, jednak dla każdej z nich istnieją takie miejsca on-line, które są szczególnie drażliwe w kontekście realizacji jej celów biznesowych. Są to często różnorakiego typu fora dyskusyjne, blogi, profile na różnego rodzajach portalach społecznościowych czy też inne obszary, w których kształtowane są opinie o firmie oraz jej działalności. Ich monitorowanie dostarczać może informacji o bieżących, banalnych i całkiem typowych zdarzeniach, wymagających rutynowej reakcji (np. wyjaśnienia pewnych kwestii na forum dyskusyjnym, blogu firmowym czy na portalu społecznościowym), sytuacjach nietypowych i nieoczekiwanych z punktu widzenia organizacji (Gazeta.pl 2010), ale również takich, które potencjalnie dotyczyć mogą rodzących się bardziej zorganizowanych akcji skierowanych przeciw firmie (Grynkiewicz 2010) czy też wyłaniających się zagrożeń w określonym sektorze. Jeśli chodzi o tę ostatnią kwestię, to z punktu widzenia organizacji takich jak banki niezwykle istotne jest monitorowanie określonych miejsc w przestrzeni elektronicznej w kontekście odpowiednio szybkiego pozyskiwania informacji krytycznych z punktu widzenia bezpieczeństwa ich klientów i odpowiednio szybkiego ich ostrzegania, jak również przygotowania własnego do ujawniających się zagrożeń.

Drugie zagadnienie to kwestia środków technicznych wspomagających zarządzanie przestrzenią elektroniczną i podmiotami w niej funkcjonującymi, jakie wykorzystywać będzie organizacja. Dotyczy to narzędzi i rozwiązań wspomagających monitorowanie określonych obszarów przestrzeni elektronicznej, zarządzanie wiedzą o niej oraz reagowania na zachodzące tam zdarzenia. Jeśli chodzi o pierwszy aspekt, to istnieje całe spektrum możliwości w tym względzie. Z jednej strony jest to kwestia ręcznej kontroli określonych miejsc w przestrzeni elektronicznej (serwisów internetowych, blogów, portali społecznościowych itd.) prowadzonej przez odpowiedzialne za to osoby (np. monitorowania i korygowania wpisów dotyczących własnej firmy pojawiających się w Wikipedii tak jak robi to IBM) (Friedman 2006: 134). Odnosi się to również do przeszukiwania zawartości tzw. Internetu głębokiego (*invisible Web*, *deep Web*), z wykorzystaniem do tego celu specjalistycznych wyszukiwarek (Unold 2011: 152–153). Jednocześnie dostępnych jest coraz więcej narzędzi wspomagających monitorowanie przestrzeni elektronicznej. Są to z jednej strony darmowe rozwiązania takie jak Google Alerts, umożliwiające automatyczne prowadzenie tych procesów pod kątem pojawiania się w niej wybranego przez użytkownika tematu czy też tematów. Z drugiej strony dostępne są płatne specjalistyczne serwisy wspomagające monitorowanie i raportowanie w odniesieniu do całej przestrzeni elektronicznej lub też określonych miejsc on-line, np. portali społecznościowych, pod kątem zdefiniowanych słów kluczowych. Przykładami tego typu produktów są takie serwisy jak NewsPoint i NewsPoint Social Media (NewsPoint 2011).

Jednocześnie same narzędzia monitorowania to zdecydowanie za mało, zważywszy na ilość danych i informacji, jakie są generowane w przestrzeni elektronicznej. Aby skutecznie zarządzać nią i operującymi tam interesariuszami organizacji, niezbędne jest posiadanie rozwiązań analitycznych przetwarzających dostarczone dane i łatwo integrowalnych z systemami dostarczającymi wygenerowanych informacji i wiedzy wszelkim odpowiedzialnym za kwestie zarządzania przestrzenią elektroniczną podmiotom w organizacji, tak aby mogły one podejmować szybko i sprawnie niezbędne decyzje oraz działania. Stąd też rozwój rozwiązań takich jak Buzzient Enterprise, dostarczających różnego typu możliwości analitycznych. Może być bezpośrednia integracja z różnego typu systemami CRM, zasilanie systemów klasy *business intelligence* lub też analiza i wizualizacja danych za pomocą aplikacji webowych (Buzzient 2011). Jeśli chodzi natomiast o platformę integrującą informacje i wiedzę dotyczące przestrzeni elektronicznej i podmiotach w niej funkcjonujących oraz aplikacje wspierające zarządzanie nią, to niewątpliwie przydatnym rozwiązaniem w tym kontekście są takie systemy jak portale korporacyjne.

Generalnie rzecz biorąc, rozwiązania wspierające zarządzanie przestrzenią elektroniczną powinny łączyć w sobie elementy takie jak (Wielki i Ziemba 2008: 149–152):

- systemy oparte na wykorzystaniu technologii internetowych i mobilnych, wspierające szeroko pojęte procesy komunikacji, umożliwiające dzielenie się informacją i wiedzą czy też wymianę opinii dotyczących przestrzeni elektronicznej i podmiotów tam funkcjonujących;
- systemy pracy grupowej, zapewniające wymianę informacji i wiedzy wewnątrz organizacji, istotnych z punktu widzenia zarządzania przestrzenią elektroniczną, stymulujące i wspomagające organizowanie współpracy wewnątrzorganizacyjnej;
- system zarządzania dokumentami, pozwalający na przechowywanie, klasyfikację i wyszukiwanie dokumentów dotyczących poszczególnych podmiotów funkcjonujących w przestrzeni elektronicznej;
- systemy przepływu pracy, wspierające wszelkiego typu procesy przebiegające wewnątrz organizacji, jak również w ramach jej powiązań sieciowych, związane z zarządzaniem przestrzenią elektroniczną;
- systemy *business intelligence*, umożliwiające analizę zgromadzonych danych związanych z przestrzenią elektroniczną i podmiotami tam operującymi;
- rozwiązania klasy *Web mining*, umożliwiające automatyczne odkrywanie informacji i wiedzy na podstawie dokumentów umieszczonych na witrynach WWW oraz dające możliwość analizy zachowań użytkowników na stronach WWW;
- systemy szkoleń elektronicznych, wspierające rozwój umiejętności i kwalifikacji, jak również pozyskiwanie i poszerzanie wiedzy pracowników niezbędnej w kontekście zarządzania przestrzenią elektroniczną;

- technologie wyszukiwania informacji i wiedzy, takie jak narzędzia kategoryzacji i taksonomii, ontologie czy też wyszukiwarki;
- intranet lub inna sieć wewnątrzorganizacyjna dająca pracownikom dostęp do informacji i wiedzy dotyczącej przestrzeni elektronicznej i podmiotów w niej funkcjonujących.

Jednocześnie, oprócz omówionych powyżej narzędzi i rozwiązań technicznych, istotnym elementem z punktu widzenia zarządzania przestrzenią elektroniczną jest – podobnie jak w obszarze wewnętrznym – uszczegółowienie działań w wymiarze organizacyjnym.

Ostatnie ze sformułowanych wcześniej pytań wiąże się z określeniem, jakie typy aktywności w przestrzeni elektronicznej w stosunku interesariuszy organizacji, w ramach działań prewencyjno-zabezpieczających, są dopuszczalne i akceptowalne, a jakie absolutnie nie. Jest to kwestia związana z wymiarem normatywnym zarządzania interesariuszami (Donaldson i Preston 1995: 71, 81–82), która powinna być zdefiniowana na poziomie komitetu sterującego.

3. Działania związane z aktywnym wpływem organizacji na przestrzeń elektroniczną

Jednocześnie, poza podejmowaniem działań prewencyjno-zabezpieczających w odniesieniu do swojej obecności i funkcjonowania w przestrzeni elektronicznej, każda organizacja ma cały szereg możliwości aktywnego oddziaływania na nią i kształtowania jej na pięciu zasadniczych poziomach: własnym, sektorowym, krajowym, regionalnym i globalnym.

Jeśli chodzi o pierwszy z nich, jest to kwestia wprowadzania własnych rozwiązań, systemów czy produktów, ale również tworzenia i implementacji własnych polityk czy regulaminów dotyczących różnych aspektów funkcjonowania on-line (np. *privacy policies*). Inne kluczowe możliwości oddziaływania na przestrzeń elektroniczną na poziomie własnym to podejmowanie działań prawnych skierowanych przeciwko innym podmiotom tam funkcjonującym, szczególnie takim, które w sposób istotny tworzą lub też oddziałują na jej kształt i ład w niej panujący (np. Google).

Jeżeli chodzi o możliwości związane z poziomem sektorowym, to dotyczą one przede wszystkim takich aspektów, jak tworzenie rozwiązań sprzyjających i stymulujących rozwój danej branży (np. SET – system płatności on-line) czy też podejmowanie różnego typu działań prawnych (np. działania branży muzycznej przeciwko użytkownikom ściągających pliki mp3, działania branży wydawniczej przeciwko Google Books).

Z kolei w kontekście oddziaływania na poziomie krajowym najważniejsze jego elementy obejmują: tworzenie własnych produktów i rozwiązań ukierunkowanych lokalnie, udział we wszelkiego rodzaju ciałach pracujących nad określonymi rozwiązaniami istotnymi dla jej kształtu i funkcjonowania czy też opiniującymi je, podejmowanie działań lub też organizowanie różnego

typu akcji skierowanych przeciw określonym rozwiązaniom mogącym, z ich punktu widzenia, w istotny sposób niekorzystnie wpływać na jej funkcjonowanie na poziomie lokalnym oraz podejmowanie działań prawnych skierowanych przeciwko innym podmiotom działającym na poziomie krajowym.

Jeśli chodzi natomiast o poziom regionalny, najważniejsze możliwości oddziaływania organizacji to: bezpośredni udział w pracach różnych ciał (np. grup roboczych) lub też poprzez organizacje je reprezentujące w tworzeniu i opiniowaniu kluczowych aktów prawnych wpływających na funkcjonowanie przestrzeni elektronicznej (np. takich jak na terenie UE dyrektywy unijne), podejmowanie określonych działań prawnych czy też lobbowanie na rzecz określonych rozwiązań pożądanych z ich punktu widzenia (dotyczy to szczególnie większych firm).

W przypadku poziomu globalnego możliwości oddziaływania na tym poziomie dotyczą dwóch zasadniczych aspektów. Pierwszy z nich związany jest z udziałem firm w pracach organizacji czuwających nad całościowym rozwojem Internetu (np. The Internet Society, W3C), a co za tym idzie przestrzeni elektronicznej, oraz wypracowywujących rozwiązania sprzyjające temu. Drugi natomiast odnosi się do udziału organizacji wraz z innymi podmiotami w tworzeniu produktów oddziaływujących na nią w wymiarze globalnym (Wielki 2011: 110–118).

Podobnie jak w przypadku działań prewencyjno-zabezpieczających, podstawowym zadaniem komitetu sterującego w tym obszarze jest zdefiniowanie polityki przedsiębiorstwa w odniesieniu do tej kwestii. Dlatego też w tym kontekście niezbędna jest odpowiedź na dwa kluczowe pytania:

- czy organizacja zamierza w ogóle podejmować aktywność w tym obszarze;
- jeżeli tak, to na którym bądź też których z pięciu możliwych poziomów będzie ona prowadzona.

W tym kontekście niezbędne jest przeprowadzenie analizy istniejących możliwości oraz kierunkowy wybór metod działań, jakie wykorzystywać będzie organizacja. Kolejnym elementem jest ustalenie osób odpowiedzialnych za realizację poszczególnych zadań oraz określenie zakresów odpowiedzialności w tej mierze. Tak jak w poprzednich przypadkach, istotnym aspektem jest zdefiniowanie sposobów oraz częstotliwości przekazywania informacji zwrotnych w odniesieniu do podejmowanych działań, a także wyłaniających się problemów. Trzeci poziom działań to ich uszczegółowienie zarówno w wymiarze organizacyjnym, jak i technicznym (rysunek 1).

Jednocześnie całość działań związanych z aktywnym oddziaływaniem na przestrzeń elektroniczną i operujących tam interesariuszy wiąże się ściśle ze wspomnianym wcześniej wymiarem normatywnym zarządzania interesariuszami, czyli określenia norm, jakie będą leżeć u ich podstaw i jasno wskazywać, jakiego rodzaju typy działań są dopuszczalne w ramach polityki organizacji, a jakie nie. Odnosi się to w dużej mierze do podejmowanych przez firmę szeroko pojętych działań marketingowych, ale również innego typu, takich jak np. prawne czy nawet hakerskie. W pierwszym przypadku

jest to kwestia akceptowalności działań takich jak wykorzystanie wynajętych osób w celu podszywania się na forach dyskusyjnych czy portalach społecznościowych pod zadowolonych klientów własnej firmy (Lemański 2011: 14–15), generowanie fałszywych opinii o konkurentach (Gaudin 2011), próby manipulowania wynikami wyszukiwania przy użyciu zabronionych technik optymalizacyjnych (Grynkiewicz 2012) czy też generowaniem tzw. fałszywych kliknięć (Elgin i in. 2006).

Z drugiej strony są to kwestie przyzwolenia na aktywne działania, jakie miały miejsce w branży muzycznej na początku nowego millenium, jak pokazowe wytaczanie procesów sądowych skierowanych przeciwko własnym interesariuszom, sięganie po takie rozwiązania jak finansowanie firm softwarowych w celu tworzenia przez nie oprogramowania mogącego uszkodzić komputery oraz łącza internetowe osób ściągających pliki mp3 czy też wykorzystanie wyspecjalizowanych wirusów komputerowych w celu losowego usuwania tego typu plików z dysków twardych (Wielki 2004: 921). Odnosi się to również do kwestii dopuszczalności takich działań jak ataki DDoS (*Distributed Denial of Service*) na firmy konkurencyjne, które stają się coraz częściej faktem w różnych branżach (Garnajewa i Namiestnikow 2012).

4. Zakończenie

Organizacje decydujące się na wykorzystanie Internetu w swej działalności biznesowej coraz powszechniej zaczynają mieć świadomość, iż środowisko elektroniczne, do którego wkraczają nie jest tylko źródłem różnorakich możliwości rozwoju, ale również generuje cały szereg nowych, a często nieznanych wcześniej, ale nieustannie ewoluujących wyzwań związanych zarówno z własnymi pracownikami, jak i wszelkiego typu interesariuszami zewnętrznymi. Stąd też, aby móc jak najskuteczniej wykorzystywać pojawiające się liczne, obecne i przyszłe szanse związane z aspektami marketingowymi, implementacją nowych modeli biznesowych i całym szeregiem innych kwestii związanych z praktycznie wszystkimi sferami funkcjonowania firmy, przedsiębiorstwa muszą nauczyć się całościowo spoglądać na swą obecność w przestrzeni elektronicznej. Oznacza to w praktyce konieczność uważnego projektowania własnej aktywności w niej i ciągłego oraz jak najbardziej efektywnego zarządzania nią w kontekście realizacji celów biznesowych. Odnosi się to zarówno do kwestii zabezpieczenia i ochrony działalności on-line w wymiarze wewnętrznym, jak i zewnętrznym, jak również wykorzystania możliwości związanych z aktywnym oddziaływaniem na przestrzeń elektroniczną w celu kształtowania jej rozwoju, aby był on jak najbardziej przyjazny i sprzyjający organizacji z punktu widzenia realizowanych przez nią celów.

Obydwa wspomniane powyżej obszary wymagają dobrze przemyślanych i zorganizowanych działań związanych z zarządzaniem w szeroko rozumianym sensie, przestrzenią elektroniczną, biorąc przy tym pod uwagę wszelkie

kwestie zarówno organizacyjne, jak też techniczne, oraz konieczność szerokiego zaangażowania kadry zarządzającej oraz pozostałych pracowników.

Koncentrując się wyłącznie na wykorzystaniu nowych możliwości pojawiających się wraz z rozwojem Internetu i przestrzeni elektronicznej bez odpowiedniego przygotowania własnej obecności on-line i zarządzania nią, organizacje ryzykują, iż podejście takie doprowadzić może do zupełnie innych rezultatów od tych oczekiwanych. Odnosi się to do wszelkiego typu przedsiębiorstw wykorzystujących w różnorodnym zakresie i skali tą globalną strukturę sieciową, w oczywisty sposób najbardziej tych, dla których środowisko elektroniczne staje się podstawowym obszarem prowadzenia działalności biznesowej.

Informacje o autorze
Dr inż. Janusz Wielki – Wydział Ekonomii i Zarządzania, Politechnika Opolska.
E-mail: janusz@wielki.pl.

Bibliografia

Buzzient 2011. *Social Media Analytics*, http://www.buzzient.com.

Deloitte 2011. *Raising the Bar 2011 TMT Global Security Study – Key Findings*, http://www.deloitte.com/assets/DcomCroatia/Local%20Assets/Documents/2011/TMT_2011_Global_Security_Survey_hr.pdf.

Donaldson, T. i L. Preston 1995. The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications. *Academy of Management Review*, nr 1 (20), DOI: 10.2307/258887.

Elgin, B. i in. 2006. Click Fraud: The Dark Side of Online Advertising. *BusinessWeek*, http://www.businessweek.com/magazine/content/06_40/b4003001.htm.

Faas, R. 2012. How Mobile, BYOD and Younger Workers are Reinventing IT. *Computerworld*, http://www.computerworld.com/s/article/print/9224568/How_mobile_BYOD_and_younger_workers_are_reinventing_IT?taxonomyName=IT%20Ind.

Friedman, T. 2006. *Świat jest płaski*, Poznań: Dom Wydawniczy Rebis.

Garnajewa, M. i J. Namiestnikow 2012. *Ataki DDoS w drugiej połowie 2011 roku*, http://www.viruslist.pl/ news.html?newsid=700.

Gaudin, S. 2011. Caught! Facebook Admits Running Anti-Google Campaign. *Computerworld*, http://www.computerworld.com/s/article/9216656/Caught_Facebook_admits_running_anti_Google_campaign.

Gazeta.pl 2010. *HTC pyta – fani odpowiadają*, http://technologie.gazeta.pl/internet/2029022,104530,7793096,HTC_pyta ___fani_odpowiadaja.html?logo_druk=.

Grynkiewicz, T. 2010. Antypampersowa kampania na Facebooku i nie tylko. *Gazeta Wyborcza*, http://wyborcza.biz/biznes/2029020,100896,7885824.html.

Grynkiewicz, T. 2012. Nokaut znokautowany: dotkliwa kara Google'a dla polskich porównywarek. *Gazeta Wyborcza*, http://wyborcza.biz/biznes/2029020,100896,11530949.html/.

Hamblen, M. 2012. Consumerization Trend Creates IT Worries, Worker Benefits. *Computerworld*, http://www.computerworld.com/s/article/print/9227238/Consumerization_trend_creates_IT_worries_worker_ benefits?taxonomyName=Mobile+a/.

Kaplan, J. i in. 2011. Meeting the Cybersecurity Challenge. *McKinsey Quarterly*, https://www.mckinseyquarterly.com/ article_print.aspx?L2=13&L3=112&ar=2821.

Lemański, A. 2011. Opinia światłowodem się niesie. Czyli rozważania o etycznych aspektach internetowego public relations. *Computerworld Polska*, 24 maja.
Marciniak, M. 2011. Smartfony w firmach. *Computerworld Polska*, 23 sierpnia.
NewsPoint 2011. *Monitorowanie mediów*, http://www.newspoint.pl/o-nas/newspoint-monitoring-mediow.
Ponemon Institute 2012. *The Impact of Cybercrime on Business*, http://www.checkpoint.com/products/downloads/whitepapers/ponemon-cybercrime-2012.pdf.
Raszkowska, G. 2011. Freelancera zatrudnię od zaraz. *Rzeczpospolita*, http://www.rp.pl/artykul/661807.html?print=tak.
Stackpole, B. 2011. iPads run amok: Does your company need a tablet policy? *Computerworld*, http://www.computerworld.com/s/article/9216208/iPads_run_amok_Does_your_company_need_a_tablet_policy_.
Symantec 2012. *2011 Internet Security Threat Report*, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf.
Unold, J. 2011. Cyberspace Information Retrieval and Processing with the Use of the Deep Web, w: A. Korowicki i B. Kubiak (red.). *Information Management*, Prace i Materiały Wydziału Zarządzania Uniwersytetu Gdańskiego, nr 3. Gdańsk: Wydział Zarządzania Uniwersytetu Gdańskiego, Fundacja Rozwoju Uniwersytetu Gdańskiego.
Urbanowicz, J. 2011. *Sony ujawnia szczegóły włamania*, http://technologie.gazeta.pl/internet/1,104665,9543776,Sony_ujawnia_szczegoly_wlamania.html/.
Wielki, J. 2004. Social and Ethical Implications of the Virtualization of the Business Environment in the Music Sector, w: T. Bynum i in. (red.) *Proceedings of the Seventh International Conference on Challenges for Citizen of the Information Society ETHICOMP 2004*, Volume 2, Syros: University of Aegean.
Wielki, J. 2007. Social and Ethical Aspects Connected with e-Space Development. *Journal of Information, Communication and Ethics in Society*, nr 4 (5), DOI: 10.1108/14779960710846173.
Wielki, J. 2008. Search Engines as a New Type of Stakeholder of Contemporary Organizations, w: H. Dudycz, M. Dyczkowski i J. Korczak (red.) *Advanced Information Technologies for Management – AITM 2008*, Wroclaw University of Economics – Research Papers, nr 35. Wrocław: Publishing House of the Wroclaw University of Economics.
Wielki, J. 2011. Analiza możliwości oddziaływania organizacji na kształt i funkcjonowanie przestrzeni elektronicznej, w: W. Chmielarz, J. Kisielnicki i O. Szumski (red.) *Informatyka 4 przyszłości. Miejsce i rola serwisów internetowych w rozwoju społeczeństwa informacyjnego*, Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego.
Wielki, J. i E. Ziemba 2008. The Use of Corporate Portals in Managing Knowledge on Entities Operating in the Electronic Space, w: S. Wrycza (red.) *Proceedings of BIR'2008 – The Seventh International Conference On Perspectives In Business Informatics Research*, Gdańsk: Wydawnictwo Uniwersytetu Gdańskiego.
Williams, M. 2011. *PlayStation Network hack will cost Sony $170M*, http://www.networkworld.com/news/2011/052311-playstation-network-hack-will-cost.html.