PORTFOLIO:

Opracowanie koncepcji metodyki oceny ryzyka bezpieczeństwa systemów informatycznych

Autorzy: Paweł Skrzyński, Piotr Szwed

Centrum Inteligentnych Systemów Informatycznych Akademia Górniczo-Hutnicza im. Stanisława Staszica al. Mickiewicza 30, 30-059 Kraków
budynek C 2 pokój 426 tel.: 12 617 44 53 www.isi.agh.edu.pl **isi@agh.edu.pl**

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Koncepcja metodyki oceny ryzyka bezpieczeństwa systemów informatycznych
Raport SPIN

Piotr Szwed i Paweł Skrzyński

29 październik 2014

1 Wstęp

Wraz z rozpowszechnieniem technologii internetowych, większość współcześnie rozwijanych systemów informatycznych wykorzystuje publiczną infrastrukturę sieciową do celów komunikacji, integracji i zdalnego dostępu. Rozwiązania te, przynosząc duże możliwości rozwoju i zyski, zwiększają podatność systemów na nowy typ zagrożeń. W rezultacie, problemy bezpieczeństwa zaczynają odgrywać ważną rolę podczas rozwoju oprogramowania i analiza ryzyka związanego z bezpieczeństwem jest postrzegana, jako niezbędna czynność podczas wdrożenia oprogramowania.

Pojawieniu się nowych technologii towarzyszył zwiększony nacisk na produktywność, redukcję kosztów oraz wykorzystanie zwinnych metodyk rozwoju oprogramowania. Zmianom obserwowanym w ostatnich latach w niewielkim stopniu towarzyszyła ewolucja metodyk oceny ryzyka definiowanych przez różne standardy, których korzenie sięgają lat osiemdziesiątych XX wieku. Standardy te są najczęściej opracowywane przez publiczne organizacje i przeznaczone są zazwyczaj dla sektora publicznego lub dużych instytucji. Przeprowadzenie oceny ryzyka zgodnie z tymi metodykami może być bardzo znacznym wysiłkiem, które całkowicie zniwelowałoby zyski płynące ze zwinnego rozwoju.

Obecne rozwiązania praktyczne, zwłaszcza w przypadku małych i średnich systemów, pomijają ocenę ryzyka opartą na standardowych modelach zagrożeń i ich prawdopodobieństw, podatności i oczekiwanych strat. Raczej stosowane są takie podejścia, jak najlepsze praktyki, wartościowanie zasobów lub analizy scenariuszowe.

Prowadzi to do powstania potencjalnej luki w procesie zarządzania ryzykiem: dla konkretnego systemu zagrożenia nie są w wyczerpujący sposób analizowane, wybór funkcji bezpieczeństwa nie jest oparty na modelach ryzyka, ale na rzadko uaktualnianych listach zabezpieczeń, które odzwierciedlają najlepsze praktyki w ramach organizacji.

W raporcie opisano koncepcję lekkiej metodyki oceny ryzyka, która w zamierzeniu ma na celu wypełnienie luki pomiędzy ciężkimi metodykami oceny ryzyka i praktykami towarzyszącymi zwinnym zasadom rozwoju. Metodyka zakłada budowę modeli ryzyka, a następnie przeprowadzenie obliczeń wykorzystujących techniki wnioskowania charakterystyczne dla rozmytych map kognitywnych (ang. *FCM: Fuzzy Cognitive Maps*). Mapy FCM są użyte do opisu zależności pomiędzy aktywami i do agregacji ryzyka związanego z aktywami niższego poziomu (np.: sprzętu, modułów oprogramowania, ludzi) i ich wpływu na profile ryzyka takich aktywów wyższego poziomu, jak procesy lub usługi.

Zastosowanie metodyki jest przedstawione na rzeczywistym przykładzie systemu telemedycznego SWOP zapewniającego zdalne monitorowanie stanu zdrowia pacjentów, usługi składowania i dostępu do danych oraz zdalne konsultacje.

2 Bezpieczeństwo systemów informatycznych i metody oceny ryzyka

Zgodnie z [10, 25] *bezpieczeństwo to zabezpieczenie zastosowane w systemie informatycznym w celu zapewnienia integralności danych i funkcji systemu, ich dostępności, autentyczności oraz poufności.*

Pierwsze próby zastosowania oceny ryzyka związanego z bezpieczeństwem dotyczyły przemysłu nuklearnego, dla którego budowano modele probabilistyczne służące ocenie możliwości pojawienia się katastroficznych awarii w instalacjach atomowych [25]. W 1979 roku *National Bureau of Standards*[1], amerykańska organizacja rządowa zajmująca się opracowaniem standardów i wdrożeniami technologii, zaproponowała metrykę oceny ryzyka znaną jako *ALE* (*Annual Loss Expectancy*) [12]. Metryka ta, dedykowana dla systemów niekrytycznych ze względu na bezpieczeństwo, oparta była na analizie konsekwencji zdarzeń mających szkodliwy wpływ na funkcjonowanie systemu. Jeżeli zbiór tych zdarzeń oznaczymy jako E, wówczas metryka obliczana jest zgodnie z (1) jako sumę iloczynów częstotliwości wystąpienia szkodliwych zdarzeń $f(e)$ i spowodowanych przez nie strat $l(e)$ wyrażonych w dolarach.

$$r = \sum_{e \in E} f(e) \cdot l(e) \tag{1}$$

To podejście do definiowania ryzyka znalazło zastosowanie w wielu znanych metodykach i standardach, np.: CRAMM [8] lub NIST 800-30 [22]. W wybranych opracowaniach statystyczny termin częstość (ang. *frequency*) został zastąpiony przez prawdopodobieństwo (ang. *likelihood*, *probability*), natomiast starta (ang. *loss*) przez wpływ (ang. *impact*).

[1] obecnie *NIST: National Institute of Standards and Technology*

Opracowane standardy definiując ryzyko często posługują się następującymi elementami składowymi:

1. Listą zagrożeń (ang. *threats*) T oraz prawdopodobieństwem ich pojawienia się $p(t)$
2. Listą aktywów (użytecznych i wartościowych składników systemu lub osób) A
3. Oszacowaniem podatności (ang. *vulnerability*) aktywów na zagrożenia $v(a,t)$
4. Oszacowaniem straty, która może być wynikiem pojawienia się zagrożenia w odniesieniu do konkretnego aktywa $l(a,t)$

Przy takich założeniach, wyznaczana wartość ryzyka podana jest wzorem (2). Formuła ta pośrednio definiuje zakres czynności niezbędnych do oceny ryzyka. Obejmuje on zebranie list zagrożeń i aktywów oraz ustalenie prawdopodobieństw, podatności i możliwych strat.

$$r = \sum_{t \in T} \sum_{a \in A} p(t) \cdot v(a,t) \cdot l(a,t) \tag{2}$$

Warto zwrócić uwagę na nakłady organizacyjne niezbędne do przeprowadzenia oceny. Dla n zagrożeń i m aktywów niezbędne jest podanie $n+2n \cdot m$ liczbowych wartości. Przyjmując n i m rzędu 50, jako typowe wartości dla systemów średniej wielkości, konieczne jest ustalenie ponad 5000 współczynników liczbowych. Mogą być one ustalane na podstawie zdarzeń historycznych (np. częstotliwości wystąpienia zdarzeń), a także wywiadów przeprowadzanych z ekspertami. W większości przypadków podanie konkretnych wartości jest niemożliwe, stąd stosowane są skale porządkowe określające poziomy, np. L (niski), M (średni) i H (wysoki).

Pomimo dużej popularności metryki ALE, jej zastosowanie do oceny ryzyka jest niejednokrotnie krytykowane [11], ze względu na uzależnienie od nastawienia oceniającego (ang. *cognitive bias*), częsty brak danych statystycznych, problemy z oceną strat i doborem przedziałów skal porządkowych, zależnych od charakteru prowadzonej działalności, np. czy M (poziom średni strat) to 100$–1000$, czy raczej 500$–10000$. Na podkreślenie zasługuje także bardzo wysoki koszt całego procesu (setki osobogodzin spędzonych na wywiady z ekspertami).

Zgodnie z [25] *ocena ryzyka* to proces analizy i interpretacji ryzyka składająca się z trzech głównych etapów:

1. Określenia zakresu oceny i wybrania jej metody
2. Zbierania i analizy danych
3. Interpretacji rezultatów

W rozlicznych standardach i metodach zebranych w *ENISA Inventory* [9], w tym najbardziej popularnych: ISO/IEC 27005 [13], NIST 800-30 [22] and CRAMM [8], ocena ryzyka nie jest więc traktowana wyłącznie jako analityczna metoda szacowania ryzyka. Raczej jest przedstawiana jako złożony proces zarządzania ryzykiem bezpieczeństwa systemów informatycznych, na który składają się takie czynności, jak identyfikacja aktywów, zagrożeń i podatności, prawdopodobieństw ich wystąpienia, potencjalnych strat, a także efektywności i kosztów zabezpieczeń. Uwzględniają one także typowe decyzje: akceptację ryzyka, zmniejszenie ryzyka poprzez zastosowanie zabezpieczeń oraz transfer ryzyka (np. ubezpieczenie). Te dwie ostatnie decyzje wiążą się zazwyczaj z dodatkowymi kosztami, które powinny być nie większe niż oczekiwana strata. Stąd standardy, oprócz definiowania metod oceny, zazwyczaj definiują także ramy organizacyjne dla kontroli ryzyka w szerszym kontekście zarządzania bezpieczeństwem. Jak można zauważyć, ocena ryzyka przy zapewnieniu zgodności z wybranym standardem może być dużym i kosztownym zadaniem, często regularnie wykonywanym przez dedykowane zespoły wewnątrz organizacji.

Praktyczne realizacje oceny ryzyka i zarządzania nim obejmują różne podejścia:

- Zintegrowane ramy zarządzania ryzykiem biznesowym (ang. *Integrated Business Risk-Management Frameworks*) pozwalają na pominięcie szczegółów technicznych i rozważają bezpieczeństwo systemów informatycznych w szerszym kontekście zarządzania ryzykiem biznesowym obejmującym różne elementy architektury korporacyjnej. Przykładem dojrzałej metodyki zaliczającej się do tej grupy jest SABSA [24].

- Metodyki oparte na wartościowaniu aktywów (ang. *Valuation-Driven Methodologies*) pomijają trudne do oceny prawdopodobieństwa wystąpienia zagrożeń. Istotą tych metod jest dobór zabezpieczeń do szacowanej wartości aktywów (bardziej cenne aktywa, kluczowe dla funkcjonowania systemu powinny mieć mocniejsze zabezpieczenia).

- Analizy scenariuszowe (ang. *Scenario Analysis Approaches*) skupiają się na identyfikacji i testowaniu scenariuszy działań, które mogłyby zagrozić bezpieczeństwu systemu. Zazwyczaj przeprowadzane są testy w oparciu o znane scenariusze naruszeń bezpieczeństwa, testy te są powtarzane okresowo, zwłaszcza po opublikowaniu nowych metod włamań do systemów.

- Najlepsze praktyki (ang. *Best Practices*) polegają na zastosowaniu predefiniowanego zbioru zabezpieczeń i rozwiązań charakterystycznych dla danego typu aktywów. Zbiór ten jest określony jako standard obowiązujący w danej organizacji.

Równolegle do praktyki biznesowej, od wielu lat w środowisku akademickim były prowadzone prace mające na celu budowę modeli ryzyka wykraczających poza metrykę ALE oraz zastosowanie ich do ewaluacji rzeczywistych lub hipotetycznych systemów. W wielu przypadkach towarzyszyły im propozycje metodyk lub wytycznych, także często były one wspierane przez dedykowane prototypowe oprogramowanie. Wśród modeli używanych się do analizy niezawodności i bezpieczeństwa można wymienić drzewa błędów (ang. *Fault Trees*), drzewa zdarzeń (ang. *Event Trees*, drzewa ataków (ang. *Attack Trees*), modele Markowa i wiele innych [32, 4, 23, 26, 7, 19, 5, 27, 6]. Bardziej wyczerpujący przegląd omawianych zagadnień można znaleźć w [29, 30].

3 Rozmyte mapy kognitywne

Mapy kognitywne zostały zaproponowane przez Axelroda [3], jako narzędzie badania decyzji politycznych, następnie zostały rozszerzone przez Kosko [15, 16] do postaci rozmytych map kognitywnych (ang. *FCM: Fuzzy Cognitive Map*) przez wprowadzenie rozmytych wartości. Opisano wiele zastosowań FCM, np.: w modelowaniu ryzyka projektowego [18], zarządzaniu kryzysowym i podejmowaniu decyzji, analizie rozwoju systemów ekonomicznych, wprowadzaniu technologii [14], analizie ekosystemów [20], prognozowaniu rozwoju jednostek naukowych [28], analizie sygnałów, wsparciu procesów decyzyjnych w medycynie. Przegląd zagadnień związanych z zastosowaniami FCM i szerszą listę literatury można znaleźć w [1] and [21].

Mapy FCM mają postać grafu skierowanego, którego wierzchołki reprezentują pojęcia, natomiast krawędzie występujące pomiędzy nimi związki przyczynowe. Zbiór rozpatrywanych pojęć $C = \{c_1, \ldots, c_n\}$ opisuje zdarzenia, warunki lub inne czynniki istotne z punktu widzenia opisu modelowanego systemu. Stan systemu A jest n-wymiarowym wektorem poziomów aktywacji pojęć ($n = |C|$). W odróżnieniu od sieci Petriego warunków i zdarzeń lub maszyn skończenie-stanowych, gdzie rozpatruje się dwa poziomy aktywacji: 0 - nieaktywne i 1 – aktywne, stopień aktywacji pojęcia w FCM może być rozmyty: można mu przypisać dowolną wartość z przedziału $[0, 1]$ lub $[–1, 1]$.

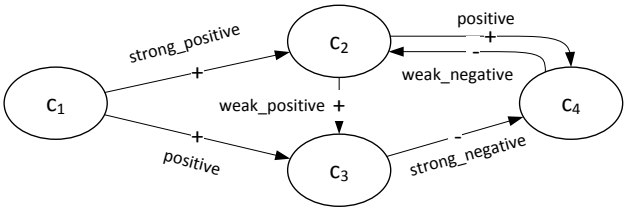
Zależności przyczynowe pomiędzy pojęciami są w FCM reprezentowane są przez łuki i nadane im wagi. Dodatnia waga łuku łączącego dwa pojęcia c_i i c_j oznacza, że wzrost poziomu ci skutkuje wzrostem poziomu c_i, natomiast ujemna oznacza przeciwny kierunek zmian. W najprostszej postaci FCM jako wagi łuków e_{ij} wykorzystuje się wartości $\{-1, 0, 1\}$. Są one przedstawiane graficznie jako, odpowiednio, znak (+) przypisany do łuku, brak łuku lub znak (−). Budując model FCM stosuje się również bardziej finezyjne specyfikacje zależności: mają one postać wartości lingwistycznych, np.: *strong_negative*, *negative*, *medium_negative*, *neutral*, *medium_positive*, *positive*, *strong_positive*, które mogą być odwzorowane w odpowiednie wartości

liczbowe z zakresu $[-1, 1]$.

W celu przeprowadzenia wnioskowania konstruowana jest macierz wpływów $E = [e_{ij}]$ o rozmiarach $n \times n$. Element eij macierzy określony jest na podstawie wagi wpływu c_j na c_i lub ma wartość 0, jeżeli takiego wpływu nie ma.

Rys. 1 pokazuje przykład grafu FCM, którego wierzchołkom przypisano cztery pojęcia c_1, c_2, c_3 i c_4, natomiast krawędziom lingwistyczne wagi wpływu. Odpowiadająca mu macierz E jest określona wzorem (3). Dobór współczynników macierzy odpowiadających wartościom lingwistycznym określającym wpływ jest arbitralny: w tym przypadku są to wartości: -1, -0.66, -0.33, 0, 0.33, 0.66 i 1.

$$E = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -0.33 \\ 0.66 & 0.33 & 0 & 0 \\ 0 & 0.66 & -1 & 0 \end{bmatrix} \tag{3}$$



Rysunek 1: Przykład grafu FCM. Wierzchołkom przypisano pojęcia, natomiast skierowanym krawędziom lingwistyczne wagi wpływu.

Wnioskowanie na podstawie FCM ma na celu określenie scenariusza rozwoju systemu mającego postać ciągu stanów:

$$\alpha = A(0), A(1), \ldots, A(k), \ldots$$

Pierwszym elementem ciągu $A(0)$ jest początkowy wektor poziomów aktywacji pojęć wykorzystywanych w FCM. Kolejne wyrazy ciągu obliczane są zgodnie z równaniem (4). W $k + 1$ iteracji wektor $A(k)$ jest mnożony przez macierz wpływów E, a następnie jego elementy są sprowadzane do standardowego zakresu za pomocą funkcji aktywacji (ang. *activation function*, *splashing function*).

$$A_i(k+1) = S_i(\sum_{j=1}^{n} e_{ij}\, A_j(k)) \tag{4}$$

Dobór funkcji aktywacji uzależniony jest założeń modelu obliczeniowego: zakresu zmienności poziomów aktywacji oraz decyzji, czy poziomy aktywacji mają przybierać wartości dyskretne, czy też ciągłe. Wynikiem pomnożenia n-wymiarowej macierzy E przez wektor $A(k)$, gdzie $|e_{ij}| \leqslant 1$ i $|a_i| \leqslant 1$

jest wektor, którego elementy mieszczą się w przedziale $[-n, n]$. Zakres ten musi zostać sprowadzony przez funkcję aktywacji do przedziału $[-1, 1]$ lub $[0, 1]$ przy zachowaniu warunku monotoniczności oraz spełnieniu odpowiednio $S(0) = 0$ lub $S(0) = 0.5$.

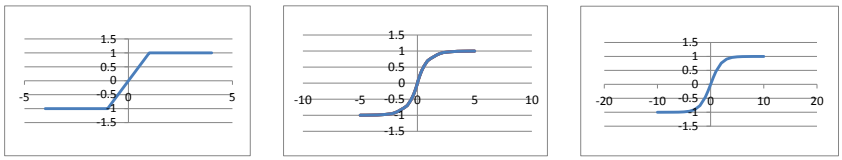
Podczas analiz wykorzystano trzy funkcje aktywacji:

$$S_{cut}(x) = \begin{cases} -1, & \text{if } x < -1 \\ +x, & \text{if } x \geqslant -1 \text{ and } x \leqslant 1 \\ 1, & \text{if } x > 1 \end{cases} \tag{5}$$

$$S_{exp}(x) = \begin{cases} 1 - \exp(-mx), & \text{if } x \geqslant 0 \\ -1 + \exp(-mx), & \text{if } x < 0 \end{cases} \tag{6}$$

$$S_{tanh}(x) = \frac{\exp(mx) - \exp(-mx)}{\exp(mx) + \exp(-mx)} \tag{7}$$

Funkcja $S_{cut}(x)$ (Rys. 2a) sprowadza wartość wejściową do przedziału $[-1, 1]$ zastępując wartości spoza przedziału wartościami granicznymi. Funkcja $S_{exp}(x)$ (Rys. 2b) ma przebieg podobny do $S_{cut}(x)$ ale bardziej wygładzony i spłaszczony (za co odpowiada stała dodatnia stała m o wartości rzędu $1 - 5$. Funkcja $S_{tanh}(x)$ (Rys. 2c) to zmodyfikowany tangens hiperboliczny; stała m występująca we wzorze (7) pozwala na sterowanie nachyleniem krzywej.



(a) (b) (c)

Rysunek 2: Wykresy funkcji: (a) $S_{cut}(x)$, (b) $S_{exp}(x)$ oraz (c) $S_{tanh}(x)$

Warto zwrócić uwagę, że w literaturze, np.: [21] można spotkać się z inną postacią równania (4):

$$A_i(k+1) = S_i(\sum_{\substack{j=1 \\ j \neq i}}^{n} e_{ij}\, A_j(k) + A_i(k)) \tag{8}$$

Formuła (8) jawnie zakłada, że wyznaczone w danej iteracji $k+1$ zmiany poziomu aktywacji pojęcia c_i kumulują się z poprzednią wartością $A_i(k)$. Odpowiada to ukrytemu założeniu, że współczynniki $e_i i$ mają wartość 1. W ogólnym przypadku nie musi to być prawdą; z tego powodu w analizowanym modelu posłużono się równaniem (4), jako bardziej ogólnym, ustalając indywidualne wartości wpływów eii.

Ciąg kolejnych stanów $\alpha = A(0), A(1), \ldots, A(k), \ldots$ wyznaczonych w wyniku wnioskowania jest w zasadzie nieskończony. Jednakże pokazano, że po k iteracjach, gdzie k jest liczbą bliską rzędu macierzy E osiągany jest stan ustalony lub można stwierdzić wystąpienie cyklu. Stąd, kryterium zatrzymania algorytmu wnioskowania w kroku k:

$$\exists j < k \colon d(A(k), A(j)) < \epsilon, \tag{9}$$

gdzie d jest odległością, a ϵ małą liczbą, np.: 10^{-2}.

Ciag stanów α może być interpretowany na dwa sposoby:

1. Jako reprezentacja zachowania modelowanego systemu. W tym przypadku kolejno wyznaczone stany stanowią scenariusz ewolucji systemu.

2. Jako niemonotoniczny rozmyty proces wnioskowania, w którym wybrane elementy ustalonego stanu mogą być traktowane jako rezultaty końcowe. Przy takiej interpretacji wystąpienie cyklu może być traktowane jako pojawienie się problemu nierozstrzygalnego.

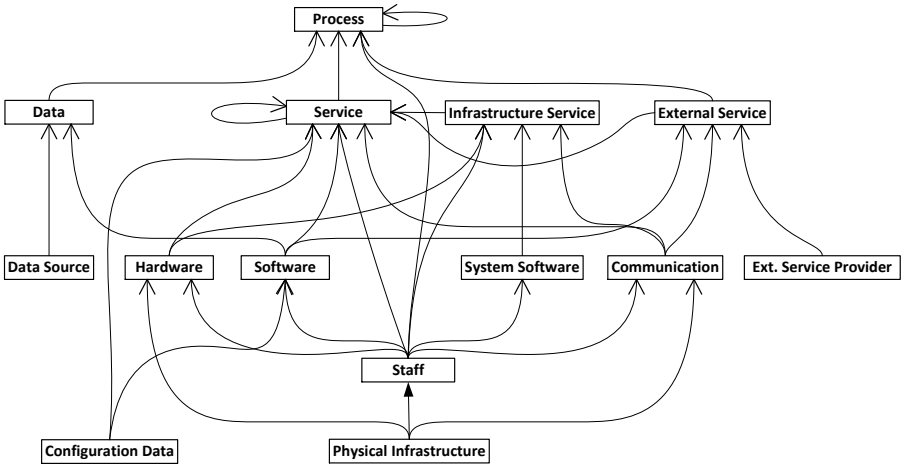
W niniejszym raporcie mapy FCM są narzędziem modelowania ryzyka, dlatego też użyto je w drugim z wymienionych trybów.

4 Metodyka oceny ryzyka

Metodyka oceny ryzyka obejmuje podstawowe czynności występujące w różnych standardach i wytycznych, np.: [10, 13, 22, 17]. Jednakże jej cechą charakterystyczną jest użycie modelu FCM dla wyrażenia wzajemnych zależności pomiędzy aktywami, co pozwala na uwzględnienie ich podczas agregacji ryzyka.

4.1 Model koncepcyjny

Przyjęty model koncepcyjny (Fig. 3) przypisuje aktywom abstrakcyjną wartość – *użyteczność* oraz definiuje ich powiązania, jako *drzewo wartości dodanej* (ang. *AVT - Added Value Tree*). Drzewo AVT jest hierarchiczną strukturą, w której komponenty niższego poziomu są źródłem wartości użytkowej dla elementów nadrzędnych. U góry drzewa są umieszczone są kluczowe procesy, są one identyfikowane zgodnie z kierunkami rozwoju biznesowego (ang. *business drivers*). Wartość użytkowa procesów zależy od danych i wykorzystywanych usług. Z kolei Źródłami wartości danych mogą być: użytkownicy, czujniki, zewnętrzni dostawcy danych, itd. Usługi uzależnione są od oprogramowania, sprzętu, infrastruktury komunikacyjnej, obiektów fizycznych (budynki, pomieszczenia, klimatyzacja, zasilanie) oraz usług zewnętrznych (np.: PKI – Public Key Infrastructure). Relacje zależności pomiędzy klasami zasobów zilustrowano na Rys. 3 za pomocą strzałek. Ich kierunek wskazuje przepływ wartości użyteczności.



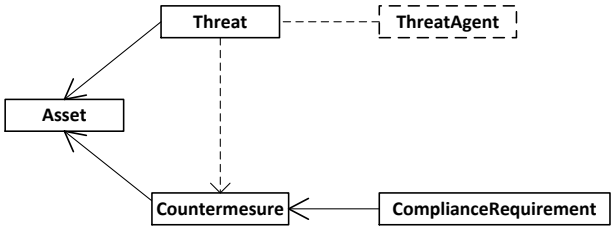
Rysunek 3: Aktywa i ich zależności

Poziomy użyteczności przypisane aktywom mogą być interpretowane jako agregacje różnych atrybutów jakości: bezpieczeństwa, niezawodności, użyteczności, itd. Zmiany wartości dla aktywów niższego poziomu mają wpływ na wartość użytkową elementów wyższego poziomu, które je wykorzystują. Należy zauważyć, że drzewiasta struktura zależności pomiędzy klasami aktywów generuje kratę zależności pomiędzy ich instancjami, np. usługi analizy danych, składowania danych i dostępu zależą od bazy danych (rodzaju oprogramowania).

Model ryzyka przedstawiony na Rys. 4 zakłada, że wartość użytkowa aktywów może zostać zmniejszona przez zagrożenie. W prezentowanym podejściu opowiedziano się za identyfikacją zagrożeń opartą na aktywach, w przeciwieństwie do modeli koncentrujących się na modelowaniu wrogich działań agentów, np. drzew ataków [23].

Negatywne wpływy zagrożeń na aktywa mogą zostać skompensowane przez odpowiednio dobrane zabezpieczenia. Same zabezpieczenia nie są źródłem dodatkowej wartości użytkowej – pozwalają jedynie na ograniczenie ryzyka. Z drugiej strony, pewne komponenty związane z zabezpieczeniami, n.p. LDAP lub centralne usługi monitorowania dostępu do danych moga być postrzegane jako aktywa, a nie wyłącznie zabezpieczenia.

Przy takich założeniach pojawia się problem definicji ryzyka. Dla wielu obszarów analizy bezpieczeństwa ryzyko powiązane jest z oszacowaniem możliwych strat finansowych. W szczególności dotyczy to systemów informatycznych wdrożonych w instytucjach finansowych: bankach lub firmach ubezpieczeniowych. Zarejestrowane straty finansowe powstałe w wyniku zdarzeń określonego typu są akumulowane. Uznaje się je za istotne dla profilu ryzyka, jeżeli ich suma w pewnym okresie (np.: w ciągu roku) przekracza



Rysunek 4: Relacje pomiędzy aktywami, zagrożeniami i zabezpieczeniami

pewien ustalony poziom. Z drugiej strony, dla systemów krytycznych ze względu na bezpieczeństwo, np.: lotniczych, kolejowych czy wybranych medycznych, każda awaria systemu jest traktowana jako zdarzenie o katastrofalnych skutkach i zazwyczaj jest podstawą do odrzucenia oprogramowania podczas oceny.

Na potrzeby oceny ryzyka zdefiniujemy:

- *Wartość użytkową*, inaczej *Użyteczność* przypisaną aktywom, jako liczbę z zakresu $[-1, 1]$
- *Ryzyko* powiązane z aktywem, jako różnicę pomiędzy założoną wartością użytkową oraz wartością wyznaczoną na końcu procesu wnioskowania.

Podczas obliczania ryzyka brane są pod uwagę zarówno wpływy zagrożeń i zabezpieczeń bezpośrednio powiązanych z aktywami, jak i zmiany wartości użytkowej wynikające z zależności opisanych drzewem wartości dodanej.

4.2 Proces oceny ryzyka

Przebieg procesu oceny ryzyka zilustrowano na Rys. 5. Zaokrąglone prostokąty reprezentują aktywności wewnątrz procesu, prostokąty oznaczone linią ciągłą – informacje wejściowe lub wyjściowe, natomiast prostokąty narysowane linią kropkowaną: wewnętrznie tworzone artefakty. Proces zawiera sześć kroków, krótko scharakteryzowanych poniżej.

1. *Identyfikacja aktywów.* Celem tego etapu jest sporządzenie listy aktywów obejmujących kluczowe procesy, usługi, obiekty danych, moduły oprogramowania, zasoby sprzętowe, infrastrukturę komunikacyjną, zewnętrznych dostawców usług i danych, ludzi oraz obiekty fizyczne. Aktywa są identyfikowane na podstawie dokumentów specyfikujących

wizję systemu, koncepcję działania oraz widoków architektonicznych. Źródłem informacji mogą być także wywiady przeprowadzone z zespołem wykonawców.

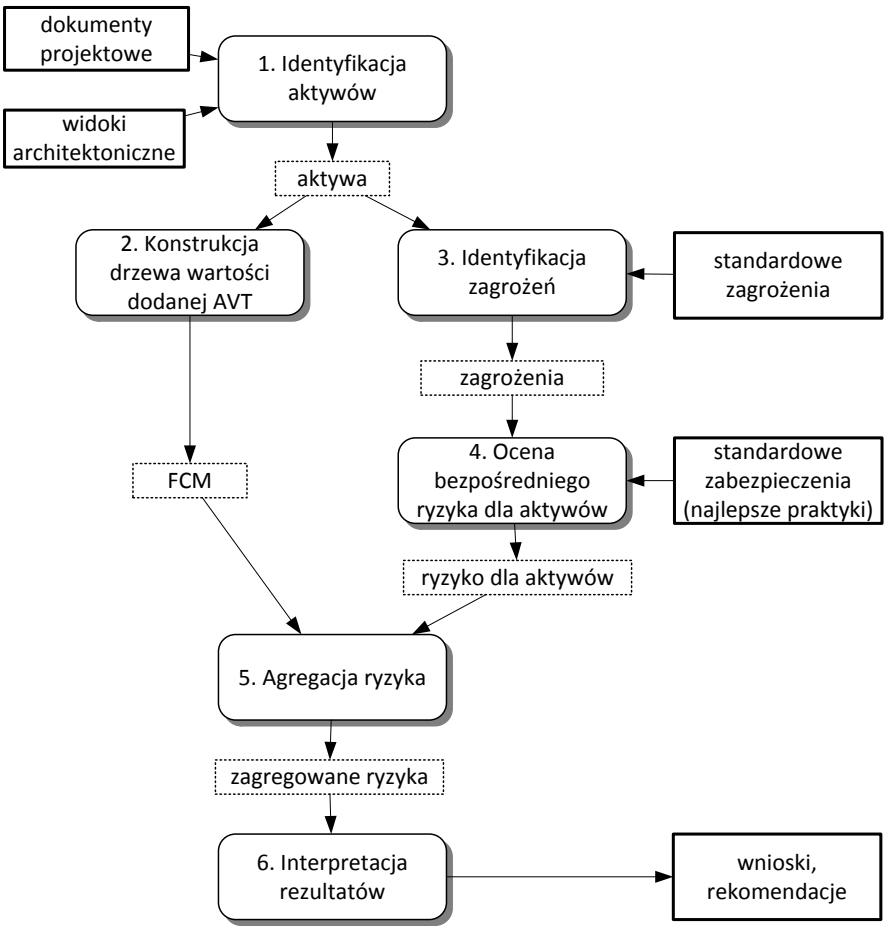
2. *Konstrukcja drzewa wartości dodanej AVT.* W tym kroku określa się, w jakim stopniu aktywa niższego poziomu mają wpływ na wartość aktywów nadrzędnych, np. sprzęt, oprogramowanie i infrastruktura komunikacyjna są wykorzystywane przez usługi i dane, te z kolei przez procesy. Wpływy są wyrażone za pomocą wartości lingwistycznych, które są ustalane podczas wywiadów i sesji burzy mózgów przeprowadzanych w obecności rożnych interesariuszy. Wyznaczone drzewo wartości dodanej jest reprezentowane przez macierz wpływów FCM.

3. *Identyfikacja zagrożeń.* Celem kroku jest określenie listy zagrożeń istotnych z punktu widzenia oceny ryzyka. W tym celu może zostać wykorzystana ogólna taksonomia zagrożeń, np.: dostępna jako ontologia. Powinna ona zostać dostosowana do specyfiki analizowanego systemu. Identyfikacja zagrożeń przebiega poprzez analizę poszczególnych aktywów, czyli poszukiwana jest odpowiedź na pytanie: *Na jakie zagrożenie może być narażony obiekt danego typu?*

4. *Ocena bezpośredniego ryzyka dla aktywów.* Podstawowym narzędziem oceny jest kwestionariusz zestawiający pytania związane z zastosowanymi zabezpieczeniami. Odpowiedzi udzielają różni interesariusze: twórcy oprogramowania, projektanci, zespół odpowiedzialny za wdrożenie, przyszli użytkownicy. Podstawą do opracowania kwestionariusza jest lista standardowych zabezpieczeń odzwierciedlających najlepsze praktyki w dziedzinie bezpieczeństwa systemów informatycznych. Lista ta jednak jest dostosowana do typów aktywów i specyfiki systemu. Wynikiem tego etapu jest przypisanie aktywom współczynników ryzyka (wartości znormalizowanych w przedziale $[0, 1]$).

5. *Agregacja ryzyka.* W tym kroku następuje ustalenie wartości ryzyka przypisanych aktywom różnych poziomów poprzez przeprowadzenie wnioskowania z użyciem rozmytych map kognitywnych. Podczas kolejnych iteracji wartości ryzyka przypisane aktywom dolnych poziomów przenoszą się w górę i sumują. Proces agregacji poprzedzony jest niezbędnymi przygotowaniami, np.: normalizacją macierzy wpływów FCM.

6. *Interpretacja rezultatów.* W tym kroku oceniane są profile ryzyka, zwłaszcza dla aktywów wysokiego poziomu. Krok ten może obejmować analizę alternatywnych scenariuszy, podczas których wprowadzane są dodatkowe zabezpieczenia na różnych poziomach drzewa, a następnie krok piąty jest powtarzany i przeprowadzana kolejna ocena.



Rysunek 5: Proces oceny ryzyka

4.3 Dyskusja

Niektóre kroki zaprezentowanej metodyki, w szczególności te związane z zbieraniem informacji, np.: identyfikacja aktywów i zagrożeń, są również obecne w innych metodykach i standardach. Jednakże, zakres zbieranych danych i narzędzia analizy są odmienne w przypadku klasycznych "ciężkich" metod jak CRAMM lub NIST 800-30.

Metody oparte na metryce ALE wymagają dostępności danych historycznych oraz przeprowadzenia analizy porównawczej dla określenia prawdopodobieństwa wystąpienia zagrożenia. Wiarygodna ocena jest możliwa wyłącznie wtedy, kiedy dostępne są stosowne dane. W innych przypadkach, przypisane wartości są wybierane arbitralnie.

Kontrowersyjnym etapem innych metod jest ocena strat finansowych

wywołanych przez zagrożenia. Wymaga to ustalenia miejsca analizowanych aktywów w modelu biznesowym. Co więcej, oszacowanie powinno uwzględniać dwa typy informacji: głęboką wiedzę o architekturze systemu, a także profil biznesowy. Przykładem może być: liczba transakcji w pewnym okresie (cecha architektury), jak i średnią wartość transakcji (cecha wdrożenia biznesowego).

Zaproponowana metodyka może być traktowana jako lekka, ponieważ:

- Wykorzystuje dokumenty opracowane podczas procesu wytwarzania oprogramowania, na przykład poprzez import widoków architektonicznych. Proces ten może zostać częściowo zautomatyzowany poprzez zbudowanie odpowiedniego narzędzia, które na podstawie modelu wyrażonego w określonym języku opisu architektur, na przykład ArchiMate [31], sporządzi listę aktywów i wskaże możliwe zależności (bez podania wartości wpływów).
- Metodyka nie korzysta bezpośrednio z analizy statystycznej. Jednakże dane historyczne mogą być niejawnie uwzględnione jako najlepsze praktyki: rekomendowane zabezpieczenia na poziomie aktywów.
- Proces oceny ryzyka przebiega niezależnie od środowiska biznesowego, stąd oszacowanie strat finansowych, które jest z reguły trudne do przeprowadzenia i obarczone dużymi błędami nie jest wymagane. Z drugiej strony, metodyka może uwzględniać dane pochodzące z biznesu, np.: poprzez skupienie się na wybranych (kluczowych) procesach i usługach.

Ta ostatnia cecha w pewnym stopniu ogranicza zastosowanie metodyki w przypadku dużych systemów, dla których granice pomiędzy warstwami biznesową i aplikacji są rozmyte. Dla dużych systemów zawierających dziesiątki lub setki procesów biznesowych bardziej odpowiednie wydają się standardy zintegrowanego zarządzania ryzykiem biznesowym, jak np.: SABSA.

5 Przykład analizy ryzyka dla systemu SWOP

W rozdziale przedstawiono zastosowanie metodyki na przykładzie zaimplementowanego na AGH systemu telemedycznego SWOP. Zaprezentowana architektura systemu pozwala na określenie zbioru aktywów systemu. W dalszej części omówiono kolejne etapy procesu oceny ryzyka.

5.1 System SWOP

SWOP jest systemem telemedycznym wspomagającym opiekę nad pacjentami przewlekle chorymi (SWOP jest skrótem: *System Wspomagania Opieki*

Przewlekłej). Głównym celem systemu było dostarczenie narzędzia umożliwiającego chorym samodzielne monitorowanie stanu zdrowia, powiadamianie pacjenta o niezbędnych do wykonanie akcjach, gdy zachodzi taka konieczność oraz automatyczne powiadamianie placówki medycznej w przypadku gdy wyniki pomiarów są alarmujące.

W ramach samodzielnego monitorowania stanu choroby pacjent dokonuje w sposób manualny lub automatyczny szeregu pomiarów, których wyniki są następnie przesyłane do placówki medycznej i analizowane. Dane dotyczące pomiarów są zbierane w specjalnie przygotowanej aplikacji mobilnej SWOP i przesyłane poprzez bezpieczne połączenie (WiFi, WAN, GPRS) z wykorzystaniem protokołów kryptograficznych dostarczanych przez TLS. Przesłane dane są zapisywane w centralnej bazie danych i analizowane przez dedykowany moduł analityczny, którego zadaniem jest ustalenie aktualnego statusu choroby/pacjenta, trendów rozwoju choroby, ryzyka nasilenia symptomów oraz działań, które powinny zostać wykonane przez pacjenta w celu złagodzenia objawów. W przypadku, gdy w wyniku analizy konieczne okaże się wykonanie przez pacjenta określonych akcji, jest on o tym powiadamiany poprzez SMS.

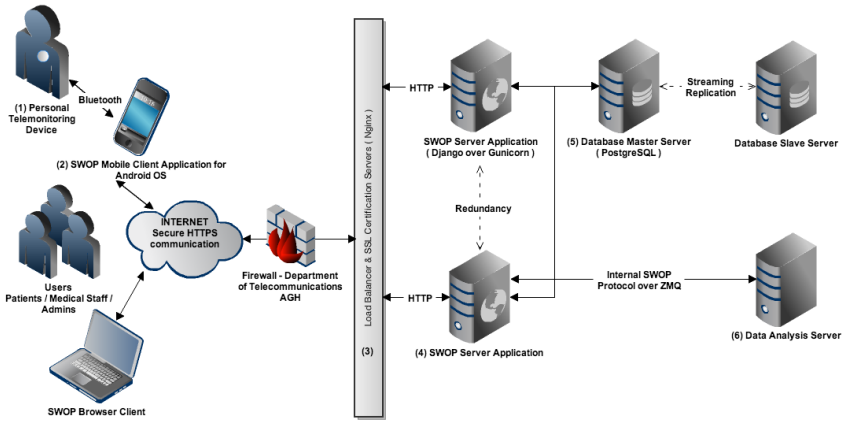
Personel medyczny posiada zestaw narzędzi informatycznych (dedykowane panele systemu webowego) poprzez, które ma możliwość konfiguracji ustalonych parametrów charakterystycznych dla danej choroby, podglądu danych medycznych oraz możliwość komunikacji z pacjentem. Dodatkowo system posiada moduł umożliwiający import danych dotyczących pacjenta z zewnętrznego systemu z wykorzystaniem standardu HL7.

Architektura systemu jest przedstawiona na rysunku 6. Osobiste urządzenia monitorujące pacjenta zbierają dane i przekazuję je poprzez interfejs Blutetooth do dedykowanej aplikacji mobilnej. Zapewnia ona walidację danych, ich prezentację oraz możliwość przesłania do centralnego serwera SWOP. Dodatkowo, poprzez tę aplikacje pacjent ma możliwość ręcznego wprowadzenia danych opisowych, które są zbierane w formie kwestionariusza. Komunikacja z serwerem odbywa się z wykorzystaniem SSL. Jako serwer WWW został wykorzystany nginx, logika biznesowa została stworzona w języku Python z wykorzystaniem frameworka Django i udostępniona na serwerze aplikacyjnym Gunicorn, który odpowiada za autoryzację, walidację danych, komunikacje z bazą danych, przesyłanie powiadomień SMS/email i komunikację z modułem analitycznym. Wysoka dostępność zapewniona jest poprzez konfigurację systemu na klastrze działającym w trybie master-slave.

5.2 Analiza ryzyka dla systemu SWOP

Ustalając dla potrzeb przykładu zastosowania metodyki zakres analizy ryzyka wybrane zostały następujące trzy obszary:

- Bezpieczeństwo IT: zabezpieczenie przed atakami oraz wyciek poufnych danych,



Rysunek 6: Architektura systemu SWOP.

- Ciągłość biznesowa: dostępność usług,
- Operacyjne zdarzenia losowe: błędy wprowadzonych danych lub wykonania procesów, których przyczyną może być niewykwalifikowany personel medyczny brak doświadczenia pacjenta w zakresie użytkowania urządzeń składających się na system, niska jakość sensorów etc.

5.2.1 Identyfikacja aktywów

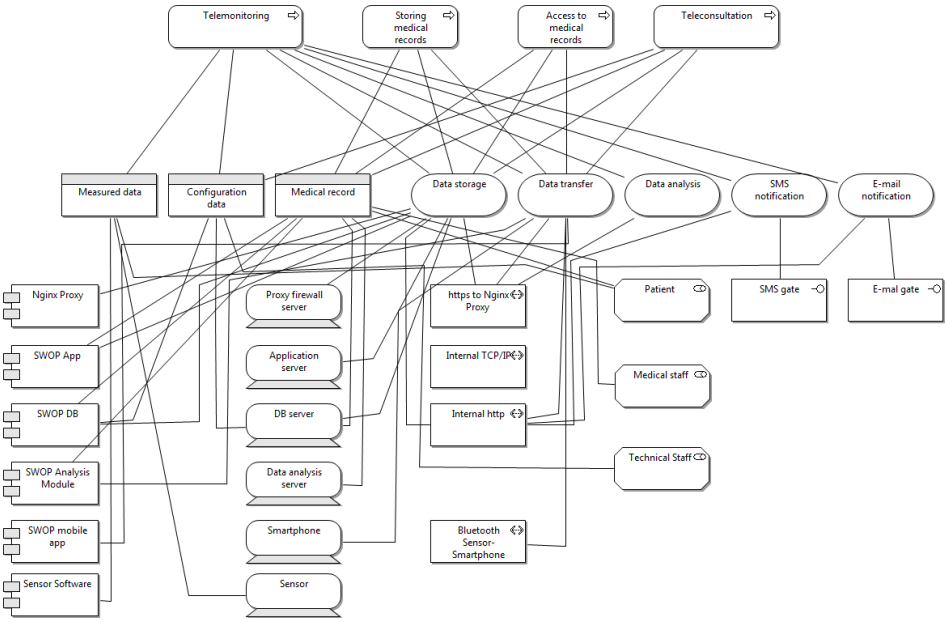
Podczas analizy zidentyfikowane zostały następujące aktywa:

1. *Procesy*: Telemonitoring, Przechowywanie danych medycznych, Dostęp do danych medycznych, Telekonsultacje,
2. *Usługi*: Składowanie danych i odczyt danych, Transfer danych, Analiza, Powiadomienia email i sms,
3. *Dane*: wyniki pomiarów, dane medyczne i dane konfiguracyjne,
4. *Moduły programowe*: Nginx Proxy, Aplikacja SWOP, Baza danych SWOP, Aplikacja mobilna SWOP, Sensory wraz z oprogramowaniem, Moduł analizy danych SWOP,
5. *Sprzęt*: Serwer proxy firewall, serwer aplikacyjny, serwer bazodanowy, serwer dla modułu analitycznego, telefony i czujniki,
6. *Komunikacja*: sieć WLAN (HTTPS), LAN i GPRS, sieć wewnętrzna (HTTP), bluetooth (sensor z telefonem)
7. *Ludzie*: pacjenci, personel medyczny i techniczny,
8. *Infrastruktura od podmiotów trzecich* (np. energia elektryczna).

5.2.2 Konstrukcja drzewa wartości dodanej AVT

Aktywa zidentyfikowane w poprzednim krokuskładają się na graf powiązań, np. procesy zależą od usług, które z kolei zależą od sprzętu i modułów programowych. Wszystkie zależności w ramach systemu zostały przedstawione na Rys. 7.

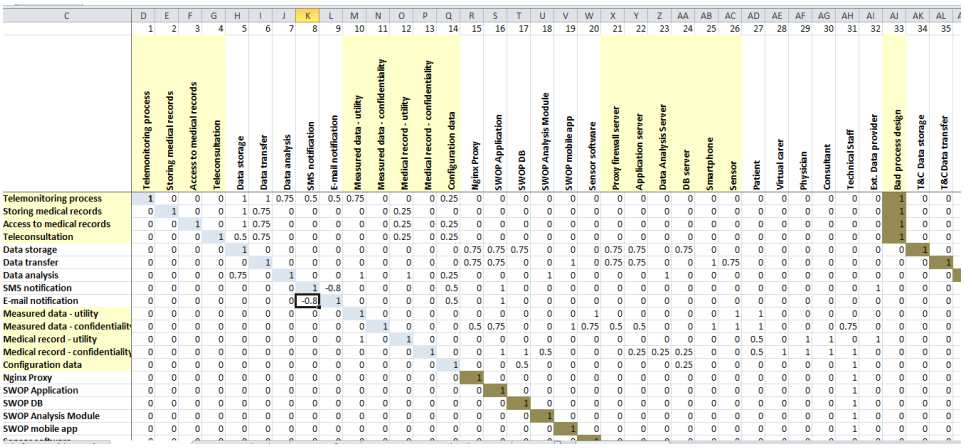
Powiązania pomiędzy elementami zostały ustalone na bazie dostępnych w dokumentacji perspektyw architektonicznych systemu natomiast wagi zostały ustalone w wyniku wywiadów z architektami systemowymi, programistami i użytkownikami. Wykorzystane zostały następujące wartości lingwistyczne jako wagi: *high, wysoki*, *significant, istotny*, *medium, średni*, *low, niski* and *none, żaden*. Przykładowo: użyteczność procesu telemonitorowania jest *wysoko* uzależniona od usług przechowywania i transferu danych, *istotnie* od usługi analizy danych. Analogiczne wnioskowanie przeprowadzone zostało dla wszystkich aktywów. W paru przypadkach posłużono się wartościami ujemnymi żeby pokazać, że niektóre usługi mogą zostać zastąpione przez inne (np. powiadomienia email i SMS zostały połączone powiązaniem z ujemna wagą *medium*).



Rysunek 7: Drzewo wartości dodanej aktywów: hardware, software, komunikacja, ludzie i zewnętrzne usługi wpływają na obiekty danych i usługi a te mają wpływ na użyteczność procesów na górze diagramu. Diagram został zbudowany na bazie opisu architektury w ArchiMate.

Na Rys. 8 pokazano fragment macierzy wpływów FCM. W tym przypadku wartości lingwistyczne (wysoki, istotny, średni, niski i żaden) zostały

już zastąpione wartościami liczbowymi: 1.0, 0.75, 0.5, 0.25 i 0.



	Telemonitoring process	Storing medical records	Access to medical records	Teleconsultation	Data storage	Data transfer	Data analysis	SMS notification	E-mail notification	Measured data - utility	Measured data - confidentiality	Medical record - utility	Medical record - confidentiality	Configuration data	Nginx Proxy	SWOP Application	SWOP DB	SWOP Analysis Module	SWOP mobile app	Sensor software	Proxy firewall server	Application server	Data Analysis Server	DB server	Smartphone	Sensor	Patient	Virtual carer	Physician	Consultant	Technical Staff	Ext. Data provider	Bad process design	T&C Data storage	T&C Data transfer
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
Telemonitoring process	1	0	0	0	1	1	0.75	0.5	0.5	0.75	0	0	0	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Storing medical records	0	1	0	0	1	0.75	0	0	0	0	0	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Access to medical records	0	0	1	0	1	0.75	0	0	0	0	0	0.25	0	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Teleconsultation	0	0	0	1	0.5	0.75	0	0	0	0	0	0.25	0	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Data storage	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0.75	0.75	0.75	0	0	0	0.75	0.75	0	0.75	0	0	0	0	0	0	0	0	0	1	0
Data transfer	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0.75	0.75	0	0	1	0	0.75	0.75	0	0	1	0.75	0	0	0	0	0	0	0	1	1
Data analysis	0	0	0	0	0.75	0	1	0	0	1	0	1	0	0.25	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
SMS notification	0	0	0	0	0	0	0	1	-0.8	0	0	0	0	0.5	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
E-mail notification	0	0	0	0	0	0	0	-0.8	1	0	0	0	0	0.5	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Measured data - utility	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0
Measured data - confidentialit	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0.5	0.75	0	0	1	0.75	0.5	0.5	0	0	1	1	1	0	0	0	0.75	0	0	0	0
Medical record - utility	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	0	1	1	0	1	0	0	0
Medical record - confidentiality	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0.5	0	0	0	0.25	0.25	0.25	0	0	0.5	1	1	1	1	0	0	0	0
Configuration data	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0.5	0	0	0	0	0	0	0.25	0	0	0	0	0	0	1	0	0	0	0
Nginx Proxy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
SWOP Application	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
SWOP DB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
SWOP Analysis Module	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
SWOP mobile app	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0

Rysunek 8: Fragment mapy FCM dla systemu SWOP

5.2.3 Zagrożenia

Identyfikacja zagrożeń została przeprowadzona na podstawie dostępnych źródeł[10, 22, 17] oraz doświadczenia uzyskanego podczas realizacji złożonych systemów informatycznych. Lista zidentyfikowanych zagrożeń składa się z 58 pozycji pogrupowanych w 11 obszarów odpowiadających klasom aktywów.

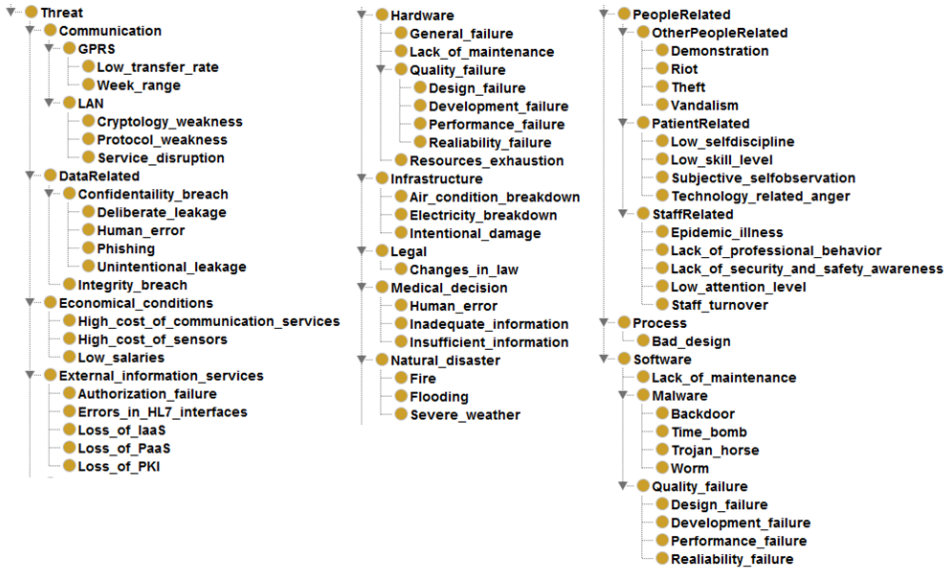
Obszary te zawierają:

1. *Procesy* (np. błędny projekt),
2. *Software* (np. brak prac utrzymaniowych, kiepska jakość, malware),
3. *Hardware* (np. kiepska jakość, zużycie),
4. *Komunikacja* (np. słabość protokołu, zakłócenia),
5. *Dane* (np. poufność, integralność),
6. *Zewnętrzne usługi* (np. PKI, bramka SMS),
7. *Dostawcy danych zewnętrznych* (np. błędy w interfejsach HL7),
8. *Infrastruktura fizyczna* (np. energia elektryczna, klimatyzacja),
9. *Ludzie*,
10. *Klęski żywiołowe*,
11. *Decyzje medyczne*,

12. *Warunki ekonomiczne*

13. *Kwestie prawne.*

Na Rys. 9 przedsatwiono taksonomię zidentyfikowanych zagrożeń dla systemu SWOP w postaci ontologii (wizualizacja w edytorze Protég'e).



Rysunek 9: Ontologia zagrożeń dla systemu SWOP

5.2.4 Ocena bezpośredniego ryzyka dla aktywów

Krok ten składa się z dwóch podstawowych czynności, które powszechnie występują w innych metodykach:

- analiza podatności,
- ocena efektywności zabezpieczeń.

Techniczna realizacja tego kroku powinna polegać na przygotowaniu kwestionariuszy, w których odpowiedziom reprezentującym najlepsze praktyki z danej dziedziny są przypisywane odpowiednie wagi liczbowe, które z kolei reprezentują ich wpływ na profil ryzyka.

W przypadku systemu SWOP kwestionariusz liczył 140 pytań, które zostały podzielone na 11 grup:

1. Aplikacja mobilna,
2. Serwer bazodanowy,
3. Serwer aplikacyjny,

4. Autentykacja,
5. Kryptografia,
6. Serwer/hardware,
7. Integralność serwera,
8. Polityka backupowania„ odtwarzania, zapewnienie ciągłości biznesowej,
9. Procedury bezpieczeństwa,
10. Administracja serwerami i zagrożenia związane z urządzeniami sieciowymi.

Logiczna struktura kwestionariusza w odniesieniu do aplikacji mobilnej została pokazana w Tabeli 1. Dla każdego pytania podane są co najwyżej trzy możliwe odpowiedzi, do których przydzielone są wagi liczbowe reprezentujące ich wpływ na profil ryzyka danego aktywa. Sposób ustalenia wag jest różny – w przypadku systemu SWOP został ustalony poprzez głosowania w gronie ekspertów dziedzinowych. W tabeli 1 odpowiedzi dla systemu SWOP zostały oznaczone poprzez podkreślenie.

Warto zwrócić uwagę, że kwestionariusz taki definiuje de facto strukturę mapy kognitywnej, w której zdefiniowane wagi wyrażają wpływy.

Ryzyko $R_a(s)$ dla aktywa s jest obliczane z wykorzystaniem wzoru (10) przy czym podstawiane są wartości odpowiedzi a_{ij} dla k pytań Q_i, $i = 1, \ldots, k$. Wartości 1 oraz 0 są wykorzystywane dla odpowiedzi pozytywnych i negatywnych. W związku z tym $a_{ij} = 1$, jeśli wybrana jet odpowiedź j-ta na i-te, a 0 w pozostałych przypadkach.

$$R_a(s) = \frac{w_i}{W} \sum_{j=1}^{3} a_{ij} q_{ij}, \text{ gdzie } W = \sum_{i=1}^{k} w_i \tag{10}$$

Parametr normalizacyjny W w równaniu (10) pełni rolę analogiczną do funkcji aktywacji z równania (4).

Dla łatwego zobrazowania obliczeń wartości odpowiedzi w tabeli 1 zostały zaznaczone pogrubioną czcionką i podkreślone. W wyniku zastosowania równania (10) obliczana została wartość 0.38, która oznacza, że zagrożenie nie może być w pełni zneutralizowane poprzez zastosowanie zabezpieczeń (pełna neutralizacja miała by miejsce w przypadku gdyby wynik wynosił 0). Uzyskane z kwestionariusza wartości odnoszące się do określonych aktywów są następnie wykorzystywane w kolejnym kroku.

Tablica 1: Ocena ryzyka aplikacji mobilnej – kwestionariusz

Pytanie Q_i	Odp_1	q_{i1}	Odp_2	q_{i2}	Odp_3	q_{i3}	w_i
Czy aplikacja mobilna przechowuje nazwę użytkownika/hasło w pamięci lokalnej?	tak, w formie niezakodowanej	1.0	nie	**0.0**	tak, w formie zakodowanej	0.5	1.0
Czy kod aplikacji został podany zaciemnieniu (ang. obfuscation)?	tak	0.2	nie	**0.8**			0.6
Czy komunikacja z middleware odbywa się poprzez serwer proxy innego podmiotu?	tak	0.9	nie	**0.1**			0.7
Czy aplikacja została pobrana z oficjalnego kanału dystrybucyjnego (Google Play, AppStore)?	tak	0.2	nie	**0.8**			0.4
Czy w komunikacji jest wykorzystany SSL?	tak	**0**	nie	1	brak walidacji poprawności certyfikatu	0.5	1.0
Czy na urządzeniu jest zainstalowane oprogramowanie antywirusowe?	tak	0.1	nie	0.9	brak informacji	**0.5**	0.4

5.2.5 Agregacja ryzyka

Obliczenia zostały poprzedzone normalizacją macierzy wpływu. Wykorzystane zostały cztery opisane wcześniej wartości lingwistyczne: *high*, *significant*, *medium*, *low* oraz *none*. Wartości te zostały zmapowane na wartości liczbowe $\{1.0, 0.75, 0.5, 0.25, 0\}$ i dla każdego wiersza $i = 1, \ldots, n$ znormalizowane wartości wpływu zostały wyznaczone w oparciu o formułę (11).

$$\overline{e}_{ij} = \begin{cases} 0, & \text{if } e_{ij} = 0 \\ \exp(m \cdot e_{ij})/Z_i, & \text{if } e_{ij} \geqslant 0 \end{cases}, \tag{11}$$

gdzie $Z_i = \sum_{\substack{j=1 \\ e_{ij} \neq 0}}^{n} \exp(m \cdot e_{ij})$ oraz m jest stałą dodatnią.

Normalizacja zapewnia zgodność wag FCM z pewnym szczególnym rozkładem prawdopodobieństwa. Motywacja dla takiego podejścia płynie z teorii gier. Przypuśćmy, że aktywo wyższego poziomu a_h zależy od aktywów niższego rzędu $a_{l_1}, \ldots, a_{l_k}$. Wpływy tych aktywów na a_h wyrażone są wartościami: $e_{hl_1}, \ldots, e_{hl_k}$. Jeśli *Zagrożenie* w postaci przeciwnika w grze wybierze aktywo niższego rzędu do przeprowadzenia ataku, gracz atakujący powinien wybrać element a_{l_m} mający najwyższy wpływ e_{hl_m} na profil ryzyka a_h. Gracze mogą jednak popełniać błędy w ocenie wpływów. Zatem wynikające z tego prawdopodobieństwo działań zależy od rozkładu błędów, który w ogól-

nym przypadku jest trudny do wyznaczenia. Jednak zakładając podwójne wykładniczy rozkład błędów dostajemy model [2] opisany formułą (11).

Dla końcowych obliczeń zagregowanego ryzyka konstruuje się dwa wektory:

$$\alpha^{nr} = A^{nr}(0), \ldots, A^{nr}(k), \ldots$$

oraz

$$\alpha^{r} = A^{r}(0), \ldots, A^{r}(k), \ldots$$

poprzez iteracyjne zastosowanie równania stanu (4).

Sekwencja reprezentująca brak ryzyka α^{nr} wyznaczona jest przez wektor $A^{nr}(0)$, w którym wszystkie wartości oznaczające użyteczność aktywów są ustawione na 1. Dla sekwencji α^{r} początkowy wektor $A^{r}(0)$ jest sumą wektorów użyteczności aktywów $A^{nr}(0)$ i pojedynczych zagrożeń R_a wyznaczonych w poprzednim kroku poprzez formułę (10): $A^{r}(0) = A^{nr}(0) + R_a$.

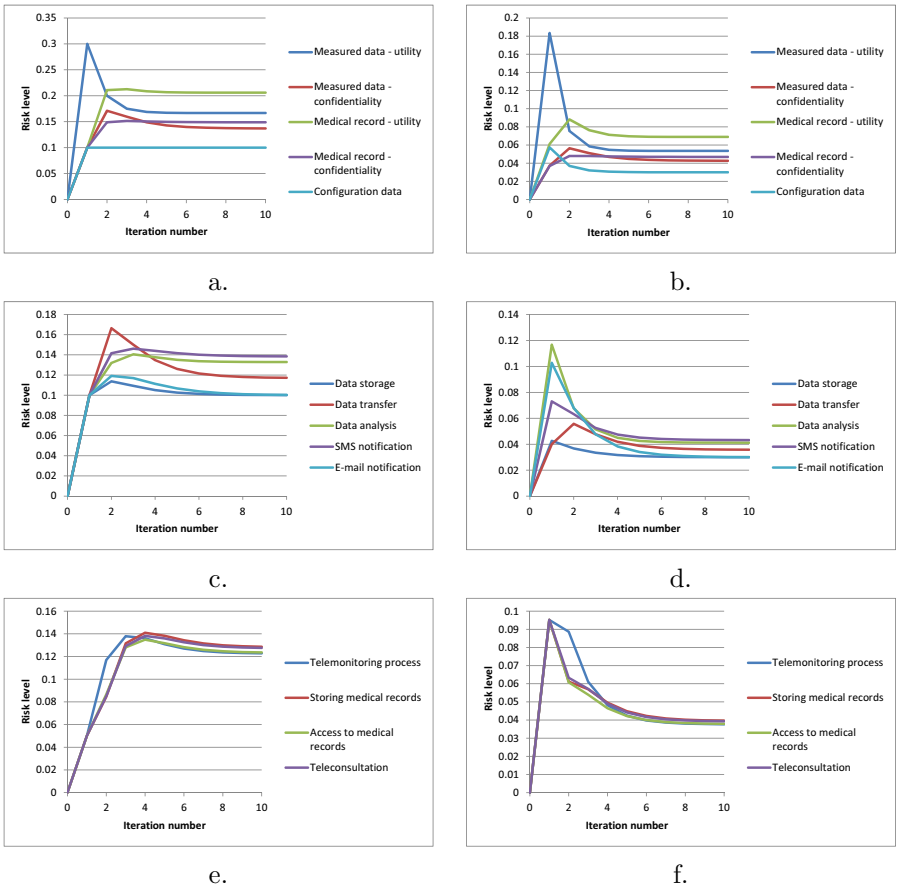
W końcu poprzez odjęcie odpowiadających sobie elementów α^{nr} oraz α^{r} otrzymujemy sekwencję zagregowanych wartości ryzyka $R(0), \ldots, R(k), \ldots$, gdzie $R(i) = A^{nr}(i) - A^{r}(i)$. Ciąg ten jest zbieżny do wartości, które wyrażają zagregowane ryzyko dla wszystkich aktywów na różnych poziomach drzewa wartości dodanej.

Rysunek 10 pokazuje wynik obliczeń dla trzech grup aktywów w systemie SWOP: dane, usługi i procesy. Otrzymano go z wykorzystaniem funkcji aktywacji S_{cut} (po lewej stronie) oraz *expcut* (po prawej) zadefiniowanej formułami (5) oraz (6). Porównanie pokazuje, że wyniki jakościowo są tożsame.

Podczas interpretacji wyników pojawia się problem konwersji wyniku z powrotem na wartości lingwistyczne: niskie, wysokie, średnie etc. W celu zapewnienia wsparcia dla tego procesu ustalone zostały wartości progowe $LM = 0.26$ and $MH = 0.52$. Eksperyment, który pozwolił na ich wyznaczenie był następujący: wyznaczono ryzyka dla sytuacji granicznych z wszystkimi zabezpieczeniami oraz bez żadnych zabezpieczeń. Uzyskany przedział $[0.07, 0.86]$ został równomiernie podzielony na trzy odstępy odpowiadające niskim, średnim i wysokim poziomom ryzyka. Uzyskane wartości progowe odnoszące się do funkcji aktywacyjnej S_{cut} są ok. trzy razy mniejsze.

5.2.6 Interpretacja rezultatów

Formułując wnioski stwierdzono niski poziom zagregowanego ryzyka dla aktywów umieszczonych u szczytu drzewa wartości dodanej (procesy, dane i usługi). Średni poziom ryzyka dla aktywów środkowego poziomu, np. aplikacji mobilnej, związany był z prototypowym charakterem ocenianej instancji systemu. Zakłada się, że dla docelowego wdrożenia uaktywnione zostaną dodatkowe mechnizmy bezpieczeństwa, np. użyty zostanie zaufany wydawca certyfikatów, oficjalne kanały dystrybucji dla aplikacji mobilnej, UPS, kopie zapasowe, kontrola dostępu do pomieszczeń, itd.



Rysunek 10: Wnioskowanie z wykorzystaniem Map Kognitywnych w odniesieniu do: danych (a-b), usług (c-d) i procesów (e-f). Funkcja aktywacji: cut (a,c,e), exp-cut (b,d,f)

Zwrócono także uwagę na podwyższony poziom ryzyka dla użyteczności danych medycznych i zmierzonych danych. W istocie, ryzyka te mają raczej charakter operacyjny, niż bezpośrednio związany z bezpieczeństwem systemów informatycznych. Są one spowodowane przez zagrożenia zaliczające się do kategorii *Ludzie* (np. niski poziom umiejętności, subiektywna samoobserwacja) dla pacjentów oraz: niski poziom uwagi, epidemia, fluktuacja kadr dla pracowników. Ten rodzaj ryzyk, zwłaszcza w przypadku pacjentów, może zostać złagodzony przez szkolenia oraz implementację brakującej w momencie oceny funkcji przypomnień o konieczności wprowadzenia danych.

6 Podsumowanie

W raporcie została przedstawiona metodyka oceny ryzyka systemów informatycznych. Metodyka opiera się na koncepcji rozmytych map kognityw-

nych FCM. Jej cechą charakterystyczną jest łatwość jej zastosowania oraz stosunkowo niskie koszty analizy. Poszczególne kroki metodyki takie jak: identyfikacja aktywów, zagrożeń, ocena efektywności zabezpieczeń, itp. są znane z innych metod oceny ryzyka. Na niskim poziomie metodyka adaptuje wszystkie mechanizmy, które zostały uznane za dobre praktyki w obszarze oceny ryzyka systemów IT natomiast na wysokim poziomie, do przeprowadzenia samych obliczeń, wykorzystuje Mapy Kognitywne. Istotnym punktem metodyki jest budowa drzewa wartości dodanej AVT, które opisuje zależności pomiędzy aktywami. Zaproponowana metodyka wykorzystuje również znane z teorii ekonomii pojęcie *Użyteczności* w miejsce finansowej straty, która jest ciężka do oszacowania zwłaszcza w przypadku systemów teleinformatycznych.

Zastosowanie metodyki zostało przedstawione na przykładzie analizy ryzyka dla systemu telemedycznego SWOP. W ramach przykładu przedstawione zostały wszystkie kroki metodyki:

- przygotowanie listy aktywów na bazie wywiadu i widoków architektonicznych systemu,
- budowa macierzy wpływów i drzewa wartości dodanej AVT,
- identyfikacja zagrożeń i przeciwdziałań,
- obliczenia niezagregowanego ryzyka dla aktywów,
- wnioskowanie z użyciem map kognitywnych FCM.
- interpretacja rezultatów

Biorąc pod uwagę powyższe cechy metodyka może zostać uznana za metodykę lekką gdyż koszty jej praktycznego użycia są nieduże a wynik uzyskiwany jest szybko. W przypadku systemu SWOP wszystkie dane potrzebne do zastosowania metodyki zostały zebrane podczas analizy dokumentacji i trzech spotkań, w których brali udział architekci systemowi oraz programiści.

Zdaniem autorów metodyka stanowi ciekawa alternatywę dla ciężkich metodyk oferowanych przez standardy. Może być również wykorzystywana jako uzupełnienie dla metodyk tradycyjnych.

Literatura

[1] Jose Aguilar. A Survey about Fuzzy Cognitive Maps Papers (Invited Paper). *International Journal*, 3(2):27–33, 2005.

[2] S.P. Anderson, A. De Palma, and J.F. Thisse. *Discrete Choice Theory of Product Differentiation*. MIT Press, Boston, MA, 1992.

[3] Robert M Axelrod. *Structure of Decision: The Cognitive Maps of Political Elites*. Princeton University Press, 1976.

[4] A. Birolini. *Reliability engineering: theory and practice; 3rd ed.* Springer Verlag, Berlin, 2000.

[5] J. B. Bowles and C. Wan. Software failure modes and effects analysis for a small embedded control system, 2001.

[6] I. Cervesato and C. Meadows. Fault-tree representation of NPATRL security requirements, 2003.

[7] Rick Craft, Ruthe Vandewart, Greg Wyss, and Don Funkhouser. An open framework for risk management 1, 1998.

[8] CRAMM. CRAMM. `http://www.cramm.com/`, Last accessed: Jan 2013.

[9] ENISA. Inventory of risk management / risk assessment methods. `http://rm-inv.enisa.europa.eu/methods/rm_ra_methods.html`, Last accessed: Jan 2014.

[10] B Guttman and E A Roback. An introduction to computer security : The NIST handbook. *Security*, 800(12):1 – 290, 1995.

[11] D Hubbard and D Evans. Problems with scoring methods and ordinal scales in risk assessment. *Journal of Research and Development*, 54(3):1–10, 2010.

[12] Institute for Computer Sciences and Technology. *Guideline for automatic data processing risk analysis*. National Bureau of Standards, Institute for Computer Sciences and Technology, 1979.

[13] ISO/IEC. Information technology – security techniques – information security risk management, ISO/IEC 27005:2011. Technical report, International Organization for Standardization, 2011.

[14] Antonie Jetter and Willi Schweinfort. Building scenarios with Fuzzy Cognitive Maps: An exploratory study of solar energy. *Futures*, 43(1):52–66, 2011.

[15] Bart Kosko. Fuzzy Cognitive maps. *International Journal of Machine Studies*, 24:65–75, 1986.

[16] Bart Kosko. *Neural networks and fuzzy systems: a dynamical systems approach to machine intelligence*. Prentice Hall, 1992.

[17] Douglas J Landoll. *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. Auerbach Publications, 2005.

[18] Beatrice Lazzerini and Lusine Mkrtchyan. Analyzing risk impact factors using extended fuzzy cognitive maps. *IEEE Systems Journal*, 5(2), jun 2011.

[19] M. Modarres, M. Kaminskiy, and Krivtsov V. *Reliability engineering and risk analysis*. CRC Press, 1999.

[20] S. Ozesmi, U. Ozesmi. Ecological models based on people's knowledge: a multi-step fuzzy cognitive mapping approach. *Ecological Modelling*, 176(1-2):43–64, 2004.

[21] E.I. Papageorgiou. Learning algorithms for fuzzy cognitive maps: A review study. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 42(2):150–163, March 2012.

[22] Ronald S. Ross. Guide for conducting risk assessments. *NIST Special Publication*, NIST SP 800-30rev1(September):85, 2011.

[23] Bruce Schneier. Attack trees. *Dr. Dobb's journal*, 24(12):21–29, 1999.

[24] Sherwood Applied Business Security Architecture. SABSA, Last accessed: Jan 2013.

[25] Kevin John Soo Hoo. *How Much is Enough: A Risk Management Approach to Computer Security*. PhD thesis, Stanford University, Stanford, CA, USA, 2000. AAI9986202.

[26] D. H. Stamatis. *Failure mode and effect analysis: FMEA from theory to execution*. Milwaykee, Wisconsin: ASQ Quality press, 2003.

[27] N Stathiakis, Ce Chronaki, E Skipenes, E Henriksen, E Charalambus, A Sykianakis, G Vrouchos, N Antonakis, M Tsiknakis, and S Orphanoudakis. Risk assessment of a cardiology ehealth service in hygeianet, 2003.

[28] Piotr Szwed. Application of fuzzy cognitive maps to analysis of development scenarios for academic units. *Automatyka/Automatics*, 17(2):229–239, 2013.

[29] Piotr Szwed and Pawel Skrzynski. A new lightweight method for security risk assessment based on Fuzzy Cognitive Maps. *Applied Mathematics and Computer Science*, 24(1):213–225, 2014.

[30] Piotr Szwed, Pawel Skrzynski, and Wojciech Chmiel. Risk assessment for a video surveillance system based on Fuzzy Cognitive Maps. *Multimedia Tools and Applications*, pages 1–24, 2014.

[31] The Open Group. Open Group Standard. Archimate 2.0 Specificattion, 2012.

[32] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl. Fault tree handbook, technical report nureg-0492, 1981.