PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1081 — 2005
Nowoczesne technologie informacyjne w zarządzaniu

Hanna Mazur, Zygmunt Mazur, Teresa Mendyk-Krajewska

NORMY BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

1. Wprowadzenie

Za system informatyczny uważa się zbiór powiązanych ze sobą elementów składowych, takich jak ludzie, sprzęt (głównie komputerowy), zbiory informacji oraz oprogramowanie, służące do przetwarzania zgromadzonych informacji. Przyjmując taką definicję, w artykule podjęto próbę określenia, na czym polega bezpieczeństwo systemu informatycznego. Czy można je zmierzyć, a jeśli tak, to w jaki sposób? Kiedy można powiedzieć, że dany system informatyczny jest bezpieczny? W artykule autorzy starają się udzielić odpowiedzi na tak postawione pytania.

Bezpieczeństwo systemu informatycznego jest związane ze wszystkim, co się wiąże ze zdefiniowaniem, osiąganiem i utrzymywaniem jego poufności, integralności, dostępności, autentyczności i niezawodności.

Bezpieczeństwo systemu informatycznego obejmuje dwa poziomy:

- zewnętrzny, czyli kontrolę dostępu do systemu i ochronę systemu przed naturalnymi, sprzętowymi lub wywołanymi przez człowieka katastrofami,
- wewnętrzny, czyli przeciwdziałanie atakom przeprowadzanym przez osoby z zewnątrz oraz przez nieuczciwych pracowników czy też błędy lub zaniedbania osób upoważnionych do obsługi systemu.

W rzeczywistości nawet upoważnieni użytkownicy systemu mogą starać się o dostęp do danych przed nimi chronionych i nieodpowiednio wykorzystywać nadane im przywileje. Dlatego też dostęp do szczególnie chronionych obszarów powinny mieć jedynie wybrane osoby, według wybranych trybów dostępu.

Do oceny poziomu bezpieczeństwa systemu informatycznego służą standardy bezpieczeństwa, ustanowione przez wyspecjalizowane organizacje. Stanowią one podstawę kwalifikacji danego systemu do określonej klasy bezpieczeństwa w ramach obowiązujących norm. Standardy narodowe nie oparte na międzynarodowych zaleceniach utrudniają, a niekiedy wręcz uniemożliwiają współpracę i wymianę różnych elementów systemu. Znaczącą rolę w opracowywaniu międzynaro-

dowych standardów odgrywa ISO (International Organization for Standarization), zrzeszająca krajowe organizacje normalizacyjne uwzględniające międzynarodowe kryteria. Członkami ISO są m.in.: PKN (Polski Komitet Normalizacyjny), AFNOR (Association Francaise de Normalisation), ANSI (American National Standards Institute), BSI (British Standard Institute), DIN (Deutsches Institut für Normung). Pełna lista członków ISO znajduje się w [ISO, Internet 2005a].

2. Polityka bezpieczeństwa

Ogólnie biorąc, polityka bezpieczeństwa systemu informatycznego jest ściśle zależna od środowiska, w którym system jest wykorzystywany, i od względów ekonomicznych. Wprowadzenie dodatkowych mechanizmów bezpieczeństwa wiąże się ze zwiększeniem kosztów, zwykle wpływa również na osłabienie wydajności systemu ze względu na wzrost jego złożoności. Często potrzebne są również dodatkowe osoby, a także specjalny sprzęt i oprogramowanie do tworzenia i konserwowania systemu oraz zarządzania. Z kolei brak zabezpieczeń systemu wystawia go na ryzyko włamań i utraty danych. Ryzyko to powinno być dokładnie szacowane na podstawie obserwacji, typologii środowiska i jego użytkowników. Z pewnością inne zabezpieczenia i inne ryzyko są związane z systemem bankowym czy wojskowym, a inne z osobistym rejestrem adresowym.

Aby zaprojektować system informatyczny poprawnie gromadzący i przetwarzający dane lub zabezpieczyć istniejący system, należy określić politykę bezpieczeństwa, czyli reguły określające m.in., co ma podlegać ochronie, jakie dane mają być chronione i przed kim, a jakie udostępniane (komu i na jakich zasadach), a także kto i w jaki sposób ma chronić określone dobra. Istotne jest również określenie, jaki będzie koszt zabezpieczania danych i jakie mogą być skutki ich utraty lub udostępnienia niewłaściwym osobom, czy warto podejmować trud zabezpieczania danych, a jeśli tak, to w jakim zakresie. Polityka bezpieczeństwa jest więc związana z dogłębnym poznaniem intruza, czyli ze znalezieniem odpowiedzi na pytania: Co chronić? Dlaczego chronić? Przed kim chronić? Jak chronić? Taka polityka obejmuje bezpieczeństwo firmy (ogólne zasady ochrony), bezpieczeństwo całości systemów informatycznych (zasady dostępu i odpowiedzialności) i bezpieczeństwo każdego konkretnego systemu informatycznego (jego zabezpieczenia fizyczne, logiczne i organizacyjne). Politykę bezpieczeństwa opracowuje się z uwzględnieniem prawa, norm bezpieczeństwa i metodyk, np. MARION (metodyka nielicencjonowana, zalecana przez Związek Banków Polskich do przeprowadzania audytów w instytucjach finansowych), TISM *(total information security manager)* czy metodyka CRAMM *(*CCTA *risk analysis& management method)*, czyli metodyka oparta na analizie ryzyka i zarządzaniu nim, opracowana w 1989 r. przez agencję CCTA (Central Computer and Telecommunications agency) działającą przy rządzie Wielkiej Brytanii.

Ostatnio bardzo często używa się określenia audyt w odniesieniu do działalności finansowej firmy, całego przedsiębiorstwa, baz danych, serwerów, systemów informatycznych, sieci komputerowych i teleinformatycznych itd. Na internetowej stronie Fundacji Rozwoju Społeczeństwa Informacyjnego znajduje się następująca definicja pojęcia audyt: „Audyt (ang. *audit*) to szczegółowa analiza działalności danej organizacji, prowadzona przez zewnętrznych, niezależnych specjalistów w celu ujawnienia ewentualnych problemów czy nieprawidłowości w jej funkcjonowaniu. Audyt może dotyczyć każdego aspektu funkcjonowania firmy".

Audyt powinien być przeprowadzany rzetelnie, przez audytora – czyli najczęściej zespół audytowy składający się z tzw. audytora wiodącego, audytorów i ekspertów. Audytor musi posiadać odpowiednie kwalifikacje oraz być niezależny od audytowanej organizacji i producenta np. sprzętu czy oprogramowania podlegającego audytowi. Audyt bezpieczeństwa (ang. *security audit*) systemu informatycznego polega głównie na ocenie działania systemu i zastosowanych zabezpieczeń, ich zgodności z określoną polityką bezpieczeństwa, wskazaniu rozbieżności z założonymi wymaganiami, na wskazaniu luk i braków w zabezpieczeniach oraz określeniu sytuacji krytycznych i możliwych zagrożeń (np. ze strony osób nieuprawnionych lub czynników niezależnych, takich jak brak prądu, awaria urządzeń itp.). Firma Gartner wyróżnia trzy etapy w opracowywaniu planów awaryjnych: (1) fundamentalny – wyznaczenie osoby odpowiedzialnej za plan i powołanie grupy ludzi do jego opracowania, (2) przygotowanie i implementacja planów, (3) utrzymywanie i doskonalenie planów.

W celu zapewnienia bezpieczeństwa systemów informatycznych oraz baz danych gromadzi się informacje z przebiegu pracy systemu w postaci dodatkowych plików (tzw. logi), których analizowanie jest czasochłonne, a w sytuacji zagrożenia czas zawsze jest czynnikiem krytycznym. Należy więc tak zorganizować generowanie danych o pracy systemu, aby zawierały niezbędne i wyczerpujące informacje i umożliwiały ich szybką analizę. Spełnienie tych zaleceń jest oczywiście bardzo trudne.

Audyt projektów informatycznych prowadzony jest np. pod kątem ich zgodności z wymaganiami funkcjonalnymi, technicznymi, finansowymi i harmonogramem, celem zmniejszenia ryzyka niepowodzenia projektu. Częstość przeprowadzania audytu ustala się na podstawie częstości zmian oprogramowania, sprzętu, zmian organizacyjnych w firmie, ważności danych, zaistniałych sytuacji krytycznych itp. Wyniki z przeprowadzonego audytu powinny być przedstawione w uzgodnionej formie (raporty, wytyczne, plany, wnioski), według ustalonych reguł i z podaniem zasad kontroli realizacji wniosków z przeglądu bezpieczeństwa. Wyróżnia się audyty wewnętrzne i zewnętrzne (np. testy penetracyjne dokonywane przez Internet).

Chwila postoju pracy banku czy giełdy powoduje straty tysięcy dolarów, dlatego pewne firmy nie mogą sobie pozwolić na żadne przestoje i muszą przewidywać scenariusze wydarzeń prowadzących do przerwania ciągłości dzia-

łania w celu ich wyeliminowania lub opracowania planów awaryjnych działań. Zagadnienia bezpieczeństwa danych, sieci, serwerów i centrów archiwizujących (*back up*) oraz zagadnienia związane z podpisem elektronicznym, infrastrukturą kluczy, antykrackerstwem i planowaniem ciągłości prowadzenia biznesu (ang. *business continuity planning*) mają obecnie bardzo wysoki priorytet.

3. Normy bezpieczeństwa

Bezpieczeństwo systemów informatycznych i danych można zapewnić poprzez przestrzeganie obowiązujących krajowych lub międzynarodowych norm (np. PN-ISO/IEC 17799:2003, BS 7799-2:2002, ISO/IEC TR 13335), tworzenie własnych, indywidualnych procedur i regulaminów dotyczących bezpiecznego użytkowania sieci korporacyjnej, a także poprzez projektowanie oraz wdrożenie polityki bezpieczeństwa danych, wspartej szkoleniami i mającej formalne odzwierciedlenie w odpowiednim dokumencie.

Normy ISO/IEC są normami międzynarodowymi opracowywanymi wspólnie przez ISO – International Organization for Standarization (Międzynarodowa Organizacja Normalizacyjna) i IEC – International Electrotechnical Commission (Międzynarodowa Komisja Elektrotechniczna). Normy PN (Polska Norma) są polskimi wdrożeniami odpowiednich norm. Normy BS (British Standard) są normami obowiązującymi w Wielkiej Brytanii. Symbol TR (*technical report*) oznacza raport techniczny, IS (*international standard*) oznacza normę międzynarodową. Na końcu normy po dwukropku podawany jest czterocyfrowy rok ustanowienia normy. Wykaz oznaczeń literowych stosowanych w normach i narodowych organizacjach normalizacyjnych znajduje się np. w [WPRZ, Internet 2005c].

Ostatnio coraz więcej firm jest zainteresowanych opracowaniem polityki bezpieczeństwa informacji opartej na odpowiednich normach, np. BS 7799-2: 2002, ISO/IEC TR 13335, ISO/IEC-17799 lub jej polskim odpowiedniku PN-ISO/IEC 17799:2003 (trwają już prace nad wersją ISO/IEC 17799:2005). Przeprowadza się w tym celu liczne seminaria i szkolenia. Bezpieczeństwo informacji (ang. *information security*) obejmuje wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, spójności, dostępności, niezaprzeczalności, rozliczalności i niezawodności informacji lub systemów przetwarzających informacje.

Spośród wielu norm w tabeli 1 wymieniono kilka najpopularniejszych.

Normy ISO 17799 i BS 7799 są rozpoznawanymi, międzynarodowymi standardami (zbiorami praktyk) w zakresie bezpieczeństwa informacji elektronicznej, papierowej i ustnej. Stanowią kontynuację rozwiązań wdrożonych w zakresie ISO 9001, ISO 14001, PN-N 18001 i umożliwiają pełną integrację z powyższymi systemami. Opisują możliwe sytuacje utraty informacji w organizacji, uwzględniają aspekty teleinformatyczne, organizacyjne, ludzkie, bezpieczeństwo fizyczne i

prawne. Można je wykorzystać w każdej organizacji (np. zajmującej się produkcją, usługami, administracją). Opierają się na analizie ryzyka utraty informacji, a nie na sztywnych wymaganiach, przez co są wiarygodne.

Tabela 1. Zestawienie wybranych norm

Normy brytyjskie	Normy międzynarodowe i raporty techniczne	Norma polska	Wersje w opracowaniu
BS 7799-1:2002	ISO/IEC IS 17799: 2000	PN ISO/IEC 17799:2003	ISO-IEC 17799:2005
BS 7799-2:2002	ISO/IEC TR 13335-1:1997	PN-I-07799-2:2004	ISO/IEC IS 13335-2:2006
	ISO/IEC TR 13335-1:2000	PN-I-13335-1:1999	
	ISO/IEC TR 13335-1:2001	ISO/IEC TR 13335-2: 2003	
	ISO/IEC TR 13335-1:2004	ISO/IEC TR 13335-3: 2003	
	ISO/IEC TR 13335-2:1998		
	ISO/IEC TR 13335-3:1998		
	ISO/IEC TR 13335-4:2000		
	ISO/IEC TR 13335-5:2001		

Źródło: opracowanie własne.

Coraz więcej firm i organizacji jest zainteresowanych wdrożeniem odpowiedniego systemu zabezpieczenia informacji ze względu na spodziewane liczne korzyści, takie jak pewniejsze działanie w sytuacji zagrożeń wywoływanych przez czynniki wewnętrzne i zewnętrzne, dobra organizacja pracy, zgodność z wymaganiami prawnymi, oszczędności finansowe, ochrona interesów firmy i dobrego wizerunku firmy, podnoszenie kwalifikacji pracowników poprzez szkolenia oraz zwiększanie konkurencyjności wobec innych firm.

Lekceważenie zasad bezpieczeństwa danych i niezabezpieczanie informacji może narazić firmę na straty materialne i podejmowanie niewłaściwych decyzji, utratę danych lub podejmowanie decyzji na podstawie danych nieprawdziwych lub niespójnych, utratę wiarygodności i dobrego wizerunku wśród klientów, a czasem spowodować pociągnięcie firmy do odpowiedzialności karnej lub cywilnej.

Z bezpieczeństwem danych pośrednio jest również związane bezpieczeństwo wszelkich dokumentów w biurze, sposób ich obiegu, przechowywania, archiwizacji i niszczenia. Zbiór przepisów związanych z tą tematyką znajduje się np. na stronie internetowej [WB, Internet 2005b].

Normy brytyjskie. Brytyjskim standardem stanowiącym podstawę systemów zarządzania bezpieczeństwem informacji opracowanym w 1995 r. przez BSI (British Standards Institute) jest norma BS 7799. Norma ta zawiera ok. 130 zdefiniowanych wymagań związanych z bezpieczeństwem informacji, m.in. z organiza-

cją systemu bezpieczeństwa (*organizational information protection*), odpowiedzialnością kierownictwa (*policy*), pracownikami (*people issues*), sposobami kontroli dostępu, rozwoju i utrzymania systemu (*system access control, development and maintenance*); zarządzanie systemem i infrastrukturą (*system and infrastructure management*), ochroną fizyczną zasobów (*physical protection*), planowaniem zmian czyli ciągłości prowadzenia biznesu (*business continuity planning*), zgodnością z wymaganiami zewnętrznymi (*compliance*), warunkami pracy. Norma BS 7799:1999 składa się z dwóch części: BS 7799-1:1999 i BS 7799-2:1999. Obecnie ok. 800 firm na świecie (głównie z Wielkiej Brytanii i Japonii, a ostatnio również z Włoch, Niemiec i Finlandii) stosuje normę BS 7799.

Norma BS 7799:2002 zawiera dwie części:

- BS 7799-1:2002 – standardowy kodeks praktyki, katalog zagadnień, jakie należy uwzględniać w ramach zapewniania bezpieczeństwa informacji (Code of Practice for Information Security Management);
- BS 7799-2:2002 – standardową specyfikację dla systemów zarządzania bezpieczeństwem informacji (Information Security Management System. Specification with Guidance for Use).

Główne korzyści wynikające z wdrożenia normy BS 7799 to korzyści biznesowe i marketingowe, takie jak podniesienie skuteczności zabezpieczenia odpowiednich zasobów, zwiększenie wiarygodności i zaufania u klientów oraz zwiększenie konkurencyjności.

Norma brytyjska BS 7799-1 została zgłoszona przez BSI do ISO jako podstawa ustanowienia międzynarodowego standardu zarządzania bezpieczeństwem informacji. Nadany został jej numer ISO/ IEC 17799-1 i w lutym 2000 r. rozpoczął się proces legislacyjny, zakończony w sierpniu 2000 roku. Zdezaktualizowana brytyjska norma BS 7799-2:1999 październik 2002 r. została zastąpiona normą BS 7799-2:2002, w celu zharmonizowania jej z innymi normami systemów zarządzania, takimi jak BS EN ISO 9001:2000 (polski odpowiednik PN-EN ISO 9001:2001) i BS EN ISO 14001:1996, oraz w celu wprowadzenia modelu **PDCA** (**plan-do-check-act**, czyli planuj-wykonaj-sprawdzaj-działaj) w podejściu do tworzenia, wdrażania i zwiększania efektywności systemów informacyjnych i sieci oraz systemu zarządzania bezpieczeństwem informacji (ISMS – *information security management system*) w organizacji. Etap **Plan** obejmuje określenie polityki bezpieczeństwa, **Do** – wdrożenie i eksploatację wybranej polityki, procesów i procedur, **Check** – monitorowanie, przeglądanie ISMS, wyciąganie wniosków i przekazywanie ich kierownictwu, **Act** – podejmowanie działań korygujących w celu doskonalenia ISMS.

Normy międzynarodowe. Zestawienie kilku ważniejszych norm międzynarodowych i raportów technicznych w dziedzinie IT (*information technology*) znajduje się w tab. 2.

Tabela 2. Zestawienie wybranych norm międzynarodowych

Norma	Tytuł
ISO/IEC IS 17799: 2000	IT. Code of Practice for Information Security Management
ISO/IEC TR 13335-1:1997	IT. Concepts and Models for IT Security
ISO/IEC TR 13335-1:2004	Concepts and Models for Information and Communications Technology Security Management
ISO/IEC TR 13335-2:1998	IT. Managing and Planning IT Security
ISO/IEC TR 13335-3:1998	IT. Techniques for The Management of IT Security
ISO/IEC TR 13335-4:2000	IT. Selection of Safeguards
ISO/IEC TR 13335-5:2001	IT. Management Guidance on Network Security
ISO/IEC 15408-1,2,3	IT. Evaluation Criteria for IT Security
ISO TR 18028-1	IT. Network Security. Part 1. Generalities, Models, Policies and Management. Part 2. Security Gateways. Part 3. Virtual Private Network. Part 4. Remote Access
ISO/IEC 24743:2005	IT. 'Information security management systems requirements specification

Źródło: opracowanie własne.

Międzynarodowa norma ISO/IEC IS 17799:2000 zawiera praktyczne zasady zarządzania bezpieczeństwem informacji oraz określa sposoby postępowania z informacją w firmie, zwracając uwagę na poufność, dostępność i spójność danych. Jest to szczególnie ważne w organizacjach przetwarzających dane poufne, prowadzących produkcję specjalną oraz w firmach obawiających się nieuczciwych działań konkurencji. Norma ta określa podstawowe zagadnienia, metody i środki konieczne do ochrony informacji i obowiązuje w Polsce od połowy 2003 roku. ISO/IEC 17799:2000 jest normą dotyczącą głównie zarządzania, a w dużo mniejszej części – zagadnień technicznych i informatycznych. Norma wskazuje procesy, które powinny być nadzorowane w celu zmniejszenia ryzyka utraty ochrony danych. Norma ISO/IEC-17799 jest tylko zbiorem wytycznych, a nie zaleceń, nie definiuje miary oceny bezpieczeństwa, przez co nie można opracować systemu certyfikacji, przedstawia tylko jedną wybraną metodę opisu, natomiast nie wspomina o innych, np. o GMITS (Guidelines for Management of IT Security Systems – ISO/IEC 13335), wprowadza inną terminologię niż GMITS, zawęża pojęcie bezpieczeństwa.

W fazie opracowywania jest norma ISO/IEC TR 13335-2:2006.

Polskie normy. Obecnie wiele firm polskich stosuje standardy i metody pracy oparte na powszechnie uznanych praktykach oraz polskich i międzynarodowych dokumentach normalizacyjnych z zakresu bezpieczeństwa informacji wymienionych w tab. 3.

Tabela 3. Zestawienie wybranych norm krajowych

Norma	Tytuł
ISO/IEC TR 13335-2:2003	Technika informatyczna. Zarządzanie i planowanie bezpieczeństwa systemów informatycznych
ISO/IEC TR 13335-3:2003	Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych
PN ISO/IEC 17799: 2003	Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji
PN-I-13335-1:1999	Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych
PN-I-07799-2:2004	Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne do stosowania (polskie tłumaczenie normy BS 7799-2:2002)

Źródło: opracowanie własne.

Norma PN-ISO/IEC-17799 jest polskim odpowiednikiem międzynarodowej normy ISO/IEC 17799. Audyt zgodności z normą PN-ISO/IEC-17799 ma na celu zbadanie aktualnego stanu zabezpieczenia zasobów informacyjnych pod względem poufności, integralności i dostępności oraz wskazanie zaleceń związanych z koniecznymi mechanizmami służącymi do ich realizacji. Kontrola obejmuje zabezpieczenia zdefiniowane w przedsiębiorstwie, poprawność ich wdrożenia i funkcjonowania, ich efektywność i wpływ na działalność firmy, natomiast kontroli nie podlega poprawność konfiguracji sprzętu komputerowego i oprogramowania.

Spośród wielu norm krajowych należy również wymienić normę PN-ISO 9000-3:1994 oraz PrPN-ISO 9000-3, które zawierają „Wytyczne do stosowania normy ISO 9001 podczas opracowywania, dostarczania i obsługiwania oprogramowania". Wytyczne te powinny być uwzględniane przy zawieraniu umów dotyczących oprogramowania. Normy te podają metody zarządzania i produkcji oprogramowania spełniającego wymagania nabywcy. Dokument PN-ISO 9000-4:1996 zawiera normy dotyczące zarządzania jakością i zapewnienia jakości oraz wytyczne dotyczące zarządzania programem niezawodności („Quality management and quality assurance standards – Part 4: Guide to dependability programme management").

Warto również wspomnieć o słownikach terminologicznych PN-ISO/IEC 2382 (części od 1 do 34, np. cz. 1 – Terminy podstawowe z 1996 r., cz. 17 – Bazy danych z 2004 r.), które definiują pojęcia m.in. z następujących dziedzin: terminy ogólne, organizacja i reprezentacja informacji, bezpieczeństwo, bazy danych, rozproszone przetwarzanie danych, programowanie komputerów, teoria informacji, języki programowania, niezawodność, obsługiwalność i dostępność, sztuczna inteligencja i grafika komputerowa, sieci komputerowe, lokalne sieci komputerowe (indeksy alfabetyczne w językach polskim, angielskim i francuskim) [WS, Internet 2005d].

4. Bezpieczeństwo systemów komputerowych

Do oceny poziomu bezpieczeństwa systemów komputerowych został opracowany w 1983 r. przez NCSC (National Computer Security Center) amerykański standard bezpieczeństwa TCSEC (Trusted Computer Security Evaluation Criteria), znany jako „Pomarańczowa księga" [„The Orange Book"]. Jest to zestaw kryteriów oceny bezpieczeństwa określonych dla systemów użytkowych różnych sektorów. Wyróżnia się w nim cztery poziomy bezpieczeństwa, oznaczone literami alfabetu: D (poziom najniższy), C, B i A (najwyższy stopień zabezpieczenia systemu) [Stokłosa, Bilski, Pankowski 2001]. W ramach każdego poziomu wyróżniono klasy bezpieczeństwa, określające bezpieczeństwo w taki sposób, że rośnie ono wraz ze wzrostem numeru (liczby). Wszystkie poziomy i klasy charakteryzują się pewnymi właściwościami, spośród których należy wymienić:

- politykę bezpieczeństwa (ang. *security policy*),
- identyfikację, kontrolę i sprawdzanie podmiotu (ang. *accountability*),
- ubezpieczenie eksploatacyjne i okres trwałości ubezpieczenia (ang. *assourance*),
- testy sprawdzające system oraz opis polityki bezpieczeństwa systemu (ang. *documentation*).

System należący do danej klasy musi spełniać wszystkie wymagania stawiane klasie niższej oraz dodatkowe, ściśle sprecyzowane wymagania, np. system klasy B3, oprócz spełnienia wszystkich wymagań przypisanych klasie B2, musi m.in.:

- zapewnić dostęp tylko osobom o odpowiednich prawach,
- wykazywać się odpornością na wszelkie próby ataków i włamań,
- być wystarczająco zwarty, aby można go było poddać analizom i testom,
- charakteryzować się małą złożonością w celu łatwości przeprowadzania analiz,
- mieć wyznaczonego administratora zabezpieczeń, wyposażonego w mechanizmy kontrolne oraz procedury odtwarzania systemu po awarii bez obniżania poziomu bezpieczeństwa.

System tej klasy stosuje dodatkową identyfikację użytkownika za pomocą zewnętrznych protokołów bezpieczeństwa. Wszystkie wymagania muszą być spełnione, aby dostęp został przyznany, a każda próba uzyskania nielegalnego dostępu jest rejestrowana. Istotna jest także izolacja wybranych kanałów komunikacyjnych.

Najwyższy poziom bezpieczeństwa (A1) wymaga realizowania metod weryfikacji, które gwarantują, że zastosowane obowiązkowe i uznaniowe mechanizmy ochrony efektywnie zabezpieczają ważne i poufne dane podczas ich przechowywania i przetwarzania w systemie.

W Europie w 1991 r. opracowano zestaw podobnych kryteriów określanych akronimem ITSEC [Information Technology Security Evaluation Criteria], stanowiący rozszerzenie standardu amerykańskiego. W obu zestawach wyróżnia się prawie dokładnie takie same poziomy bezpieczeństwa. W ITSEC funkcjonalność systemu oceniana jest dodatkowo w aspekcie wierności (która stanowi rozszerzenie

integralności o wykrywanie zmian i zapobieganie takim niepożądanym działaniom), niezawodności pracy (gwarantującej dostęp do zasobów systemu w wymaganym czasie) i wymiany danych (dotyczy bezpieczeństwa transmisji). W ITSEC wyróżniono 10 klas funkcjonalności systemu; niektóre z nich stanowią odpowiedniki standardu amerykańskiego (F-C1, F-C2, F-B1, F-B2, F-B3), inne zawierają dodatkowe, zwiększone wymagania, które nie zostały uwzględnione w „Pomarańczowej księdze" (F-IN, F-AV, F-DI, F-DC, F-DX). Oprócz klas funkcjonalności, ITSEC definiuje również 7 klas pewności, od najmniej pewnego poziomu (E0) do najbardziej pewnego (E6). Każdy kolejny poziom stanowią wymagania objęte poziomem niższym, uzupełnione o dodatkowe wymagania.

Poziom wbudowanych zabezpieczeń systemu operacyjnego dla poszczególnych sektorów (wojskowość, bankowość, sektor rządowy) jest określony przez spełnianie dodatkowo innych, specyficznych wymagań. W przypadku niektórych systemów kładzie się szczególny nacisk na takie cechy, jak identyfikacja nadawcy i odbiorcy, niezaprzeczalność nadania i odbioru itp. Na przykład dla sektora bankowego istnieją standardy w kilku wersjach różniących się poziomem bezpieczeństwa (wersja standardowa – o poziomie niższym, wersja o podwyższonym poziomie bezpieczeństwa oraz wersja o wysokim poziomie bezpieczeństwa), które muszą spełniać kryteria wybranych poziomów omówionych standardów.

5. Podsumowanie

Często bezpieczeństwo systemu informatycznego oparte jest na wiedzy i intuicji informatyka, na niejasnych zasadach funkcjonowania i zależy od poziomu świadomości możliwych zagrożeń jego użytkowników. Dlatego tak ważne jest określenie precyzyjnej polityki bezpieczeństwa, najlepiej opartej na sprawdzonych normach i standardach, wyznaczenie zespołu odpowiednio przeszkolonych ludzi odpowiedzialnych za tę politykę i przydzielenie im konkretnych zadań, określenie i spisanie procedur tworzenia kopii zapasowych i odtwarzania danych po awarii, śledzenia wydajności pracy, reagowania na zmiany i okresowej reorganizacji dla podniesienia wydajności, opracowanie scenariuszy postępowania w sytuacjach kryzysowych (brak prądu, pożar, huragan, katastrofa budowlana, włamanie, akcja terrorystyczna), prowadzenie ciągłej dokumentacji, a także inwentaryzacji i kopii zapasowych.

W pracy omówiono zagadnienia związane z bezpieczeństwem systemów informatycznych i przeprowadzaniem audytów bezpieczeństwa. Przedstawiono wybrane normy bezpieczeństwa. Praca w żaden sposób nie wyczerpuje poruszanej tematyki, która jest niezwykle obszerna i obecnie bardzo popularna i ważna. Zapewnienie bezpieczeństwa systemów komputerowych (danych, sprzętu itd.) stanowi obecnie priorytetowe zadanie dla wszystkich firm i organizacji.

Literatura

Stokłosa J., Bilski T., Pankowski T., *Bezpieczeństwo danych w systemach informatycznych*, WNT, Warszawa-Poznań 2001.
ISO, http://www.iso.org/iso/en/aboutiso, Internet 2005a.
WB, http://biuro.dokumenta.pl/?s=3,2, Internet 2005b.
WPRZ, http://www.prz.rzeszow.pl/biblio/oznacz.htm, Internet 2005c.
WS, http://www.citib.hg.pl/citib/normy/01.040.35.htm, Internet 2005d.

INFORMATION SYSTEMS SECURITY NORMS

Summary

The work presents Polish and international norms for the security of electronic, written and spoken information and information computer systems. We also analyse the aspect of the security level in the context of carrying out audits.

Mgr Hanna Mazur jest pracownikiem Instytutu Informatyki Stosowanej Wydziału Informatyki i Zarządzania Politechniki Wrocławskiej
e-mail: hanna.mazur@ pwr.wroc.pl

Dr hab. Zygmunt Mazur jest profesorem nadzwyczajnym Politechniki Wrocławskiej, pracownikiem Instytutu Informatyki Stosowanej Wydziału Informatyki i Zarządzania Politechniki Wrocławskiej
e-mail: zygmunt.mazur@ pwr.wroc.pl

Dr inż. Teresa Mendyk-Krajewska jest pracownikiem Instytutu Informatyki Stosowanej Wydziału Informatyki i Zarządzania Politechniki Wrocławskiej
e-mail: teresa.mendyk-krajewska @ pwr.wroc.pl