ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2014
Seria: ORGANIZACJA I ZARZĄDZANIE z. 74 Nr kol. 1921

Artur SZLESZYŃSKI
Wydział Zarządzania
Wyższa Szkoła Oficerska Wojsk Lądowych imienia gen. T. Kościuszki

POMIAR BEZPIECZEŃSTWA INFORMACJI W ZARZĄDZANIU BEZPIECZEŃSTWEM W SYSTEMIE TELEINFORMATYCZNYM

Streszczenie. W artykule przedstawiono metody oszacowania wpływu incydentów na atrybuty bezpieczeństwa informacji znajdujących się wewnątrz systemu teleinformatycznego. Wykonując pomiary pośrednie związane z występowaniem incydentów w elementach infrastruktury technicznej systemu teleinformatycznego, można oszacować ich wpływ na atrybuty bezpieczeństwa informacji. W pracy przedstawiono propozycje metryk oceniających stopień zmian poszczególnych atrybutów bezpieczeństwa informacji.

Słowa kluczowe: atrybuty bezpieczeństwa informacji, pomiar bezpieczeństwa informacji.

MEASUREMENT OF INFORMATION ON SECURITY OF SAFETY MANAGEMENT IN INFORMATION AND COMMUNICATION SYSTEM

Summary. Paper presents the methods for incident influence on information security attributes which is inside the Information and Communication System. Making the indirect measurements of incident occurrence at elements of technical infrastructure there is a possibility to evaluate their affectation on information security attributes. At the paper the metrics evaluating a degree of changes each of information security attributes are shown.

Keywords: information security attributes, information safety measurement.

1. Wprowadzenie

Zarządzanie bezpieczeństwem informacji jest jednym z elementów zarządzania bezpieczeństwem organizacji. Norma ISO/IEC 27001 zaleca zarządzanie bezpieczeństwem oprzeć na cyklu Deminga, w skład którego wchodzą: planowanie, wykonywanie, sprawdzanie

efektów wprowadzonych działań oraz reagowanie na wykryte odstępstwa [11]. Planowanie działań związanych z bezpieczeństwem informacji wymaga poznania zbioru zasobów informacyjnych, obiektów przechowujących lub przesyłających zasoby informacyjne, elementów przetwarzających i wymieniających dane. Dodatkowo należy poznać zbiór potencjalnych zagrożeń dla posiadanych zasobów informacyjnych oraz przewidywalne konsekwencje naruszenia atrybutów poufności, integralności i dostępności. Łącząc wymienione elementy, opracowuje się dokument nazywany analizą ryzyka [3].

Żeby analiza ryzyka nie była prowadzona tylko na podstawie subiektywnych ocen dotyczących zagrożeń mających wpływ na bezpieczeństwo zasobów informacyjnych organizacji, należy wykonywać okresowy pomiar bezpieczeństwa zasobów informacyjnych, a następnie ich wyniki należy porównywać z metrykami [10]. Wyniki pomiarów porównane z metrykami umożliwią ocenę poziomu bezpieczeństwa systemu teleinformatycznego. Jest to pomiar pośredni, ponieważ mierzone są zdarzenia występujące w elementach systemu teleinformatycznego. Wyniki pomiarów posłużą do oceny zagrożeń dla poszczególnych atrybutów bezpieczeństwa informacji. Liczba zdarzeń klasyfikowanych jako incydenty w bezpieczeństwie systemu teleinformatycznego będzie wskazywać możliwe naruszenia atrybutów bezpieczeństwa informacji.

Pomiar zmian atrybutów bezpieczeństwa zasobów informacyjnych nie jest omówiony w literaturze przedmiotu. Literatura opisuje metody pomiaru bezpieczeństwa opierające się na rejestrowaniu zdarzeń w bezpieczeństwie występujących w elementach infrastruktury technicznej systemu [10]. Normy stwierdzają, że bezpieczeństwo informacji należy rozpatrywać w kontekście niezmienionych atrybutów bezpieczeństwa informacji. Analizując dostępną literaturę przedmiotu, autor nie znalazł metody, która pozwala wskazać, jak dany incydent będzie wpływał na wartość atrybutów bezpieczeństwa zasobu informacyjnego znajdującego się wewnątrz ocenianego elementu.

2. Geneza problemu

Pomiar zmian atrybutów bezpieczeństwa informacji będzie prowadzony w odniesieniu do elementów infrastruktury technicznej rozwiązania. Założenie to wynika z faktu, iż możliwe jest określenie podatności występujących w tej grupie elementów. Znając podatności w elementach systemu teleinformatycznego, można ocenić, jakie zagrożenia mogą wystąpić, a następnie oszacować zmiany atrybutów bezpieczeństwa informacji znajdującej się wewnątrz elementu.

Określenie zmian wartości atrybutów bezpieczeństwa informacji jest trudne, podobnie jak wpływu incydentu na ich wartość. Oszacowanie to opiera się na przewidywanych konsekwencjach wystąpienia zagrożenia w elemencie, w którym znajduje się pojedyncza

wiadomość lub grupa wiadomości. Jest to ocena niepewna, a jedynym sposobem weryfikacji poprawności rozumowania jest wystąpienie incydentu i związane z nim poznanie jego konsekwencji dla zasobu informacyjnego.

Oszacowanie możliwych zmian atrybutów bezpieczeństwa rozpoczęto od atrybutu dostępności zasobu informacyjnego. Może on być wyrażony miarą binarną oznaczającą dwa stany: dostępności lub braku dostępności informacji [4]. Trudniej jest zweryfikować wpływ incydentu na integralność zasobu informacyjnego, a jeszcze trudniej jest stwierdzić naruszenie atrybutu poufności wiadomości [4, 6]. Najtrudniej zaś ocenić wpływ incydentu na atrybut poufności [4]. W pierwszym przypadku należy mieć wzorzec informacji oraz informację znajdującą się w elemencie systemu po wystąpieniu incydentu. Oznacza to, że musiałoby istnieć repozytorium informacji zawierające wszystkie zasilenia do poszczególnych elementów. Po każdej operacji uważanej za incydent należałoby pobierać z repozytorium wzorzec i porównywać go z obecną postacią wiadomości. Takie działanie zwiększa koszt rozwiązania, ponieważ wymaga posiadania repozytorium, oraz zmniejsza jego bezpieczeństwo. Repozytorium staje się atrakcyjnym obiektem ataku dla potencjalnego intruza. Podmiana lub usunięcie wiadomości z repozytorium będzie powodować występowanie błędów w identyfikacji wpływu incydentu na zasób. Dodatkowo, zmienione wzorce mogą zakłócać pracę systemu jako całości.

Kolejnym wskaźnikiem zdarzeń naruszających atrybut integralności informacji są błędy występujące w oprogramowaniu wykorzystującym zmieniony zasób informacyjny. Błędy wskazują, że format zasobu informacyjnego został zmieniony i kolejny element rozwiązania nie jest w stanie z niego korzystać. Jednak nadal nie są znane źródło zdarzenia oraz rozmiar zmian w zasobie informacyjnym. Zadanie identyfikacji zmian atrybutu integralności komplikuje się w przypadku zmiennej struktury zasobu informacyjnego. Następnym zagadnieniem, które należy rozważyć, jest kwestia postępowania z informacją, której wzorca nie znaleziono w repozytorium. Czy można przyjąć regułę decyzyjną, która w przypadku braku wzorca ignoruje odebraną wiadomość? Czy można umieszczać taką informację w systemie, ale z zaznaczeniem, że jest ona niewiarygodna? Jak postępować z brakiem wiarygodności informacji w procesie decyzyjnym?

Największy problem to oszacowanie naruszenia atrybutu poufności informacji. Można domniemywać, że atrybut ten został naruszony. Wynika to z faktu, iż do momentu, kiedy osoba nieuprawniona nie wykorzysta informacji, do której nie powinna mieć dostępu, można tylko przypuszczać, że atrybut poufności informacji został naruszony. W pracy autorstwa E. Jonssona i L. Pirzadeha stwierdzono, że atrybut poufności może być mierzony za pomocą rejestracji zachowania systemu, takiego, które uniemożliwia dostęp do informacji nieuprawnionemu użytkownikowi [2]. Autorzy nazywają taką relację związkiem bezpieczeństwa związanego z zachowaniem analizowanego rozwiązania [2]. Pisząc o metryce dotyczącej pomiaru bezpieczeństwa atrybutu poufności, nie przedstawiono przykładu takiego

pomiaru. Zatem nadal nie jest znana, o ile wystąpiła, ilościowa zmiana wartości atrybutu bezpieczeństwa.

Problemem, który należy rozwiązać, jest opracowanie metod pozwalających na oszacowanie zmian atrybutów bezpieczeństwa informacji znajdujących się systemie teleinformatycznym na podstawie pomiaru wpływu incydentów w bezpieczeństwie elementów infrastruktury technicznej. Na podstawie pomiarów zostaną opracowane metryki, które umożliwią kontrolę poziomu bezpieczeństwa informacji w ocenianym systemie teleinformatycznym. Podejście to jest zgodne z zaleceniami znajdującymi się w literaturze przedmiotu [6, 7].

3. Propozycja rozwiązania

Pomiar bezpieczeństwa zasobów informacyjnych jest pomiarem pośrednim, opierającym się na analizie incydentów występujących w elementach systemu, które daną informację przetwarzają lub przechowują. W następnym kroku należy określić, jak incydenty mogą wpływać na atrybuty bezpieczeństwa informacji znajdującej się wewnątrz danego elementu. Na koniec należy oszacować wielkość możliwych zmian atrybutów bezpieczeństwa informacji.

Oszacowanie wpływu zdarzeń na atrybuty bezpieczeństwa informacji należy rozpocząć od określenia sposobu zmierzenia związków pomiędzy incydentem a atrybutem bezpieczeństwa zasobu informacyjnego. Jako pierwszy zostanie określony związek pomiędzy incydentem w bezpieczeństwie elementu a naruszeniem atrybutu dostępności zasobu informacyjnego.

Pomiar dostępności zasobu informacyjnego można zrealizować dwuetapowo. Pierwszy etap to binarne stwierdzenie dostępności zasobu informacyjnego w momencie wykonywania pomiaru. Pomiar ten zostanie wykorzystany do określenia dostępności zasobu informacyjnego. Zatem pierwszy z pomiarów można opisać zależnością (1):

$$A_j(t_i) = 0 \vee 1 \tag{1}$$

gdzie: $A_j(t_i)$ – dostępność zasobu informacyjnego znajdującego się w j-tym elemencie systemu teleinformatycznego w chwili t_i.

Pomiar ten można wykonać, rejestrując dostępność np. rekordu lub grupy rekordów testowych zapisanych w bazie danych w danej chwili t_i. Jeżeli zasób informacyjny jest dostępny, w rejestrze pomiarowym zapisywana jest wartość 1, jeżeli nie, zapisywana jest wartość 0. W drugim etapie opierającym się na pomiarach binarnych dostępności należy wyznaczyć dostępność zasobu informacyjnego w j-tym elemencie systemu

teleinformatycznego w pewnym przyjętym okresie. Działanie to będzie się odbywać przy wykorzystaniu zależności (2):

$$A_j(t_i,t_j)=\frac{\sum_{t=t_i}^{t_j} A_j(t)=1}{\sum_{t=t_i}^{t_j} A_j(t)=1+\sum_{t=t_i}^{t_j} A_j(t)=0} \tag{2}$$

gdzie: $Aj(t_i,t_j)$ – dostępność zasobu informacyjnego w okresie $t\in [t_i,t_j]$, $Aj(t) = 1$ – dostępność zasobu informacyjnego w elemencie j w chwili t, $Aj(t) = 0$ – brak dostępności zasobu informacyjnego w elemencie j w chwili t.

Wartość dostępności zasobu informacyjnego w j-tym elemencie systemu teleinformatycznego zawiera się w przedziale od 0 do 1. Wartość 0 oznacza brak dostępności zasobu informacyjnego w ocenianym okresie, a wartość 1 oznacza dostępność zasobu informacyjnego w ocenianym okresie. Dla każdego elementu w ścieżce krytycznej[1] systemu teleinformatycznego wyznacza się wartość parametru A_j. Wartość wskazuje dostępność informacji w elemencie. Jeżeli w wyniku wystąpienia incydentu informacja nie będzie dostępna, wówczas – mierząc liczbę zdarzeń braku dostępności – można określić, w jaki sposób incydent wpłynie na atrybut dostępności informacji. Można zaproponować metrykę oceniającą krytyczność incydentu występującego w elemencie systemu teleinformatycznego dla atrybutu dostępności informacji. Proponowaną metrykę przedstawiono w tabeli 1.

Tabela 1
Metryka wyznaczania krytyczności incydentu w elemencie systemu teleinformatycznego na podstawie dostępności zasobu informacyjnego

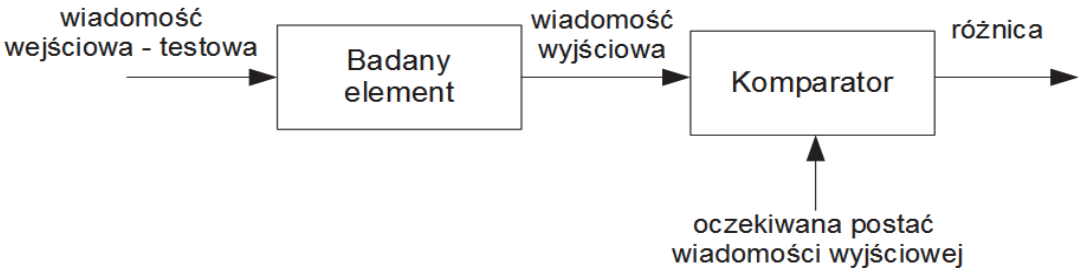
Lp.	Zakres wartości dostępności informacji w elemencie	Krytyczność incydentu dla atrybutu dostępności zasobu informacyjnego
1.	[0;0,45]	wysoka
2.	[0,46;0,64]	średnia
3.	[0,65;1]	niska

Źródło: opracowanie własne.

Kolejnym z atrybutów, którego zmiany należy wyznaczyć, jest integralność. W tym celu do ocenianego elementu zostanie wprowadzona wiadomość testowa. Wiadomość ta zostanie porównana z wiadomością na wyjściu danego elementu. Pomiar zmian integralności wiadomości polega na porównaniu wiadomości z wyjścia elementu z oczekiwaną postacią wiadomości. Schemat pomiaru przedstawiono na rysunku 1. Posługiwanie się zbiorem

[1] Ścieżka krytyczna jest wyznaczana na podstawie wrażliwości zasobu informacyjnego.

wiadomości testowych eliminuje konieczność tworzenia repozytorium wiadomości na wejściu i wyjściu elementów. Ograniczony zbiór wiadomości testowych powoduje ograniczenie obciążenia systemu teleinformatycznego związanego z testowaniem występowania incydentów.



Rys. 1. Pomiar zmiany integralności wiadomości w elemencie systemu teleinformatycznego (źródło: opracowanie własne)
Fig. 1. Measurement of message integrity change at ICT system element (source: author's own work)

Pomiar wpływu incydentu będzie wykonany na podstawie pomiaru liczby zmienionych bajtów w wiadomości wyjściowej w stosunku do postaci oczekiwanej wiadomości. Zmiana bajtów w wiadomości będzie wskazywać stopień zmiany jej integralności. Ocena wyników pomiaru jest realizowana według wzoru (3):

$$dbm = \frac{n_{eb}}{n_{cb}} \tag{3}$$

gdzie: dbm – iloraz liczby błędnych bajtów występujących w wiadomości wyjściowej i liczby bajtów poprawnych w wiadomości wyjściowej wyznaczonej na podstawie oczekiwanej postaci wiadomości wyjściowej, n_{eb} – liczba błędnych bajtów w wiadomości wyjściowej po porównaniu z postacią oczekiwaną wiadomości wyjściowej, n_{cb} – liczba bajtów poprawnych w wiadomości wyjściowej po porównaniu z oczekiwaną postacią wiadomości wyjściowej.

Przedstawiony sposób wyznaczania zmiany atrybutu integralności na podstawie stosunku liczby błędnych (zmienionych w wyniku incydentu) bajtów w wiadomości testowej do liczby poprawnych bajtów w wiadomości nie informuje o rozkładzie błędów [9]. W pomiarze skupiono się na określeniu rozmiaru zmiany (dbm) wiadomości powstałej w wyniku incydentu, a nie rozważano wpływu incydentu na semantyczną zawartość wiadomości. Wiedza ta posłuży do wyznaczenia jakościowej wielkości zmiany atrybutu integralności wiadomości.

Na podstawie pomiarów opracowano metrykę łączącą stopień zmian atrybutu integralności wiadomości. Przykład metryki pokazano w tabeli 2.

Tabela 2

Metryka relacji między liczbą zmienionych bajtów w wiadomości wyjściowej a naruszeniem atrybutu integralności wiadomości

Lp.	Zakres zmian wartości dbm w elemencie	Wpływ incydentu na rozmiar zmian atrybutu integralności wiadomości
1.	[0;0,15]	niska
2.	[0,16;0,3]	średnia
3.	[0,31;1]	wysoka

Źródło: opracowanie własne.

Stwierdzenie naruszenia atrybutu poufności jest oparte na wiedzy niepewnej [1]. Analizując zapisy w dziennikach systemu operacyjnego, można domniemać, że w wyniku incydentu wystąpiło zjawisko naruszające atrybut poufności. Skwantyfikowanie rozmiaru naruszenia atrybutu poufności informacji będzie wartością szacunkową. Pomiar wielkości zmian wartości atrybutu będzie się opierał na liczbie zewidencjonowanych nieudanych prób dostępu do zasobu informacyjnego. Im większa jest liczba zdarzeń, tym większa jest determinacja atakującego, żeby uzyskać dostęp do zasobu informacyjnego. Nie można się zgodzić z twierdzeniem E. Jonssona oraz L. Pirzadeha, że odrzucenie przez system, a ściślej przez podsystem weryfikacji użytkownika, próby dostępu do zasobu przez nieuprawnionego użytkownika jest dowodem na bezpieczeństwo systemu [2]. Autorzy pomijają kwestię procesów uruchamianych przez użytkowników w ramach przysługujących im uprawnień. Proces uruchomiony na koncie użytkownika uzyskuje dostęp do wszystkich zasobów informacyjnych, do których uprawniony jest użytkownik.

Kolejną kwestią jest możliwość wykorzystania zdobytego zasobu informacyjnego przez atakującego. Zważywszy, że liczba systemów teleinformatycznych całkowicie odłączonych od sieci komputerowych jest coraz mniejsza, należy stwierdzić, że sieć komputerowa oraz zewnętrzne nośniki danych mogą stanowić medium wykorzystane do wycieku danych. Jednoznaczne stwierdzenie zaboru zasobu informacyjnego jest trudne, ponieważ informacja jest bytem niematerialnym i jej kradzież nie wiąże się z jej brakiem w miejscu składowania [7].

Zatem o naruszeniu atrybutu poufności można tylko domniemywać na podstawie zgromadzonych faktów, takich jak: liczba odrzuconych prób dostępu do zasobu informacyjnego, liczba zaakceptowanych prób dostępu do zasobu informacyjnego. Oceniając te dwie wielkości, można wyznaczyć współczynnik informujący o determinacji atakującego do zdobycia dostępu do zasobu informacyjnego.

$$IDC = \frac{n_{rar}}{n_{ga}} \tag{4}$$

gdzie: IDC – współczynnik determinacji atakującego, n_{rar} – liczba odrzuconych prób dostępu do zasobu informacyjnego, n_{ga} – liczba zaakceptowanych prób dostępu do zasobu informacyjnego.

Jeżeli wartość współczynnika IDC wyniesie 0, nie zarejestrowano w systemie odrzucenia próby dostępu do zasobu informacyjnego przez użytkownika; nie oznacza to, iż nie doszło do zmiany atrybutu poufności informacji. Kolejnym działaniem weryfikującym potencjalną zmianę wartości atrybutu poufności jest weryfikacja liczby udzielonych poprawnie dostępów do zasobu informacyjnego oraz czas ich przydzielania.

Skokowa zmiana liczby zdarzeń[2] może być sygnałem, że użytkownik lub proces złośliwy zainstalowany w jego urządzeniu pobiera dane w celu ich przekazania poza sieć organizacji. Takie zdarzenie nazywa się wyciekiem danych i jest trudne do ustalenia w przypadku posługiwania się przez użytkownika urządzaniem mobilnym, np. tabletem lub smartphone'em. Zarejestrowanie opisanych zdarzeń nie jest jednoznaczną przesłanką pozwalającą na konkluzję, że atrybut poufności zasobu informacyjnego został zmieniony oraz jak został zmieniony. Przedstawiona w pracy autorstwa I. Jóźwiaka oraz A. Szleszyńskiego kwantyfikacja 0 lub 1 nie jest adekwatna. Miara ta zakłada wiedzę pewną [4]. Wiedza pewna jest wówczas, gdy treść zasobu zostaje ujawniona [12]. Większość zagrożeń klasyfikowanych do grupy zaawansowanych zagrożeń trwałych stara się ukrywać swoją obecność w systemie operacyjnym urządzenia lub grupy urządzeń tak długo, jak jest to możliwe [12]. Celem ich działania jest wyprowadzanie informacji wrażliwych z organizacji w celu ich upublicznienia lub wykorzystania przeciwko właścicielowi [12].

Konkludując, należy zauważyć, że na obecnym etapie opracowanie pojedynczej miary wskazującej zmianę atrybutu poufności zasobu informacyjnego jest niemożliwe. Miara ta będzie złożona oraz niepewna, bezpośrednie zaś powiązanie pomiędzy incydentami rejestrowanymi w elementach infrastruktury technicznej systemu teleinformatycznego ze zmianami atrybutu poufności będzie się opierać na heurystyce. Jeszcze trudniejsze będzie opracowanie metryk oceniających wykonany pomiar.

4. Podsumowanie

W artykule podjęto próbę skwantyfikowania zmian atrybutów bezpieczeństwa dla zasobów informacyjnych znajdujących się w elementach infrastruktury technicznej systemu teleinformatycznego. Przedstawiona koncepcja łączenia incydentów pojawiających się w elementach systemu teleinformatycznego z atrybutami bezpieczeństwa zasobu (zasobów) informacyjnego stanowi nowość w stosunku do obecnie prezentowanych metod pomiaru bezpieczeństwa w systemach teleinformatycznych.

[2] Celowo użyto pojęcia zdarzenia, a nie incydentu, gdyż dostęp do zasobu informacyjnego jest udzielany uprawnionemu użytkownikowi. Przez użytkownika uprawnionego rozumie się podmiot, który został zweryfikowany przez podsystem ochrony urządzania przechowującego zasób informacyjny.

Adekwatność opisanych metod pomiarowych oraz ich wartości zostaną zweryfikowane za pomocą eksperymentu symulacyjnego. Największym problemem pozostaje opracowanie heurystyki umożliwiającej szacowanie stopnia naruszenia atrybutu poufności zasobu informacyjnego. Opisany wstępny algorytm postępowania z kwantyfikacją atrybutu poufności będzie stanowił punkt wyjścia do dalszych badań w opisanym obszarze.

Posługiwanie się w metrykach ocenami jakościowymi wynika z faktu ich lepszego zrozumienia przez decydentów. Oceny ilościowe są potrzebne inżynierom odpowiedzialnym za poprawne funkcjonowanie rozwiązania. Ocena ilościowa jest wykorzystywana do informowania o stanie diagnozowanego obiektu.

Bibliografia

1. Bubnicki Z.: Teoria i algorytmy sterowania, PWN, Warszawa 2005.
2. Jonsson E., Pirzadeh L.: A Framework for Security Metrics Based on Operational System Attributes, ieeexplore.org 2011 [dostęp on-line 23.04.2014 r.]. http://publications.lib.chalmers.se/records/fulltext/local_147441.pdf
3. Jóźwiak I.J., Laskowski W., Szleszyński A.: Wykorzystanie drzewa użyteczności w procesie planowania i wdrożenia systemu bezpieczeństwa informacji, Zeszyty Naukowe Politechniki Śląskiej, Organizacja i Zarządzanie, z. 45, Gliwice 2008, s. 149-158.
4. Jóźwiak I.J., Szleszyński A.: Ocena poziomu bezpieczeństwa zasobów informacyjnych z wykorzystaniem techniki analizy architektury systemu informatycznego, Zeszyty Naukowe Politechniki Śląskiej, Organizacja i Zarządzanie, z. 68, Gliwice 2014, s. 321-334.
5. Karbowski M., Podstawy kryptografii, Helion, Gliwice 2008.
6. Kuchta D., Szleszyński A., Witkowski M.: Metodyka opracowania scenariuszy przebiegu incydentów w bezpieczeństwie systemu, wykorzystywanych w zarządzaniu bezpieczeństwem informacji w wojskowych systemach teleinformatycznych. Etap II. Opracowanie scenariuszy przebiegu incydentów na podstawie analiz zagrożeń dla funkcjonowania wojskowego systemu teleinformatycznego, WSOWL, Wrocław 2013.
7. Liderman K.: Analiza ryzyka i bezpieczeństwo teleinformatyczne, PWN, Warszawa 2008.
8. Liderman K.: Czy „audyt bezpieczeństwa teleinformatycznego" jest tym samym co „audyt informatyczny"?, Biuletyn IAR WAT nr 21, WAT, Warszawa 2004, s. 77-104.
9. Mochnacki M.: Kody korekcyjne i kryptografia, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2000.

10. Payne S.: A Guide to Security Metrics, SANS Institute, June 2006 [dostęp on-line 23.04.2014 r.], http://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55.
11. PN ISO/IEC-270001 Technika informatyczna. Techniki bezpieczeństwa. System zarządzania bezpieczeństwem. Wymagania, PKN, Warszawa 2007.
12. Thomson G.: APTs: a pourly undestood challenge, Network Security, Elsevier, November 2011 [dostęp on-line 24.04.2014], http://www.sciencedirect.com/science/article/pii/S1353485811701180#

Abstact

Paper presents the methodology of measurement changes information security attributes. The indirect measures of security incidents that occur in elements of ICT system are used. Then author tries to present a relation between the incident and its influence on information security attributes. The formula (1) shows the simple binary measure of information availability. And security subsystem should to collect a series of availability measures and calculate changes of availability attribute. Table 1 presents the metrics which is qualitative measure of changes availability attribute. An integrity is the next measured information security attribute. To provide the measure standard message is used. By comparison outcome of standard message affected by the incident with expected message shape there is a possible to evaluate a degree of changes the integrity attribute. Table 2 shows the metrics which is a qualitative measure of integrity attribute changes. The most difficult attribute to measure is a confidentiality attribute. The paper presents only a concept of these measures.