PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1094 — 2005
Informatyka Ekonomiczna 8

Artur Rot

NARZĘDZIA INFORMATYCZNE WSPOMAGAJĄCE ZARZĄDZANIE BEZPIECZEŃSTWEM SYSTEMU INFORMACYJNEGO

1. Wstęp

Informacja w dzisiejszych czasach jest elementem podlegającym szczególnym zabezpieczeniom ze względu na jej dużą wartość dla działalności biznesowej. Zabezpieczanie informacji biznesowych staje się coraz poważniejszym wyzwaniem. Przy swobodnym przepływie danych i wysokiej dostępności wielu zasobów opracowanie i wdrożenie bezpiecznego systemu zarządzania informacją staje się w przedsiębiorstwach istotnym problemem. Wdrożenie systemu bezpieczeństwa odpowiedniego do potrzeb instytucji polega na umiejętnym zaprojektowaniu zabezpieczeń – w taki sposób, aby znaleźć kompromis pomiędzy nakładami finansowymi związanymi z zastosowaniem mechanizmów ochronnych a osiągnięciem faktycznie pożądanego poziomu bezpieczeństwa systemu informacyjnego w przedsiębiorstwie.

Na rynku produktów informatycznych istnieje wiele aplikacji i narzędzi służących zabezpieczaniu systemu informacyjnego. Dostępne są różnorodne systemy zabezpieczające: skanery antywirusowe, filtry treści, systemy zaporowe, serwery autoryzacyjne, skanery luk w zabezpieczeniach, systemy wykrywania włamań, systemy zdalnego powiadamiania itd. Istnieje również wiele firm konsultingowych świadczących usługi doradcze w zakresie zarządzania bezpieczeństwem systemów informacyjnych. Jednak niewiele jest produktów programowych wspomagających procesy zarządzania bezpieczeństwem w przedsiębiorstwie – zwłaszcza na rynku polskim.

Celem artykułu jest wprowadzenie w problematykę zarządzania bezpieczeństwem SI, dokonanie prezentacji dwóch pakietów programowych wspomagających procesy zarządzania bezpieczeństwem w przedsiębiorstwie oraz prezentacja normy ISO 17799, na której te pakiety się opierają.

2. Istota zarządzania bezpieczeństwem systemu informacyjnego w przedsiębiorstwie

Funkcjonowanie współczesnych przedsiębiorstw nie jest możliwe bez zastosowania nowoczesnych technologii informacyjnych. Technologie te warunkują działalność obiektów gospodarczych, w coraz większym stopniu uzależnionych od najnowszych, lecz jednocześnie bezpiecznych narzędzi informatycznych. Rosnąca wartość informacji powoduje wzrost zagrożeń wobec systemu informacyjnego, stąd niezwykłej wagi problemem staje się zagadnienie bezpieczeństwa SI. Wraz z rozwojem systemów informacyjnych zmieniano technologię zabezpieczeń, jednak dziś same zabezpieczenia już nie wystarczają – należy je optymalnie dobierać, właściwie stosować i wreszcie odpowiednio nimi zarządzać.

Zarządzanie bezpieczeństwem nie jest aktem jednorazowym, polegającym na implementacji zabezpieczeń, lecz ciągłym, dynamicznym, a przy tym bardzo złożonym procesem, wymagającym stałego nadzoru i przystosowywania się do turbulentnych warunków otoczenia. Musi być rozpatrywane nie tylko w aspekcie technologicznym, ale również społecznym, organizacyjnym oraz prawnym, a ponadto powinno być zawsze dziełem interdyscyplinarnego zespołu specjalistów [Białas 2001].

Zarządzanie bezpieczeństwem to ciągły i złożony proces umożliwiający bezpieczną realizację misji, do której instytucję powołano. Zarządzanie bezpieczeństwem systemu informacyjnego obejmuje zespół złożonych procesów zmierzających do osiągnięcia i utrzymywania ustalonego poziomu bezpieczeństwa systemu informacyjnego, tzn. jego poziomu poufności, integralności, dostępności, autentyczności i niezawodności (por. [Rot 2001; Rot 2002a]). Jego realizacja obejmuje działania, takie jak:

- określenie potrzeb, celów i strategii bezpieczeństwa systemów informacyjnych,
- analiza ryzyka naruszenia zasobów SI,
- planowanie i projektowanie adekwatnych zabezpieczeń,
- monitorowanie i ocena systemu zabezpieczeń,
- opracowanie i wdrożenie programu szkoleniowo-uświadamiającego,
- ciągłe doskonalenie zabezpieczeń (na podstawie: PN-I-02000; por. [Wawrzyniak 2002]).

Wiąże się to z zapewnieniem gwarantowanego poziomu jakości informacji – informacje muszą być poprawne, dostępne tylko dla uprawnionych podmiotów, w odpowiednim czasie i tylko na odpowiednich stanowiskach w organizacji [Białas 2001].

Jak każda dziedzina, zarządzanie bezpieczeństwem wykształciło swoją terminologię, modele i metody działania. Istnieje również wiele norm i standardów w tym zakresie. Jedną z istotniejszych jest norma *Praktyczne zasady zarządzania bezpieczeństwem informacji* ISO17799, stanowiąca podstawę oprogramowania wspomagającego procesy zarządzania bezpieczeństwem SI w przedsiębiorstwach.

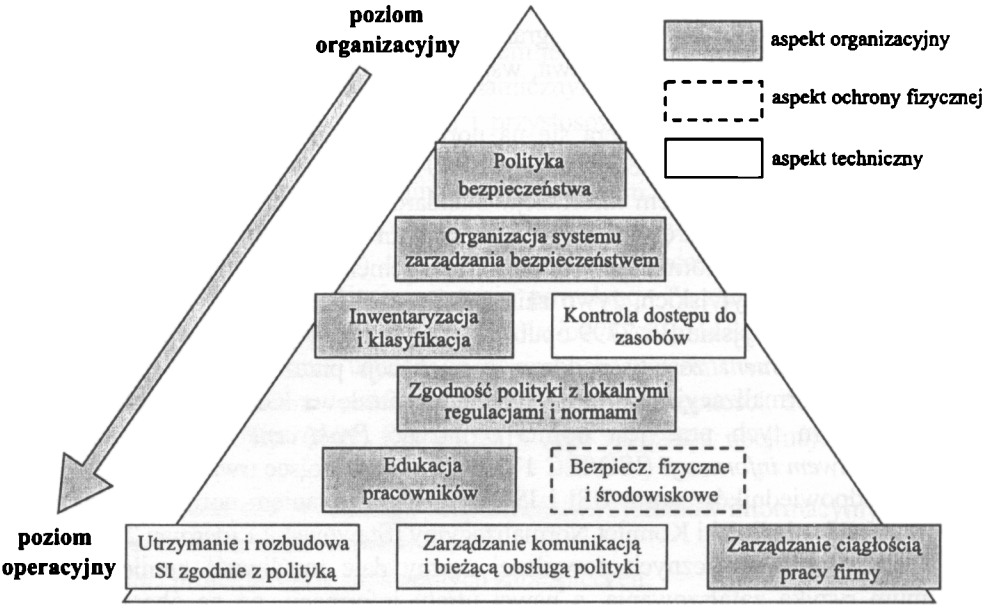
3. Standardy zarządzania bezpieczeństwem informacji BS 7799/ISO 17799

Systemy informatyczne stają się coraz bardziej rozbudowane i skomplikowane. Istnieje stała zależność, polegająca na tym, że bardziej złożony system informatyczny wymaga bardziej złożonych zabezpieczeń. Producenci zabezpieczeń zdają sobie z tego sprawę i w miarę możliwości starają się dostarczać wraz ze swoimi rozwiązaniami narzędzia ułatwiające ich utrzymanie i zarządzanie nimi. Głównie sprowadza się to do dostarczania graficznych, intuicyjnych w obsłudze edytorów polityki bezpieczeństwa oraz narzędzi wspomagających analizę i raportowanie rejestrowanych zdarzeń. Podejmowane są także próby opracowania systemu wizualizacji polityki bezpieczeństwa oraz monitorowania stanu rozproszonych geograficznie komponentów zabezpieczeń. Powstaje oprogramowanie, które wspomaga proces tworzenia dokumentacji polityki bezpieczeństwa, wspomaga proces audytu zarządzania bezpieczeństwem itp.

Wiele z tych narzędzi opiera się na normie ISO 17799, która wywodzi się z brytyjskiego standardu bezpieczeństwa BS 7799, stanowiącego podstawę systemów zarządzania bezpieczeństwem informacji. Standard ten opracowany został w 1995 r. przez BSI-DISC, strukturę BSI (Brytyjski Instytut Normalizacyjny) funkcjonującą pod nazwą BDD/2 Information Security Management i skupiającą przedstawicieli wielu organizacji brytyjskich, żywo zainteresowanych rozwojem e-biznesu. W roku 2000 zalecenia brytyjskie BS 7799 opublikowane w *Code of practice for Information Security Management* zostały poddane normalizacji przez ISO (Międzynarodowa Organizacja Normalizacyjna) oraz IEC (Międzynarodowa Komisja Elektrotechniczna). Wynikiem tych prac jest norma o nazwie *Praktyczne zasady zarządzania bezpieczeństwem informacji* (ISO/IEC 17799). Także w Polsce trwają prace nad stworzeniem odpowiedników norm BSI i ISO/IEC. Opracowaniem normy PN-ISO/IEC-17799 zajmuje się Polski Komitet Normalizacyjny [Stawowski; Liderman 2002].

Zastosowanie wytycznych powyższej normy daje możliwość zmniejszenia do minimum ryzyka zafałszowania, a nawet utraty informacji, co na obecnym etapie rozwoju w zakresie technologii informacyjnych jest niemalże koniecznością. Coraz częściej to właśnie informacja jest najcenniejszym zasobem, jej bowiem odzyskiwanie w razie utraty jest niezmiernie kosztownym i bardzo trudnym procesem. Ponadto ujawnienie istotnych informacji może prowadzić do utraty konkurencyjności przez przedsiębiorstwo. Z tego też względu informacja powinna w każdym przedsiębiorstwie podlegać szczególnej ochronie. Zastosowanie ISO 17799 pozwala określić wymagania przedsiębiorstwa w zakresie bezpieczeństwa, sformułować politykę ochrony i bezpieczeństwa informacji oraz wybrać środki, dzięki którym bezpieczeństwo informacji zostanie zapewnione. Norma wspomaga więc procesy organizacyjne w sposób umożliwiający racjonalne podwyższenie bezpieczeństwa informacji, koncentrując się na sferze organizacyjnej oraz kontrolując obszary zwiększonego ryzyka [Jakubowski 2002]. W dokumencie ISO 17799 wyróżniono 10 obszarów tematycznych (rys. 1). Są to:

1. Polityka bezpieczeństwa
2. Organizacja systemu zarządzania bezpieczeństwem w firmie
3. Inwentaryzacja i klasyfikacja posiadanych zasobów
4. Edukacja pracowników
5. Bezpieczeństwo fizyczne i środowiskowe
6. Zarządzanie komunikacją i bieżącą obsługą polityki bezpieczeństwa
7. Kontrola dostępu do zasobów
8. Utrzymanie i rozbudowa systemów informatycznych zgodnie z polityką bezpieczeństwa
9. Zarządzanie ciągłością pracy firmy
10. Zgodność polityki bezpieczeństwa z lokalnymi regulacjami i normami



Rys. 1. Obszary tematyczne wyróżnione w normie ISO 17799
Źródło: opracowanie własne na podstawie [Bisson, Saint-Germain 2004].

Pierwszym z wymienionych obszarów jest polityka bezpieczeństwa. Definiuje się ją w literaturze jako „zestaw praw, reguł i praktycznych zasad określających sposób, w jaki informacja (w szczególności informacje niejawne) i pozostałe aktywa są zarządzane, zabezpieczane i dystrybuowane" [Białas 1999]. Dokument polityki bezpieczeństwa stanowi podstawę wytyczającą strategię przedsiębiorstwa w zakresie bezpieczeństwa SI [Gałach 2004]. Jego opracowanie jest podstawowym wymogiem, który w rezultacie pozwala na określenie oczekiwań organizacji dotyczących bezpieczeństwa i kierunków działania w tym zakresie. Dokument z opisaną polityką bezpieczeństwa może być stosowany jako podstawa późniejszych audytów.

Drugi obszar odnosi się do struktur zarządzania bezpieczeństwem w obrębie organizacji. Podaje wytyczne dotyczące struktury decyzyjnej, ustalania grup odpowiedzialnych za określone działania oraz sposoby postępowania w przypadku wystąpienia incydentów. Trzeci odnosi się do zasobów informatycznych, znajdujących się w posiadaniu przedsiębiorstw. Według omawianego standardu, jednym ze wstępnych elementów działań na rzecz bezpieczeństwa jest inwentaryzacja i klasyfikacja wszystkich posiadanych zasobów, co pozwala dobrać odpowiednie środki ochrony, zarówno ze względu na ich skuteczność, jak i ze względu na koszt) [Jakubowski 2002].

Kolejny – czwarty obszar tematyczny związany jest z pracownikami firmy. Standard wskazuje potrzebę szkolenia zatrudnionych osób, uświadamiania im oczekiwań wobec nich, związanych z kwestiami bezpieczeństwa i poufnością posiadanych przez nich informacji. Każdy pracownik powinien zdawać sobie również sprawę ze swojej roli w polityce bezpieczeństwa całej organizacji. Istota czynnika ludzkiego w polityce bezpieczeństwa przejawia się głównie w postawie kierownictwa, w odpowiednim doborze i przeszkoleniu kadry pracowniczej (szczególnie tej, która ma dostęp do informacji podlegających ochronie). Dbałość o tych pracowników, o ich nastawienie i postawę wpływa w sposób niezwykle istotny na poziom bezpieczeństwa informacji. Istotną rolę odgrywają również kierownicy jednostek organizacyjnych, inspektorzy bezpieczeństwa oraz administratorzy systemów informatycznych. Dokument ISO 17799 traktuje także o konieczności przygotowania planu raportowania przez personel potencjalnych incydentów uważanych za naruszenie bezpieczeństwa.

Piąty obszar dotyczy bezpieczeństwa fizycznego, czyli np. sposobów ochrony dostępu do pomieszczeń czy ochrony urządzeń, a szósty – zarządzania komunikacją i wszelkich działań związanych z obsługą polityki bezpieczeństwa: zapewnienia poprawnego działania centrom przetwarzania danych, minimalizowania ryzyka awarii, ochrony integralności oprogramowania i informacji, a także ciągłości przetwarzania i komunikacji. Oba te obszary traktują również o ochronie informacji w sieciach i ochronie infrastruktury pomocniczej, o przeciwdziałaniu zniszczeniu zasobów i przerwom w pracy firmy oraz o przeciwdziałaniu utracie, modyfikacji czy niewłaściwemu wykorzystaniu informacji przesyłanych pomiędzy przedsiębiorstwami.

Siódmy obszar odnosi się do kontroli dostępu do sieci i zasobów, by chronić organizację nie tylko przed zagrożeniami zewnętrznymi, ale także wewnętrznymi. Ósmy dotyczy konieczności konsultowania z polityką bezpieczeństwa firmy wszelkich działań związanych z utrzymaniem pracy systemów informatycznych bądź realizacji nowych przedsięwzięć – tak by nie były one ze sobą sprzeczne.

Dwa ostatnie obszary odnoszą się do zarządzania ciągłością pracy organizacji oraz konieczności stwierdzenia zgodności polityk bezpieczeństwa stworzonej na podstawie ISO 17799 z obowiązującymi w danym kraju przepisami prawnymi, dotyczącymi np. ochrony danych osobowych [Jakubowski 2002].

Wyróżnia się wiele bardzo różnorodnych metod ustalania wymagań związanych z bezpieczeństwem informacji. Niewątpliwie podstawowe to:

- znajomość uregulowań prawnych dotyczących wymaganych działań zapewniających bezpieczeństwo informacji,

- oszacowanie poziomu ryzyka utraty informacji,
- wypracowanie w przedsiębiorstwie odpowiedniej postawy wobec zapewnienia bezpieczeństwa informacji,
- wskazanie obszarów, w których zachodzi konieczność poprawy.

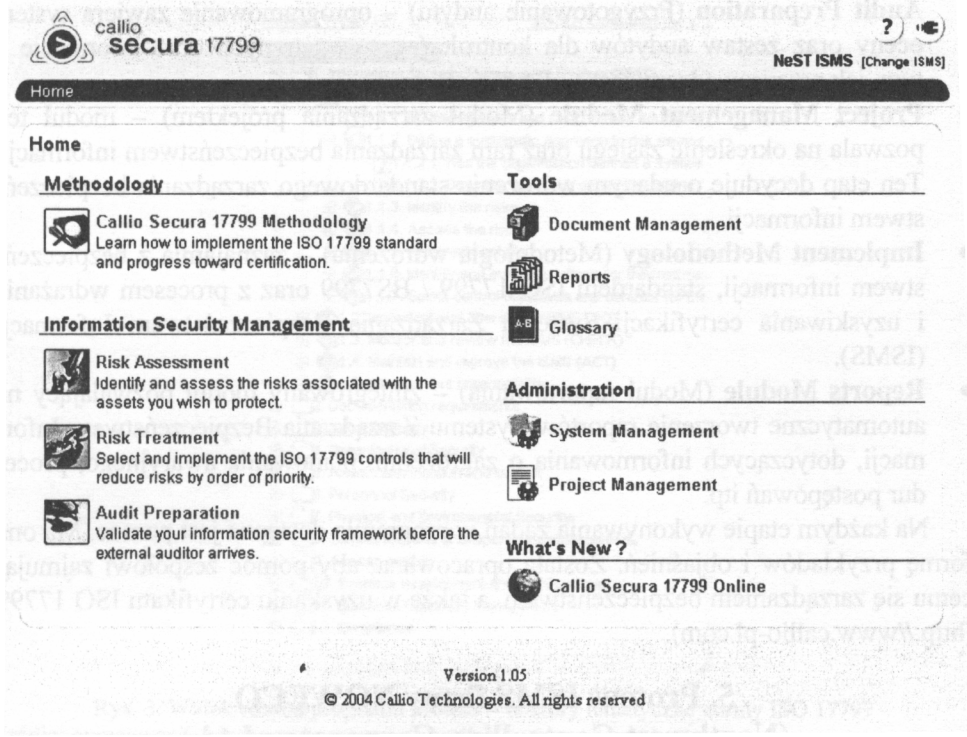
Dotychczas na świeci ponad 80 tys. firm wdrożyło normę BS 7799/ISO 17799, m.in.: Fujitsu Limited, Insight Consulting Limited, KPMG, Marconi Secure Systems, Samsung Electronics Co Ltd., Sony Bank Inc., Symantec Security Services, Toshiba IS Corporate.

Wdrożenie standardu ISO 17799 przez organizację może być potwierdzone certyfikatem. Nawet jeśli dana organizacja nie zamierza decydować się na przejście procesu certyfikacji, ISO 17799 może służyć jako zarys strategii podniesienia bezpieczeństwa systemów informatycznych. Certyfikat ISO 17799 stanowi świadectwo, że w przedsiębiorstwie stosuje się właściwe środki techniczne i organizacyjne gwarantujące ochronę poufności, autentyczności i spójności informacji na wszystkich etapach jej przetwarzania (http://www.qualityprogress.com.pl).

4. Oprogramowanie wspomagające zarządzanie systemem bezpieczeństwa informacji firmy Callio Technologies

Firma Callio Technologies powstała w 2001 r. Specjalizuje się w dziedzinie zabezpieczeń komputerowych. Produkty informatyczne tej firmy: Callio Secura 17799, Callio Toolkit Pro oraz Callio Toolkit, to oprogramowanie mające pomagać firmom w spełnianiu standardów zarządzania bezpieczeństwem informacji BS779/ISO IEC 17799 oraz projektowaniu polityki bezpieczeństwa informacji. Technologiczne rozwiązania, wyposażenie oraz produkty nie są już wystarczające przy zarządzaniu bezpieczeństwem informacji. Obecnie firmy muszą posiadać efektywny system zabezpieczenia. Rozwiązaniem są omówione wcześniej normy BS7799/ISO 17799. Oparte na metodologii BS7799 oprogramowanie Callio Secura 17799 (rys. 2) oferuje kompletny zestaw funkcji pomocnych do oceny zagrożenia, oraz prowadzeniu dokumentacji wymaganej przez BS7799/ISO 17799. Jest to aplikacja sieciowa, wspomagająca procesy tworzenia, wdrażania, monitorowania oraz uzyskiwania certyfikacji Systemu Zarządzania Bezpieczeństwem Informacji. Podstawowa funkcja aplikacji to możliwość generowania polityki bezpieczeństwa dostosowanej do sytuacji konkretnej organizacji, program ma jednak znacznie większe możliwości. W jego skład wchodzą następujące moduły:

- **Risk Assessment Module/ Risk Treatment Module** (Moduł szacowania ryzyka) – moduły umożliwiające ustalenie poziomu dostosowania firmy do standardu ISO 17799. Drogą gromadzenia informacji o zasobach (aktywach) w celu ochrony i oceny oraz rozpoznawania zagrożeń i niezabezpieczonych zasobów administrator (inspektor) bezpieczeństwa jest w stanie ocenić rozmiary ryzyka.



Rys. 2. Widok ekranu oprogramowania Callio Secura 17799
Źródło: opracowanie własne.

- **Policy Generator** (Generator polityki bezpieczeństwa) – wykorzystując wskazówki i wytyczne sugerowane w Callio Secura 17799, administrator (inspektor) bezpieczeństwa może szybko i sprawnie stworzyć własną politykę bezpieczeństwa (35 zabezpieczeń oraz ponad 500 wytycznych spełnia dziesięć głównych punktów standardu BS7799/ISO 17799).
- **Document Management** (Zarządzanie dokumentami) – moduł ten umożliwia firmie zarządzanie polityką bezpieczeństwa i postępowanie z aktualnymi informacjami oraz innymi dokumentami w sposób systematyczny i standardowy. Administrator bezpieczeństwa będzie w stanie tworzyć, modyfikować oraz rewidować dokumenty.
- **Implementation Templates** (Szablony implementacji) – w celu wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji opartego na standardzie BS7799/ ISO 17799 należy użyć szablonów oraz dokumentów roboczych, które zawierają modele, listy, przykłady, dodatkowe informacje oraz narzędzia. W module tym użytkownik znajdzie ponad 100 dokumentów spełniających dziesięć punktów standardu, łącznie z dotyczącymi gromadzenia informacji o zasobach oraz klasyfikacji szablonów, poufnych dokumentów, formularzy rekrutacyjnych oraz plany na wypadek nadzwyczajnych zajść.

- **Audit Preparation** (Przygotowanie audytu) – oprogramowanie zawiera system oceny oraz zestaw audytów dla kontrolerów wewnętrznych oraz informacje o tym, jak przeprowadzany jest audyt zewnętrzny.
- **Project Management Module** (Moduł zarządzania projektem) – moduł ten pozwala na określenie zasięgu oraz ram zarządzania bezpieczeństwem informacji. Ten etap decyduje o udanym wdrożeniu standardowego zarządzania bezpieczeństwem informacji.
- **Implement Methodology** (Metodologia wdrożenia) – zaznajamia z bezpieczeństwem informacji, standardem ISO 17799 / BS7799 oraz z procesem wdrażania i uzyskiwania certyfikacji Systemu Zarządzania Bezpieczeństwem Informacji (ISMS).
- **Reports Module** (Moduł raportowania) – zintegrowany moduł pozwalający na automatyczne tworzenie raportów Systemu Zarządzania Bezpieczeństwem Informacji, dotyczących informowania o zagrożeniu, planowania awaryjnego, procedur postępowań itp.

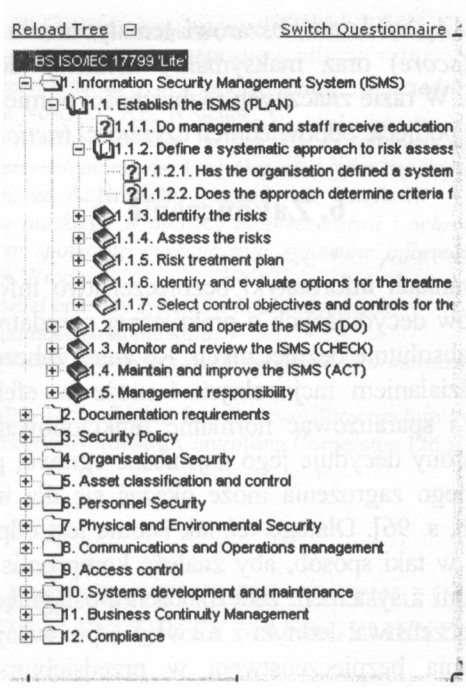
Na każdym etapie wykonywania zadań w programie dostępna jest pomoc. Ma ona formę przykładów i objaśnień. Została opracowana, aby pomóc zespołowi zajmującemu się zarządzaniem bezpieczeństwem, a także w uzyskaniu certyfikatu ISO 17799 (http://www.callio-pl.com).

5. Proteus ISMS firmy NOWECO (Northwest Controlling Corporaton Ltd.)

Proteus ISMS Information Security Management Software jest oprogramowaniem firmy NOWECO, wspomagającym procesy zarządzania bezpieczeństwem informacji w przedsiębiorstwie. Jest to program integrujący wiele zagadnień z zakresu bezpieczeństwa w jednym narzędziu. Jest to zintegrowany system do analizy, oszacowania ryzyka, tworzenia i kontroli polityki bezpieczeństwa oraz procedur w tym zakresie, planowania i ewidencji szkoleń oraz planowania i wspomagania audytu zgodnie z omówionym wcześniej standardem ISO 17799. Jego podstawową cechą jest całkowita kontrola nad polityką wszystkimi procedurami bezpieczeństwa w przedsiębiorstwie. Oprogramowanie to zawiera zestaw kwestionariuszy i ankiet dotyczących wymogów BS 7799/ISO 17799 i poszczególnych obszarów tematycznych zawartych w tym standardzie (rys. 3).

Proteus ISMS to oprogramowanie do analizy luk w systemie, wspomagające przede wszystkim proces audytu systemu zarządzania bezpieczeństwem, zawierające ponad 1100 kwestionariuszy.

Tworzenie, edycja, dystrybucja oraz wypełnienie poszczególnych kwestionariuszy prowadzą do wygenerowania raportu – analitycznego wyniku analizy luk w systemie zarządzania bezpieczeństwem. Generowany raport określa luki i słabe punkty w systemie zarządzania bezpieczeństwem SI i wskazuje konieczność podjęcia działań naprawczych w wyszczególnionych obszarach tematycznych (rys. 4).



Rys. 3. Widok ekranu programu Proteus – obszary tematyczne normy ISO 17799
Źródło: opracowanie własne na podstawie (http://www.noweco.com).

Questionnaire Summary

Information Governance Ltd.

Questionnaire	*BS7799:2002*
Site	*London Office (United Kingdom)*
Completed	*75.06%*
Author	*Andreas Fiedler*
Printed	*September 3 2004 (22:12)*

Section	Section Title	Score	Maximum Obtainable	Threshold	Action Needed?
1.	Information Security Management System	31.77%	86.67%	100.00%	Yes
2.	Documentation requirements	4.46%	100.00%	100.00%	Yes
3.	Security Policy	50.95%	100.00%	100.00%	Yes
4.	Organisational Security	27.82%	100.00%	100.00%	Yes
5.	Asset Classification and Control	58.33%	100.00%	100.00%	Yes

Rys. 4. Fragment raportu wygenerowanego w programie Proteus
Źródło: opracowanie własne na podstawie (http://www.noweco.com).

Jak wynika z rys. 4, każdemu obszarowi tematycznemu (*section title*) przypisywany jest wynik (*score*) oraz maksymalny możliwy do osiągnięcia rezultat (*maximum obtainable*). W razie znacznych rozbieżności pomiędzy tymi wskaźnikami Proteus ISMS sugeruje podjęcie odpowiednich czynności (*action needed*).

6. Zakończenie

W wielu zastosowaniach informatyki bezpieczeństwo informacji jest jednym z podstawowych kryteriów decydujących o praktycznej przydatności systemu. Nie ma oczywiście systemów absolutnie bezpiecznych. Również zabezpieczanie wszystkiego i wszędzie nie jest działaniem racjonalnym i może w efekcie doprowadzić do nadmiernych kosztów i sparaliżować normalne funkcjonowanie danej organizacji. O jakości systemu ochrony decyduje jego najsłabsze ogniwo, przeoczenie bądź zbagatelizowanie konkretnego zagrożenia może okazać się dla instytucji katastrofalne w skutkach [Rot 2002b, s. 96]. Dlatego też tak istotne jest odpowiednie zarządzanie bezpieczeństwem SI – w taki sposób, aby znaleźć kompromis pomiędzy nakładami finansowymi związanymi z systemem zabezpieczeń a osiągnięciem faktycznie pożądanego poziomu bezpieczeństwa. Jednym z rozwiązań pozwalających na zwiększenie efektywności zarządzania bezpieczeństwem w przedsiębiorstwie jest wdrożenie normy BS 7799/ISO 17799. Rozwiązaniem może być również stosowanie oprogramowania wspomagającego procesy zarządzania bezpieczeństwem systemu informacyjnego opartego na wymienionym standardzie. Programy te umożliwiają generowanie dokumentacji polityki bezpieczeństwa, odpowiedniej do specyfiki wymogów danej instytucji. Ułatwiają również dostosowanie procesów zarządzania bezpieczeństwem systemów informacyjnych do uznanych standardów, co w efekcie prowadzi do minimalizacji ryzyka naruszenia zasobów SI. Aplikacje te są także narzędziem wspomagającym proces audytu bezpieczeństwa, wskazując administratorom i inspektorom bezpieczeństwa konkretne słabe punkty systemu.

Literatura

Białas A. (1999), *Zarządzanie bezpieczeństwem informacji*, [w:] *Bezpieczeństwo systemów komputerowych i telekomunikacyjnych*, red. A. Grzywak, Wydawnictwo Sotel, Chorzów.

Białas A. (2001), *Zarządzanie bezpieczeństwem informacji*, „Networld" 1.03.2001.

Bisson J., Saint-Germain R. (2004), *The BS 7799/ISO 17799 Standard for a Better Approach to Information Security*, (http://www.callio.com).

Gałach A. (2004), *Instrukcja zarządzania bezpieczeństwem systemu informatycznego.* Ośrodek Doradztwa i Doskonalenia Kadr, 2004.

Jakubowski R. (2002), *Bezpieczeństwo w standardzie*, „ComputerWorld", raport „Bezpieczeństwo danych w sieci" 24.06.2002.

Liderman K. (2002), *Standardy w ocenie bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki WAT" nr 17.

Quality Progress „*Materiały tematyczne – zarządzanie bezpieczeństwem informacji*", http://www.qualityprogress.com.pl/strony/1/i/48.php.

Rot A. (2002a), *Modele bezpieczeństwa i ochrony informacji w przedsiębiorstwie*, Informatyka Ekonomiczna nr 5, red. A. Nowicki, AE, Wrocław.

Rot A. (2002b), *Organizacja zasobów ludzkich na potrzeby kształtowania polityki bezpieczeństwa i ochrony informacji w przedsiębiorstwie*, [w:] *Organizacyjne aspekty doskonalenia systemów informacyjno-decyzyjnych*, red. A. Nowicki, J. Unold, AE, Wrocław.

Rot A. (2001), *Rola czynnika ludzkiego w polityce bezpieczeństwa i ochrony informacji w przedsiębiorstwie*, [w:] *Aspekty społeczne doskonalenia systemów informacyjno-decyzyjnych*, red. A. Nowicki, J. Unold, AE, Wrocław.

Stawowski M., *Strategie i techniki ochrony systemów informatycznych*, http://www.iniejawna.pl/pomoce/strategie.html.

Wawrzyniak D. (2002), *Zarządzanie bezpieczeństwem systemów informatycznych w bankowości*, AE, Wrocław.

Witryna internetowa firmy Callio Technologies, http://www.callio.com http://www.callio-pl.com.

Witryna internetowa firmy Noweco (Northwest Controlling Corporaton Ltd.) http://www.noweco.com.

SOFTWARE IMPLEMENTATIONS SUPPORTING INFORMATION SYSTEM SECURITY MANAGEMENT

Summary

The rapid progress in the area of information technology brings new threats of information disclosure. The subject of IS/IT security has become very significant. Every organisation has to apply adequate methods, tools and organisational requirements to protect its information resources.

The aim of this article is to present the essence and the importance of the information system security management. The paper also presents the software applications, which support information system security management processes. The information security isn't complete without the development and publication of security policies, procedures and processes like employee awareness and training programs. The information security is really an ongoing management process and therefore requires tools that meet these needs. One of these tools is software applications, supporting information security management, based on the international standard ISO 17799. Two of these applications will be presented – Callio Secura is a software that helps companies comply with the BS7799/ ISO IEC 17799 information security management standard. It helps to develop, implement, manage and certify information security management system (ISMS) in accordance with this standard. The second presented application – Proteus ISMS is the system, which supports all phases and aspects of ISMS in accordance with the discussed standard.