PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1132 — 2006
Koncepcje, modele i metody zarządzania informacją i wiedzą

Aleksander Binsztok, Tomasz Radziszewski

PODEJŚCIE SYSTEMOWE W OCHRONIE INFORMACJI

„[...] jeśli lata osiemdziesiąte określano mianem dekady jakości,
lata dziewięćdziesiąte dekadą produktywności,
to pierwsze dziesięciolecie naszego wieku będzie ***dekadą bezpieczeństwa"***

Edward Yourdon

„Wojny na bity: Wpływ wydarzeń z 11 września na technikę informacyjną"

1. Wstęp

Widoczny rozwój cywilizacji zmierzający w kierunku tzw. społeczeństwa informacyjnego (*information society*) wspierany jest przez nowoczesne technologie i coraz to ciekawsze wynalazki w tym obszarze. Mowa tu oczywiście o powszechnej informatyzacji naszego codziennego życia, o masowości wykorzystania Internetu oraz o zataczającej coraz szersze kręgi gospodarce elektronicznej. Nikogo już dziś nie dziwi korzystanie z telefonów komórkowych, bankowości elektronicznej czy kart płatniczych. Zaawansowane technologie teleinformatyczne, będące ich podstawą, umożliwiają szybki przepływ informacji. Społeczeństwo, wskutek wykorzystania tych narzędzi, staje się „przezroczyste". Klarowne stają się procesy gospodarcze, mamy jasny obraz przeprowadzanych transakcji, możemy prześledzić historię działania poszczególnych klientów – sprawdzić ich wiarygodność czy poziom ewentualnych zobowiązań rynkowych. Dobrodziejstwa związane z rozwojem wspomnianych technologii przynoszą nam wszystkim ewidentne korzyści przede wszystkim w postaci łatwego, błyskawicznego dostępu do informacji. Z drugiej jednak strony ich wykorzystanie kryje także szereg niebezpieczeństw. Jednym z podstawowych jest szeroko rozumiana utrata bezpieczeństwa informacji – czynnika, który stanowi coraz częściej o przewadze konkurencyjnej i trwałości organizacji związanej z ciągłością działania jej krytycznych procesów.

2. Konieczność ochrony informacji

W otoczeniu prawnym organizacji funkcjonują nakazy szczególnego postępowania z określonymi grupami informacji, nakładające na kierownictwo obowiązek podjęcia szeregu działań o charakterze organizacyjno-technicznym w zakresie ochrony informacji (np. Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych DzU nr 101, poz. 926 z 2002 r. z późn. zm. oraz Ustawa z 22 stycznia 1999 r. o ochronie informacji niejawnych DzU nr 11, poz. 95 z 1999 r. z późn. zm., tajemnice zawodowe – bankowa, lekarska, wynalazcza).

Konieczność ochrony informacji przez organizację wynika często również z wymagań kontraktowych. Istnieje jednak pewna grupa informacji, do której należą:
- patenty, posiadane i opanowane technologie,
- prace badawcze i rozwojowe zakończone lub w toku,
- sekrety handlowe całej organizacji lub jej poszczególnych członków,
- bazy danych,
- wiedza nt. sfery publicznej,
- know-how, którym dysponują pracownicy firmy, dostawcy, dystrybutorzy i inni partnerzy,
- kultura przetwarzania informacji, reagowania na nowości, debaty, formułowania pytań i poszukiwania odpowiedzi.

Informacje te zalicza się do grona wrażliwych dla danej organizacji i stanowią one nieuchwytne (*intangible*) zasoby firmy, które tak jak inne ważne aktywa biznesowe, mają dla organizacji wartość, a zdecydowanie łatwiej można je upłynnić. Z tego właśnie powodu należy je szczególnie chronić, tak aby:
- gwarantować ciągłość prowadzenia działań,
- zminimalizować ewentualne straty,
- maksymalizować zwrot nakładów na inwestycje i działania biznesowe.

Instrumentem wspomagającym tego rodzaju działania jest Ustawa z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (DzU nr 47, poz. 211 z 1993 r. z późn. zm.).

3. Triada bezpieczeństwa informacji

Jak pisze T. Rochala, mimo dobrych perspektyw rozwojowych, informacja jest zasobem nie w pełni jeszcze dojrzałym. Dlatego też musi się rozwijać, uwzględniając następujące kryteria:
- **przydatność**, tj. dopasowanie do potrzeb użytkowników,
- **aktualność**, czyli dostosowanie do czasu jej użytkowania,
- **jakość**, czyli poprawność i wiarygodność,
- **własność** (jako prawo), czyli określenie praw dostępu do niej [Rochala 1997, s. 341-342].

Powyższy zestaw cech, jakie powinna mieć informacja, należy zatem skomentować w kontekście jej bezpieczeństwa, budując zestawienie:

- **przydatność** rozumiana jako użyteczność, odpowiedniość, dopasowanie do potrzeb użytkowników, w tym potrzeb konkurencji – powinna być rozwijana z uwzględnieniem **dostępności** rozumianej w aspekcie bezpieczeństwa jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów i tylko wtedy, gdy jest to uzasadnione;
- **aktualność** rozumiana jako ustawiczna modyfikacja mająca na celu budowanie informacji adekwatnej do przesłanek dynamicznego otoczenia organizacji np. w celu skutecznego zarządzania jej ryzykiem operacyjnym; **jakość** jako niezawodność, poprawność i wiarygodność. Pryzmat bezpieczeństwa wiąże te cechy z **integralnością** informacji rozumianą jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania, poprzez wdrożenie odpowiednich zabezpieczeń;
- **własność** rozpatrywaną w aspekcie zarządzania należy traktować jako element triady bezpieczeństwa informacji, zwany **poufnością**, która rozumiana jest jako zapewnienie dostępu do informacji tylko osobom upoważnionym.

Zachowanie poufności, dostępności i integralności jest podstawą bezpieczeństwa informacji.

4. Zagrożenia związane z bezpieczeństwem informacji

Należy wskazać, że zapewnienie bezpieczeństwa informacji w organizacji związane jest z koniecznością bronienia się przed różnego rodzaju zagrożeniami, które można określić jako potencjalne przyczyny niepożądanego incydentu, skutkującego szkodą dla systemu lub organizacji.

Podstawową identyfikację tych zagrożeń przedstawiono w tab. 1.

W sytuacji, gdy kierownictwo organizacji nie podejmuje działań mających na celu ochronę informacji, istnieje wiele potencjalnych i realnych zagrożeń dla bezpieczeństwa przetwarzanych informacji. Wśród najczęściej spotykanych kategorii tych zagrożeń można wymienić:

- brak zasad dotyczących ochrony informacji w firmie,
- brak założeń bezpieczeństwa dla systemów,
- brak zasad stałego monitorowania systemów i usuwania błędów,
- brak zasad bezpieczeństwa korzystania z Internetu,
- brak przeprowadzania analizy zagrożeń i ryzyka dla systemów,
- brak zdefiniowania sytuacji kryzysowych,
- brak procedur postępowania w sytuacjach kryzysowych,
- brak szkoleń pracowników – niska kultura ochrony informacji [Byczkowski 2005],
- brak odpowiedniego zarządzania konfiguracją systemów.

Tabela 1. Przykłady różnego rodzaju zagrożeń bezpieczeństwa informacyjnego w organizacji

Kryterium wyróżnienia danego rodzaju zagrożenia	Rodzaj zagrożenia bezpieczeństwa informacyjnego w organizacji
Źródło zagrożenia	Wewnętrzne – wynikające z dostępu do konkretnych informacji osób bezpośrednio związanych z danym systemem komputerowym (np. pracownicy danej firmy); zagrożeniem jest np. występowanie tylko jednego administratora sieci, który zna wszystkie hasła i loginy do systemów i aplikacji, a także ma wiedzę dotyczącą standardów konfiguracyjnych wszystkich serwerów. Zagrożenie to może się zmaterializować w przypadku zwolnienia administratora z pracy, jego choroby lub wyjazdu na urlop. Wówczas może nastąpić zakłócenie ciągłości działania organizacji. Zewnętrzne – pochodzące od osób trzecich, niezwiązanych z organizacją (np. pracownicy innych firm, partnerzy biznesowi, dostawcy, konkurenci, klienci); zagrożeniem może być np. pozostawienie bez nadzoru personelu firmy sprzątającej, mającego dostęp do pomieszczeń kadry zarządzającej. Brak wprowadzenia zasad czystego biurka i czystego ekranu w takiej sytuacji może doprowadzić do wycieku wrażliwych informacji.
Charakter działania	Przypadkowe – wynikające z nieświadomego postępowania pracowników lub osób spoza organizacji; np. dokonywanie zmian w konfiguracji stacji roboczej, przypadkowa dezaktywacja zabezpieczeń, co w konsekwencji może doprowadzić do włączenia stacji do sieci komputerów zombi, na których mogą zastać umieszczone niechciane dane (np. dziecięca pornografia itd.). Brak świadomości zagrożeń może przyczynić się do wzrostu skuteczności rozwijającego się dynamicznie phisingu (wyłudzania od użytkowników poufnych danych za pomocą spreparowanych maili i stron WWW). Celowe – działania zaplanowane, zmierzające do naruszenia bezpieczeństwa informacji; pochodzące zarówno z wewnątrz, jak i z zewnątrz organizacji; np. działanie insiders – działających z pobudek ideologicznych czy też materialnych.
Oprogramowanie i sprzęt	Programowe – powstałe na skutek występowania błędów w oprogramowaniu; np. celowe zaszywanie w kodzie oprogramowania bomb logicznych, pozostawianie wrót, którymi programista może w sposób nieautoryzowany wniknąć do systemu. Sprzętowe – różnego rodzaju awarie sprzętu bądź anomalia zasilania, np. awarie, które mają miejsce na skutek niewłaściwej konserwacji systemu i nieprawidłowej eksploatacji przez użytkowników końcowych.

Źródło: opracowanie własne.

Nietrudno również zauważyć, że skoro informacja staje się dziś najbardziej pożądanym towarem, to pojawia się coraz więcej osób, które chcą dokonać jej kradzieży. Wśród najczęściej spotykanych form nieuczciwego pozyskiwania informacji można wskazać:

- stosowanie socjotechnik, które polegają na wykorzystaniu braku świadomości pracowników danej organizacji nt. wartości informacji, jaką dysponują,

Tabela 2. Przykłady działań związanych z naruszeniem bezpieczeństwa informacyjnego w organizacji

Przykład działania związanego z naruszeniem bezpieczeństwa informacyjnego	Opis działania mającego na celu naruszenie bezpieczeństwa informacyjnego w organizacji
Wykradanie oraz świadome i nieświadome udostępnianie nośników informacji	Jest to jeden z najczęstszych sposobów nieuczciwego pozyskiwania informacji, przysparzający najwięcej kłopotów. Związany jest głównie z wykradaniem i udostępnianiem wydruków papierowych, dyskietek, taśm z kopiami zapasowymi oraz płyt CD-ROM z zapisanymi informacjami nt. firmy lub klientów, działalności.
Udostępnianie usług WWW z zainstalowanym „w tle" wrogim oprogramowaniem	Zdarza się, że pracownicy, którzy przetwarzają informacje chronione w organizacji, łączą się także z wieloma serwerami WWW i ściągają ciekawie opracowane graficznie, migocząco-grające strony z informacjami, które często nie są związane z wykonywaną przez nich pracą. Ściągnięcie takiej strony wprowadza zagrożenie uruchomienia na stacji użytkownika różnych programów, które w tle aktywują „inne użyteczne" programy, mające na celu wyciąganie, modyfikację bądź usuwanie zawartych tam informacji. Łączenie się zatem z serwerem WWW może powodować nieświadome „użyczenie" naszego komputera do „nieznanej działalności".
Włamania do systemów związane z nieautoryzowanym dostępem do informacji	Włamań tych dokonuje się przede wszystkim takimi metodami, jak: – odgadnięcie lub podsłuchanie hasła dostępu; – zastosowanie specjalnego programu typu „exploit", pozwalającego wykorzystać błędy bezpieczeństwa w oprogramowaniu, – podesłanie specjalnego programu typu „koń trojański", umożliwiającego zdalny dostęp do informacji w systemie.
Blokowanie dostępu do serwerów usług internetowych / intranetowych organizacji	Podmioty mające na celu destabilizację systemów bezpieczeństwa informacji określonej organizacji blokują dostęp do poczty elektronicznej, WWW i innych usług inter- czy intranetowych. W związku z tym w sytuacji, gdy firma prowadzi interesy przez Internet, za pomocą własnego serwera WWW, klienci nie mogą skorzystać z jej usług, a w przypadku wykorzystania poczty elektronicznej do wymiany informacji niemożliwe jest jej przesłanie.
Ataki na oprogramowanie organizacji konkurencyjnych	W celu destabilizacji pracy w organizacji stosowane są ataki na informacje, wykorzystujące różnego typu wirusy czy bomby logiczne.
Podsłuchiwanie pola elektromagnetycznego emitowanego przez urządzenia komputerowe	Przy użyciu specjalnego sprzętu wydobywane są z organizacji informacje wskutek podsłuchiwania pola elektromagnetycznego, jakie emitowane jest przez monitory, kable itp.
Stosowanie klasycznych podsłuchów pomieszczeń	Informacje wyprowadzane są z organizacji poprzez standardowe pluskwy oraz niezwykle popularne „nadajniki", jakimi są np. telefony komórkowe.

Źródło: opracowanie własne na podstawie [Byczkowski 2005].

- wkradanie się do systemów informatycznych (np. różnego rodzaju baz danych personalnych czy finansowych) zarówno z zewnątrz, jak i od wewnątrz organizacji,
- zwyczajne włamanie do pomieszczeń firmy.

Lista działań mających na celu kradzież informacji lub destabilizację poziomu bezpieczeństwa informacyjnego nie kończy się jednak na wyżej wskazanych. Wśród innych przykładów zagrożeń bezpieczeństwa informacji w organizacji można wymienić działania wyszczególnione w tab. 2.

5. Podejście systemowe związane z bezpieczeństwem informacji

Jak wynika z badań literaturowych, w przypadku wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji (SZBI) zachęca się do przyjęcia podejścia procesowego. Taki kierunek działania został sprawdzony podczas budowania systemów zarządzania jakością (SZJ). Otrzymane wyniki potwierdzają skuteczność takiego rozwiązania. W odniesieniu do bezpieczeństwa informacji podejście procesowe pozwoli zwrócić uwagę użytkownika SZBI na:

- zrozumienie biznesowych wymagań bezpieczeństwa informacji oraz potrzeb ustanowienia polityki i celów bezpieczeństwa informacji,
- wdrażane i eksploatowane zabezpieczenia w kontekście kompleksowego zarządzania ryzykiem w organizacji,
- monitorowanie i przegląd wydajności oraz skuteczności SZBI,
- ciągłe doskonalenie systemów na podstawie obiektywnego pomiaru.

Do wszystkich procesów związanych z SZBI można wykorzystać znany model PDCA.

Najlepsze rezultaty w budowie skutecznego SZBI daje oparcie się na takich aktach normatywnych, jak: norma PN ISO/IEC 17799:2003, BS 7799-2:2002, ISO 27001 oraz na sprawdzonych metodach wdrożeń, jak np. metodyka European Network Security Institute, zwana TISM.

To ostatnie rozwiązanie stanowi platformę organizacyjną, której przyjęcie związane jest z następującymi celami:

I. Trwanie i rozwój przedsiębiorstwa oparte na,

1) gwarantowaniu płynności procesów biznesowych,

2) niezawodności organizacji dzięki systemowemu podejściu do jakości,

3) minimalizacji strat na odtwarzanie utraconych danych, jak również przywracaniu odpowiednich procesów biznesowych,

4) zminimalizowaniu zagrożenia utraty krytycznych aktywów firmy,

5) unikaniu konsekwencji prawnych wynikających z niespełnienia obowiązujących przepisów.

II. Dostosowanie do wymogów unijnych:

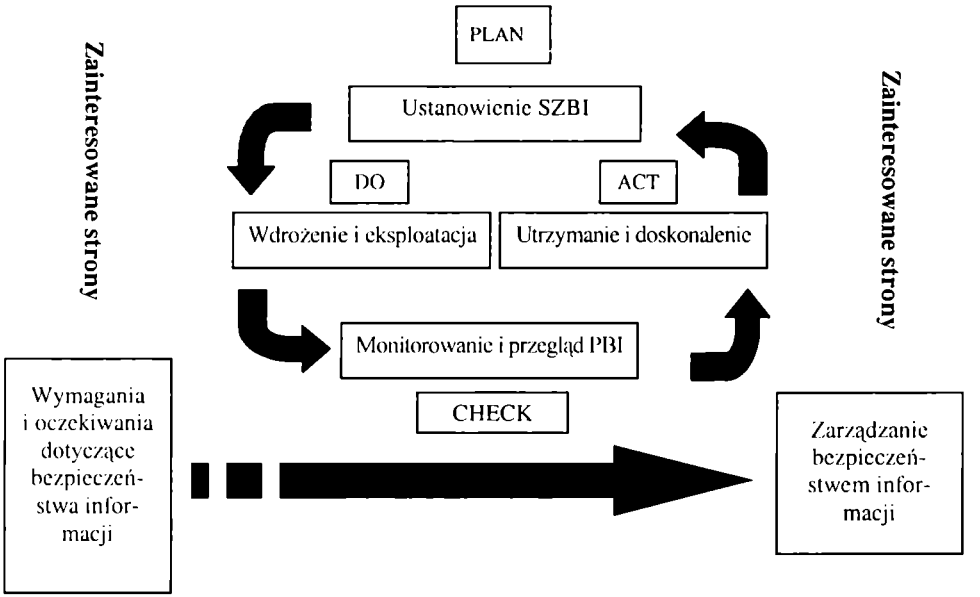
1) standardów zarządzania jakością,

2) standardów ochrony informacji,

3) standardów bezpieczeństwa systemów teleinformatycznych.

III. Spełnianie warunków prawnych, w tym:

1) o ochronie informacji/tajemnicy przedsiębiorstwa, danych osobowych, informacji niejawnych, tajemnic zawodowych.



Rys. 1. Implementacje modelu PDCA w procesach SZBI [PN-i-07799-2:2005]

Tak więc wdrożenie SZBI powinno być związane z:

1) określeniem, jakiego rodzaju informacje są przetwarzane w organizacji oraz które z nich powinny podlegać ochronie[1],

2) analizą ryzyka przetwarzanych informacji, prowadzoną na podstawie audytu i testów bezpieczeństwa systemów, w których informacje są przetwarzane,

3) opracowaniem dokumentów SZBI,

4) wdrożeniem SZBI tak, aby był on akceptowany i przestrzegany przez wszystkich pracowników firmy.

6. Czynniki warunkujące skuteczność SZBI

Minimalnym wymaganiem dotyczącym zarządzania systemem bezpieczeństwa informacji jest uczestnictwo w systemie wszystkich członków organizacji. Kryterium to można wzmocnić przez wymaganie udziału dostawców, klientów i udziałowców oraz specjalistyczne doradztwo osób spoza organizacji. Decyzja o budowie, wdrożeniu, doskonaleniu SZBI powinna mieć charakter strategiczny, powinna być wspierana stworzeniem na najwyższym szczeblu zarządzania poli-

[1] Chodzi tu przede wszystkim o tajemnice przedsiębiorstwa, dane osobowe i inne tajemnice prawnie chronione.

tyki bezpieczeństwa, określającej ramy do definiowania celów BI ściśle związanych z charakterem działalności biznesowej organizacji. Przyjęte podejście do wdrażania rozwiązań związanych z bezpieczeństwem informacji powinno być zgodne z kulturą organizacyjną organizacji. Nie bez znaczenia jest również właściwe zrozumienie wymagań bezpieczeństwa, szacowania ryzyka i zarządzania ryzykiem. Nade wszystko podstawą realizacji wszystkich założeń BI jest odpowiednia komunikacja:

a) w organizacji – między jej pracownikami,

b) w otoczeniu – między organizacją a podmiotami rynkowymi (klientami, dostawcami, instytucjami samorządowymi i in.).

Bezpieczeństwo informacji można też rozpatrywać na powyższych dwóch poziomach ogólności. Pierwszy z nich buduje kontekst wspierający efektywne propagowanie bezpieczeństwa wśród pracowników i kierownictwa, tworzy podwaliny mechanizmów informowania o incydentach związanych z bezpieczeństwem informacji i celach związanych z doskonaleniem SZBI stosowanych w ramach wszechstronnego i adekwatnego systemu pomiarowego używanego do oceny jakości zarządzania bezpieczeństwem informacji. Efektywna komunikacja zewnętrzna gwarantuje transparentność działań związanych z bezpieczeństwem, budując tym samym zaufanie klientów i partnerów biznesowych. Zazwyczaj budowana jest na podstawie uzgodnień kontraktowych i przyjętych w organizacji zwyczajów.

Odpowiednia komunikacja następuje wówczas, gdy mają miejsce następujące zalecenia:

1) stworzony jest odpowiedni model przepływu informacji (wysoka przepustowość kanałów komunikacyjnych – ich drożność i pojemność),

2) informacja dostępna jest dla wszystkich pracowników,

3) kreowana jest właściwa atmosfera współpracy (kształtowanie kultury organizacyjnej),

4) zachowana jest tolerancja popełniania błędów (każdy pracownik ma prawo do błędów),

5) pracownicy wykazują zachowania kreatywne i proinnowacyjne,

6) stosowane są różnego rodzaju metody i techniki heurystyczne (kreatywnego rozwiązywania problemów).

Podczas budowania sprawnego systemu przekazywania i wykorzystywania informacji w organizacji powinno się koncentrować na następujących elementach:

- identyfikacji problemów i przedstawianiu ich w postaci możliwej do rozwiązania na każdym szczeblu,
- wskazywaniu metod rozwiązywania tych problemów,
- jasnym formułowaniu celów strategicznych dla wszystkich obszarów funkcjonalnych,
- analizowaniu możliwości własnego pionu lub sekcji na tle organizacji,
- pozycji firmy w otoczeniu,

- formułowaniu strategii osiągnięcia zamierzonych celów,
- kreowaniu wartości, które są istotne do prawidłowego rozwoju i organizacji firmy [Perechuda 2005, s. 72].

7. Zakończenie

Niewątpliwie poruszone w niniejszym artykule problemy zabezpieczania informacji z dnia na dzień będą zmieniały swój jakościowy charakter. Dzieje się tak na skutek starzenia się stosowanych nie tylko poprzednio, ale także współcześnie technologii. Mówi się bowiem o tym, że obecnie wykorzystywany Internet (czyli tzw. Web 1.0) będzie wypierany przez Web 2.0, nad stworzeniem którego trwają obecnie prace, a nowe możliwości, jakie będzie on oferował, pozwolą na samodzielne kształtowanie dynamicznych strumieni przepływów informacyjnych. Możliwe, że mowa będzie nawet nie o sprzedaży konkretnych produktów w przestrzeni internetowej, ale o „sprzedaży przestrzeni produktowej". W praktyce będzie to oznaczało, że np. firma turystyczna nie będzie oferowała klientowi kompletnie skomponowanego produktu, ale będzie dawała możliwość w pełni samodzielnego kreowania wycieczki, dostosowanej do dalece zaawansowanej, zindywidualizowanej potrzeby klienta, co będzie rodziło konieczność nowego spojrzenia na zarządzanie informacją oraz kwestię jej bezpieczeństwa w organizacji.

Warto też wspomnieć, że trwająca od lat walka o informacje w Internecie powoduje coraz większe straty finansowe w wyniku ataków na systemy informatyczne, dokonywanych przez wspomniany kanał informacyjny. Przykładowo głośne ataki blokujące dostęp do serwerów giełdowych spółek internetowych w USA w lutym 2000 r. przyniosły 1,5 mld USD strat, a popularny wirus „I love you" rozsyłany w maju 2000 r. blisko 10 mld. Te i inne niepokojące wiadomości dobitnie wskazują na aktualność problemu zabezpieczania systemów informatycznych przed atakami odbywającymi się na trzech poziomach: personalnym (walka o dane osobowe, wykorzystanie słabości zasobów ludzkich, co w najbliższej przyszłości ukierunkuje zarządzanie bezpieczeństwem informacji na problem bezpieczeństwa osobowego jako jednego z obszarów materializowania się ryzyk operacyjnych), korporacyjnym (pozyskiwanie danych firmowych) czy globalnym (określana jako cyberterroryzm) [Byczkowski 2005].

Literatura

Byczkowski M., *Konieczność i obowiązek wdrożenia polityki bezpieczeństwa informacji w organizacji*. materiały udostępnione przez autora drogą elektroniczną.

Metodyka ENSI Total Information Security Management ver. 1.4.1 , Warszawa 26.01.2004.

Perechuda K., *Zarządzanie wiedzą w przedsiębiorstwie*, Wydawnictwo Naukowe PWN, Warszawa 2005.

PN – I – 0799-2:2005 Systemy zarządzania bezpieczeństwem informacji, cz. 2. Specyfikacja i wytyczne do stosowania.
PN – ISO/IEC 17799:2003 Technika informatyczna, praktyczne zasady zarządzania bezpieczeństwem informacji.
Rochala T., *Społeczeństwo informacyjne: znaczenie informacji jako infrastruktury rozwoju*, [w:] M. Moszkowicz (red.), *Tożsamość i strategia przedsiębiorstwa – modele i doświadczenia*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 1997.
Tapscott D., *Gospodarka cyfrowa. Nadzieje i niepokoje Ery Świadomości Systemowej*, Wydawnictwo Business Press, Warszawa 1998.

SYSTEM APPROACH IN THE INFORMATION PROTECTION

Summary

In this article the authors show the actual problems of the management of information protection in the space of virtual relations. In this field authors present such important issues as:
- necessity of implementation of the information security,
- trial of the information protection,
- treatment connected with the information protection,
- system treatment to the information protection,
- factors which condition the efficiency of information protection management system.

Dr Aleksander Binsztok jest adiunktem w Katedrze Zarządzania Informacją i Wiedzą Akademii Ekonomicznej we Wrocławiu oraz adiunktem w Katedrze Komunikacji i Zarządzania w Sporcie Akademii Wychowania Fizycznego we Wrocławiu; e-mail: aleksander.binsztok@ae.wroc.pl tel. (071) 3680 323 lub (0602) 717 555.
Mgr inż. Tomasz Radziszewski jest wykładowcą studiów podyplomowych realizowanych przez Wrocławskie Centrum Transferu Technologii Politechniki Wrocławskiej, prowadząc wykłady dotyczące bezpieczeństwa informacji, członek Komisji bezpieczeństwa biznesu w Krajowej Izbie Gospodarczej, praktyk zarządzania bezpieczeństwem informacji, audytor Systemów Zarządzania Bezpieczeństwem Informacji. Współzałożyciel firmy doradczej specjalizującej się we wdrażaniu SZBI; e-mail: t.radziszewski@sisfactor.com.pl tel. (0509) 202 997.