ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2012
Seria: ORGANIZACJA I ZARZĄDZANIE z. 61 Nr kol. 1873

Ireneusz J. JÓŹWIAK
Wydział Informatyki i Zarządzania,
Politechnika Wrocławska

Artur SZLESZYŃSKI
Wydział Zarządzania,
Wyższa Szkoła Oficerska Wojsk Lądowych
im. gen. T. Kościuszki we Wrocławiu

OCENA WPŁYWU ZABEZPIECZEŃ NA POZIOM OCHRONY ZASOBÓW INFORMACYJNYCH W SYSTEMACH TELEINFORMATYCZNYCH

Streszczenie. W artykule przedstawiono metodę oceny wpływu zabezpieczeń na funkcjonowanie elementów systemu teleinformatycznego. Prezentowane treści zostały zilustrowane dwoma przykładami. Na ich podstawie przedstawiono wymagania bezpieczeństwa oraz sposób ich oceny. Istotne jest stwierdzenie, czy wdrożone wymaganie poprawia poziom bezpieczeństwa systemu, czy jest przyczyną nieprawidłowego działania systemu. Porównano aktualny poziom zabezpieczeń obiektu ze stawianymi wymaganiami.

EVALUATION OF SAFEGUARDS INFLUENCE ON PROTECTION LEVEL OF INFORMATION RESOURCES IN INFORMATION AND TELECOMMUNICATION SYSTEMS

Summary. In the paper, a method of evaluation the safeguards influence on operate system's elements is presented. Content on the basis of two examples of ITC systems is presented. For both of them security requirements and the methods of evaluation are presented. It is important to show if implemented requirement improves a level of object security or if it is a source of disturbance in the system operation. During a process of evaluation, the current state of object's protection is compared to what is suggested by requirement state of protection.

1. Wprowadzenie

Ochrona zasobów informacyjnych jest wymagana przez regulacje prawne oraz potrzeby biznesowe podmiotów. Termin potrzeby biznesowe należy rozumieć jako zapewnienie ciągłości działania danej organizacji, wykorzystującej zasoby informacyjne. Norma PN ISO/IEC-17799 stwierdza, że zasoby informacyjne należy traktować na równi z innymi zasobami znajdującymi się w posiadaniu firmy lub instytucji [8]. Chcąc określić oczekiwania dotyczące ochrony, jakie będzie miał podmiot eksploatujący zasoby informacyjne, należy opracować dokument zawierający zbiór wymagań bezpieczeństwa. Wymagania te zawierają opis zasobu oraz potencjalnych zagrożeń związanych z danym zasobem. Definiują sposób ochrony zasobu oraz metody oceny uzyskanych efektów [5]. Metodyka ta jest zgodna z wymaganiem zawartym w normie ISO/IEC-15408, cz. 1, która stwierdza, że wymagania bezpieczeństwa mają umożliwić opracowanie takich mechanizmów ochrony, które skutecznie zabezpieczą dany zasób lub grupę zasobów [3].

2. Geneza problemu

Wymagania bezpieczeństwa powstają jako wynik: analizy ryzyka, oceny wymagań ochrony zawartych w przepisach prawa powszechnego i w wewnętrznych przepisach ochrony informacji danej organizacji, kontroli funkcjonowania systemu teleinformatycznego. Wymagania bezpieczeństwa powinny udzielić odpowiedzi na pytania o zagrożeniach powiązanych z danym zasobem oraz o sposobach zmniejszania ich wpływu. W pracy Jennexa metody ochrony są określane mianem zapór redukujących (lub niwelujących) dane zagrożenie [4]. Wilander i Gustavsson poddali analizie 11 specyfikacji wymagań systemowych dla systemów informatycznych zamawianych przez agencje rządowe i samorządowe w Szwecji. Z analizy przedstawionej w pracy wynika, że specyfikacja wymagań bezpieczeństwa umieszczona w dokumencie specyfikacji wymagań systemowych jest zróżnicowana [2]. Autorzy opisują przypadki specyfikacji wymagań systemowych, w których kwestie bezpieczeństwa tworzonych systemów były opisane w bardzo lakoniczny sposób. Znaleziono specyfikacje wymagań systemowych, w których wymagania dotyczące bezpieczeństwa były bardzo szczegółowe. Pierwsza sytuacja, w opinii autorów, wynikała z braku wiedzy osób przygotowujących specyfikację wymagań systemowych, dotyczącej specyfikacji elementów ochrony, która jest zawarta w normie ISO/IEC-15408, cz. 2 [2]. Skutkiem opisanego braku wiedzy była niekompletna specyfikacja wymagań bezpieczeństwa. Druga sytuacja, w której specyfikacja wymagań bezpieczeństwa była opisana bardzo szczegółowo, wynikała

z zaangażowania do opracowania tej części dokumentu administratorów systemów teleinformatycznych. Przygotowany przez nich fragment dokumentacji oparty był na posiadanych przez nich doświadczeniach. Dlatego pewne wymagania były opisane w sposób bardzo szczegółowy i miały postać procedur wykonania określonych czynności, np. wykonanie kopii bezpieczeństwa danych składowanych na twardym dysku serwera. Należy zauważyć, iż rozważania autorów są związane z procesem opracowania i wdrażania systemów informatycznych. Zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych dotyczy całego cyklu życia systemu informatycznego, a nie tylko procesów opracowania i wdrożenia rozwiązania. Oznacza to konieczność rozszerzenia analiz na stacje robocze, serwery, urządzenia telekomunikacyjne oraz inne urządzania wchodzące w skład systemu. Wspomniane rozszerzenie wymaga oceny wpływu wdrażanych wymagań na poszczególne elementy systemu teleinformatycznego.

Nie można zapominać o wpływie użytkowników na bezpieczeństwo funkcjonowania omawianego systemu. Wprowadzając zabezpieczenia, należy uwzględnić działania użytkowników będące przyczyną powstawania incydentów w bezpieczeństwie funkcjonowania systemu, co wpływa na bezpieczeństwo informacji przetwarzanych i przesyłanych w systemie teleinformatycznym [7].

W dostępnej literaturze przedmiotu nie znaleziono propozycji kryteriów oceny efektów wdrożenia wymagań bezpieczeństwa dla funkcjonowania systemu. Brak kryteriów utrudnia ilościową ocenę uzyskanych efektów, wymuszając korzystanie z oceny jakościowej. Taka ocena jest subiektywna, a jej wynik – akceptacja poziomu ochrony zasobu lub jego odrzucenie – zależy od wiedzy i doświadczenia osoby oceniającej.

Problemem, który będzie rozwiązywany, jest opracowanie metody oceny wpływu wymagań bezpieczeństwa na funkcjonowanie poszczególnych elementów systemu teleinformatycznego. Konsekwencją wdrożenia zabezpieczeń będzie wzrost lub pogorszenie poziomu bezpieczeństwa informacji przetwarzanych przez ten system.

3. Badania empiryczne

Problem oceny efektywności zostanie rozpatrzony na podstawie dwóch przykładowych elementów systemów teleinformatycznych. Pierwszym będzie ochrona serwera poczty elektronicznej organizacji przed niechcianą pocztą elektroniczną, potocznie nazywaną spamem. Skuteczna klasyfikacja odbieranych wiadomości chroni użytkownika konta pocztowego przed atakami przeprowadzanymi za pomocą niechcianych przesyłek. Drugi przykład dotyczy serwera zarządzającego pracą lokalnej sieci komputerowej. Serwer

wypełnia w sieci zadania związane z weryfikacją i uwierzytelnianiem użytkowników oraz procesów programowych. Dodatkowo pełni funkcję bramy wyjściowej do sieci zewnętrznych.

W pierwszym przykładzie analizie został poddany mechanizm ochrony przed niechcianą pocztą. Z kont użytkowników pobrano próbkę przesyłek zakwalifikowanych do grupy niechcianych wiadomości [6]. Parametry próby przestawiono w tabeli 1.

Tabela 1

Liczność próby niechcianych wiadomości [6]

Parametr	**Wartość**
Liczność próby	100
Liczba adresów IP identyfikująca nadawcę	100
Liczba powtórzonych adresów IP identyfikująca nadawcę	2
Liczba wystąpień adresów IP należących do klasy A	68
Liczba wystąpień adresów IP należących do klasy B	8
Liczba wystąpień adresów IP należących do klasy C	24

Przy założeniu że ochrona serwera poczty elektronicznej będzie realizowana z wykorzystaniem techniki „czarnych list" adresów IP nadawców poczty [6, 9], skuteczność takiego rozwiązania jest bardzo niska. Na podstawie danych przedstawionych w tabeli 1 wynosi ona 2%. Taka wartość jest nie do zaakceptowania, oznacza ona brak skutecznej ochrony przed niechcianymi przesyłkami. Korzystanie z techniki „czarnej listy" adresów IP nadawców poczty elektronicznej będzie skutkować koniecznością tworzenia, a w dalszej kolejności zarządzania i aktualizacji bazy danych, zawierającej kolejne adresy IP serwerów poczty internetowej. Przeszukanie, a następnie modyfikacja zawartości bazy danych mogą być przyczyną dużych opóźnień w pracy serwera poczty elektronicznej.

Inne rozwiązanie zaproponowane w literaturze przedmiotu wykorzystuje analizę bayesowską zawartości treści wiadomości. Badając słowa użyte w otrzymanej wiadomości, można określić ich przynależność do dwóch zbiorów. Pierwszy jest zbiorem słów najczęściej występujących w wiadomościach akceptowanych. Drugi jest zbiorem słów występujących w wiadomościach nieakceptowanych. Porównując stosunek przynależności słowa do obu zbiorów, można zakwalifikować wiadomość jako akceptowaną lub nieakceptowaną. Przykładowe wymagania bezpieczeństwa dla serwera poczty elektronicznej są następujące:

- instalacja oprogramowania wykrywającego przesyłki niechciane,
- sprawdzenie przesyłek niechcianych przez oprogramowanie wykrywające kod złośliwy, który może znajdować się w załącznikach do wiadomości,

– składowanie wiadomości zakwalifikowanych jako niechciane w katalogu celem ich weryfikacji przez użytkownika poczty,

– cykliczne kasowanie wiadomości w katalogu z niechcianą pocztą.

Drugi przykład dotyczy serwera lokalnej sieci komputerowej. Serwer, co opisano wcześniej, pełni funkcje uwierzytelniania i weryfikacji. Dodatkowo jest on bramą wyjściową dla komputerów pracujących w lokalnej sieci komputerowej. Uzyskanie nieuprawnionego dostępu do zasobów serwera mogłoby skutkować naruszeniem wszystkich atrybutów bezpieczeństwa informacji składowanych, przetwarzanych i przesyłanych przez serwer. W okresie 32 dni w dzienniku bezpieczeństwa systemu zostały zaewidencjonowane 84 254 zdarzenia. Parametry statystki opisowej wymienionej próby zostały przedstawione w tabeli 2.

Tabela 2

Parametry statystyki opisowej zdarzeń zawartych w dzienniku bezpieczeństwa systemu

Parametr	**Wartość**
Liczność próby testowej	84 254
Średnia	2055
Odchylenie standardowe	3073
Minimum	121
Maksimum	10 868

Źródło: opracowanie własne.

Szereg czasowy, przedstawiający częstość występowania zdarzeń zapisanych w dzienniku bezpieczeństwa serwera, przedstawiono na rysunku 1. Analizując dane zapisane w dzienniku bezpieczeństwa systemu, stwierdzono, że największa liczba zdarzeń była związana z działaniem oprogramowania złośliwego. Na jednej ze stacji roboczych został zainstalowany złośliwy kod, który generował hasła użytkownika, starając się uzyskać dostęp do serwera kontrolującego pracę środowiska sieciowego. Opisana sytuacja jest przykładem ataku nazywanego w literaturze atakiem brute force, który służy intruzowi do podwyższenia uprawnień (ang. *lift of privileges*). Atak ten polega na generowaniu kolejnych haseł użytkownika, a następnie na oczekiwaniu na reakcję serwera. W przypadku potwierdzenia poprawności wprowadzonych danych przez serwis weryfikujący systemu operacyjnego serwera nazwa użytkownika wraz z hasłem była przesyłana przez program do stacji odbiorczej. Czynność ta umożliwiała przejęcie kontroli nad stacją przez zdalnego użytkownika, np. program zarządzający siecią botów.

Wymagania bezpieczeństwa, które zostały opracowane dla przykładowego serwera, były następujące:

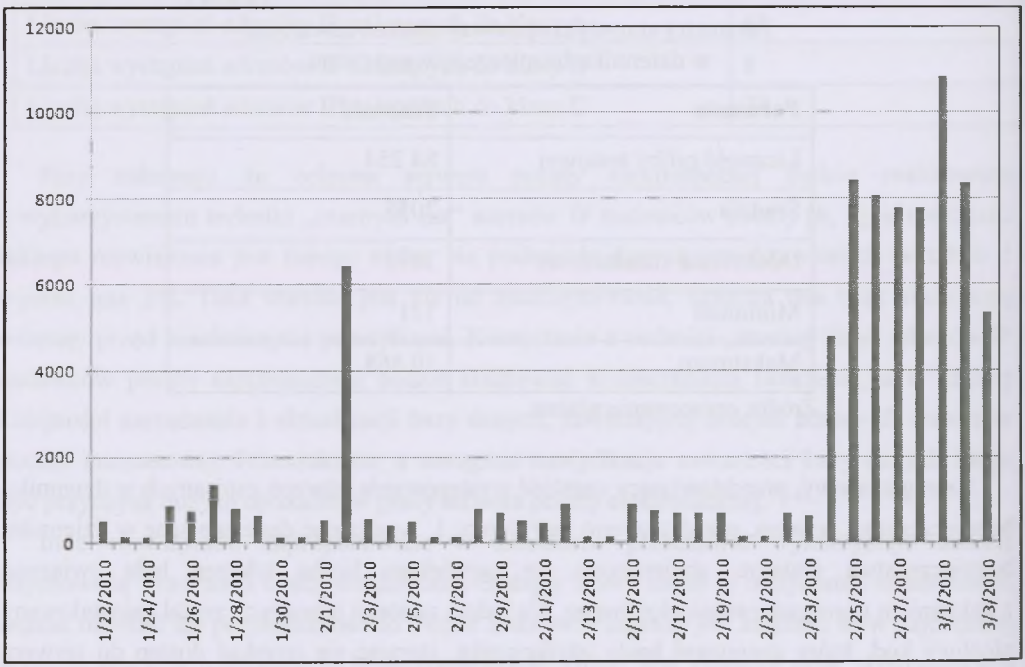
– skorelowanie informacji zawartych w dzienniku aplikacji z danymi z dziennika bezpieczeństwa serwera,

– ustalenie kont użytkowników, które były źródłem zdarzeń zarejestrowanych w dzienniku bezpieczeństwa,

– rekonfiguracja lub zablokowanie wymienionych wcześniej kont użytkowników,

– konfiguracja oprogramowania blokującego działanie kodu złośliwego – dotyczy stacji roboczych,

– aktualizacja systemu operacyjnego – instalacja poprawek usuwających podatności wykryte w systemie operacyjnym.



Rys. 1. Liczba zdarzeń zapisanych w dzienniku bezpieczeństwa systemu operacyjnego serwera [źródło: opracowanie własne]

Fig. 1. Number of events which were recorded into security log of server operating system [resource: own work]

Wymagania bezpieczeństwa w odniesieniu do poszczególnych elementów systemu teleinformatycznego można opisać za pomocą następujących zależności. Zależność (1) opisuje przypadek szczególny, kiedy jedno wymaganie jest odnoszone do pojedynczego elementu systemu teleinformatycznego:

$$\exists(a_i \in A) \wedge \exists(e_j \in E) \Leftrightarrow (a_i, e_j) \subset A \times E, \quad (1)$$

gdzie:

a_i – i-te wymaganie bezpieczeństwa, i = 1,2,...,n,

A – zbiór wymagań bezpieczeństwa dla analizowanego systemu teleinformatycznego,

e_j – j-ty element systemu teleinformatycznego, np. system operacyjny serwera, j = 1,2,...,m,

E – zbiór wszystkich elementów systemu teleinformatycznego.

Przedstawione wcześniej wymagania dotyczyły dwóch lub więcej elementów systemu. Dla tego przypadku zależność jest następująca:

$$\exists(a_i,...,a_n \in A) \wedge \exists(e_j,...,e_m \in E) \Leftrightarrow \{(a_i, e_j),...,(a_i, e_m),...,(a_n, e_j),...,(a_n, e_m)\} \subset A \times E, \quad (2)$$

gdzie:

$a_i, ..., a_n$ – podzbiór wymagań bezpieczeństwa, i = 1,2,...,n,

A – zbiór wymagań bezpieczeństwa dla analizowanego systemu teleinformatycznego,

e_1 ... $,e_j, ..., e_m$ – podzbiór elementów systemu teleinformatycznego, j = 1,2,...,m,

E – zbiór wszystkich elementów systemu teleinformatycznego.

W dalszej części przedstawiono kryteria oceny wymagań bezpieczeństwa oraz oceny uzyskanych wyników. W pierwszym z przykładów celem wdrożenia wymagań bezpieczeństwa jest ograniczenie liczby niechcianych wiadomości, które przesyłane są na konta użytkowników. Duża liczba niechcianych wiadomości, umieszczona w kolejkach oraz na kontach użytkowników, może doprowadzić do zablokowania pracy serwera poczty elektronicznej. Blokada będzie wynikiem zapełnienia obszaru dysków twardych przez masowo przysłane, niechciane listy elektroniczne. Z analizy danych przedstawionych w tabeli 1 wynika, że filtrowanie adresów IP serwerów nadawców pozwala filtrować wiadomości ze skutecznością 2%. Rozszerzenie reguł filtracji na numer sieci (zawarty w adresie IP) nie poprawia znacząco skuteczności procesu filtrowania. Skuteczność ta wzrasta do 4% [6]. Przeszukiwanie dużych zbiorów danych w przypadku odbierania kilku tysięcy wiadomości będzie skutkowało wydłużeniem czasu obsługi klientów korzystających z serwera. To zaś zmienia atrybut dostępności informacji. Zastąpienie zbiorów adresów IP bayesowskimi filtrami zawartości, wyposażonymi w mechanizmy oceny przynależności treści do jednej z dwóch grup, eliminuje konieczność obsługi dużych baz danych [6, 9]. Instalacja oprogramowania filtrującego spowoduje powstanie opóźnienia związanego z działaniem filtra, którego dopuszczalną wartość należy zdefiniować.

Pierwszym kryterium oceny jest spadek liczby niechcianych wiadomości, znajdujących się w skrzynkach odbiorczych użytkowników serwera poczty elektronicznej, o 50% (np. nie więcej niż 10 wiadomości w ciągu dnia pracy). Kolejnym kryterium jest minimalny czas

zwłoki w pracy serwera. Jest to istotne, gdyż w przypadku dużego obciążenia serwera (wiele żądań wysłania wiadomości oraz duża liczba wiadomości czekających w kolejce na sprawdzenie) korzystanie z serwera może być utrudnione lub niemożliwe. Definiując poziom bezpieczeństwa, można stwierdzić, iż w przypadku gdy w kolejce znajduje do 1000 wiadomości oraz gdy 200 użytkowników żąda obsługi przez serwer, jego inercja nie powinna przekraczać 5 s. Rozmiar bufora z wiadomościami do weryfikacji przez użytkowników nie powinien przekraczać 500 MB, a maksymalny czas pozostawania w buforze niechcianej wiadomości nie powinien być dłuższy niż 10 dni. Wymagania te wynikają z konieczności zapewnienia obszaru pamięci na potrzeby obsługi kolejek z wiadomościami wysyłanymi i odbieranymi przez serwer.

W drugim przypadku należy zidentyfikować te procesy programowe, które są przyczyną wpisów w dzienniku aplikacji, a następnie sprawdzić ich powiązanie z wpisami w dzienniku bezpieczeństwa. Wymaga się zablokowania lub usunięcia tych procesów, które są przyczyną powstawania incydentów. Następnie należy zidentyfikować te konta użytkowników, których działanie zostało zablokowane. Konta były zablokowane w wyniku działania złośliwego oprogramowania, które generowało hasła dostępu. Konta użytkowników należy skonfigurować ponownie, na stacjach roboczych należy zaś zainstalować oprogramowanie usuwające złośliwy kod. Następnie należy zaktualizować system operacyjny komputera klienta. Na serwerze należy zainstalować system wykrywający i przeciwdziałający działaniom potencjalnych intruzów z zewnątrz i wewnątrz sieci. Wskazana jest instalacja oprogramowania usuwającego złośliwy kod. Należy zwrócić uwagę na funkcjonowanie serwera po wykonaniu wymienionych czynności. Instalacja tego typu rozwiązań będzie skutkowała zmniejszeniem takich zasobów serwera, jak pojemność dysków twardych oraz dostępna ilość pamięci RAM. W przypadku wykorzystywania wewnętrznego routingu pomiędzy kartami sieciowymi w serwerze mogą pojawić się problemy w dostępie użytkowników do sieci zewnętrznych, np. klientów korzystających z usługi zamiany adresów (ang. Network Address Translating).

Powstaje pytanie o weryfikację wymagań bezpieczeństwa dla obu przedstawionych przypadków. Proces sprawdzenia należy rozpocząć od ustalania aktualnego stanu ochrony danego obiektu. Jeżeli poziom ochrony jest wyższy niż przedstawiony w wymaganiu, wdrażanie zmian jest bezcelowe. Jeżeli jest mniejszy lub równy, wymaganie należy wdrożyć. Kolejnym krokiem jest ocena wpływu wdrożonego wymagania na funkcjonowanie elementów systemu, które wymieniają informacje z danym elementem. Narzędziem, które można wykorzystać do oceny wpływu planowanego do wdrożenia wymagania, jest drzewo decyzyjne. Prawdopodobieństwa zdarzeń będą przyjmowane albo na podstawie danych z monitoringu środowiska, albo na podstawie oceny subiektywnej [1].

Najtrudniejszą częścią jest przewidywanie negatywnego wpływu wdrożonego wymagania na działanie współpracujących z nim elementów. Oceniając efekty, należy sprawdzić, czy postawione wymagania zostały spełnione. Proces ten wymaga doświadczenia oraz znajomości procesów przepływu danych pomiędzy poszczególnymi fragmentami systemu. Niewłaściwa ocena może być przyczyną obniżenia niezawodności działania systemu. Proces oceny wpływu wdrożonych wymagań będzie realizowany w czasie kontroli funkcjonowania wybranych elementów systemów. Wiedza uzyskana na podstawie tych obserwacji posłuży do podniesienia poziomu niezawodnego i bezpiecznego działania systemu.

4. Wnioski

Przedstawione kryteria oceny poziomu ochrony elementów systemu teleinformatycznego pozwalają wstępnie ocenić wymagania oraz umożliwiają zaplanowanie działań mających na celu ich wdrożenia. Należy pamiętać, że z każdym wdrażanym wymaganiem są związane zasoby ludzkie lub sprzętowe. Potrzebny jest również czas na wykonanie prac przewidzianych w przedsięwzięciu. Celem tych działań jest bezpieczny i niezawodny system teleinformatyczny, wspomagający funkcjonowanie organizacji lub instytucji.

Umiejętność przewidzenia potencjalnych problemów pozwala na utrzymanie ciągłości działania danego podmiotu. Jest to jedno z podstawowych wymagań biznesowych, jakie musi wypełniać system teleinformatyczny.

Konieczne jest opracowanie mechanizmów pozwalających na efektywne identyfikowanie podatności w wybranej grupie elementów systemu w celu uniknięcia incydentów w bezpieczeństwie informacyjnym.

Bibliografia

1. Aczel A.: Statystyka w zarządzaniu. PWN, Warszawa 2007.
2. Wilander J., Gustavsson J.: Security Requirements. A Field Study of Current Practice, http://www.sreis.org/SREIS_05_Program/full18_wilander.pdf [dostęp: 5.05.2011].
3. International Standard ISO/IEC-15408-1. Information technology Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. Second editio, 2005-10-01. International Organization for Standardization, Geneva 2005.
4. Jennex M.: Modeling Security Requirements for Information Systems Development, http://www.sreis.org/SREIS_05_Program/full39_jennex.pdf [dostęp: 5.05.2011].

5. Jóźwiak I.J., Nowakowski T., Szleszyński A.: Methodology of specification of information security requirements for Information and Communication Technology systems, [in:] Reliability, Risk and Safety. Back to Future, B.J.M. Ale, I.A. Papazoglu, E. Zio (eds.), CRC Press Taylor & Francis Group, London 2010, p. 2126-2131.
6. Józwiak I.J., Szleszyński A.: Redukcja niechcianej poczty elektronicznej w aspekcie bezpieczeństwa informacji systemu teleinformatycznego. Zeszyty Naukowe Politechniki Śląskiej, s. Organizacja i Zarządzanie, z. 49, Gliwice 2009, s. 123-132.
7. Liderman K.: Analiza ryzyka i ochrona informacji w systemach komputerowych. PWN, Warszawa 2008.
8. Polska Norma PN ISO/IEC – 17799:2007. Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji. Polski Komitet Normalizacyjny, Warszawa 2007.
9. Zdziarski J.S.: Spamowi stop! Bayesowskie filtrowanie zawartości i sztuka statystycznej klasyfikacji języka. PWN, Warszawa 2005.

Abstract

In the paper, two selected elements of ITC systems and their vulnerabilities are considered. The first of them is an electronic mail server attacked by unsolicited bulk messages. The second one is a local area network server fulfilling a role of users authorization and authentication centre for users and software process. It is also a network gateway. The statistical parameters of analyzing sample distributions for both of the objects were presented in the paper. There was presented a time series of events recorded into systems security log. Then an exemplary of security requirements for the electronic mail server and the network server is presented. The next step is an evaluation of influence of the security requirement on proper work of the elements connected to protected object. A crucial thing here is a comparison between current state of the object protection and the actions suggested by the security requirements.