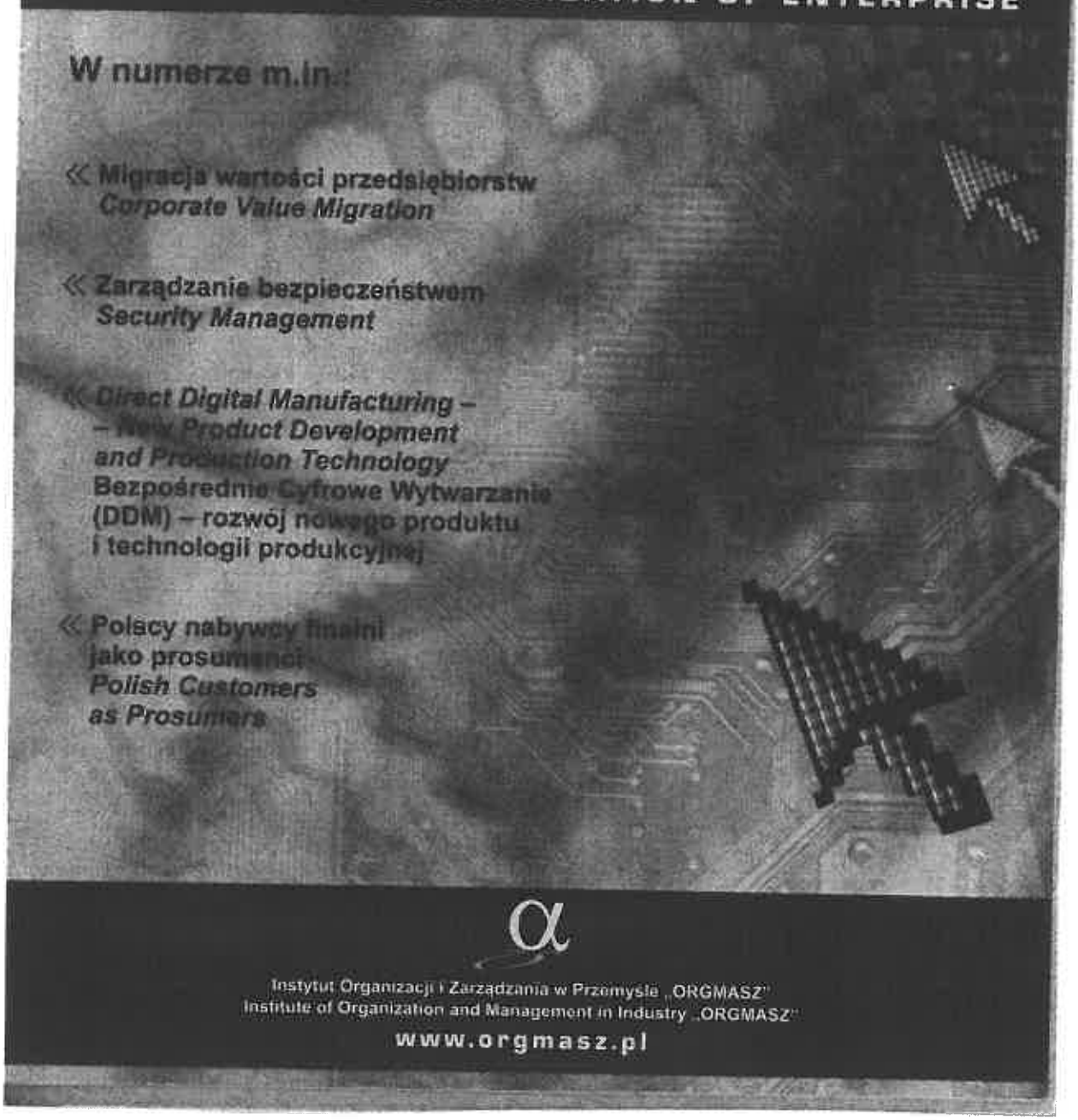
Indeks 357022 Cena 23,50 zł (VAT 0%) PL ISSN 0860-6846

EKONOMIKA I ORGANIZACJA PRZEDSIĘBIORSTWA

NR 10 (705) PAŹDZIERNIK 2008

ECONOMICS AND ORGANIZATION OF ENTERPRISE



Instytut Organizacji i Zarządzania w Przemyśle „ORGMASZ"
Institute of Organization and Management in Industry „ORGMASZ"
www.orgmasz.pl

■ **Wydawca/Publisher**

Instytut Organizacji i Zarządzania w Przemyśle „ORGMASZ"
00–879 Warszawa, ul. Żelazna 87
tel. centr. +48 22 654 60 61
www.orgmasz.pl

■ **Adres redakcji/Address of editors**
Instytut Organizacji i Zarządzania w Przemyśle „ORGMASZ"
00–879 Warszawa, ul. Żelazna 87
tel. centr. +48 22 654 60 61, fax +48 22 620 43 60
e-mail: eiop@orgmasz.pl

Wszystkie artykuły zamieszczone w czasopiśmie są recenzowane.
All articles published in the monthly are subject to reviews.

Publikacja naukowa zamieszczona w EiOP – 6 punktów.

Nakład: 950 egz.

Redakcja, korekta, projekt i skład
Wydawnictwo Urbański
87–100 Toruń
ul. Tłoczka 4/13
tel./fax +48 56 652 86 11

Druk
P.W. FORMATOR Sp. z o. o.
87-100 Toruń, ul. Grudziądzka 163
tel. +48 56 652 72 18; fax +48 56 652 72 19

Spis treści Contents

Zarządzanie bezpieczeństwem

Leszek J. Buller*

Minęło już kilka lat od ataku terrorystycznego na Nowy Jork z 11-ego września 2001 roku. Wydarzenie to skierowało uwagę całego świata na aspekt bezpieczeństwa – bezpieczeństwa państwowego, publicznego, osobistego oraz bezpieczeństwa prowadzenia działalności gospodarczej. W każdym z tych obszarów dotychczasowe standardy zostały obalone. I tak stało się w Stanach Zjednoczonych – w państwie, które pod każdym względem, także pod względem bezpieczeństwa, należy do światowej czołówki.

W Polsce pojęcie „bezpieczeństwo" kojarzone jest przede wszystkim z bezpieczeństwem osobistym lub narodowym. Bezpieczeństwo organizacji sprowadza się w praktyce do ochrony mienia i osób oraz zabezpieczeń elektronicznych. Inne elementy bezpieczeństwa działalności gospodarczej są lekceważone jako przesadne lub zaniedbywane ze względu na koszty. Nic bardziej mylnego! Każdy błąd w ocenie zagrożeń może doprowadzić nawet do utraty całego dorobku organizacji, jej pracowników, zarządu i właścicieli. Zagrożeniem może być konkurent, który umieścił podsłuch w sali zebrań kierownictwa organizacji, lub pracownik, który nie czując się doceniany, bardziej niż swą lojalność będzie cenił pieniądze. Niebezpieczeństwo może stanowić związanie się z bankiem, który prowadzi ryzykowną działalność inwestycyjną, lub przedpłata dla kooperanta, stojącego u progu bankructwa. Brak przeszkolenia personelu i korzystanie z usług niesprawdzonych firm może na przykład skutkować kłopotliwymi artykułami w czasopismach i rozgłosem w innych mediach elektronicznych, tym samym niwecząc długo przygotowywaną transakcję. Do tego dochodzą jeszcze: włamania komputerowe hakerów, zwykła kradzież, napad rabunkowy czy szantaż. Jak zatem zminimalizować istniejące ryzyko?

Zintegrowany system zarządzania bezpieczeństwem organizacji to kompleksowe podejście do zagadnień bezpieczeństwa, oparte na przekonaniu, że bezpieczeństwo jest tak samo ważnym czynnikiem dla sukcesu organizacji, jak profesjonalna kadra menedżerska, stabilna sytuacja finansowa i silna pozycja rynkowa. Jednym z fundamentów budowy „nowych struktur" w zakresie bezpieczeństwa (na przykład: ochrony tajemnicy państwowej, służbowej, handlowej i innej chronionej przepisami) jest przyjęcie obowiązującej w krajach Unii Europejskiej zasady *need to know*[1], zgodnie z którą dostęp do informacji ważnych i chronionych można uzyskać w takim zakresie, jaki jest niezbędny

* dr Leszek J. Buller – Wydział Zamiejscowy Nauk o Społeczeństwie KUL w Stalowej Woli; Kierownik Instytutu Organizacji i Zarządzania w Przemyślu ORGMASZ

[1] Standardy bezpieczeństwa i ochrony informacji w NATO (Materiał informacyjny), Warszawa, luty 1998, s. 2.

do wykonywania zadań. Strategia organizacji powinna określać priorytety oraz wskazywać słabe punkty w systemie kompleksowej ochrony organizacji.

Wstąpienie Polski do struktur NATO spowodowało dostosowanie przepisów prawnych dotyczących ochrony informacji niejawnych do wymogów określanych w terminologii NATO jako minimalne standardy bezpieczeństwa[2]. Standardy te regulują we wszystkich państwach członkowskich szczegółowe kwestie związane z szeroko rozumianą problematyką bezpieczeństwa nie tylko państwowego, ale i bezpieczeństwa w innych dziedzinach życia społecznego i gospodarczego. W państwach członkowskich NATO i należących do Unii Europejskiej mechanizmy ochrony informacji i bezpieczeństwa organizacji koncentrują się na rozbudowanych procedurach i czynnościach profilaktycznych oraz sprawdzeniowych, a nie – jak było w krajach byłego Układu Warszawskiego – rozbudowanej represji za naruszenie przepisów obejmujących wszystkie sfery życia społecznego i gospodarczego.

Standardy bezpieczeństwa złożone z szeregu czynności i procedur stanowią o funkcjonalności systemu, a jego zdolność do osiągania zamierzonych celów jest podstawowym kryterium oceny.

■ Bezpieczeństwo osobowe

Bezpieczeństwo osobowe rozumiane jest jako system czynności zmierzających do wszczęcia procedur w dwóch aspektach: badania odpowiedzialności, gdzie sprawdza się, czy osoba nie była karana; kwalifikacje zawodowe, stosunek do pracy, kontakty zawodowe oraz kondycję finansową, oraz badania lojalności – jako drugi etap procedury – weryfikowane są cechy charakteru i osobowości kandydata oraz sytuacje, które mogłyby spowodować nielojalne zachowanie i zagrożenie bezpieczeństwa (wyklucza się narkomanię, alkoholizm, dewiacje seksualne, negatywne cechy charakteru, choroby psychiczne itp.).

Warto tutaj zwrócić uwagę na wnioski płynące z badań ewaluacyjnych prowadzonych w ramach Pracowni Bezpieczeństwa Biznesu Instytutu Organizacji i Zarządzania w Przemyśle „ORGMASZ" wśród uczestników studiów podyplomowych. Wynika z nich, że ważność problematyki bezpieczeństwa lepiej rozumieją przedstawiciele administracji rządowej. W innych sektorach rzeczywistości społecznej i gospodarczej zagadnienia bezpieczeństwa nie odgrywają takiej roli. Sfera bezpieczeństwa zdominowana jest przez mężczyzn, chociaż coraz częściej zainteresowanie bezpieczeństwem wykazują kobiety. Zdecydowana większość osób zajmujących się problematyką bezpieczeństwa ma już bogate doświadczenia zawodowe i ogromną wiedzę z tego zakresu. Jednakże, ze względu na szybkie zmiany technologiczne, gospodarcze, społeczne i polityczne, istnieje wymóg ciągłego podnoszenia kwalifikacji

[2] Ibidem, s. 1.

i dokształcania się, zatem studia podyplomowe z zakresu zarządzania bezpieczeństwem są potrzebne i przydatne[3].

■ Bezpieczeństwo informacji i dokumentów

Zespół czynności i procedur, jakie musi przejść wytworzenie dokumentu klasyfikowanego (chronionego ze względu na ważne informacje), jego rejestrowanie, przesyłanie, kontrolowanie, archiwizowanie i niszczenie[4].

■ Bezpieczeństwo urządzeń i systemów teleinformatycznych

Kompleks środków bezpieczeństwa stosowanych w telekomunikacji w celu uniemożliwienia przechwycenia informacji z tych systemów przez osoby nieupoważnione, ograniczenia zjawiska ubocznej emisji (tzw. elektromagnetycznej).

Bezpieczeństwo komputerowe rozumiane jest jako stosowanie zabezpieczeń sprzętu, oprogramowania firmowego i użytkowego w systemach komputerowych w celu zapobieżenia ujawnianiu informacji, próbom jej zmiany lub usunięcia.

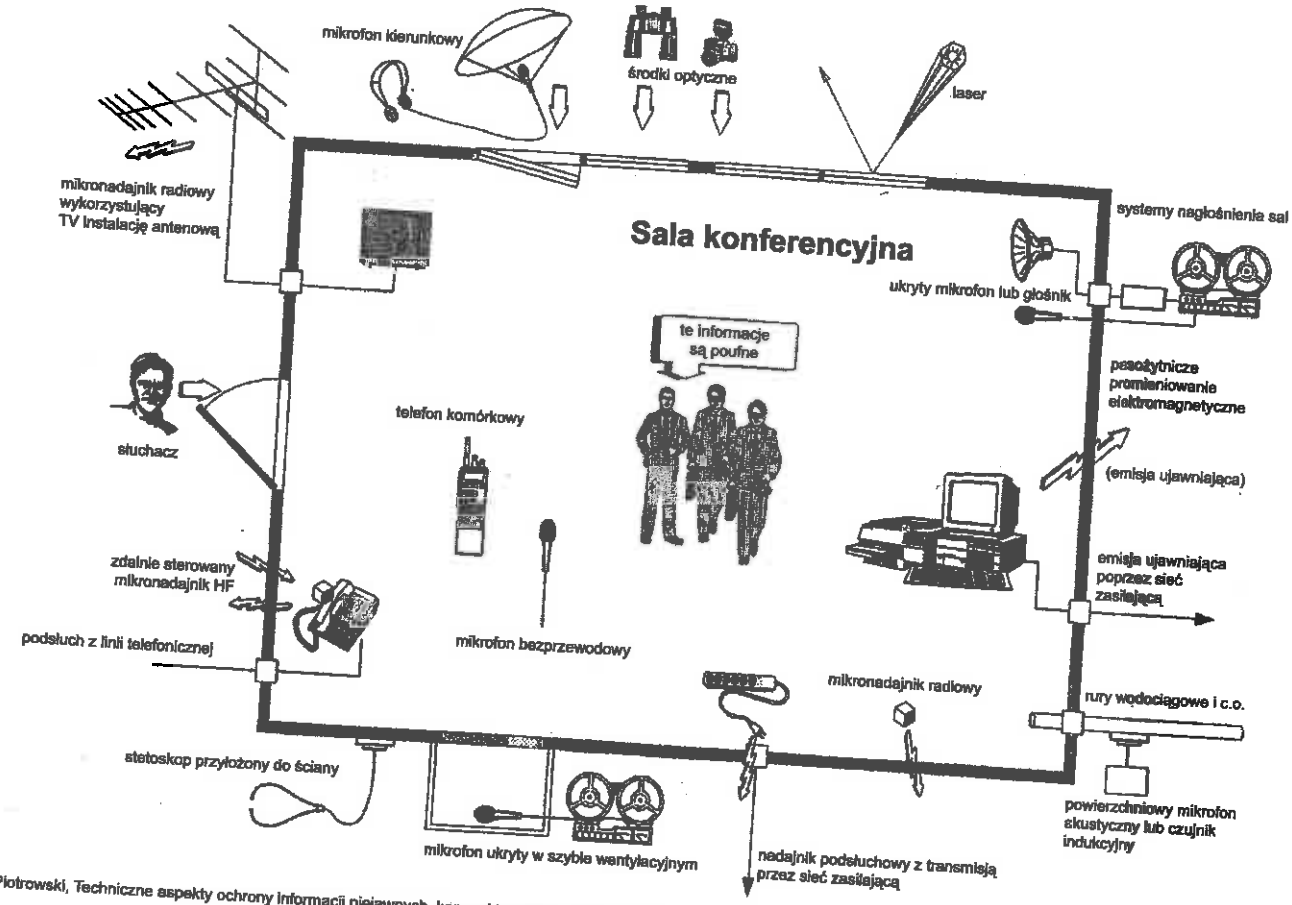
Standardy te szczegółowo opisują warunki funkcjonalne i techniczne urządzeń oraz systemów, a także procedury w zakresie bezpieczeństwa fizycznego (osobowego, obiektowego), emisji (w tym kompatybilność elektromagnetyczna), transmisji i bezpieczeństwa kryptograficznego.

W Polsce w ostatnich latach nastąpił szybki rozwój telefonii komórkowej. Rozwój systemów telefonii ruchomej z jednej strony umożliwił błyskawiczne przekazywanie informacji, z drugiej zaś spowodował specyficzne dla tego medium zagrożenia. Do najważniejszych zagrożeń związanych z użytkowaniem telefonu komórkowego możemy zaliczyć:

1. Możliwość podsłuchiwania przesyłanych informacji (utrata ich poufności) – telefony komórkowe nie są wyposażone w mechanizmy zabezpieczające przekazywane informacje przed możliwością ich przechwycenia i odtworzenia przez osoby dysponujące specjalistycznym sprzętem do monitorowania kanałów radiowych, którymi transmitowane są informacje w systemach telefonii komórkowej.
2. Możliwość określenia miejsca lub obiektu, w którym znajduje się lub przebywa użytkownik telefonu komórkowego – w chwili uruchomienia telefonu komórkowego urządzenia zarządzające systemem mobilnym identyfikują użytkownika telefonu komórkowego, określając między innymi obszar, w którym się znajduje.

[3] L. J. Buller, Przydatność studiów podyplomowych z zakresu zarządzania bezpieczeństwem publicznym w administracji państwowej i samorządowej, referat wygłoszony 25 września 2008 r. w ramach seminarium podsumowującego międzynarodowy projekt badawczy zatytułowany „Analiza badań z obszaru bezpieczeństwa i ich aplikacje do sfery kształcenia specjalistów zarządzania bezpieczeństwem i zarządzania kryzysowego w szkołach wyższych" (MVTS Bil/Pol'/SR/ŽU/06/1) w Katedrze Zarządzania Bezpieczeństwem Wydziału Inżynierii Specjalnej Uniwersytetu w Żylinie na Słowacji.

[4] Ibidem, s. 3.



Źródło: S. Piotrowski, Techniczne aspekty ochrony informacji niejawnych, konspekt wykładu, Warszawa 2003.

3. Możliwość identyfikacji osób, z którymi kontaktuje się korzystający z telefonu komórkowego – urządzenia pracujące w systemach telefonii komórkowej rejestrują dane dotyczące połączeń realizowanych z udziałem użytkownika telefonu komórkowego (tzw. biling).
4. Możliwość zdalnego uruchomienia w telefonach komórkowych funkcji o specjalnym przeznaczeniu – skala integracji układów scalonych oraz powszechne wykorzystywanie mikroprocesorów w sprzęcie elektronicznym pozwala na zaimplementowanie w nich dodatkowych, nieudokumentowanych funkcji. Telefon komórkowy z wbudowanym modułem elektronicznym o specjalnym przeznaczeniu może być na przykład zdalnie zablokowany, uniemożliwiając jego użytkownikowi komunikowanie się z systemem mobilnym. Natomiast przy zastosowaniu mikronadajnika telefon komórkowy może służyć do podsłuchiwania prowadzonych w nim rozmów[5].
5. Możliwość zainstalowania w telefonie komórkowym nadajnika – urządzenie emitujące może znajdować się w baterii telefonu komórkowego, gdyż tam ma stałe źródło zasilania.

■ Bezpieczeństwo fizyczne i techniczne obiektów podlegających ochronie

Wymogi, którym powinny odpowiadać obiekty i pomieszczenia oraz elementy ich wyposażenia (szafy, biurka etc.), w których przechowywane są dokumenty klasyfikowane. Określają one także zasady podziału na strefy obiektów chronionych oraz rozwiązania odnośnie do barier fizycznych i technicznych (np. ogrodzeń), systemów dostępowych, a także procedur funkcjonowania służb ochronnych.

Bezpieczeństwo przemysłowe określa ogólne kierunki sprawdzeń, którym podlega firma-kandydat do wykonywania kontraktu rządowego wiążącego się z dostępem do informacji niejawnych (zgodnie z ustawą o ochronie informacji niejawnych). Współczesne standardy NATO i Unii Europejskiej ustanawiają instytucję „Certyfikatu Bezpieczeństwa Firmy", dopuszczającego ją do realizacji takiego kontraktu. Nadają również instytucji państwowej prawo sformułowania wymogów odnośnie do ochrony, których dopełnić musi ewentualny kontrahent. Podmiot realizujący kontrakt z mocy prawa podlega kontroli oraz ochronie ze strony Krajowej Władzy Bezpieczeństwa.

W większości organizacji krajów Unii Europejskiej istnieją tzw. piony ochrony instytucji[6], do zadań których należy zapewnienie ochrony i bezpieczeństwa całokształtu działalności danej instytucji, w tym zwłaszcza informacji niejawnych, prawidłowości naboru personelu, przestrzegania wewnętrznych i ogólnych norm prawnych oraz ochrona fizyczna i techniczna obiektów. Istnieją one praktycznie we wszystkich instytucjach państwowych i gospodarczych. Obligatoryjnie są tworzone w instytucjach i firmach, w których znajdują się informacje niejawne.

---

[5] *„Ściśle jawne" tajemnice – o czym należy pamiętać, co należy wiedzieć, jak je chronić. Dla pracowników administracji terenowej, przedsiębiorstw, banków, urzędów państwowych oraz firm ubiegających się o świadectwo bezpieczeństwa przemysłowego*, Warszawa 2000, s. 14–16.

[6] Standardy bezpieczeństwa..., s. 4; w mniejszych organizacjach zazwyczaj powoływany jest tzw. oficer bezpieczeństwa.

Bezpieczeństwo wymaga znajomości czułych punktów narażonych na atak przez osoby chcących pozyskać informację poufną, a także podjęcia następujących działań:

1. Za pomocą systemów telefonii (zarówno komórkowej, jak i stacjonarnej), faksów, e-maili nie należy przekazywać informacji stanowiących tajemnicę lub zachowania ich poufności, o ile urządzenia te nie zostały wyposażone w systemy kryptograficzne.
2. Po wejściu do budynków o szczególnie ważnym przeznaczeniu (np. obiekty rządowe, ministerstwa, urzędy centralne) lub w czasie spotkań wymagających zachowania ich poufności (np. negocjacje, rozmowy biznesowe) należy posiadany telefon komórkowy zdeponować w stanie wyłączonym u odpowiednich służb dyżurnych lub pozostawić na przykład w samochodzie.
3. W przypadku zaistnienia okoliczności wymuszających maskowanie miejsca pobytu lub trasy przejazdu w urządzeniu telefonii komórkowej należy wyłączyć zasilanie lub pozostawić je w miejscu pracy albo w domu[7].
4. Należy w firmie wydzielić strefy ograniczonego dostępu, do których wejście powinno być reglamentowane. W każdej firmie winno znajdować się wydzielone, bezpieczne pomieszczenie do prowadzenia poufnych rozmów.
5. Personel sprzątający firmę musi składać się z osób wiarygodnych i mających zaufanie pracodawcy.
6. Należy personel firmy zachęcać do niszczenia projektów poufnych dokumentów w niszczarkach oraz do stosowania zasady „czystych biurek".
7. System informatyczny powinien być w odpowiedni sposób zabezpieczony przed dostępem z zewnątrz, a informacje poufne powinny znajdować się na wydzielonym z sieci (zarówno zewnętrznej – Internet, jak i wewnętrznej – intranet) komputerze.
8. Zalecane jest, aby nie rzadziej niż raz na kwartał poddawać szczegółowemu badaniu antypodsłuchowemu pomieszczenia do prowadzenia poufnych rozmów, gabinety osób decyzyjnych, linie telefonii stacjonarnej, telefony komórkowe, linie energetyczne i samochody.

Wiele wartościowych informacji pozostawionych jest na widoku podczas dnia pracy, a także po godzinach. Korespondencja, instrukcje, terminarze spotkań, tablice naścienne, przypominające o ważnych wydarzeniach, oraz inne materiały pisemne; wszystko to pozostawione jest na widoku. Niektóre z tych informacji mogą być przeczytane lub sfotografowane (na odległość) przez okna.

Szpiegostwu gospodarczemu, wykradaniu informacji niejawnych można jednak skutecznie zapobiegać, wiedza na temat taktyki postępowania „szpiega" jest zaś pierwszym krokiem w kierunku zabezpieczenia własnych interesów.

[7] Por. *„Ściśle jawne"*..., s. 16.

Zintegrowany system zarządzania bezpieczeństwem organizacji to kompleksowe podejście do zagadnień bezpieczeństwa, oparte na przekonaniu, że bezpieczeństwo jest tak samo ważnym czynnikiem dla sukcesu organizacji, jak profesjonalna kadra menedżerska, stabilna sytuacja finansowa i silna pozycja rynkowa. Jednym z fundamentów budowy „nowych struktur" w zakresie bezpieczeństwa jest przyjęcie obowiązującej w krajach Unii Europejskiej zasady *need to know*, zgodnie z którą dostęp do informacji ważnych i chronionych można uzyskać w takim zakresie, jaki jest niezbędny do wykonywania zadań.

Streszczenie

Wstąpienie Polski do struktur NATO spowodowało dostosowanie przepisów prawnych dotyczących ochrony informacji niejawnych do wymogów – określanych w terminologii NATO – jako minimalne standardy bezpieczeństwa. Standardy te regulują we wszystkich państwach członkowskich szczegółowe kwestie związane z szeroko rozumianą problematyką bezpieczeństwa nie tylko państwowego, ale i bezpieczeństwa w innych dziedzinach życia społecznego i gospodarczego.

Summary

Poland's access to NATO structures caused a necessity of adjustment of legal regulations concerning protection of secret information to requirements of NATO minimum security standards. These standards regulate in all member countries detailed issues regarding not only state security, but also problems of social or economic life security.