Halina Tańska

Wydział Matematyki i Informatyki
Uniwersytet Warmińsko-Mazurski w Olsztynie

Agnieszka Władzińska

Zeto Software (Olsztyn)

Zróżnicowane aspekty bezpieczeństwa wytwarzanych systemów informatycznych

1. Wstęp

Konstruując system, zakłada się zwykle, że będzie on pracował w określonych warunkach. Bezpieczeństwo jest więc jednym z ważniejszych czynników (endo- i egzogenicznych) w procesie wytwarzania oprogramowania[1]. Powszechnie jest utożsamiane z podejmowaniem decyzji dotyczących szeregu zabezpieczeń mających na celu zapewnienie poufności, integralności i dostępności do informacji związanych z procesami wytwarzania oprogramowania oraz informacjami przetwarzanymi w systemach informatycznych. Warto uwzględnić również aspekt związany z zapewnieniem bezpieczeństwa użytkownikom korzystającym z wytworzonych już systemów za pomocą zaimplementowania odpowiednich funkcjonalności, gwarantujących bezpieczne przetwarzanie informacji. Wdrożenie odpowiednich procedur bezpieczeństwa pozwoli firmom na szybkie reagowanie i elastyczne działania w razie wystąpienia awarii, incydentów i ataków.

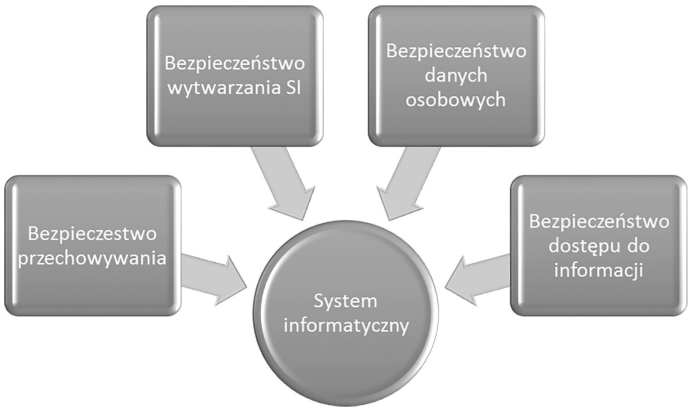
Ważne jest – jak pisze Ł. Kaliś – by pamiętać, że „zabezpieczenie informatyczne powinno wpisywać się w ogólną politykę bezpieczeństwa informacji, tzn. powinno być kilkuetapowe i kompleksowe, aby wykluczyć słabe punkty łańcucha bezpieczeństwa. Punkty zapalne powinny zostać formalnie zdefiniowane w formie procedur, a sam zakres zagrożeń – omówiony i wyjaśniony pracownikom”[2].

---

[1] Każde niespełnione wymaganie, każda awaria i każde naruszenie ochrony mogą spowodować nieprzewidziane działanie systemu.

[2] Ł. Kaliś, *Praktyczne zalecenia w zarządzaniu bezpieczeństwem informacji*, w: *Wybrane problemy zarządzania bezpieczeństwem informacji*, red. J. Brdulak, P. Sobczak, Oficyna Wydawnicza SGH, Warszawa 2014, s. 105.

Na rysunku 1 zobrazowano cztery warstwy mające istotne znaczenie w procesie wytwarzania systemu informatycznego, w tym bezpieczeństwo dostępu do informacji, bezpieczeństwo danych osobowych itd.



Rysunek 1. Płaszczyzny (warstwy) bezpieczeństwa
Źródło: opracowanie własne.

Warto przeanalizować różne aspekty bezpieczeństwa systemów informatycznych[3], mające w kontekście procesu wytwarzania systemów, a następnie ich użytkowania istotny wpływ na zapewnienie bezpieczeństwa informacji.

2. Zapewnienie bezpieczeństwa podczas procesu wytwarzania systemów informatycznych

Wytwarzanie systemów informatycznych to bardzo skomplikowany proces, składający się z różnorodnych elementów oraz absorbujący wiele zasobów (zarówno ludzkich, jak i infrastrukturalnych). Warunkiem koniecznym zapewnienia

[3] Międzynarodowa Organizacja Normalizacyjna (ISO) zajęła się zagadnieniem bezpieczeństwa i utworzyła międzynarodowe standardy dotyczące zarządzania bezpieczeństwem w organizacji. Standardy te obowiązują również w Polsce i są to: PN-ISO/IEC 27001:2007 – technika informatyczna, technika bezpieczeństwa, systemy zarządzania bezpieczeństwem informacji; PN-ISO/IEC 17799:2007 – technika informatyczna, technika bezpieczeństwa, praktyczne zasady zarządzania bezpieczeństwem informacji. B. Księżopolski, P. Szałachowski, *Audyt bezpieczeństwa systemów IT – ścieżka techniczna (rekonesans i skanowanie)*, Wydawnictwo UMCS, Lublin 2011, s. 7.

bezpieczeństwa wytwarzania oprogramowania jest określenie jasnych zasad, reguł, procedur obowiązujących wszystkie osoby biorące udział w tym procesie. Szczególnie chodzi tu o zasady dotyczące: postępowania z różnymi nośnikami informacji, tworzenia repozytoriów, dokumentacji i kodów źródłowych, odpowiedniego zabezpieczanie tych repozytoriów, archiwizacji dokumentacji powstającej podczas procesu wytwarzania. Należy uwzględnić (ustalić) także zasady określające postępowanie z danymi osobowymi (jeżeli dostęp do nich jest konieczny w trakcie wytwarzania oprogramowania, zwłaszcza gdy testuje się oprogramowanie na kopii systemu produkcyjnego) oraz bezpieczeństwo dostępu do informacji niezbędnych do tworzenia oprogramowania (standardy wytwarzania, system uprawnień do odpowiednich zasobów zależne od rodzaju wykonywanej pracy).

Do przechowywania dokumentacji w zakresie kodów źródłowych stosuje się bardzo popularne repozytorium CVS[4]. Jego funkcjonalność pozwala zabezpieczyć powstające kody na każdym etapie wytwarzania i w razie potrzeby wrócić do odpowiedniej wersji oprogramowania. Do przechowywania dokumentacji projektowej, analitycznej i testowej stosuje się repozytorium SVN[5]. Podobnie jak poprzednie narzędzie pozwala na każdym etapie wytwarzania wrócić do odpowiedniej wersji dokumentacji, jednak zdecydowanie lepiej sprawdza się w przechowywaniu dokumentacji w formie tekstowej.

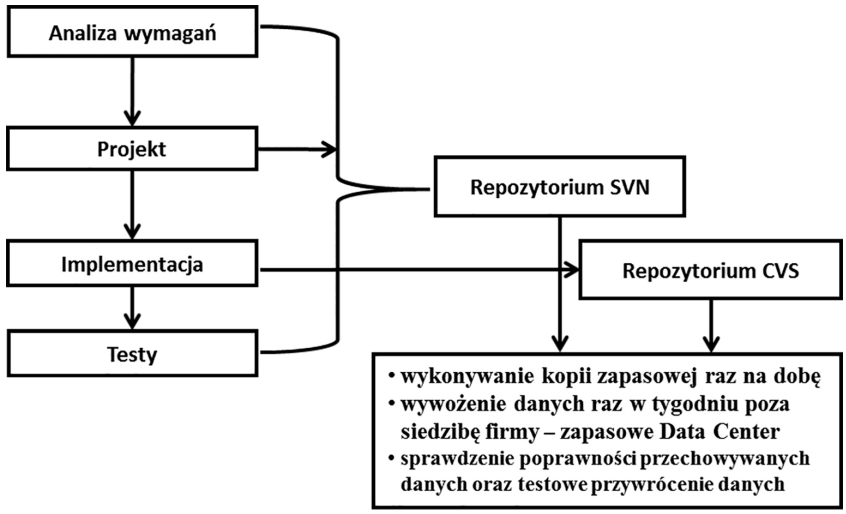
Dane gromadzone w repozytoriach powinny być archiwizowane przynajmniej raz na dobę, aby w przypadku awarii koszt straty i odtworzenia tych danych nie był zbyt duży. Zarchiwizowane dane nie powinny być przechowywane na tych samych nośnikach co dane w repozytoriach. Preferowane jest również wywożenie tych nośników poza siedzibę firmy wytwarzającej oprogramowanie (bezpieczeństwo fizyczne).

Podczas wytwarzania systemów informatycznych istotną rolę odgrywają także zasady organizacyjne obowiązujące zarówno kierownictwo szczebla strategicznego, jak i osoby z niższych szczebli, szczególnie bezpośrednio zaangażowane w proces wytwarzania oprogramowania. Chodzi tu o określenie: stref

[4] *Concurrent Version System* (CVS) to system kontroli wersji udostępniany na licencji GPL (*General Public License*). Przeznaczony do pracy grupowej nad kodem programów lub projektów realizowanych w zapisie elektronicznym.

[5] *Subversion* (znany również jako SVN) to system kontroli wersji, który powstał w celu zastąpienia CVS. Z założenia SVN jest w większości przypadków funkcjonalnie zgodny ze swoim poprzednikiem, z kompatybilności zrezygnowano tam, gdzie było to niezbędne do wprowadzenia nowych rozwiązań. SVN jest wolnym i otwartym oprogramowaniem na licencji Apache.

dostępu do odpowiednich pomieszczeń, zasad poruszania się osób trzecich, zasad pozostawiania informacji na urządzeniach pomocniczych (tj. drukarka, tablica, ekran komputera), zasad identyfikacji osób, zasad stosowania ochrony antywirusowej oraz legalnego oprogramowania. Przykładowa procedura zabezpieczająca wytwarzanie oprogramowania została przedstawiona w syntetyczny sposób na rysunku 2.



Rysunek 2. Przykładowa procedura zabezpieczenia danych

Źródło: opracowanie własne na podstawie: J. Górski, *Inżynieria oprogramowania*, Wydawnictwo Naukowe PWN, Warszawa 2011; K. Sacha, *Inżynieria oprogramowania*, Wydawnictwo Naukowe PWN, Warszawa 2010.

Opracowanie skutecznych zabezpieczeń jest zagadnieniem obszernym i bardzo złożonym. Wymaga więc ciągłej uwagi i systematyczności na każdym etapie projektowania[6]. Praktyka wskazuje, że decydujące znaczenie mają etapy „analiza wymagań" i „projektowanie", błędy popełnione w ich trakcie mogą być bowiem trudne do naprawienia w kolejnych etapach. Procedura przedstawiona na rysunku 2 składa się z siedmiu etapów, w których aktywnie uczestniczy zespół, w tym analityk, projektant, programista, tester oraz administrator danych. Wspólne działania doprowadzą do stworzenia repozytorium SVN i repozytorium CVS.

[6] B. Bereza-Jarociński, B. Szomański, *Inżynieria oprogramowania. Jak zapewnić jakość tworzonym aplikacjom*, Helion, Gliwice 2009.

3. Zapewnienie bezpieczeństwa danych osobowych przechowywanych w systemach informatycznych

W wielu systemach informatycznych są przechowywane dane osobowe (zasoby krytyczne, newralgiczne). Systemy te muszą zapewnić bezpieczeństwo przechowywania i przetwarzania tych danych. Niezbędne jest określenie i wprowadzenie odpowiednich funkcjonalności, które zabezpieczą użytkowników przed nieuprawnionym dostępem. Przykładowo, powinien istnieć odpowiedni system uprawnień lub system do gromadzenia logów z pracy użytkowników. Każdy system przetwarzający i przechowujący dane osobowe powinien zapewnić w sposób przejrzysty możliwość kontroli dostępu do tych danych, a każda organizacja powinna zabezpieczyć to odpowiednią procedurą.

Zapewnienie bezpieczeństwa przechowywanych danych osobowych jest warunkiem niezbędnym funkcjonowania systemów wytwarzanych i użytkowanych przez administrację publiczną. Minimalne zasady zabezpieczeń stosowanych w tych systemach określa rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[7]. Dokument ten został opracowany na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Rozporządzenie to określa:

- Krajowe Ramy Interoperacyjności;
- minimalne wymagania wobec rejestrów publicznych i wymiany informacji w postaci elektronicznej;
- minimalne wymagania wobec systemów teleinformatycznych, tzn. specyfikację formatów danych oraz protokołów komunikacyjnych i szyfrujących, które mają być stosowane w oprogramowaniu interfejsowym, sposoby zapewnienia bezpieczeństwa przy wymianie informacji, standardy techniczne zapewniające wymianę informacji z udziałem podmiotów publicznych z uwzględnieniem wymiany transgranicznej oraz sposoby zapewnienia dostępu do zasobów informacji podmiotów publicznych osobom niepełnosprawnym.

Szczególnie systemy informatyczne używane przez podmioty administracji publicznej powinny mieć opracowaną architekturę, tzn. opis systemu, powiązań i relacji pomiędzy jego składnikami. Odpowiednie udokumentowanie systemu

[7] http://isap.sejm.gov.pl/DetailsServlet?id=WDU20120000526.

informatycznego zapewnia niezależność w rozwoju, naprawie i usprawnianiu zakresu funkcjonalnego. Praktyka dowodzi, że uzależnienie się od jednego wykonawcy, brak wiedzy na temat zasad działania systemów wiążą się z ogromnym ryzykiem podejmowanym przez użytkownika.

Systemy informatyczne używane przez podmioty administracji publicznej powinny zapewniać autentyczność przechowywanych danych. Oznacza to, że pochodzenie lub zawartość danych opisujących obiekt są takie jak deklarowane. Ponadto powinny zawierać dane referencyjne, czyli dane opisujące cechę informacyjną obiektu pierwotnie wprowadzone do rejestru publicznego w wyniku określonego zdarzenia, opatrzone atrybutem autentyczności.

Inne cechy wskazane w rozporządzeniu to m.in.:

- dostępność – właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
- integralność – właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony.

Określone ustawodawstwo w jasny sposób precyzuje również sposoby postępowania podmiotu realizującego zadania publiczne w zakresie doboru środków, metod i standardów wykorzystywanych do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i udoskonalania systemu teleinformatycznego wykorzystywanego do realizacji zadań tego podmiotu oraz procedur organizacyjnych.

4. Bezpieczeństwo dostępu do informacji

System uprawnień to niezbędny element zapewnienia bezpieczeństwa dostępu do danych przechowywanych i przetwarzanych w programach informatycznych. Odpowiednia granulacja tego systemu gwarantuje niezbędny poziom bezpieczeństwa. Każdy użytkownik systemu powinien mieć przypisaną rolę, dla której zdefiniowano zestaw uprawnień do odpowiednich funkcjonalności lub grup funkcjonalności. Natomiast odpowiednia kontrola nad uprawnieniami w systemie zmniejsza ryzyko dostępu przez osoby nieuprawnione.

Tabela 1 zawiera przykładową siatkę uprawnień uwzględniającą funkcjonalność, rolę wybranych pracowników, a także działania oznaczone odpowiednio: RW to możliwość zapisu i odczytu, RO to tylko odczyt, – to brak uprawnień

dostępu. Zakres dostępnych funkcji został określony w zależności od stanowiska zajmowanego przez pracownika.

Tabela 1. System praw dostępu w procesie wytwarzania oprogramowania

Rola / Funkcjonalność	Kierownik działu	Pracownik	Stażysta	Administrator
Administracyjna	RW	RW	RW	RW
Obsługa kontrahentów	RW	RO	–	RW
Sporządzanie raportów	RW	RO	RW	RW
Przygotowanie harmonogramów	RW	RW	RW	RW
Przygotowanie wydruków	RW	RW	RO	RW
Przygotowanie umowy	RW	RW	RO	RW
Wystawianie faktury	RW	RW	RW	RW
Przydzielanie zadań	RW	RW	-	RW
Zakup środków trwałych	RW	RW	-	RW
Zarządzanie produktami	RW	RW	RW	RW
Sporządzanie zestawień	RW	RW	RW	RW
Zarządzanie produkcją	RW	RW	RO	RW

Źródło: opracowanie własne.

Zwykle przez pojęcie systemu uprawnień rozumie się odpowiedni system praw dostępu dla pracowników uczestniczących w procesie wytwarzania oprogramowania, zarządzany przez kierownika danego projektu. Ważnym czynnikiem tego procesu jest zdefiniowanie, a następnie zarządzanie i monitorowanie systemem uprawnień w kontekście zasobów[8]. Odpowiednie uprawnienia mogą być przyznawane na cały czas trwania projektu lub na czas realizacji określonego zadania. Przykładem tego może być danie analitykowi dostępu do dokumentacji analitycznej, listy wymagań lub modelu dziedziny wytwarzanego systemu. Programista powinien mieć dostęp do kodów źródłowych i odpowiedniej dokumentacji analitycznej, tester – do planów testów i przypadków testowych. Kierownik projektu to odpowiednik administratora w systemie uprawnień, tzn. osoba, która ma dostęp do całej dokumentacji i odpowiednio zarządza całym procesem wytwarzania oprogramowania[9].

[8] R. Cegiełka, A. Zalewski, *Racjonalne zarządzanie przedsięwzięciami informatycznymi i systemami komputerowymi*, Wydawnictwo Nakom, Poznań 2000, 190–191.

[9] J. Górski, *Inżynieria oprogramowania*, Wydawnictwo Naukowe PWN, Warszawa 2011.

Jednym z istotnych czynników zapewnienia bezpieczeństwa jest prowadzenie polityki bezpiecznych haseł. Dotyczy to zarówno procesu wytwarzania, jak i odpowiednich funkcjonalności zaimplementowanych w systemach informatycznych. Hasła powinny być unikalne w skali całego systemu oraz składać się z minimum ośmiu znaków. Hasła nie mogą być oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imion, numerów telefonów, daty urodzenia itp. Zaleca się, by były złożone z małych i wielkich znaków, liter, cyfr oraz znaków specjalnych. Jednocześnie powinny być łatwe do rozszyfrowania dla jego autora. W celu uniknięcia ryzyka ataku słownikowego hasła nie powinny składać się ze słów zamieszczonych w słownikach języka polskiego lub np. angielskiego. Nie mogą zawierać ciągu jednakowych znaków ani być złożone z samych cyfr lub liter. System informatyczny lub procedura organizacyjna powinna przynajmniej raz w miesiącu wymuszać zmianę hasła. Żadne z nadanych haseł nie może powtarzać się w ciągu określonego przedziału czasowego, np. roku.

5. Bezpieczeństwo przechowywania informacji w systemach informatycznych

M. Cieciura zwraca uwagę na fakt, że utrata cennych danych lub poufnych informacji w organizacji może spowodować nieobliczalne skutki. Ponadto kradzież czy zniszczenie informacji nie tylko zagraża przestojem w sprawnym funkcjonowaniu organizacji, ale również może doprowadzić do jej bankructwa[10].

Bezpieczeństwo przechowywania informacji w systemach informatycznych to także odpowiedni system backupu oraz archiwizacja danych. Archiwizacja może odbywać się w sposób fizyczny (automatyczna lub ręczna) oraz logiczny, tzn. w logikę systemu jest wbudowany odpowiedni algorytm archiwizowania.

Zakłada się, że backup danych z systemu wykonuje się raz na dobę, a w przypadku danych, które nie ulegają częstym zmianom, raz na tydzień. Dane pochodzące z backupu powinny być przechowywane na dyskach niezależnych od stacji, na których są zainstalowane systemy informatyczne. Wskazane jest również przechowywanie tych danych w innych pomieszczeniach lub budynkach,

[10] M. Cieciura, *Podstawy technologii informacyjnych z przykładami zastosowań*, Vizja Press&IT, Warszawa 2006.

zwłaszcza jeżeli chodzi o dane wyjątkowo wrażliwe. Pomieszczenia te powinny mieć odpowiedni system dostępu.

Archiwizacja danych jest niezbędna zwłaszcza w systemach, w których następuje bardzo szybki przyrost wielkości danych. Podobnie jak w przypadku backupu dane zarchiwizowane powinny być przechowywane w wyznaczonych do tego pomieszczeniach, najlepiej innych niż eksploatowane systemy informatyczne. Odpowiedni mechanizm archiwizacji ma również wpływ na wydajność działania systemu. Dane zarchiwizowane nie podlegają mechanizmom przetwarzania i nie uczestniczą w procesach biznesowych.

6. Procedury zarządzania bezpieczeństwem informacji

Dobrą praktyką stosowaną w wielu przedsiębiorstwach wytwarzających oprogramowanie jest wprowadzenie wystandaryzowanych procedur zarządzania bezpieczeństwem informacji. Wytyczne do wprowadzenia takich procedur określa międzynarodowa norma ISO/IEC 27001. Zgodnie z nią wyspecyfikowano 11 obszarów, które mają wpływ na bezpieczeństwo. Są to: polityka bezpieczeństwa, organizacja bezpieczeństwa informacji, zarządzanie aktywami, bezpieczeństwo zasobów ludzkich, bezpieczeństwo fizyczne i środowiskowe, zarządzanie systemami i sieciami, kontrola dostępu, zarządzanie ciągłością działania, pozyskiwanie, rozwój i utrzymanie systemów informatycznych, zarządzanie incydentami związanymi z bezpieczeństwem informacji, zgodność z wymaganiami prawnymi i własnymi standardami.

Autorki dokonały analizy rejestrowanych zdarzeń mających wpływ na bezpieczeństwo informacji w jednym z przedsiębiorstw, w którym od 2010 r. stosuje się procedury zarządzania bezpieczeństwem informacji. W związku z tym są rejestrowane zdarzenia niezgodności z wprowadzonymi procedurami. Zestawienie liczbowe dotyczące lat 2010–2014 przedstawia tabela 2.

Łatwo zauważyć, że liczba zdarzeń maleje, co może świadczyć o dojrzałości procedur oraz rosnącej świadomości pracowników firmy. W tabeli 2 zaznaczono pogrubioną czcionką zdarzenia spowodowane czynnikami zewnętrznymi, niezależnymi od pracowników przedsiębiorstwa, np. awarię zasilania lub atak na serwis WWW. Pozostałe incydenty mają charakter wewnętrznych problemów związanych z przestrzeganiem procedur, np. używanie nielegalnego oprogramowania lub niewłaściwy nadzór nad kluczami biurowymi. Należy podkreślić

fakt, że incydenty zewnętrzne stanowią zaledwie 30% wszystkich zarejestrowanych zdarzeń.

Tabela 2. Zestawienie liczby zdarzeń związanych z naruszeniem procedur bezpieczeństwa

Rodzaj zdarzeń	Liczba zdarzeń w latach				
	2010	2011	2012	2013	2014
Łącze internetowe	**–**	**1**	**–**	**1**	**–**
Sieć	**–**	**3**	**1**	**2**	**3**
Zasilanie	**1**	**4**	**–**	**1**	**–**
Oprogramowanie	1	–	–	1	–
Pliki	1	–	–	1	–
Uprawnienia	3	–	–	2	–
Baza danych	–	–	–	1	–
Klucze	4	3	–	1	1
Dane	1	–	2	2	2
Serwer danych	–	2	4	–	1
Awaria systemu	–	1	2	–	–
Okablowanie	**–**	**–**	**1**	**–**	**–**
Serwer WWW	1	1	1	–	1
Stacja robocza	–	–	–	–	1
Centrala telefoniczna	1	–	–	–	–
Budynek	–	–	–	–	1
Suma zdarzeń	9	12	11	15	14

Źródło: opracowanie własne.

7. Podsumowanie

Reasumując, trzeba stwierdzić, że bezsporne wydaje się zastosowanie odpowiedniego systemu zabezpieczeń zarówno w różnych aspektach związanych z procesem wytwarzania oprogramowania, jak i w ramach eksploatowanych systemów. Odpowiednie mechanizmy adekwatne do wartości i wrażliwości danych gwarantują prawidłowe działania w tym zakresie. Należy jednak pamiętać o tym, że najważniejszy w tych wszystkich przypadkach jest czynnik ludzki, który niestety jest najbardziej zawodny. Żadne funkcjonalności ani wprowadzone procedury nie zastąpią rozsądku i dyscypliny, których niejednokrotnie brakuje, stąd powstają liczne nieprawidłowości.

Trudności, które często pojawiają się w trakcie tworzenia i eksploatacji systemu informatycznego spełniającego wysokie wymagania w zakresie bezpieczeństwa, oznaczają zagrożenie dotyczące jego bezpieczeństwa i niezawodności, a także nieodpowiedniego wykorzystania produktu informatycznego. Opracowanie skutecznych zabezpieczeń jest problemem bardzo złożonym. Wymaga więc systematyczności na każdym etapie projektowania.

Bibliografia

Bereza-Jarociński B., Szomański B., *Inżynieria oprogramowania. Jak zapewnić jakość tworzonym aplikacjom*, Helion, Gliwice 2009.

Cegiełka R., Zalewski A., *Racjonalne zarządzanie przedsięwzięciami informatycznymi i systemami komputerowymi*, Wydawnictwo Nakom, Poznań 2000.

Cieciura M., *Podstawy technologii informacyjnych z przykładami zastosowań*, Vizja Press&IT, Warszawa 2006.

Górski J., *Inżynieria oprogramowania*, Wydawnictwo Naukowe PWN, Warszawa 2011.

Kaliś Ł., *Praktyczne zalecenia w zarządzaniu bezpieczeństwem informacji*, w: *Wybrane problemy zarządzania bezpieczeństwem informacji*, red. J. Brdulak, P. Sobczak, Oficyna Wydawnicza SGH, Warszawa 2014.

Księżopolski B., Szałachowski P., *Audyt bezpieczeństwa systemów IT – ścieżka techniczna (rekonesans i skanowanie)*, Wydawnictwo UMCS, Lublin 2011.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz. U. z 2004 r. Nr 100, poz. 1024.

Sacha K., *Inżynieria oprogramowania*, Wydawnictwo Naukowe PWN, Warszawa 2010.

Źródła sieciowe

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. z 2012 r. poz. 526, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20120000526.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 1997 r. Nr 133, poz. 883, http://isap.sejm.gov.pl/DetailsServlet?id=WDU19971330883.

* * *

Diversified manufacturing safety aspects of information systems

Summary

Due to the complexity of the issue, this paper discusses only some aspects of information systems security. Security is perceived as the ability of the system to avoid or prevent actions that pose danger to people or to the environment.

Keywords: personal data security, safety access to information, secure information storage