ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2014
Seria: ORGANIZACJA I ZARZĄDZANIE z. 68 Nr kol. 1905

Ireneusz J. JÓŹWIAK
Politechnika Wrocławska
Wydział Informatyki i Zarządzania

Artur SZLESZYŃSKI
Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. Tadeusza Kościuszki
Wydział Zarządzania

# OCENA POZIOMU BEZPIECZEŃSTWA ZASOBÓW INFORMACYJNYCH Z WYKORZYSTANIEM TECHNIKI ANALIZY ARCHITEKTURY SYSTEMU INFORMATYCZNEGO

**Streszczenie.** Praca przedstawia wykorzystanie metody oceny kompromisów architektury systemów informatycznych do oceny wpływu incydentów w bezpieczeństwie funkcjonowania systemu na bezpieczeństwo zasobów informacyjnych znajdujących się wewnątrz systemu.

Ocenę wpływu incydentów na bezpieczeństwo informacji rozpoczyna się od wyznaczenia wektorów ataku w systemie. Następnie szacuje się istotność zagrożenia, a na koniec ustala kryteria oceny zmiany poziomu atrybutów bezpieczeństwa dla zasobów informacyjnych znajdujących się wewnątrz elementów systemu teleinformatycznego.

**Słowa kluczowe:** incydent w bezpieczeństwie, analiza architektury systemu.

# EVALUATION OF THE PROTECTION LEVEL OF INFORMATIVE ASSETS BY USING A TECHNIQUE OF ESTIMATION SOFTWARE SYSTEM ARCHITECTURE

**Summary.** Work presents an application of method software system architecture evaluation to assessment of influence security incidents, which occur in time of system operation, on informative assets security that are inside solution.

The procedure starts from identification vectors of attack. Then assessment of incidents influence on information security is made. There are estimated: the probability occurrence and the importance of the incidents. At the end the criteria for assessment of changes the security attributes are set.

**Keywords:** security incident, system's architecture analysis.

## 1. Geneza problemu

Ocena bezpieczeństwa zasobów informacyjnych wymaga poznania obecnych i przyszłych zagrożeń mających wpływ na atrybuty bezpieczeństwa informacji znajdującej się wewnątrz systemu teleinformatycznego. Jak podaje E. Zio, w inżynierii niezawodności oraz inżynierii bezpieczeństwa wykonywane są trzy oceny umożliwiające poznanie zagrożeń oraz oszacowanie ich wpływu na działanie danego systemu [9]. Należą do nich: analiza ryzyka, przewidywanie przyszłych stanów systemu oraz określenie stopnia niepewności dotyczącego funkcjonowania systemu. Ocena wpływu incydentów na bezpieczeństwo zasobów informacyjnych jest elementem procesu przewidywania przyszłych stanów funkcjonowania systemu i powiązana została z określeniem stopnia niepewności.

Do działania tego wykorzystywane są informacje o incydentach w bezpieczeństwie, które wystąpiły w trakcie funkcjonowania systemu teleinformatycznego (STI), oraz ich skutkach dla ocenianego systemu. Dodatkowo należy przewidzieć możliwe przyszłe incydenty oraz ich wpływ na bezpieczeństwo funkcjonowania STI i jego zasobów informacyjnych. Opisane czynności wymagają oszacowania stopnia zmiany atrybutów bezpieczeństwa informacji poszczególnych zasobów. Oszacowanie to jest trudne, ponieważ naruszenia niektórych atrybutów bezpieczeństwa nie są łatwe do skwantyfikowania. Przykładem niech będzie trudność określenia naruszenia atrybutu poufności zasobu informacyjnego, wynikająca z faktu, że do momentu ujawnienia treści zasobu informacyjnego nie ma pewności, czy atrybut poufności danej wiadomości został naruszony oraz jaki jest stopień tego naruszenia.

Równie trudne jest określenie naruszenia atrybutu integralności informacji. Przyjęcie stosowanej w telekomunikacji miary wyrażającej stosunek liczby bitów, które uległy zmianie w trakcie transmisji sygnału w kanale komunikacyjnym w odebranej wiadomości, do całkowitej liczby bitów w wysyłanej wiadomości, oznaczanej skrótem BER (ang. Bit Error Ratio), nie przedstawia wszystkich aspektów zmiany atrybutu integralności wiadomości. Współczynnik BER informuje o zmianach bitów znajdujących się w wiadomości rozumianej jako pakiet, ramka lub plik. Nie informuje on o zmianach zawartości semantycznej przesyłanych lub przechowywanych wiadomości. Detekcję zmian bitów w wiadomości można wykryć, stosując kody korekcyjne, jednak kwestia oceny poziomu zmian w semantyce wiadomości oraz zmian istotnych elementów wiadomości wpływających na treść przekazu wymagają analizy treści każdej z wiadomości, co może wpływać na wydajność działania ocenianego STI.

Teoretycznie najprostszy do oszacowania jest wpływ incydentu na atrybut dostępności informacji – wiadomość może być dostępna lub nie. Mówimy wtedy o sytuacji binarnej, w której wyróżniane są dwa stany: dostępności lub braku dostępności informacji dla uprawnionych użytkowników [6]. Jednakże jest to podejście niedające się optymalizować. Innym sposobem określenia poziomu dostępności jest posługiwanie się czasem, w którym

informacja jest dostępna, oraz czasem, który jest potrzebny do przywrócenia dostępności informacji po wystąpieniu zdarzenia, w wyniku którego informacja jest niedostępna [6].

Zatem celem działania jest uniknięcie zdarzenia, gdy atakujący uzyska dostęp do chronionych zasobów informacyjnych. Dostęp ten przynosi korzyści atakującemu i staje się źródłem strat dla podmiotu mającego skompromitowany STI, w którym umieszczony był zasób (lub zasoby) informacyjny. Jest to sytuacja konfliktu, gdzie nie będą występowały strategie współpracy pomiędzy stronami. W opisanym przypadku będą wykorzystywane strategie typowe dla konfliktu, czyli strategie zdominowane. Strategie te mają na celu:

- dla atakującego – przejęcie kontroli nad zasobem informacyjnym i jego ewentualną kradzież,
- dla administratora systemu – niedopuszczenie do opisanego wcześniej zdarzenia.

Ocena poziomu bezpieczeństwa zasobów informacyjnych oraz predykcja przyszłych stanów systemu teleinformatycznego wymagają poznania incydentów, które wystąpiły w badanym lub podobnych rozwiązaniach. Wiedza ta umożliwia identyfikację wektorów ataków (nazywanych również ścieżkami propagacji zagrożeń), które były przyczyną (lub będą przyczyną) zakłóceń w funkcjonowaniu STI. Znajomość incydentów, które wystąpiły w STI, oraz ich skutków dla funkcjonowania rozwiązania pozwoli na:

- poznanie ich negatywnych skutków dla systemu teleinformatycznego oraz jego zasobów informacyjnych,
- opracowanie działań zabezpieczających, chroniących przed podobnymi zdarzeniami w przyszłości.

Zatem analizując STI, należy zidentyfikować zbiór możliwych incydentów, które mogą wystąpić w trakcie działania ocenianego rozwiązania, oraz przypuszczalne konsekwencje związane z pojawieniem się zidentyfikowanych zdarzeń. Czynność ta ma zapewnić działanie STI zgodnie z jego przeznaczeniem oraz skutecznie chronić zasoby informacyjne znajdujące się w nim.

Celem ataku jest uzyskanie dostępu do zasobów informacyjnych znajdujących się w STI lub uniemożliwienie dostępu do informacji użytkownikom systemu teleinformatycznego. Działanie wykonywane jest przez podwyższenie uprawnień atakującego. Intruz może być użytkownikiem STI lub znajdować się poza nim. Atakujący nie ma uprawnień, które umożliwiają mu dostęp do interesującego go zasobu informacyjnego. Celem jego działań będzie ominięcie lub oszukanie podsystemu odpowiedzialnego za weryfikację uprawnień użytkowników związanych z dostępem do pojedynczego zasobu informacyjnego lub grupy zasobów informacyjnych.

W dostępnej autorom literaturze przedmiotu nie znaleziono opisu metody, która w sposób systematyczny i powtarzalny pozwalałaby zmierzyć (oszacować) poziom bezpieczeństwa zasobów informacyjnych [8]. Dostępna autorom literatura przedmiotu opisuje wybrane typy zagrożeń dla wybranych elementów ocenianego rozwiązania. Nigdzie nie znaleziono

propozycji metody pozwalającej na powiązanie zidentyfikowanych zagrożeń z bezpieczeństwem STI oraz przechowywanymi w nim zasobami informacyjnymi.

Próbę kompleksowego podejścia do zagadnienia analizy bezpieczeństwa i niezawodności funkcjonowania systemów złożonych, do których należą STI, podjęto w pracach autorstwa I. Jóźwiaka i E. Zio [1, 9]. Obie prace prezentują wykorzystywanie grafów do identyfikacji elementów krytycznych w systemach złożonych. W procesie analizy wykorzystano drzewo użyteczności stosowane w metodzie oceny architektury systemów informatycznych określanej skrótem ATAM (ang. Architecture Trade-off Analysis Method) [3]. Metoda ta umożliwia identyfikację wymagań krytycznych dla poprawności funkcjonowania systemu informatycznego z grupy wymagań jakościowych przygotowanych dla systemu informatycznego [3, 4]. Bezpieczeństwo traktowane jest jako wymaganie jakościowe, dla którego trudno jest zdefiniować szczegółowe oczekiwania użytkownika rozwiązania, natomiast jeszcze trudniej jest określić miary weryfikujące uzyskany efekt wdrożenia wymagania [3, 4].

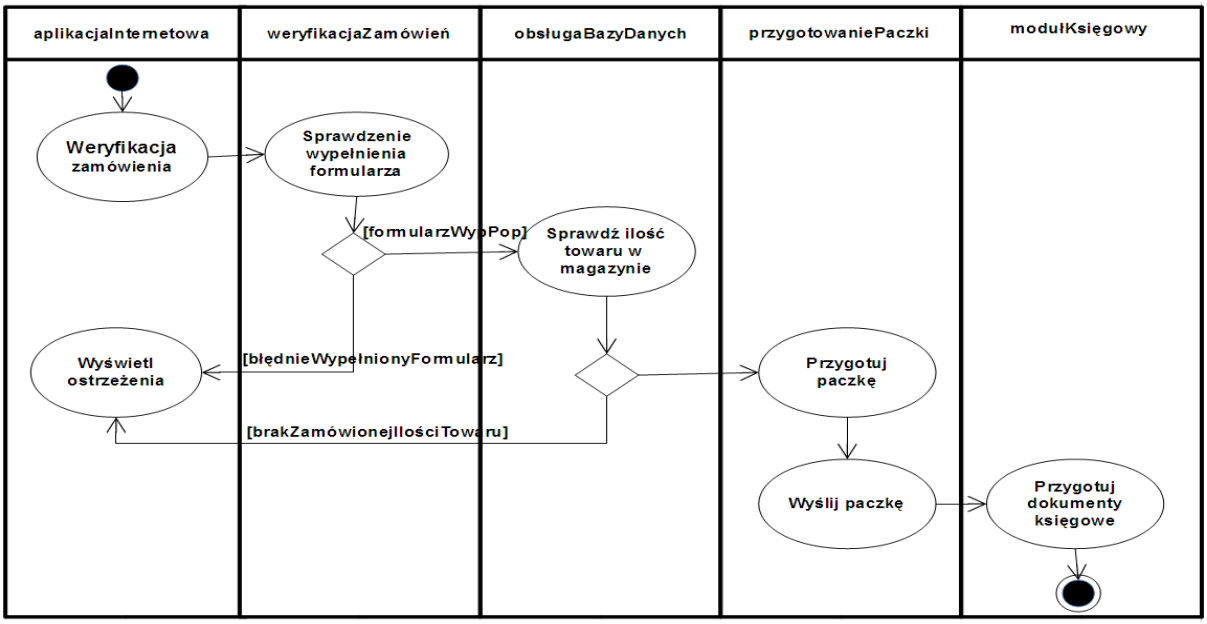
Można zatem zidentyfikować następujący problem badawczy, polegający na zweryfikowaniu możliwości wykorzystywania metody oceny architektury systemów informatycznych do ewaluacji poziomu bezpieczeństwa zasobów informacyjnych znajdujących się wewnątrz ocenianego rozwiązania. Do rozwiązania problemu zostanie wykorzystana metoda modelu symulacyjnego uproszczonego systemu teleinformatycznego.

## 2. Propozycja rozwiązania

Proces oceny zostanie przeprowadzony na przykładzie modelu STI, wykorzystywanego w obsłudze sklepu internetowego. Użytkownik łączy się z aplikacją internetową wykorzystywaną w sklepie, w celu złożenia zamówienia. Zamówienie złożone przez klienta jest weryfikowane pod względem formalnym (wypełnienie niezbędnych pól w formularzu, prawidłowo wprowadzona wielkość zamówienia itp.). Po pozytywnej weryfikacji treść zamówienia przekazywana jest do serwera bazy danych, a następnie do działu dystrybucji oraz działu księgowego firmy. W przypadku niepoprawnego wypełnienia formularza lub braku zamawianej ilości towaru, zamawiający proszony jest przez aplikację internetową o korektę zamówienia lub jego anulowanie. Po wykonaniu korekty zawartość formularza ponownie jest poddawana weryfikacji.

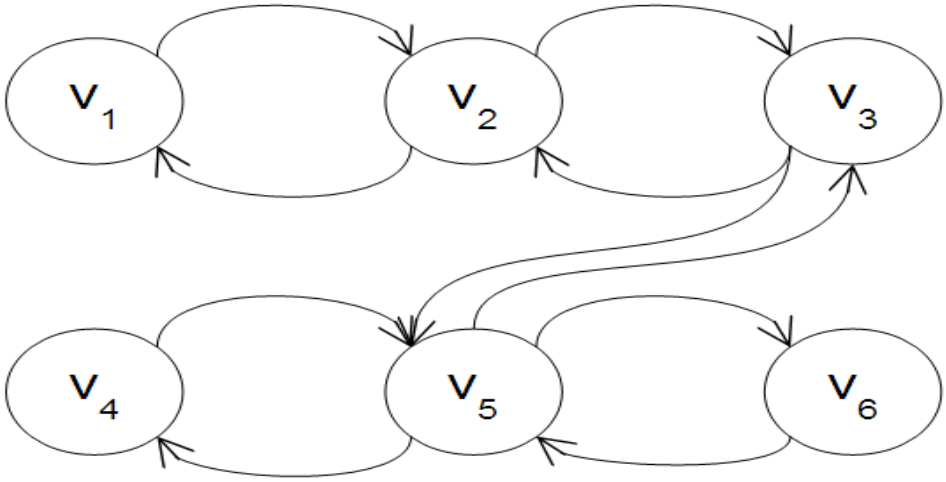
Model systemu przedstawiono na diagramie aktywności prezentującym interakcję użytkowników rozwiązania z systemem (rys. 1). Diagram prezentuje wymagania zawarte w dokumencie nazywanym specyfikacją wymagań systemowych dla ocenianego STI. Na podstawie diagramu trudno jest ustalić, który z elementów ocenianego rozwiązania ma dla niego kluczowe znaczenie. Zadanie to można wykonać, korzystając z diagramu

rozmieszczenia lub grafu będącego ekwiwalentem diagramu rozmieszczenia. Węzły grafu będą odpowiadały elementom składowym ocenianego systemu, natomiast łuki będą przedstawiać połączenia fizyczne i logiczne pomiędzy elementami systemu [1, 2, 9]. Graf jest uproszczeniem topologii połączeń ocenianego systemu teleinformatycznego. Umożliwia on identyfikację elementów kluczowych dla poprawnego funkcjonowania rozwiązania. Opisany graf przedstawiono na rysunku 2.




Rys. 1. Diagram aktywności modelu przykładowego systemu teleinformatycznego
Źródło: [2].
Fig. 1. Activity diagram of sample Information and Communication Technology system
Source: [2].

Przykładowy system zawiera następujące elementy: klienta sklepu (a dokładniej komputer, przy pomocy którego może on składać zamówienia w sklepie), serwer z oprogramowaniem obsługującym sklep z zainstalowanymi serwerami stron internetowych, bazy danych komputerów wykorzystywanych przez pracowników firmy do wykonywania zadań związanych z księgowością oraz spedycją zamawianych towarów.




Rys. 2. Graf przedstawiający połączenia pomiędzy elementami ocenianego STI
Źródło: [1].
Fig. 2. Graph shows connections between ICT system's elements
Source: [1].

Macierz incydencji zawiera informację o liczbie połączeń występujących w danym węźle. Krytyczność danego węzła będzie wyznaczona na podstawie stopnia każdego z węzłów grafu (rys. 2). W tym celu należy posłużyć się w macierzą incydencji $M$ (1), a następnie obliczyć stopnie wierzchołków grafu (2) [1]:

$$M = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 00 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 00 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 10 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 01 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 11 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 00 & 0 & 1 & 1 \end{bmatrix} \tag{1}$$

$$\begin{cases} d(v_3) = 6 \\ d(v_2) = d(v_5) = 4 \\ d(v_1) = d(v_4) = d(v_6) = 2 \end{cases} \tag{2}$$

gdzie: $v_1$ – komputer klienta, $v_2$ – sieć telekomunikacyjna, $v_3$ – aplikacja internetowa, $v_4$ – komputer w dziale dostaw, $v_5$ – serwer bazy danych, $v_6$ – komputer w dziale księgowości.

Na podstawie analizy zawartości macierzy incydencji oraz wyznaczonych stopni poszczególnych wierzchołków należy stwierdzić, że elementem kluczowym analizowanego systemu jest serwer bazy danych, który dostarcza informację do aplikacji internetowej oraz do działów księgowości i dystrybucji. Zatem jego ochrona będzie zadaniem o najwyższym priorytecie. Kolejnymi elementami mającymi kluczowe znaczenie dla realizacji zadań

ocenianego systemu są sieć telekomunikacyjna oraz aplikacja internetowa (stopnie obu węzłów wyrażone są cyfrą 4).

Elementy kluczowe dla funkcjonowania systemu, będą chronione w pierwszej kolejności gdyż ich uszkodzenie będzie skutkowało zakłóceniami w funkcjonowaniu ocenianego STI.

Opracowując plan działań zabezpieczających, poszukiwane będą odpowiedzi na następujące pytania:

- Jakich incydentów w bezpieczeństwie można się spodziewać w trakcie działania rozwiązania?
- Jak zidentyfikowane incydenty będą oddziaływać na elementy systemu teleinformatycznego przechowujące informacje?
- Jaki będzie wpływ incydentów na atrybuty bezpieczeństwa informacji?

Zatem prace związane z planowaniem działań ochronnych rozpoczyna się od identyfikacji możliwych zagrożeń, które będą stanowić incydenty w bezpieczeństwie funkcjonowania ocenianego systemu teleinformatycznego. Niepełną listę możliwych incydentów dla analizowanego przykładowego systemu teleinformatycznego przedstawiono w tabeli 1. Wymienione incydenty będą miały wpływ na bezpieczeństwo funkcjonowania analizowanego systemu. Lista jest zbiorem możliwych wektorów ataku, które mogą wystąpić w systemie. Jej wadą jest fakt, że nie przedstawia związków incydentów z atrybutami bezpieczeństwa informacji znajdującej się w systemie. Wymagana jest kolejna lista, łącząca wymienione zagrożenia z atrybutami bezpieczeństwa systemu teleinformatycznego.

Tabela 1

Lista możliwych incydentów w bezpieczeństwie funkcjonowania przykładowego STI wraz z elementami, na które one mogą oddziaływać

| Lp. | Opis incydentu | Elementy STI, na które wpływa incydent |
|---|---|---|
| 1. | zmiana treści zamówienia składnego przez klienta, wykonana przez oprogramowanie złośliwe zainstalowane w komputerze klienta | komputer klienta, aplikacja internetowa, komputer w dziale dostaw, serwer bazy danych, komputer w dziale księgowości |
| 2. | zwiększenie uprawnień przez atakującego i nieuprawniona modyfikacja danych w systemie | sieć telekomunikacyjna, serwer bazy danych |
| 3. | uszkodzenie elementów sieci telekomunikacyjnej | sieć telekomunikacyjna, aplikacja internetowa, komputer w dziale dostaw, serwer bazy danych, komputer w dziale księgowości |

Źródło: [2].

Pokazanie opisanej relacji pomoże oszacować możliwe konsekwencje incydentu dla zasobów informacyjnych znajdujących się w systemie. W tabeli 2 przedstawione zostały relacje pomiędzy incydentami a atrybutami bezpieczeństwa dla informacji przechowywanych w systemie teleinformatycznym.

Tabela 2

Wpływ incydentów w bezpieczeństwie funkcjonowania STI na atrybuty bezpieczeństwa informacji

| Lp. | Numer incydentu w tabeli 1 | Atrybuty bezpieczeństwa informacji, na które wpływa incydent | Przewidywane konsekwencje wystąpienia incydentu |
|---|---|---|---|
| 1. | 1 | Poufność, Integralność | Dla atrybutu Poufność – wysokie, dla atrybutu Integralność – średnie |
| 2. | 2 | Poufność, Integralność, Dostępność | Dla atrybutu Poufność – wysokie, dla atrybutu Integralność – wysokie, dla atrybutu Dostępność – wysokie |
| 3. | 3 | Dostępność | Dla atrybutu Dostępność – wysokie |

Źródło: opracowanie własne.

Szacowanie wpływu incydentów na bezpieczeństwo informacji znajdującej się w ocenianym systemie teleinformatycznym można zrealizować, wykorzystując odpowiednie relacje. Relacja $R_1$ łączy incydent z elementami infrastruktury technicznej ocenianego systemu. Wyrażona jest ona zależnością:

$$R_1^j = i_j \times E_j , \tag{3}$$

gdzie: $R^j_1$ – relacja prezentująca zbiór elementów wchodzących w skład wektora ataku dla j-tego zagrożenia, $j \in [1,m]$, $i_j$ – element zbioru incydentów I w bezpieczeństwie systemu teleinformatycznego, Ej – podzbiór zbioru E, zawierającego wszystkie elementy infrastruktury technicznej ocenianego systemu teleinformatycznego, które znajdują się w wybranej ścieżce ataku.

Druga relacja łączy wektor ataku (opisany w relacji $R^j_1$) z atrybutami bezpieczeństwa informacji znajdujących się wewnątrz elementów oraz przewidywanymi konsekwencjami ich wystąpienia. Konsekwencje wystąpienia incydentów podzielone zostały według nominalnej skali jakościowej, która ma trzy wartości: niskie, średnie i wysokie. Przyjęty sposób klasyfikacji wynika ze względów praktycznych. Na wstępnym etapie analizy trudno jest przewidzieć, jakie będą skutki wystąpienia incydentu dla zasobów informacyjnych. Próba kwantyfikowania skutków może być trudna, dlatego autorzy metody ATAM zalecają przyjęcie nominalnej skali jakościowej [3]. Relacja łącząca wektor ataku oraz atrybuty bezpieczeństwa wraz z szacowanymi konsekwencjami przedstawiona jest zależnością (4). Relacja ta posłuży do selekcji elementów ocenianego STI, które zostaną objęte działaniami zabezpieczającymi:

$$R_2 = R_1^j \times Aj \times Kj\,, \tag{4}$$

gdzie: $R_2$ – zbiór relacji łączących ścieżki ataku ($R^j_1$) z atrybutami bezpieczeństwa informacji oraz konsekwencjami wystąpienia incydentów dla zasobów informacyjnych, Aj – niepusty podzbiór zbioru A, zawierającego atrybuty bezpieczeństwa informacji, Kj – niepusty podzbiór zbioru K, zawierającego konsekwencje wystąpienia incydentów.

Wybór wektorów ataku wraz powiązanymi z nimi elementami infrastruktury technicznej STI będzie się odbywał na podstawie relacji $R_2$. Preferencja decydenta nie jest wykazywana w sposób jawny, jednakże ocena wartości wierzchołków grafu przedstawionego na rysunku 2 wskazuje na kluczowe znaczenie elementu infrastruktury technicznej dla ocenianego rozwiązania. Dla ocenianego rozwiązania kluczowym elementem jest baza danych, która gromadzi i udostępnia dane niezbędne do realizacji zadań wypełnianych przez sklep internetowy.

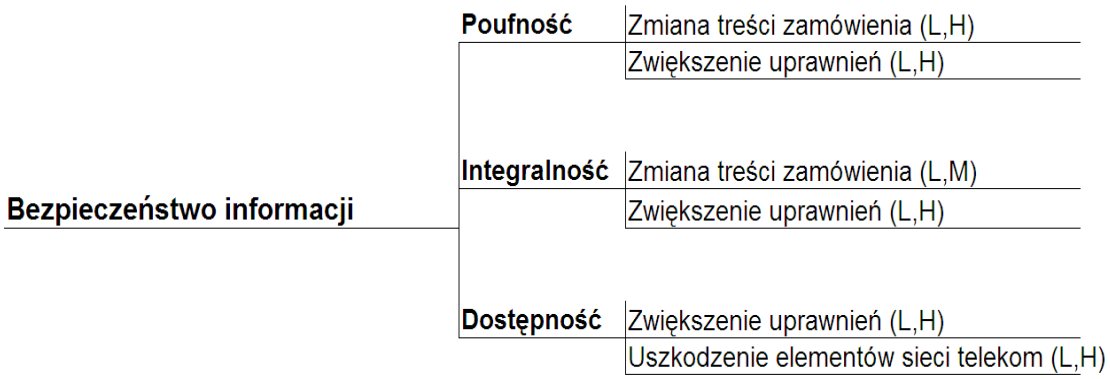
Stopnie wierzchołków będą stanowić jedno z kryteriów do selekcji tych elementów, które są istotne dla funkcjonowania ocenianego rozwiązania, oraz działań mających na celu ochronę zasobów informacyjnych. Kolejnym kryterium selekcji będzie wielkość szacowanych strat, będących konsekwencją wystąpienia w systemie incydentu.

Przetwarzanie tak zaprezentowanych relacji, nawet w przypadku nierozbudowanego systemu teleinformatycznego, wymaga zastosowania narzędzi wspomagających. Narzędzia, wykorzystując technologie relacyjnych baz danych, umożliwiają szybkie analizy wybranych przekrojów danych. Ich wadą jest fakt, że tworzone są przez wykonawców analiz. Autorzy nie spotkali narzędzia komercyjnego, które wykorzystywałoby ogólnie przyjęte techniki analizy oraz umożliwiłoby analizę wybranych przekrojów danych.

### 2.1. Ocena wpływu incydentu na bezpieczeństwo zasobu informacyjnego

Proces oceny wpływu incydentów na elementy badanego STI należy rozpocząć od poznania komunikatów wymienianych pomiędzy elementami znajdującymi się w poszczególnych wektorach ataku oraz składowanymi danymi. Następnie należy ustalić zakres zmian wartości poszczególnych atrybutów bezpieczeństwa systemu wraz z technikami pomiaru zmian. Kolejnym etapem będzie ustalenie wartości progowych, gdzie poziom zmian będzie nieakceptowany. Opisany algorytm postępowania zapewni obiektywność pomiaru oraz jego powtarzalność [7, 8].

Narzędziem wspomagającym analizy jest drzewo użyteczności, które przedstawiono na rysunku 3.




Rys. 3. Drzewo użyteczności wykorzystywane w ocenie poziomu bezpieczeństwa informacji
Źródło: opracowanie własne.
Fig. 3. The utility tree use for information security level assessment
Source: authors own work.

Szczegółowy opis zawartości drzewa użyteczności znajduje się w raporcie autorstwa R. Kazmana i innych [3]. W analizowanym systemie, na podstawie danych z tabel 1 i 2, przygotowuje się zestawienie przedstawiające szacowany poziom zmian danego atrybutu oraz możliwy poziom konsekwencji wystąpienia danego zdarzenia. W metodzie ATAM oba oszacowania wykonuje się za pomocą skali przedziałowej z jakościowym opisem wartości. Przyjmuje się, że oddziaływanie może przybierać wartości ze zbioru {S,M,H}, czyli małe, średnie lub wysokie, oraz wartość opisującą konsekwencje zdarzenia, również należącą do zbioru {S,M,H} [3]. Uzasadnieniem dla posługiwania się opisaną skalą przedziałową jest wygoda prowadzenia analizy, bez konieczności ustalania tego, co rozumie się przez poszczególne wartości. Nieposługiwanie się wartościami numerycznymi jest zdaniem autorów metody jej zaletą [3].

W analizowanym przykładzie zamówienie składane jest przez zamawiającego za pomocą formularza połączonego z bazą danych zawierającą informacje dotyczące towarów znajdujących się w ofercie sklepu internetowego. Jeżeli użytkownik nie wypełni formularza w sposób poprawny (nie zostanie wypełnione któreś z pól wymaganych) proszony jest o uzupełnienie zawartości formularza. Zawartość formularza przesyłana jest do aplikacji obsługującej zamówienia. Po pozytywnym zweryfikowaniu wypełnionego formularza, jego zawartość wprowadzana jest do bazy danych. W przypadku działania oprogramowania złośliwego, należy oczekiwać następujących zdarzeń: celowa zmiana danych identyfikacyjnych klienta, zmiana danych adresowych klienta lub zmiana wielkości zamówienia, powielenie treści zamówienia. Jeżeli oprogramowanie złośliwe uzyskało dostęp do treści zamówienia, wówczas naruszony został atrybut poufności wiadomości. Konsekwencją tego zdarzenia będą zmiany w treści zamówienia lub wielokrotne złożenie zamówienia o podobnej treści. Dla zachowania atrybutu poufności opisane zdarzenie ma wysoką istotność. Dla atrybutu integralności opisana istotność zdarzenia jest średnia,

ponieważ część zdarzeń zostanie obsłużona przez procedury weryfikacji danych umieszczonych w zamówieniu.

Ustalając kwantyfikację dla zmian dla poszczególnych atrybutów, przyjmuje się, że stwierdzenie naruszenia atrybutu poufności wyznaczane będzie w sposób binarny:

$$Z_p \in \{0,1\}, \tag{5}$$

gdzie: $Z_p$ – miara zmiany atrybutu poufności informacji, 0 – oznacza nienaruszenie atrybutu poufności, 1 – oznacza naruszenie atrybutu poufności.

Chcąc zachować klasyfikację przedziałową, należałoby zmienić sposób kwantyfikowania zmiany atrybutu poufności. Powstaje jednak pytanie, czy działanie to jest zasadne? Można przyjąć, że przyjęcie zbioru dwóch wartości 0 lub 1 spełnia zadanie opisu zmiany atrybutu poufności.

Zmiany atrybutu integralności wyznaczane będą na postawie ilorazu liczby zmienionych fragmentów przesłanego komunikatu do całkowitej liczby składników komunikatu, co pokazano w zależności (6):

$$\Delta = \frac{lzfw}{clfw}, \tag{6}$$

gdzie: $\Delta$ – miara zmiany zawartości komunikatu, lzfw – liczba zmienionych fragmentów ocenianej wiadomości, clfw – całkowita liczba fragmentów wiadomości.

Treść zamówienia należy odrzucić, kiedy $\Delta > 0{,}5$ i $\Delta \in \langle 0,1 \rangle$. Przyjęcie opisanego kryterium odrzucenia komunikatu wynika z czasu potrzebnego do naprawienia komunikatu przez system informatyczny przetwarzający zamówienia. W przypadku dużej liczby zamówień, które należy naprawić, pamięć operacyjna oraz procesory komputera realizującego naprawę komunikatów będą wykorzystane w stopniu uniemożliwiającym wykorzystanie komputera, zatem stopa uszkodzeń wynosząca 0,5 kwalifikuje wiadomość do usunięcia z systemu i ponownego wprowadzenia przez klienta sklepu.

Kryteria zmian atrybutu dostępności można wyznaczyć binarnie, korzystając z dwóch wartości {0,1} (gdzie 0 oznacza brak dostępności informacji, zaś 1 oznacza dostępność informacji). Innym sposobem oceny dostępności będzie użycie reprezentacji znanej z inżynierii niezawodności, a wykorzystanej w zintegrowanej metodzie oceny dostępności informacji opracowanej przez A. Michalskiego. Ocenę tą wyrażono za pomocą równania [6]:

$$A = \frac{MTTF}{MTTF + MTTR}, \tag{7}$$

gdzie: A – dostępności informacji, MTTF – średni czas pomiędzy rozpoczęciem pracy a chwilą utraty przez system sprawności, MTTR – średni czas niezbędny do naprawy i przywrócenia stanu gotowości [6].

Korzystając z binarnego opisu dostępności informacji, stwierdza się tylko stan dostępności lub niedostępności informacji. Druga zależność pozwala ocenić dostępność, wyznaczając czas, jaki upływa do momentu wystąpienia awarii, oraz czas niezbędny do jej usunięcia i przywrócenia dostępu do zasobu informacyjnego.

## 3. Zakończenie

Wyznaczenie przedziałów zmian atrybutów bezpieczeństwa informacji wymaga znajomości zasad działania analizowanego rozwiązania oraz struktury komunikatów przesyłanych pomiędzy jego elementami. Dalsze prace poświęcone zostaną wyznaczeniu przedziałów liczbowych zmian wartości atrybutów bezpieczeństwa dla informacji znajdujących się wewnątrz systemu teleinformatycznego.

Problemem jest skwantyfikowanie wartości atrybutu poufności informacji. Przyjęty w pracy binarny zbiór wartości okazuje się być nie zawsze adekwatny do opisu rzeczywistego naruszenia tego atrybutu. Wartość 1, odpowiadająca utracie atrybutu poufności danej wiadomości, może zostać użyta tylko wtedy, gdy dana wiadomość zostanie ujawniona. W przeciwnym razie można przypuszczać, że do takiego naruszenia doszło. Nie ma też podstaw, by stwierdzić, że nie doszło do zmiany atrybutu poufności wiadomości, do której uzyskała dostęp osoba nieuprawniona.

Zaleca się przygotowanie oprogramowania, które będzie wspomagać pracę zespołu analitycznego, umożliwi przyspieszenie procesu analizy ocenianego systemu teleinformatycznego. Posiadanie takiego narzędzia wynika z konieczności przetwarzania kilku przekroi danych. Ręczne przetwarzanie danych będzie wydłużało proces analizy.

### Bibliografia

1. Jóźwiak I.J., Szleszyński A.: The use of the evaluation method of software system architecture to assess the impacts on information security in Information and Communication Technology systems. Journal of KONBiN, No. 4(24)2012, Publishing the Air Force Institute of Technology, Warszawa 2012, p. 59-70.
2. Jóźwiak I.J., Szleszyński A.: Wykorzystanie metody modelowania zagrożeń do oceny wpływu incydentów na poziom bezpieczeństwa zasobów informacyjnych w systemach teleinformatycznych. 11th International Conference on Diagnostic of Processes and Systems, Zielona Góra 2013 (w przygotowaniu).

3. Kazman R., Klein M., Clements P.: Method for Architecture Evaluation, Technical report. CMU/SEI-2000-TR004,ESC-TR-2000-004, Carnegie Mellon Software Engineering Institute, Pitsburgh, PA 15213-3850.
4. Kuchta D., Szleszyński A., Witkowski M.: Metodyka opracowania scenariuszy przebiegu incydentów w bezpieczeństwie systemów, wykorzystywanych w zarządzaniu bezpieczeństwem informacji w wojskowych systemach teleinformatycznych. WSOWL, Wrocław 2012.
5. Michalski A.: Bezpieczeństwo informacji w przypadku awarii lub katastrofy. Zeszyty Naukowe Politechniki Śląskiej, s. Organizacja i Zarządzanie, z. 61, Politechnika Śląska, Gliwice 2012, s. 243-254.
6. Michalski A.: Dostępność informacji w organizacji gospodarczej. Wydawnictwo Politechniki Śląskiej, Gliwice 2007.
7. Sienkiewicz P.: Wartości, oceny i efektywność systemów. Zeszyty Naukowe AON, z. 4/1994, Warszawa 1994, s. 72-85.
8. Vaugh R.B., Heming R., Siraj A.: Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy, Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), IEEE Computer Society 2002.
9. Zio E., Golea L.R.: Analyzing the topological, electrical and reliability characteristics of a power transmission system for identifying its critical elements. Reliability Engineering and System Safety (2012), p. 67-74.

**Abstract**

Paper presents an application of method software systems architecture analysis to assess the influence of incidents on informative assets security stored by ICT system. The work contains a brief description of sample ICT system that supports e – commerce. The system's activity diagram is presented on figure 1. The diagram shows a selected view of ICT system operation which is related to system's requirements. Next a graph is use to presents physical and logical connections between the ICT system's elements (fig. 2). It is an equivalent for deployment diagram. The graph's vertexes are the substitute ICT system elements. An incidence matrix enables specify vertex degree. The vertex degree describes importance each of ICT element (expressions 1 and 2). The quantification the values of security attributes is provided by using utility tree (fig. 3). Approved values of changes into security attributes becomes the thresholds for decision problems. Proposed metrics for assessment probable changes of information security attributes are presented in expressions 5, 6 and 7.