PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1156 — 2007
Informatyka Ekonomiczna 11

Artur Rot, Iwona Chomiak-Orsa

IMPLEMENTACJA ZABEZPIECZEŃ JAKO ELEMENT ZARZĄDZANIA BEZPIECZEŃSTWEM SYSTEMU INFORMACYJNEGO W PRZEDSIĘBIORSTWIE

1. Wstęp

We współczesnych systemach informacyjnych same zabezpieczenia technologiczne nie są już wystarczające. Należy optymalnie dobierać różnorodne środki i metody zabezpieczeń, właściwie je stosować i odpowiednio nimi zarządzać. Nowoczesne przedsiębiorstwo musi stosować cały zestaw uzupełniających się produktów, procedur oraz odpowiednią politykę, aby chronić się przed zagrożeniami. Zapewnienie bezpieczeństwa systemu informacyjnego powinno być sumą rozwiązań organizacyjnych i technicznych. Ponieważ współczesne systemy informacyjne są często bardzo skomplikowane, heterogeniczne i mają charakter dynamiczny, pojedyncze rozwiązania nie mogą zapewnić pełnej ochrony przed wszystkimi możliwymi zagrożeniami. Dlatego warto stosować kilka odpowiednich rozwiązań, które chronią przed jak największą ich liczbą. W związku z tym bardzo istotnym elementem zarządzania bezpieczeństwem systemu informacyjnego jest właściwa implementacja systemu zabezpieczeń, a przede wszystkim opracowanie i wdrożenie odpowiedniego programu szkoleniowo-uświadamiającego. Celem niniejszego artykułu jest wprowadzenie do problematyki zarządzania bezpieczeństwem SI oraz zaprezentowanie najważniejszych wymogów dotyczących implementacji odpowiednich zabezpieczeń.

2. Zarządzanie bezpieczeństwem systemu informacyjnego w przedsiębiorstwie

W wielu zastosowaniach informatyki bezpieczeństwo informacji jest jednym z podstawowych kryteriów decydujących o praktycznej przydatności systemu. Nie ma oczywiście systemów absolutnie bezpiecznych. Zabezpieczanie wszystkiego i wszędzie również nie jest działaniem racjonalnym i może doprowadzić do nadmiernych kosztów i sparaliżować normalne funkcjonowanie danej organizacji.

Dlatego tak ważny jest wybór stosownych metod, technik i narzędzi zabezpieczania zasobów systemu informacyjnego, a co za tym idzie – odpowiednie zarządzanie bezpieczeństwem SI.

Podstawy terminologiczne dotyczące problematyki zarządzania bezpieczeństwem SI, jego istota oraz cele przedstawione zostały w artykule *Zarządzanie bezpieczeństwem systemu informacyjnego w polskich przedsiębiorstwach. Przegląd i analiza wybranych badań empirycznych*, zamieszczonym w niniejszej publikacji. Warto jednak, na potrzeby niniejszego opracowania, przypomnieć, że **zarządzanie bezpieczeństwem systemu informacyjnego to ciągły, cykliczny, złożony i racjonalnie finansowany proces umożliwiający bezpieczną realizację misji, do której instytucję powołano. Zarządzanie bezpieczeństwem systemu informacyjnego obejmuje zespół złożonych, powtarzalnych procesów zmierzających do osiągnięcia i utrzymywania oczekiwanego poziomu bezpieczeństwa systemu informacyjnego, tzn. poziomu poufności, integralności, dostępności, autentyczności i niezawodności.** Jego realizacja obejmuje takie działania, jak:

- określenie celów, strategii i polityki bezpieczeństwa systemu informacyjnego instytucji,
- określenie potrzeb bezpieczeństwa SI instytucji,
- identyfikowanie i analizowanie zagrożeń dla zasobów systemu informacyjnego przedsiębiorstwa,
- identyfikowanie i analizowanie ryzyka naruszenia zasobów SI,
- planowanie i projektowanie adekwatnych zabezpieczeń (metod, środków fizycznych, technologicznych, organizacyjnych, kadrowych itp.),
- monitorowanie i ocena wdrożenia oraz eksploatacji zabezpieczeń w celu racjonalnego zabezpieczenia SI przedsiębiorstwa,
- opracowanie i wdrożenie programu szkoleniowo-uświadamiającego,
- ciągłe doskonalenie systemu zabezpieczeń.

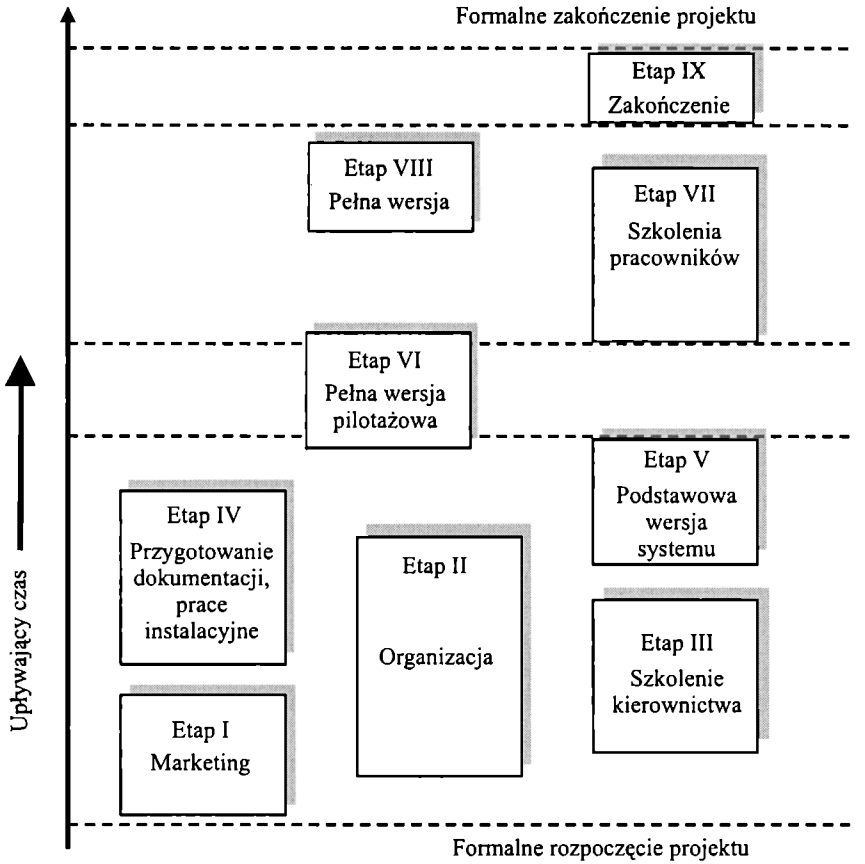
Podkreślić należy również, iż zapewnienie odpowiedniego stanu bezpieczeństwa systemu informacyjnego wymaga kompleksowego podejścia oraz konsekwencji w działaniu. Konsekwencja w zabezpieczaniu zasobów, monitorowaniu bezpieczeństwa, wykrywaniu i ściganiu nadużyć pozwala na bieżąco sprawować pełną kontrolę nad posiadanymi informacjami, co w dłuższej perspektywie, w połączeniu z otwartą polityką informacyjną, umożliwi zwiększenie zaufania do firmy wśród jej klientów i partnerów [Szafrański 2001]. Jednym z istotnych procesów zarządzania bezpieczeństwa SI jest projektowanie oraz wdrożenie adekwatnych zabezpieczeń, jego najważniejszy etap zaś to opracowanie i implementacja odpowiedniego programu szkoleniowo-uświadamiającego dla pracowników przedsiębiorstwa.

3. Organizacja i realizacja przedsięwzięć zabezpieczających

Ważnym etapem procesu zarządzania bezpieczeństwem SI jest ustalenie planu implementacji odpowiednich metod zabezpieczeń, uwzględniającego terminy, nakłady, priorytety oraz osoby odpowiedzialne. Podstawą tego procesu jest prze-

prowadzona wcześniej analiza ryzyka oraz przyjęta przez przedsiębiorstwo polityka bezpieczeństwa. Etap ten koncentruje się na wdrożeniu konkretnych rozwiązań organizacyjnych, sprzętowych i programowych. Największym ograniczeniem w dokonywaniu wyboru określonych rozwiązań są oczywiście aspekty finansowe. Proces implementacji systemu bezpieczeństwa można podzielić na kilka następujących podprocesów:

- instalacja sprzętu,
- instalacja, konfiguracja i uruchomienie oprogramowania,
- implementacja rozwiązań organizacyjnych (zarządzenia, procedury itp.),
- szeroko pojęte szkolenie użytkowników systemu (także przeprowadzanie szkoleń uświadamiających).



Rys. 1. Etapy implementacji systemu bezpieczeństwa
Źródło: opracowanie własne na podstawie [Kifner 1999, s. 104].

Wdrożenie systemu bezpieczeństwa wiąże się ściśle z innymi działaniami przedsiębiorstwa. Moment rozpoczęcia implementacji, a także kolejne jego etapy

nie powinny zakłócać normalnego funkcjonowania organizacji. Wzorcowa sytuacja to taka, kiedy pracownicy nie odczuwają momentu rozpoczęcia wdrożenia, a później aktywnie w nim uczestniczą, nie zaniedbując swych obowiązków. W związku z tym implementacji systemu zabezpieczeń nie powinno się rozpoczynać w momentach przełomowych, ważnych dla instytucji, takich jak np.:

- przekształcenia organizacyjne,
- wprowadzanie nowych produktów/usług na rynek,
- przekształcenia własnościowe, prywatyzacja.

Implementację systemu bezpieczeństwa w przedsiębiorstwie można podzielić na etapy, które ukazano na rys. 1.

W tabeli 1 omówione zostaną pokrótce poszczególne etapy implementacji systemu bezpieczeństwa w przedsiębiorstwie zaprezentowane na rys. 1.

Tabela 1. Etapy implementacji systemu bezpieczeństwa w przedsiębiorstwie

Etap	Nazwa etapu	Charakterystyka etapu
1	2	3
Etap I	Marketing	• działania marketingowe i rozpoznawcze polegające na przekonaniu pracowników o potrzebie wprowadzenia systemu bezpieczeństwa i systemowego podejścia do zarządzania bezpieczeństwem SI oraz zmierzające do określenia niebezpieczeństw dla implementacji • etap ten powinien obejmować rozmowy ze wszystkimi pracownikami
Etap II	Organizacja	• przygotowanie organizacyjne przedsiębiorstwa • pokierowanie polityką kadrową oraz polityką udzielania uprawnień i odpowiedzialności w celu osiągnięcia optymalnej sytuacji do wdrożenia i funkcjonowania systemu bezpieczeństwa
Etap III	Szkolenie kierownictwa	Przeszkolenie kierownictwa mające na celu: • przekazanie zarządowi przedsiębiorstwa i kierownikom merytorycznych informacji o samym systemie bezpieczeństwa i procesach zarządzania bezpieczeństwem SI • przekazanie informacji z zakresu implementacji systemu bezpieczeństwa, efektów/skutków wdrożenia • przekonanie niezadowolonych osób, przeciwników implementacji systemu bezpieczeństwa
Etap IV	Przygotowanie dokumentacji, prace instalacyjne	• przygotowanie odpowiedniej dokumentacji • przystosowanie pomieszczeń do nowych wymogów • instalacja odpowiedniego sprzętu, urządzeń i oprogramowania
Etap V	Podstawowa wersja systemu bezpieczeństwa	Wprowadzenie podstawowej wersji systemu bezpieczeństwa, obejmującej te działania instytucji, które dotychczas były realizowane, lecz nie były formalnie opisane, np.: • organizacja pracy strażników • wpuszczanie na teren przedsiębiorstwa osób z zewnątrz
Etap VI	Pełna wersja pilotażowa	• wprowadzenie pełnej wersji pilotażowej systemu bezpieczeństwa w wybranej jednostce (jednostkach) organizacyjnej • etap wymaga przeprowadzenia cyklu szkoleń dla pracowników wybranej jednostki organizacyjnej (w zakresie objętym etapem VII)

1	2	3
Etap VII	Szkolenia pracowników	Przeprowadzenie cyklu szkoleń dla wszystkich pracowników przedsiębiorstwa, które powinno podzielone zostać na bloki tematyczne. Należy rozłożyć je w czasie, aby nie wpływały negatywnie na bieżące obowiązki pracowników. Zakres szkoleń powinien obejmować: • ogólny opis systemu zabezpieczeń z uzasadnieniem potrzeby jego wdrożenia • szczegółowe omówienie funkcjonowania systemu w poszczególnych jednostkach organizacyjnych • szczegółowe omówienie kompetencji, zakresu obowiązków oraz procedur dotyczących każdego stanowiska pracy • przedstawienie wpływu systemu bezpieczeństwa na dotychczasowe procesy pracy, wyszczególnienie zmian wynikających z jego implementacji, • omówienie szczegółów organizacyjnych z zakresu zachowywania się pracowników w przedsiębiorstwie i poza nim, np.: – okazywanie przepustek, – tryb wymiany dokumentów z innymi działami, kontrahentami itp. • zapoznanie pracowników nie tylko z nowymi rozwiązaniami organizacyjnymi, ale i technicznymi
Etap VIII	Pełna wersja systemu bezpieczeństwa	• implementacja systemu bezpieczeństwa w każdej jednostce organizacyjnej • wdrażanie powinno się odbywać w dużych odstępach czasu, co umożliwi likwidację błędów, niedociągnięć i pozwoli pracownikom na przyzwyczajenie się do nowej sytuacji
Etap IX	Zakończenie	• zakończenie implementacji w jednostce organizacyjnej i odebranie prac przez jej kierownika • odbiór prac przez zarząd po całkowitym wprowadzeniu systemu bezpieczeństwa • niedociągnięcia systemu nie powinny być powodem niepodpisania odbioru, gdyż w rzeczywistości rzadko zdarzają się sytuacje, kiedy system zabezpieczeń nie wymaga doskonalenia

Źródło: opracowanie własne na podstawie [Kifner 1999, s. 104-106].

Implementacja systemu bezpieczeństwa może być realizowana przez własny personel organizacji gospodarczej lub przez firmę zewnętrzną. Zarówno jedno, jak i drugie podejście ma swoje wady i zalety. Podstawowe z nich zaprezentowano w tab. 2.

Nieodłączną częścią powyższych etapów wdrożenia systemu bezpieczeństwa są kontrole. Powinny być one przeprowadzane [Kifner 1999, s. 106]:

- zaraz po rozpoczęciu prac nad wdrożeniem,
- na zakończenie każdego etapu implementacji,
- przed odebraniem systemu bezpieczeństwa przez kierownika jednostki organizacyjnej,
- przed odebraniem całego systemu bezpieczeństwa przez zarząd.

Tabela 2. Zestawienie zalet i wad implementacji systemu bezpieczeństwa przez własny personel i firmę zewnętrzną

	Zalety	Wady
Własny personel	• prawdopodobnie niższy koszt • brak uzależnienia od firmy zewnętrznej • podniesienie potencjału personelu • szybka realizacja krytycznych czasowo zadań	• zwiększone obciążenie • prawdopodobnie dłuższy czas realizacji • niedostatek wiedzy o bezpieczeństwie • samokontrola • możliwa niska jakość realizacji
Firma zewnętrzna	• prawdopodobnie wyższa jakość realizacji zadania • krótszy czas realizacji projektu • wsparcie powdrożeniowe specjalistów mających dostęp do najnowszej wiedzy z zakresu bezpieczeństwa SI • kontrola zewnętrzna	• prawdopodobnie wyższy koszt realizacji • uzależnienie od firmy zewnętrznej • ewentualne opóźnienia w realizacji pilnych zadań • konieczność ingerencji konsultantów zewnętrznych w funkcjonowanie firmy • ograniczone podniesienie kwalifikacji personelu

Źródło: opracowanie własne.

W czasie kontroli należy sprawdzić, czy nie zostały naruszone obowiązujące zalecenia, normy i standardy, oraz jak postępują prace. Wynikiem kontroli powinien być także opis stanu przedsiębiorstwa oraz ocena, w jaki sposób wpływa na niego wdrażany system bezpieczeństwa. Kontrola powinna wykazać także, czy przedsiębiorstwo nie zostało „sparaliżowane" nadmiarem procedur i ograniczeń. Należy bowiem mieć na uwadze, że wdrożenie zabezpieczeń nie jest podstawową misją i celem przedsiębiorstwa, a jedynie środkiem służącym osiągnięciu jego celów strategicznych. **Nie powinna więc zaistnieć sytuacja, gdy przedsiębiorstwo koncentruje się na kwestiach związanych z wdrożeniem zabezpieczeń znacznym kosztem efektywności działalności biznesowej. Ponadto zbyt szybkie i restrykcyjne wdrażanie systemu bezpieczeństwa deprecjonuje jego wartość i rodzi kolejne zagrożenia.**

Bardzo ważną kwestią są wymogi stawiane kierownikowi odpowiedzialnemu za wdrożenie systemu zabezpieczeń. Ponieważ implementację tego systemu można traktować jako projekt polegający na wprowadzaniu pewnych zmian, można wymienić siedem podstawowych wymagań stawianych kierownikowi takiego projektu. Są to [Szyjewski 2001, s. 289]:

- zdobywanie odpowiednich zasobów,
- pozyskiwanie i motywowanie personelu,
- radzenie sobie z przeszkodami w osiąganiu celów,
- utrzymywanie się w podstawowych parametrach projektu,
- podejmowanie ryzyka przy unikaniu niepowodzeń,
- tworzenie rozległego systemu komunikacji,
- umiejętności negocjacyjne.

Koszty wdrożenia systemu zabezpieczeń wynikają w znacznej mierze z kwestii organizacyjnych i wiążą się z koniecznością szkoleń pracowników. Jest to bardzo istotne zagadnienie, które nie powinno być zaniedbywane. Niestaranność w przeprowadzaniu szkoleń może skutkować istotnym obniżeniem efektywności wdrożonych rozwiązań organizacyjnych, sprzętowych i programowych. Należy pamiętać, że człowiek jest najważniejszym elementem systemu bezpieczeństwa.

4. Opracowanie i wdrożenie programu szkoleniowo-uświadamiającego

Jak już wspominano, wdrożenie zasad bezpieczeństwa w przedsiębiorstwie musi być związane z zapoznaniem z nimi pracowników i współpracowników, jak również z przekonaniem ich do celowości stosowania zabezpieczeń. Organizacyjne przygotowanie szkoleń koordynuje osoba odpowiedzialna za przygotowanie szkoleń wewnątrz przedsiębiorstwa (może to być np. pracownik pionu zasobów ludzkich).

Szkolenia użytkowników systemu to jeden z najważniejszych elementów procesu wdrażania systemu zabezpieczeń. Ich przeprowadzanie powinno być podporządkowane dwóm podstawowym celom:

- zapoznaniu pracowników z nowymi rozwiązaniami technicznymi i organizacyjnymi,
- zwiększaniu świadomości pracowników w zakresie bezpieczeństwa systemu informacyjnego.

Szkolenia te powinny być prowadzone przez osoby o szerokiej wiedzy merytorycznej z zakresu bezpieczeństwa oraz z dużym doświadczeniem praktycznym. Podstawowe szkolenie z zakresu systemu bezpieczeństwa w przedsiębiorstwie organizowane dla pracowników powinno obejmować m.in. [Gałach 2004, s. 161-162]:

- wymagania w zakresie bezpieczeństwa systemu informacyjnego oraz ogólny opis systemu zabezpieczeń,
- uzasadnienie wprowadzonych mechanizmów bezpieczeństwa,
- znaczenie bezpieczeństwa dla prawidłowego funkcjonowania przedsiębiorstwa (możliwość efektywnej realizacji procesów biznesowych, osiągnięcie przewagi biznesowej itp.),
- wpływ systemu bezpieczeństwa na dotychczasowe procesy pracy, wyszczególnienie zmian wynikających z jego implementacji,
- dokładne omówienie funkcjonowania systemu w poszczególnych jednostkach organizacyjnych,
- znaczenie systemu bezpieczeństwa dla pracowników,
- szczegółowe omówienie kompetencji, zakresu obowiązków oraz procedur dotyczących każdego stanowiska pracy,
- szczegóły organizacyjne oraz techniczne z zakresu bezpieczeństwa,
- ograniczenia w korzystaniu z poszczególnych zasobów informacyjnych i uzasadnienie tych ograniczeń,

- obowiązujące zasady klasyfikacji informacji,
- zasady bezpiecznego korzystania z systemów informatycznych,
- niedozwolone operacje w systemach informatycznych,
- zasady postępowania w sytuacjach kryzysowych,
- zasady zgłaszania podejrzeń co do wystąpienia incydentów w zakresie bezpieczeństwa systemu informacyjnego,
- konsekwencje nieprzestrzegania obowiązujących zasad bezpieczeństwa SI w przedsiębiorstwie.

Tabela 3. Struktura specjalistycznych szkoleń w zakresie bezpieczeństwa SI w przedsiębiorstwie

Adresaci szkolenia	Zakres merytoryczny szkolenia
Kadra kierownicza	• wpływ systemu bezpieczeństwa na procesy biznesowe • rola kadry kierowniczej w procesach analizy ryzyka • rola kadry kierowniczej w procesach klasyfikacji informacji • zarządzanie uprawnieniami użytkowników • rola kadry kierowniczej w procesach planowania ciągłości działania i zarządzania planem ciągłości działania • rola kadry kierowniczej i jej współpraca w procesach reagowania na incydenty naruszenia bezpieczeństwa SI
Osoby odpowiedzialne za administrowanie systemami informatycznymi	• zasady bezpiecznego administrowania systemem informatycznym • zapewnienie bezpiecznej lokalizacji sprzętu informatycznego • zasady wprowadzania zmian w systemach informatycznych • zaimplementowane mechanizmy bezpieczeństwa • współpraca z administratorem bezpieczeństwa w celu zapewnienia bezpiecznego przetwarzania informacji • współpraca w procesach reagowania na incydenty naruszenia bezpieczeństwa systemu informacyjnego • rola osób odpowiedzialnych za administrowanie komponentami informatycznymi w procesach planowania ciągłości działania i zarządzania planem ciągłości działania
Kadra odpowiedzialna za bezpieczeństwo systemów informatycznych	• zapewnienie bezpiecznej lokalizacji sprzętu informatycznego • zaimplementowane mechanizmy bezpieczeństwa • współpraca z administratorem bezpieczeństwa i administratorami systemów w celu zapewnienia bezpiecznego przetwarzania informacji • współpraca w procesach reagowania na incydenty naruszenia bezpieczeństwa systemu informacyjnego
Kadra wykonująca obowiązki związane z utrzymaniem sprawności systemów informatycznych	• zasady bezpiecznego dostępu do systemu informatycznego i korzystania z niego • współpraca z administratorem bezpieczeństwa i administratorami systemów w celu zapewnienia bezpiecznego przetwarzania informacji • współpraca w procesach reagowania na incydenty
Pozostała kadra wykonująca obowiązki związane z bezpieczeństwem SI	• zasady dostępu do pomieszczeń • współpraca w procesach reagowania na incydenty naruszenia bezpieczeństwa

Źródło: opracowanie własne na podstawie [Gałach 2004, s. 163-164],

Administrator bezpieczeństwa powinien przeprowadzać ocenę skuteczności szkoleń na podstawie testów, wyników audytów bezpieczeństwa, jak również częstotliwości występowania incydentów. Ocena taka powinna być punktem wyjścia do udoskonalenia programów szkoleń. Jest on także osobą odpowiedzialną za przygotowanie i organizację szkoleń specjalistycznych, przeznaczonych dla osób odgrywających specjalne role w przedsiębiorstwie, szczególne ze względu na bezpieczeństwo SI. Wyszczególnienie tych osób, a także zakres merytoryczny skierowanych do nich szkoleń zawarto w tab. 3.

Oprócz samego procesu szkolenia ważnym elementem jest działanie uświadamiające oraz wpływanie na postawę pracownika. Istnieje wiele metod i technik psychologiczno-organizacyjnych prowadzących do minimalizowania nieprzewidzialnych zachowań pracownika, które w aspekcie bezpieczeństwa SI są szczególnie istotne. Ich charakterystyka i analiza zamieszczona została m.in. w pracy [Thomson, Solms 1998]. Odpowiednio przygotowany i zrealizowany program szkoleniowy powinien spowodować pozytywną zmianę postaw pracowników przedsiębiorstwa w aspekcie bezpieczeństwa systemu informacyjnego.

Podczas szkoleń niezbędne jest wyeliminowanie zjawiska bagatelizowania problemu oraz poglądu wśród pracowników, że systemy zabezpieczeń są kosztowne i powodują spowolnienie pracy.

5. Zakończenie

Sprawne funkcjonowanie współczesnych przedsiębiorstw nie jest obecnie możliwe bez zastosowania nowoczesnych technologii informacyjnych. Ich działalność w coraz większym stopniu uzależniona jest od najnowszych, lecz jednocześnie bezpiecznych narzędzi informatycznych. Dlatego też bardzo istotnym elementem zarządzania bezpieczeństwem systemu informacyjnego jest odpowiednie przygotowanie oraz przeprowadzenie procesu wdrożenia systemu zabezpieczeń w organizacji, a przede wszystkim odpowiednie opracowanie i implementacja programu szkoleniowo-uświadamiającego. W artykule zwrócono uwagę, iż jednym z najistotniejszych etapów implementacji systemu bezpieczeństwa jest proces szkolenia pracowników. Implementując jakiekolwiek mechanizmy zabezpieczeń systemu informacyjnego w przedsiębiorstwie, należy pamiętać o podstawowej zasadzie, iż **szkolenie jest najskuteczniejszym elementem profilaktyki**.

Literatura

Barczak A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy Bellona, Warszawa 2003.

Białas A., *Zarządzanie bezpieczeństwem informacji*, [w:] *Bezpieczeństwo systemów komputerowych*, red. A. Grzywak, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2000.

Białas A., *Bezpieczeństwo sieci komputerowych*, Wydawnictwo Wyższej Szkoły Informatyki i Zarządzania, Bielsko-Biała 2001a.
Białas A., *Zarządzanie bezpieczeństwem informacji*, Networld (1.03.2001b).
Bryl J., *Bezpieczeństwo systemów e-Commerce*, Gazeta IT nr 3(33) z 14 marca 2005.
Ernst & Young – *Światowe badanie dotyczące bezpieczeństwa informacji 2004 – Wyniki światowe*, http://www.ey.com/GLOBAL/content.nsf/Poland/TSRS_-_Library_-_GISS_2004.
Gałach A., *Instrukcja zarządzania bezpieczeństwem systemu informatycznego*, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 2004.
Jelonek D., *Wybrane aspekty polityki bezpieczeństwa informacji w e-przedsiębiorstwie*, www.it-investment.pl/upload/plik-42.doc.
Kifner T., *Polityka bezpieczeństwa i ochrony informacji*, Helion, Gliwice 1999.
Niemiec A., *Zarządzanie bezpieczeństwem informacji w świetle norm ISO*, http://www.prim.com.pl/referaty/wdrazanie_iso17799.htm (8.12.2003).
Szafrański M., *Bezpieczeństwo w parze z biznesem*, „Computerworld" nr 20/2002 z 20 maja 2002.
Szafrański M., *Zmowa milczenia*, Raport „Computerworld" – Bezpieczeństwo, z 9 kwietnia 2001.
Szyjewski Z., *Zarządzanie projektami informatycznymi*, Placet, Warszawa 2001.
Thomson M.E., Solms R., *Information Security Awareness: Educating your User Effectively*, „Information Management & Computer Security" 1998 nr 6/4.
Wawrzyniak D., *Zarządzanie bezpieczeństwem systemów informatycznych w bankowości*, AE, Wrocław 2002

IMPLEMENTATION OF PROTECTIONS AS AN ELEMENT OF INFORMATION SYSTEM SECURITY MANAGEMENT IN THE ENTERPRISE

Summary

In the contemporary Information Systems protections itself are no more sufficient as a standalone solution. Because contemporary Information Systems are very often sophisticated, heterogeneous and have dynamic character, individual solutions cannot ensure full protection against all possible threats. That is why it is worth to impose the layers of appropriate solutions which protect against its greatest number. In connection to the above very significant element of Information System security management it is appropriate the implementation of protection system and what is more the appropriate elaboration and implementation of education and awareness program. The aim of this article is introduction to the problems of IS security management and presentation of the crucial requirements concerning implementation of appropriate protections on the basis of Polish enterprises' experiences.

Iwona Chomiak-Orsa – dr, adiunkt w Katedrze Inżynierii Systemów Informatycznych Zarządzania Akademii Ekonomicznej we Wrocławiu.
Artur Rot – dr, asystent w Katedrze Inżynierii Systemów Informatycznych Zarządzania Akademii Ekonomicznej we Wrocławiu.