

BEZPIECZEŃSTWO INFORMACYJNE INFRASTRUKTURY KRYTYCZNEJ. SPOJRZENIE NIECO PRZEKORNE.

W cywilizacji ludzkiej informacja zawsze odgrywała kluczową rolę. Posiadanie prawdziwej i aktualnej informacji, było i jest nadal, podstawą działalności organów administracji państwowej, samorządowej, organizacji gospodarczych. Tylko w oparciu o prawdziwą, istotną, dokładną i aktualną informację, mogą one podejmować właściwe decyzje. Szczególną rolę mają tu decyzje podejmowane w sytuacji kryzysowej, która zgodnie z rodowodem słowa kryzys [gr. krino] oznacza ostateczne, nieodwołalne rozstrzygnięcie, nie dopuszczające żadnej rewizji: sukces lub klęska.

TYTUŁEM WPROWADZENIA

Poniższym artykułem chciałbym podzielić się moim nieco przekornym spojrzeniem na problematykę **bezpieczeństwa informacyjnego infrastruktury krytycznej**, jako głównego elementu **zarządzania kryzysowego** określonego w ustawie¹. Nie będzie to więc próba ukazania gotowych rozwiązań organizacyjno-technicznych mających na celu zapewnienie odpowiedniego poziomu bezpieczeństwa informacyjnego elementów infrastruktury krytycznej państwa. Postaram się jednak, w miarę syntetycznie, zaprezentować podstawowe wyznaczniki determinujące ten proces, takie jak: **bezpieczeństwo obywateli jako cel nadrzędny zarządzania kryzysowego, pojęcie i atrybuty informacji, społeczeństwo informacyjne**. To właśnie w tym podejściu kryje się tytułowa *przekorność*, oznaczająca przesunięcie na dalszy (kolejny) plan, wskazywanej często, jako najważniejszej konieczności zapewnienia poufności zasobom informacyjnym infrastruktury krytycznej, w sytuacji gdy najczęściej to **dostępność** (często oznaczająca jej jawność) **informacji staje się kluczem do rozwiązania sytuacji kryzysowej**. Należy tu także pamiętać, że **bezpieczeństwo informacyjne to pojęcie znacznie szersze od błędnie stosowanego zamiennie pojęcia ochrony informacji**. By jednak nie zostać posądzonym o skrajny subiektywizm, na poparcie swoich założeń przedstawię opinie zgłaszane przez przedstawicieli przedmiotu.

Wszystkie te rozważania należy jednak, dla poprawności wyводу, poprzedzić wskazaniem podstawowych pojęć wynikających z ustawy. Tak więc:

¹ Ustawa z dn. 26.04.2007r. o zarządzaniu kryzysowym (Dz.U. nr 89, poz. 590 z późn. zm.)

- **zarządzanie kryzysowe** to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, które polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwania ich skutków oraz odtwarzania zasobów i infrastruktury krytycznej;
- **sytuacja kryzysowa** to sytuacja wpływająca negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołująca znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków;

a wreszcie,

- **infrastruktura krytyczna** to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Obejmuje ona systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych;
- **ochrona infrastruktury krytycznej** to wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających ich prawidłowe funkcjonowanie.

Nie chciałbym jednak odnosić się do treści przedstawionych pojęć, bo nie to jest przedmiotem, głównym celem, mojego artykułu, niemniej muszę podzielić się uwagą zgłaszaną wielokrotnie przez badaczy i ekspertów problemów bezpieczeństwa państwa. A mianowicie, twórcy ustawy o zarządzaniu kryzysowym pominęli kluczowy determinant prawidłowego funkcjonowania państwa, a mianowicie fakt, że **w gospodarce rynkowej infrastruktura krytyczna w większości pozostaje w rękach prywatnych**. Fakt ten powinien znaleźć odzwierciedlenie w procedurach współpracy pomiędzy administracją państwową, a gestorami poszczególnych części infrastruktury, a w przypadku bezpieczeństwa informacyjnego, problemy asymetrii technologicznej pomiędzy tymi grupami organizacji. **Brak jest jednak pełnego zrozumienia dla idei partnerstwa publiczno-prywatnego w**

realizacji zadań bezpieczeństwa państwa, i to nie tylko w zapisach ustawowych, ale przede wszystkim w działaniach na jego rzecz².

BEZPIECZEŃSTWO OBYWATELI – CEL NADRZĘDNY

Obecna **sytuacja geopolityczna, ekonomiczna i światopoglądowa poddaje bardzo mocnej redefinicji pojęcie państwa, jego atrybutów i obowiązków**, w szczególności dotyczy to roli jednostki i grup społecznych znajdujących się w obrębie jego terytorium. A więc tym samym **kwestie zewnętrzne ustępują pola zadaniom wewnętrznym**.

Jedną z podstawowych funkcji państwa jest **zapewnienie warunków bezpiecznego, trwałego i zrównoważonego rozwoju**³. Niemniej jednak, wbrew nadmiernie często wyrażanej filozofii pierwszeństwa ochrony interesów państwa nad interesami jednostki i społeczeństwa, musimy pamiętać, że jego **bytem substancjonalnym są osoby ludzkie, których zjednoczenie się w społeczność państwową podyktowane było wspólnym celem – potrzebą bezpieczeństwa**. W podobnym tonie określa to **prof. Ryszard JAKUBCZAK**, twierdząc, że ***zapewnienie trwałego bezpieczeństwa życia każdej osoby, społeczności lokalnych i całego narodu jest największą potrzebą i wartością ludzką, stanowiąc zarazem fundamentalny cel państwa jako najważniejszej formy organizacji życia narodowego***⁴.

Na tym podłożu **prof. Marek LISIECKI** wskazał **podstawowe założenia bezpieczeństwa państwa**:

- **niezagrożone terytorium** (oczywiście to zamieszkane przez obywateli);
- **obywatele będą odczuwali bezpieczeństwo, poprzez zapewnienie ich bytu i rozwoju oraz zagwarantowanie ich praw i wolności**;
- **władze będą funkcjonowały zgodnie z normami konstytucyjnymi oraz w interesie swoich obywateli: suwerennie, sprawnie i skutecznie**.⁵

Oczywiście wszystkie te założenia muszą występować razem.

Odnosząc powyższe bezpośrednio do problematyki zarządzania kryzysowego należy jednoznacznie wskazać, że **wszelkie działania administracji publicznej mające na celu**

² por.: ŚWIEBODA H., SIENKIEWICZ P.: *Bezpieczeństwo informacyjnej infrastruktury państwa*, (w:) M. GRZYBOWSKI, J. TOMASZEWSKI (red.): *Bezpieczeństwo w administracji i biznesie*, Gdynia: WSAiB, 2007

³ SIENKIEWICZ P.: *Bezpieczeństwo informacji – wspólne dobro dla racji stanu, bezpieczeństwa i obronności kraju, firm i obywateli*, (w:) M. CIECIERSKI (red.): *Ochrona informacji niejawnych i biznesowych. Materiały IV Kongresu*, Katowice: KSOIN – UŚ, 2008, s. 15

⁴ za: BĄCZEK P.: *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń: Wydawnictwo Adam Marszałek, 2006, s. 13

⁵ LISIECKI M., KWIATKOWSKA – BASAŁAJ B.: *Pojęcie bezpieczeństwa oraz prognostyczny model jego zapewnienia*, (w:) *Zarządzanie bezpieczeństwem*, Kraków: PSB, 2000, s. 57

ochronę infrastruktury krytycznej państwa jako cel nadrzędny powinny stawiać sobie aspekt ludzki. Dlatego też ochrona jakiegokolwiek z elementów infrastruktury krytycznej musi być podyktowana uprzednio ujawnionymi, jasno określonymi i wyartykułowanymi potrzebami obywatelskimi przez niego spełnianymi.

INFORMACJA – POJĘCIE, ATRYBUTY

Nie możemy podejmować rozważań na temat bezpieczeństwa informacyjnego infrastruktury krytycznej, jego założeń, czy gotowych rozwiązań, nie mając świadomości co do przedmiotu ochrony. By poprawnie stworzyć system należy mieć wiedzę na temat jego kluczowego elementu, a w tym przypadku niematerialnego, niepoliczalnego, o niejednoznacznych definicjach. Nauki ścisłe silnie akcentują jej **niematerialny charakter**, informatyka przyjmuje, że **wiadomość niesie informacje gdy usuwa niepewność**, stwierdzając, że **każda informacja to wiadomość, ale nie każda wiadomość to informacja**, a jeszcze inna na gruncie nauk humanistycznych, filozofii i prawa, które wskazują na jej **ludzki charakter**.

Rozpoczynając od analizy słownikowej dowiadujemy się, że wyrażenie **informacja** wywodzi się od łacińskiego zwrotu **informatio**, oznaczającego: **powiadomienie, zakomunikowanie, wiadomość, pouczenie**. Natomiast **Encyklopedia powszechna** przedstawia **informację** jako **obiekt abstrakcyjny, który w postaci zakodowanej** (tzw. danych) **może być przechowywany** (na nośniku), **przesyłany** (np. dzięki wykorzystaniu głosu, fali elektromagnetycznej), **przetwarzany** (w trakcie wykonywania) **i użyty do sterowania**.

W ujęciu kognitywistycznym (nauki o poznaniu), a więc bardzo bliskim działalności człowieka **informacja jest tym co umysł jest w stanie stworzyć lub przetworzyć, a następnie wykorzystać do własnych celów, zmniejszając poczucie niepewności**. A tym samym dając już poczucie bezpieczeństwa.

W odniesieniu do zagadnień zarządzania na uwagę zasługuje definicja sformułowana przez **prof. Leszka F. KORZENIOWSKIEGO**, który stwierdza, że **informacja jest to treść przekazywana przez komunikat, umożliwiająca zrozumienie sensu (znaczenia) danych i relacji między nimi**⁶.

Na koniec tych krótkich rozważań nie można pominąć bardzo ważnego dla poprawnego rozumienia pojęcia informacji problemu związanego z terminem „dane”. **Dane są to surowe nie poddane analizie liczby i fakty dotyczące zjawisk lub wydarzeń**. Natomiast **informacja jest wynikiem uporządkowania danych lub ich przeanalizowania w znaczący sposób**. Jak więc widać są to pojęcia na zupełnie różnych poziomach, nie mogą więc być

⁶ KORZENIOWSKI L.F.: *Securitologia* ..., s.126

wykorzystywane zamiennie jako synonimy. Pamiętać o tym należy w szczególności w sytuacjach kryzysowych, gdy **podejmowane przez organy administracji państwowej decyzje mające bardzo często charakter rozstrzygający o żywotnych interesach, nie mogą być jedynie zestawieniem danych, a właśnie rzeczowo uporządkowanym wynikiem ich gruntownej analizy.**

Klasyfikacja informacji jest równie bardzo złożona jak samo pojęcie. Można wyróżnić bardzo wiele kryteriów podziału w zależności od rodzaju informacji i jej wykorzystania. Wydaje się jednak, że **najważniejszą cechą informacji jest jej jakość**, przez którą należy rozumieć **ogół właściwości wiążących się ze zdolnością zaspokojenia stwierdzonych lub przewidywanych potrzeb użytkownika informacji**⁷. Jej poziom określany jest poprzez atrybuty:

- **aktualność** – adekwatność do stanu rzeczywistego w czasie;
- **integralność** – brak nieautoryzowanej zmiany lub zniszczenia;
- **rozliczalność** – przypisanie działania w sposób jednoznaczny określonej podmiotowi;
- **dokładność** – szczegółowość, zawartość danych istotnych do prawidłowego wnioskowania;
- **rzetelność** – staranność, obiektywność, poprawność merytoryczna danych i komunikatu;
- **użyteczność** – stopień przydatności do osiągnięcia założonych celów;
- **wartość** – odwrotność prawdopodobieństwa.

Dopiero spełnienie powyższych warunków daje podstawy do zapewnienia informacji zasad **poufności**, oczywiście jeżeli istnieje taka konieczność wynikająca z potrzeb zarządzania. Nie ma sensu utrzymywanie w tajemnicy informacji, które nie są aktualne, rzetelne czy użyteczne, a tym samym ich wartość dla procesu kierowania (zarządzania) jest wątpliwa.

Podsumowując można posłużyć się sentencją wygłoszoną przez **Antoniego SŁONIMSKIEGO** – ***Lepszy jest brak informacji od złych informacji***⁸. Choć pewnie autor pod pojęciem *zła informacja* rozumiał nie jej wartość, a raczej przenoszony komunikat.

⁷ KORZENIOWSKI L.F.: *Securitologia* ... , s. 131

⁸ Cytat za: LIEDERMAN K.: *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa: Wydawnictwo Naukowe PWN, 2008, s. 7

SPOŁECZEŃSTWO INFORMACYJNE

*Życ i działać we współczesnym świecie to znaczy korzystać z informacji*⁹ – to stwierdzenie **prof. Piotra SIENKIEWICZA** wydaje się trafnie opisywać współczesną cywilizację, istotę przeobrażeń społecznych, kulturowych, politycznych i edukacyjnych. Wytwarzanie, przetwarzanie, gromadzenie i przekazywanie informacji stało się istotnym przedmiotem działalności dla dużej części społeczeństw. Głównym jednak **procesem determinującym rozwój społeczeństwa informacyjnego nie jest sam fakt posiadania informacji, lecz przede wszystkim niesłabnący rozwój technologii informatycznych**. Pozwalają one na likwidację ograniczeń w dostępie do informacji, narzucanych przez czas i odległość. Na tej podstawie trafna definicję stworzył **prof. Tomasz GOBAN-KLAS** stwierdzając, że *społeczeństwo staje się społeczeństwem informacyjnym wtedy, kiedy jego stopień rozwoju oraz skala skomplikowania procesów społecznych i gospodarczych wymagają zastosowania nowoczesnych technik gromadzenia, przetwarzania, przekazywania i użytkowania olbrzymiej ilości informacji*¹⁰.

A w związku z powyższym trudno nie zgodzić się z **Piotrem BĄCZKIEM**, który wskazuje, że *dla współczesnego społeczeństwa, informacja, jako podstawa systemu wiedzy, staje się istotnym elementem warunkującym sukces, w każdej ze sfer działalności człowieka: społecznej, kulturowo-religijnej, zarządzania, gospodarki, polityki, bezpieczeństwa narodowego i obronności czy kontaktów międzynarodowych*. By następnie stwierdzić, że *każdy system społeczno-ekonomiczny potrzebuje do normalnego funkcjonowania określonego zasobu informacji*.¹¹

Pamiętać jednak należy, że uzależnienie jednostek, grup społecznych i całych społeczeństw od informacji i technologii informacyjnych i podporządkowanie im wszelkich sfer życia i działalności spowodowało pojawienie się nowych obszarów zagrożeń, a także kumulacja i transformacji już istniejących.

BEZPIECZEŃSTWO INFORMACYJNE

Najkrócej określić można, że **bezpieczeństwo informacji jest próbą stworzenia takiego systemu by poprawnie i w całości realizował cele i zadania zgodne z intencjami właściciela**. W praktyce należy je traktować jako **ciągły proces** (działanie) **zmierzające do ograniczenia ryzyka lub prawdopodobieństwa wystąpienia szkody w obrębie chronionych**

⁹ SIENKIEWICZ P.: *Bezpieczeństwo informacji ...*, s. 16

¹⁰ GOBAN-KLAS T., SIENKIEWICZ P.: *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków: Fundacja Postępu Telekomunikacji, 1999, s. 33

¹¹ BĄCZEK P.: *op.cit.*, s. 49

zasobów informacyjnych lub otoczenia informacyjnego, obejmujący wszystkie jego cechy. W procesie tym, jak słusznie twierdzi **Piotr BĄCZEK**, należy uwzględnić ***szeroki zakres dziedzin życia mogących generować różnego typu zagrożenia, posiadających własną specyfikę i mogących oddzielnie wpływać na zasoby informacyjne***. Do tych dziedzin zalicza on między innymi sfery: ***społeczną, etyczną, kulturową, naukową, gospodarczą, polityczną, militarną czy stosunków międzynarodowych***¹².

Natomiast **prof. Piotr SIENKIEWICZ** wskazuje na konieczność odniesienia bezpieczeństwa informacyjnego do następujących obszarów:

- ***bezpieczeństwa zasobów informacji;***
- ***cyberbezpieczeństwa;***
- ***teleinformatyki;***
- ***polityki bezpieczeństwa informacyjnego państwa;***
- ***praw obywatelskich;***
- ***doktryny walki (wojny) informacyjnej.***¹³

Wobec powyższych rozważań można usiłować stworzyć założenia bezpieczeństwa informacyjnego państwa, stanowiącego stan wewnętrzny i zewnętrzny, w którym:

- **władze podejmują decyzje mające zapewnić spełnienie potrzeb społecznych w oparciu o dobre jakościowo informacje;**
- **przepływ i dostęp do informacji nie jest zakłócony;**
- **bezpieczeństwo społeczeństwa informacyjnego ma oparcie w prawie;**
- **respektowane jest prawo do prywatności.**

W tym momencie nie sposób nie wskazać przykładu Federacji Rosyjskiej, która w doktrynie bezpieczeństwa informacyjnego wyróżnia cztery grupy interesów narodowych w sferze informacyjnej:

- **realizacja konstytucyjnych praw obywatelskich w zakresie dostępu i korzystania z informacji;**
- **informacyjne wsparcie wewnętrznej i zewnętrznej polityki państwa, przy pomocy środków masowego przekazu;**
- **rozwój rodzimych nowoczesnych technologii informacyjnych;**
- **ochrona narodowych systemów i zasobów informacyjnych.**¹⁴

¹² BĄCZEK P.: *op. cit.*, s. 75-76

¹³ SIENKIEWICZ P.: *Bezpieczeństwo informacji ...*, s. 24

Oczywiście pomijając respektowanie w praktyce praw obywatelskich, na szczególną uwagę zasługuje fakt silnego akcentowania znaczenia praw obywatelskich, otoczenia informacyjnego i nowoczesnych technologii dla bezpieczeństwa państwa.

TYTUŁEM PODSUMOWANIA

Mając powyższe wywody na względzie dochodzimy do następujących konkluzji, będących jednocześnie wyzwaniem dla bezpieczeństwa informacyjnego infrastruktury krytycznej państwa:

- **otoczenie informacyjne ma charakter strategiczny**, jest głównym czynnikiem rozwoju cywilizacyjnego i gospodarczego;
- każda **dojrzała organizacja państwowa**, dla swojego bezpieczeństwa, **potrzebuje środków utrwalania ciągłości i przeciwdziałania zawodności ludzkiej pamięci**;
- **powstała cyberprzestrzeń, nieskrępowana czasem i odległością, której granice wyznacza jedynie aktualny poziom rozwoju techniki informatycznej**;
- sieci telekomunikacyjne powodują **wielopoziomowe interakcje pomiędzy organizacjami, wymuszając ich współzależność**;
- **zagrożenia informacyjne mogą się kumulować i działać synergicznie, jednocześnie na wiele elementów systemu informacyjnego** (zdarzenia kaskadowe);
- **w świetle globalizacji zagrożenia informacyjne są ponadpaństwowe**;

Ponadto analizując znaczenie informacji bezpośrednio w sytuacji kryzysowej musimy mieć na uwadze następujące jej cechy:

- **czas podejmowania decyzji – bardzo krótki**;
- **stopień przewidywalności – bardzo niski** (zaskoczenie);
- **stopień ryzyka – bardzo wysoki**;
- **niepewność – bardzo duża** (strach).¹⁵

Informacja ma wartość tylko wtedy, kiedy właściwa osoba otrzymuje ją w odpowiednim czasie¹⁶ - te słowa francuskiego eksperta ds. bezpieczeństwa informacyjnego

¹⁴ za: KOZIEJ S.: *Globalne aspekty rosyjskiej strategii bezpieczeństwa*, Zeszyty Naukowe AON, nr 1, 2003

¹⁵ SIENKIEWICZ P.: *Zarządzanie bezpieczeństwem systemów*, (w:) M. GRZYBOWSKI, J. TOMASZEWSKI (red.): *Bezpieczeństwo w administracji i biznesie*, Gdynia: WSAiB, 2007, s. 34

generała Kristen’a GUYAUX, wydają się doskonale odzwierciedlać potrzeby zarządzania kryzysowego, gdzie doświadczenia przeszłości jasno wskazują na **dostępność dobrej jakościowo informacji, jako klucz do podjęcia właściwej decyzji**. To czas jest głównym determinantem działań w sytuacji wystąpienia nagłych, nieprzewidzianych i gwałtownych sytuacji zagrożeń, wyznaczając wymogi bezpieczeństwa informacyjnego infrastruktury krytycznej państwa.

Kończąc mam nadzieję, że swoim artykułem wywołam zamierzoną dyskusję nad problemami informacyjnego bezpieczeństwa państwa, a przede wszystkim nad ignorowanymi i niedocenianymi zagrożeniami i wyzwaniem cywilizacyjnymi społeczeństwa informacyjnego XXI wieku.

LITERATURA:

1. BĄCZEK P.: *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń: Wydawnictwo Adam Marszałek, 2006
2. GOBAN-KLAS T., SIENKIEWICZ P.: *Spółeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków: Fundacja Postępu Telekomunikacji, 1999
3. JASENOVEC J.: *Kritická infraštruktúra v kontexte bezpečnosti*, (w:) HOFREITER L. (red.): *Bezpečnosť a bezpečnostná veda*, Liptovský Mikuláš – Liptovský Ján: AOS, 2009
4. KORZENIOWSKI L.F.: *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, Kraków: EAS, 2008
5. LIEDEL K.: *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń: Wydawnictwo Adam Marszałek, 2005
6. LISIECKI M., KWIATKOWSKA – BASAŁAJ B.: *Pojęcie bezpieczeństwa oraz prognostyczny model jego zapewnienia*, (w:) *Zarządzanie bezpieczeństwem*, Kraków: PSB, 2000
7. REITŠPIS J.: *Manažerstvo bezpečnostných rizik*, Žilina: ŽU, 2004
8. SIENKIEWICZ P.: *Bezpieczeństwo informacji – wspólne dobro dla racji stanu, bezpieczeństwa i obronności kraju, firm i obywateli*, (w:) M. CIECIERSKI (red.): *Ochrona informacji niejawnych i biznesowych. Materiały IV Kongresu*, Katowice: KSOIN – UŚ, 2008
9. SIENKIEWICZ P.: *Zarządzanie bezpieczeństwem systemów*, (w:) M. GRZYBOWSKI, J. TOMASZEWSKI (red.): *Bezpieczeństwo w administracji i biznesie*, Gdynia: WSAiB, 2007
10. SLOBODA A., FERENČÍKOVÁ A.: *Analyza ohrozenia a ochrana kritickéj infraštruktúry*, *Securitologia/Securitology/Секюритология*. Zeszyty Naukowe EAS 2009, nr 9
11. ŚWIEBODA H., SIENKIEWICZ P.: *Bezpieczeństwo informacyjnej infrastruktury państwa*, (w:) M. GRZYBOWSKI, J. TOMASZEWSKI (red.): *Bezpieczeństwo w administracji i biznesie*, Gdynia: WSAiB, 2007

¹⁶ za: MARTINET B., MARTI Y.M.: *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji*, Warszawa: PWE, 1999, s. 105