BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 16, 2001

Analiza ryzyka dla potrzeb bezpieczeństwa teleinformatycznego

Krzysztof LIDERMAN

Zakład Systemów Komputerowych, Instytut Automatyki i Robotyki WAT, ul. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: Artykuł omawia problematykę analizy ryzyka ukierunkowanej na bezpieczeństwo teleinformatyczne. Została w nim przedstawiona propozycja definicji analizy ryzyka i sposobu realizacji procesu analizy ryzyka w kontekście bezpieczeństwa teleinformatycznego.

1. Wprowadzenie

Od początku lat 90-tych XX wieku, w związku z rozwojem i rozpowszechnieniem techniki komputerowej oraz łączeniem systemów komputerowych w sieci, znaczenia nabrała **inżynieria ochrony danych**[1]**,** wcześniej stosowana głównie w systemach specjalnych (wojskowych, rządowych, sterowania). Wzrost tego znaczenia przejawia się również w swoistej „modzie" na bezpieczeństwo teleinformatyczne – większość uczelni wyższych, nawet luźno związanych z informatyką, proponuje w ramach zbioru wykładanych przedmiotów, przedmiot nazywany zwykle „Bezpieczeństwo sieci komputerowych", „Bezpieczeństwo komputerowe" lub podobnie.

Niniejszy artykuł koncentruje się na tzw. „bezpieczeństwie do wewnątrz", nie rozważając w zasadzie zagrożeń powodowanych przez systemy komputerowe sterujące różnego typu instalacje, obejmowane zakresem normy

[1] Pod tym terminem kryje się metodyka i narzędzia stosowane podczas projektowania i wdrażania mechanizmów ochrony danych.

IEC 61508 (tzw. „bezpieczeństwo na zewnątrz") [2], dlatego proponowana definicja terminu „bezpieczeństwo teleinformatyczne" jest następująca:

> B**ezpieczeństwo teleinformatyczne** *oznacza* ***ochronę informacji*** *przetwarzanej, przechowywanej i przesy!anej za pomoc" systemów teleinformatycznych przed niepo#"danym (przypadkowym lub $wiadomym) ujawnieniem, modyfikacj", zniszczeniem lub uniemo#liwieniem jej przetwarzania.*

Podstawowe **atrybuty informacji związane z jej bezpieczeństwem** to:

- **tajność** (ang. *confidentiality*) - termin ten oznacza, że dostęp do określonych danych i informacji posiadają wyłącznie uprawnione osoby;
- **integralność** (ang. *integrity*) - termin ten oznacza, że dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji;
- **dostępność** (ang. *availability*) - termin ten charakteryzuje system informatyczny i oznacza dostępność danych, procesów i aplikacji zgodnie z wymaganiami użytkownika.

Dla poprawnego określenia wymaganych przedsięwzięć ochrony informacji przetwarzanej, przesyłanej i przechowywanej w systemach teleinformatycznych potrzebna jest **analiza ryzyka** (ang. *risk analysis*)[2]. Termin ten w literaturze przedmiotu jest często używany (żeby nie powiedzieć - nadużywany), przy czym różni autorzy podają różny zakres przedsięwzięć składających się na proces analizy ryzyka. Również sam termin „ryzyko" jest różnie (choć podobnie) definiowany, np. „Słownik języka polskiego" (PWN, Warszawa, 1983) określa ryzyko jako:

> *„mo#liwo$%, prawdopodobie&stwo, #e co$ si' nie uda, przedsi'wzi'cie, którego wynik jest nieznany, niepewny, problematyczny*".

Czterotomowa „Encyklopedia Powszechna" (PWN, Warszawa, 1987) określa ryzyko na gruncie prawa:

> *„w prawie cywilnym niebezpiecze&stwo powstania szkody obci"#aj"ce osob' bezpo$rednio poszkodowan", chyba #e umowa lub przepis prawny zobowi"zuje inn" osob' do wyrównania szkody... ; szczególnie na zasadzie ryzyka opiera si' odpowiedzialno$% za szkody wyrz"dzone w zwi"zku z u#yciem si! przyrody... W prawie karnym dzia!anie*

[2] W literaturze można spotkać jeszcze inne określenie - ocena ryzyka.

> *w granicach dopuszczalnego ryzyka mo#e stanowi% ustawow" lub poza ustawow" okoliczno$% wy!"czaj"c" odpowiedzialno$% karn" sprawcy*".

Według normy IEC 61508 wiążącej pojęcie ryzyka z pojęciem hazardu (ang. *hazard;* definiowany jako sytuacja mogącą spowodować śmierć lub obrażenia ludzi):

> *„... ryzyko jest miar" stopnia zagro#enia, wyra#aj"c" zarówno stopie& szkodliwo$ci hazardu, jak i prawdopodobie&stwo jego wyst"pienia".*

Według normy PN-I-2000 natomiast, ryzyko to:

> *„... prawdopodobie&stwo, #e okre$lone zagro#enie wykorzysta okre$lon" podatno$% systemu przetwarzania danych";*

a według normy PN-I-13335-1:1999:

> *„ ... ryzyko jest prawdopodobie&stwem okre$laj"cym mo#liwo$% wykorzystania okre$lonej podatno$ci przez dane zagro#enie w celu spowodowania straty lub zniszczenia zasobu lub grupy zasobów, a przez to negatywnego bezpo$redniego lub po$redniego wp!yni'cia na instytucj' "*

Słowo „ryzyko" posiada zatem wiele odcieni znaczeniowych. W każdym z nich jednak jest związane z pojęciem „straty", co jest zgodne również z intuicyjnym rozumieniem tego terminu. Wydaje się, że dla potrzeb bezpieczeństwa informacji w systemach teleinformatycznych można przystosować następująco definicję podaną w normie IEC 61508:

> *„*R**yzyko** *oznacza miar' stopnia zagro#enia dla tajno$ci, integralno$ci i dost'pno$ci informacji wyra#on" jako iloczyn prawdopodobie&stwa wyst"pienia sytuacji stwarzaj"cej takie zagro#enie i stopnia szkodliwo$ci jej skutków."*

W ogólnym (systemowym) ujęciu Findeisen [1] określa analizę ryzyka[3] jako proces składający się z następujących etapów:

[3] Analiza ryzyka jest pojęciem stosowanym w analizie systemowej w odniesieniu do różnych systemów. W tym opracowaniu termin ten jest używany w odniesieniu do systemu komputerowego i jego środowiska.

- **szacowania ryzyka**[4]**:**
  - ⇒ identyfikacji zagrożeń;
  - ⇒ określeniu elementów systemu podatnych na zagrożenia;
  - ⇒ określeniu prawdopodobieństwa wystąpienia skutków zagrożeń (np. kradzieży pieniędzy z konta bankowego) w przypadku zajścia takich zagrożeń (np. złamania hasła).
- **oceny akceptowalności ryzyka:**
  - ⇒ określeniu stopnia szkodliwości skutków zagrożenia (polega zwykle na oszacowaniu kosztów poniesionych w przypadku realizacji zagrożenia w rozpatrywanym systemie w odniesieniu do ustalonego okresu czasu, np. roku);
  - ⇒ oszacowaniu kosztów zabezpieczeń (j.w.);
  - ⇒ wykonaniu analizy strat (liczonych w określonej walucie) w przypadku realizacji zagrożenia i braku zabezpieczeń oraz zysków, gdy takie zabezpieczenia zostaną zainstalowane (i przeszkodzą w realizacji zagrożenia).

Generalnie analiza ryzyka polega na ocenie wszystkich negatywnych skutków badanego przedsięwzięcia i odpowiadających im prawdopodobieństw (częstości występowania). Ocena akceptowalności ryzyka [1] z kolei, jest często procesem o charakterze „politycznym”[5], który może być jednak wspomagany metodami formalnymi.

Przy ocenie ryzyka należy pamiętać że:

- **Ryzyko można oszacować i zredukować, ale nie da się go wyeliminować.**
- **Ryzyko należy weryfikować** - procedura analizy ryzyka musi być powtarzana co pewien czas ze względu na możliwości zaistnienia z biegiem czasu nowych przyczyn mających wpływ na wartość ryzyka.

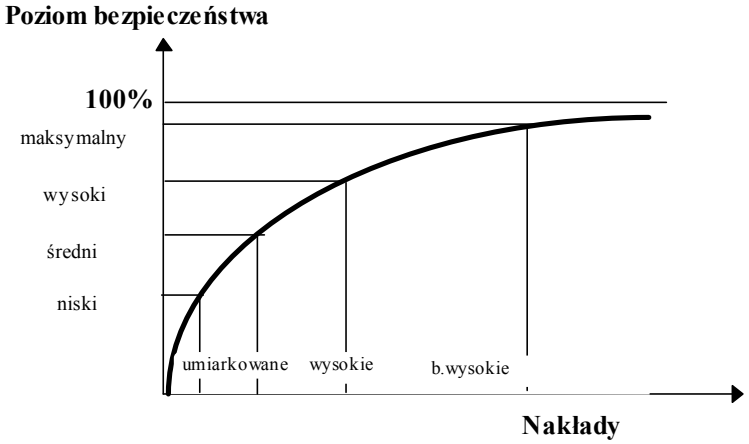
Pierwszy z tych punktów jest poglądowo przedstawiony na rys.1, gdzie wraz ze wzrostem nakładów na bezpieczeństwo (teleinformatyczne), wyidealizowana krzywa obrazująca wzrost poziomu tego bezpieczeństwa zbliża się asymptotyczne do poziomu maksymalnego 100%. W praktyce oznacza to, że **nie istnieje system który gwarantowałby stuprocentowe bezpieczeństwo informacji**, bez względu na ilość pieniędzy wydanych na różne zabezpieczenia.

---

[4] [3] określa oszacowanie ryzyka (ang. *risk assessment*) jako proces oceny znanych i postulowanych zagrożeń oraz podatności, który jest przeprowadzany w celu określenia spodziewanych strat i ustalenia stopnia akceptowalności działania systemu

[5] W tym sensie, że często kierujemy się w nim przesłankami pozamerytorycznymi, np. etycznymi, społecznymi itp.

Odstęp pomiędzy poziomem 100% a krzywą obrazuje wielkość *ryzyka szcz"tkowego*, o którym będzie mowa w dalszej części artykułu.



Rys.1 Zależność pomiędzy nakładami na bezpieczeństwo a osiąganym poziomem bezpieczeństwa teleinformatycznego.

2. Analiza ryzyka dla potrzeb bezpieczeństwa teleinformatycznego

Analiza ryzyka prezentowana w niniejszym artykule jest wariantem ogólnej analizy ryzyka, której zasadnicze elementy zostały scharakteryzowane na końcu poprzedniego rozdziału. Najbardziej ogólna definicja analizy ryzyka dla potrzeb bezpieczeństwa teleinformatycznego, może zostać sformułowana następująco:

> ***Analiza ryzyka*** *(dla potrzeb bezpiecze&stwa teleinformatycznego) jest procesem identyfikacji (jako$ciowej i ilo$ciowej) ryzyka utraty bezpiecze&stwa teleinformatycznego.*

Analiza ryzyka powinna być wykonywana systematycznie w celu utrzymania bieżącego stanu bezpieczeństwa teleinformatycznego, na który mają wpływ zmiany zagrożeń oraz zmiany organizacyjne w firmie i sprzętowo-programowe w nadzorowanych systemach teleinformatycznych.

Proces analizy ryzyka dla potrzeb bezpieczeństwa teleinformatycznego składa się z następujących czynności:

1. Identyfikacji zakresu zagrożenia i określenia (jakościowego/ilościowego) zagrożonych dóbr materialnych i informacyjnych.
2. Określenia wartości dóbr materialnych (np. sprzętu komputerowego).
3. Określenia wartości informacji w kontekście jej ujawnienia, modyfikacji, niedostępności lub utraty.
4. Identyfikacji zagrożeń (i ich stopnia) dla bezpieczeństwa teleinformatycznego.
5. Identyfikacji miejsc (elementów) systemów teleinformatycznych podatnych na te zagrożenia (i stopnia podatności).
6. Przeprowadzenia procesu ***analizy ryzyka szczątkowego***.
7. ***Akceptacji ryzyka szczątkowego*** (co oznacza koniec procesu analizy ryzyka) lub powtarzaniu procesu analizy ryzyka szczątkowego aż do uzyskania akceptowalnego wyniku.

Proces analizy ryzyka szczątkowego składa się z następujących czynności:

1. Identyfikacji istniejących środków przeciwdziałania zagrożeniom.
2. Określenia niezbędnych środków przeciwdziałania zagrożeniom oraz porównanie ich z już zastosowanymi.
3. ***Analizy kosztowej ryzyka***.
4. Wykonania listy zalecanych środków przeciwdziałania zagrożeniom.
5. Identyfikacji ryzyka szczątkowego.

Analiza kosztowa ryzyka polega na oszacowaniu kosztów potencjalnego ryzyka utraty lub naruszenia bezpieczeństwa teleinformatycznego bez stosowania określonych środków przeciwdziałania zagrożeniom, w stosunku do kosztów zastosowania tych środków. **Akceptacja ryzyka szczątkowego** jest decyzją podejmowaną najczęściej na podstawie analizy kosztowej ryzyka lub na podstawie określonych przesłanek moralnych lub politycznych.

Można przypuszczać, że w praktyce rzadko jest wykonywana rzetelna

Przyk!ad (.

Prawdopodobieństwo wystąpienia w ciągu roku pożaru w firmie określono jako równe 0,001. Przewidywane łączne straty (tzn. straty z powodu braku możliwości wykonywania pracy plus koszty przywrócenia systemu do działania) wywołane pożarem wynoszą 1 000 000 zł. Oczekiwany koszt strat (odniesiony do jednego roku) wynosi więc:

$$1\,000\,000\text{zł} \bullet 0{,}001 = 1000\text{zł}$$

Jeżeli koszty kompleksowego systemu ppoż. (system czujników, system monitorowania, działania organizacyjne, np. szkolenia) wynosi 60 000 zł, a czas jego eksploatacji przewiduje się na 5 lat, to koszty ochrony wynoszą w tym przypadku 12 000 zł rocznie. Wynika stąd, że przy tak nikłym prawdopodobieństwie pożaru nie jest opłacalne inwestowanie w rozważany system ochrony ppoż. (ale być może konieczne będą inne działania w zakresie bezpieczeństwa ppoż. wynikające np. z obowiązujących przepisów budowlanych czy resortowych w tym zakresie).

* * * *

Występujące jako część analizy ryzyka *oszacowanie podatno$ci* na zagrożenia (ang. *vulnerability assessment* - punkt 5 przedstawionego wcześniej procesu analizy ryzyka), norma [3] definiuje jako aspekt oceny skuteczności obiektu ocenianego w zakresie zabezpieczeń w praktyce, zgodnie z celami zabezpieczenia (tzn. jest to przegląd podatności na utratę zasobów lub nieuprawnione ich wykorzystanie, błędy w raportach i informacji, działania nielegalne lub nieetyczne i/lub niesprzyjające lub nieprzychylne opinii publicznej).

Natomiast pod pojęciem *akceptacji ryzyka* norma PN-I-2000 umieszcza decyzje kierownictwa, dopuszczające pewien stopień ryzyka (tzw. *ryzyko szcz"tkowe*), podejmowane zazwyczaj z przyczyn technicznych lub ekonomicznych.

Z analizą ryzyka związany jest blisko termin ***zarządzanie ryzykiem*** (ang. *risk management*). Jest to element teorii zarządzania dotyczący identyfikacji, pomiaru, nadzoru i minimalizacji możliwości wystąpienia zdarzeń niepewnych, który zawiera skuteczny program zarządzania obejmujący:

- ocenę ryzyka, określaną na podstawie oceny zagrożeń i podatności,
- decyzje zarządzające,
- wdrożenie środków kontroli,
- przegląd skuteczności zabezpieczeń.

Analiza ryzyka dotyczy zwykle zdarzeń, dla których częstości występowania nie są określone ani bezpośrednio wyznaczalne na odpowiednim poziomie ufności (najczęściej są to tzw. „zdarzenia rzadkie"). Z tego powodu przy ocenie ryzyka często używa się metod modelowania przystosowanych do

szacowania małych prawdopodobieństw - *drzew zdarze*& i *drzew b*!'*dów*. W każdej z tych metod szacowania ryzyka, zadanie złożone dekomponuje się na mniejsze (prostsze) części, które po starannej analizie łączy się ponownie, uzyskując lepsze zrozumienie całego zadania oraz możliwość określenia występujących w nim prawdopodobieństw zdarzeń składowych (poprzez wyznaczanie prawdopodobieństw cząstkowych - niezbędne jest w tym celu dysponowanie prawdopodobieństwami zdarzeń elementarnych, które nie są już dalej dekomponowane).

3. Metody oceny ryzyka - drzewa zdarzeń i drzewa błędów

Drzewo zdarze& jest graficznym modelem zależności przyczynowo-skutkowych występujących w rozpatrywanym problemie. Przy budowie drzewa zdarzeń zakłada się, że określony skutek jest wynikiem pewnego ciągu zdarzeń. Drzewo zdarzeń rozpoczyna się zatem pewnym zdarzeniem inicjującym i przedstawia wszystkie możliwe ciągi zdarzeń będące następstwami zdarzenia inicjującego. W różnych miejscach drzewa zdarzeń znajdują się punkty rozgałęzień ilustrujące fakt, że po pewnych zdarzeniach istnieje możliwość wystąpienia różnych innych zdarzeń. Prawdopodobieństwo określonego skutku otrzymuje się mnożąc przez siebie prawdopodobieństwa wszystkich zdarzeń składających się na ścieżkę w drzewie, po której dochodzimy do rozważanego skutku.

Przyk!*ad 2*.

Załóżmy, że pracownicy pewnej instytucji przy angażowaniu do pracy dostają kartę magnetyczną z wypisanymi na niej danymi osobowymi, służbowymi i zdjęciem oraz PIN. Karta magnetyczna służy jako przepustka okazywana strażnikowi na bramie oraz (wraz z PIN-em) jako elektroniczny klucz otwierający te drzwi (i tylko te!), które wolno otworzyć danemu pracownikowi. Hipotetyczny system komputerowy jest zabezpieczony następującymi zabezpieczeniami fizycznymi i programowymi: strażnik przy wejściu do budynku sprawdzający przepustki, elektroniczne zabezpieczenia wejść do korytarzy (czytnik karty magnetycznej + PIN), elektroniczne zabezpieczenia wejść do pomieszczeń służbowych (j.w.), elektroniczne zabezpieczenie komputera (czytnik karty + klawiatura do wprowadzenia PIN-u), login i hasło konieczne do uruchomienia sesji.

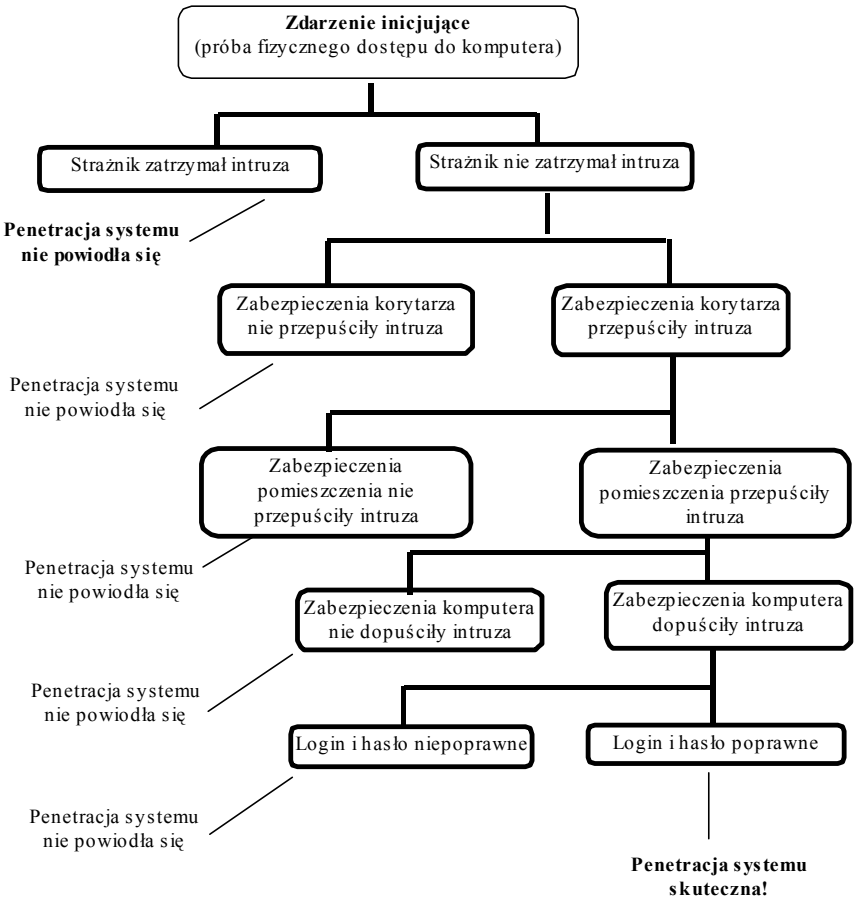
Na rys.2 jest przedstawione drzewo zdarzeń odpowiadające próbie fizycznego dostania się do komputera i uruchomienia sesji (zdarzenie inicjujące).

* * * *

Drzewo b!'*dów* (jest to również graficzny model zależności przyczynowo-skutkowych) jest budowane w przeciwnym kierunku niż drzewo zdarzeń.

Rozpoczyna się określonym skutkiem i rozwija w kierunku zdarzeń poprzedzających, pokazując wszystkie możliwe kombinacje zdarzeń niepożądanych, które mogły doprowadzić do wyspecyfikowanego skutku.

Drzewa zdarzeń i drzewa błędów wykorzystuje się zarówno do *analizy jako$ciowej* jak i *ilo$ciowej*. Po przeprowadzeniu analizy jakościowej (tj. bez oszacowania prawdopodobieństw) pomagają one zorientować się w całym zakresie ryzyka i zrozumieć sytuację, której ryzyko dotyczy. Po przeprowadzeniu analizy ilościowej, drzewa zdarzeń i drzewa błędów pomagają w wyznaczeniu prawdopodobieństw pewnych ciągów zdarzeń lub pojedynczych zdarzeń.

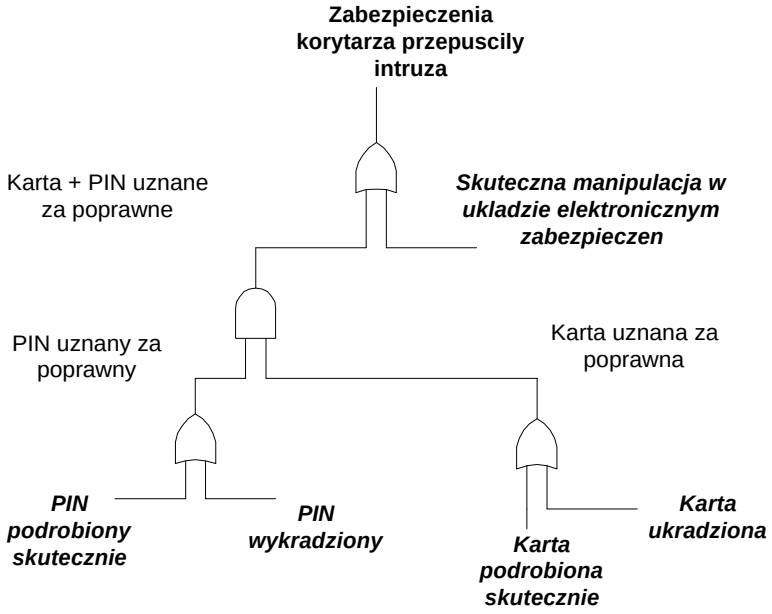


Rys. 2. Przykładowe drzewo zdarzeń.

Przyk!ad 3.

Drzewo błędów dla zdarzenia „*zabezpieczenia korytarza przepu$ci!y intruza*" (z drzewa zdarzeń w poprzednim przykładzie) może wyglądać jak na rys.3. Zdarzenia zaznaczone pogrubioną kursywą są w tym przykładzie zdarzeniami elementarnymi, dla których (metodami przedstawionymi dalej artykule) musi zostać znalezione prawdopodobieństwo ich wystąpienia.

* * * *



Rys.3. Przykładowe drzewo błędów.

W analizie ilościowej drzewa błędów czyni się zwykle dwa założenia:

1. Zdarzenia podawane na wejścia funktora **LUB** są rozłączne;
2. Wszystkie zdarzenia występujące w drzewie błędów są niezależne w sensie probabilistycznym.

Założenie 1 oznacza, że zdarzenie A na wyjściu funktora występuje wtedy, gdy występuje co najmniej jedno ze zdarzeń $B_(, B_2 , ..., B_n$ na wejściu tego funktora. W takim przypadku prawdopodobieństwo $p(A)$ zdarzenia A wynosi:

$$p(A) = p(B_() + p(B_2) + ... + p(B_n)$$

pod warunkiem, że zdarzenia $B_(, B_2, ..., B_n$ są rozłączne. W praktyce wyrażenie to stosuje się często do oszacowania prawdopodobieństwa $p(A)$, również gdy ten warunek nie jest spełniony. Aproksymację taką można uważać za zadowalającą,

gdy poszczególne prawdopodobieństwa $p(B_1)$, $p(B_2)$, ..., $p(B_n)$ są małe. Niezależnie od tego, czy zdarzenia B_1, B_2, ..., B_n są rozłączne czy nie, prawdziwa jest nierówność:

$$p(A) \leq p(B_1) + p(B_2) + ... + p(B_n)$$

która stosowana w praktyce prowadzi do zawyżenia prawdopodobieństwa zdarzenia A.

Drugie założenie, mówiące o niezależności zdarzeń w drzewie błędów w sensie probabilistycznym oznacza, że jeżeli C jest wyjściem funktora **I**, a zdarzenia $D_1, D_2, ..., D_n$ pojawiają się na jego wejściu, to

$$p(C) = p(D_1)\, p(D_2) \ ... \ p(D_n)$$

w przypadku gdy zdarzenia są zależne, zachodzi:

$$p(C) = p(D_1)\, p(D_1 / D_2) \ ... \ p(D_n / D_1 \ ... \ D_{n-1})$$

gdzie $p(D_i / D_1 \ ... \ D_j)$ oznacza prawdopodobieństwo warunkowe zdarzenia D_i pod warunkiem występowania koniunkcji zdarzeń $D_1, ..., D_j$.

W zagadnieniach analizy ryzyka mówi się w takim przypadku o zdarzeniach mających wspólną przyczynę, tj. kilka (różnych) zdarzeń występuje w sposób zależny w sensie probabilistycznym dlatego, że posiadają tę samą przyczynę. Analiza ilościowa drzew błędów w takich przypadkach jest trudna, ponieważ:

- wspólną przyczynę trzeba wykryć;
- w wielu miejscach w drzewie błędów trzeba umieścić trudne do oszacowania prawdopodobieństwa warunkowe, wynikające z zależności zdarzeń;
- w przypadku zależności zdarzeń oddalonych (w drzewie błędów) wyznaczenie prawdopodobieństwa zdarzenia na szczycie drzewa jest skomplikowane.

Podstawowym założeniem (i jednocześnie słabym punktem całej metodyki) jest przekonanie, że jeżeli skutkowi nie można przypisać prawdopodobieństwa w sposób natychmiastowy i bezpośredni, to **skutek ten da się rozłożyć na ciągi zdarzeń prowadzących do niego i znajdzie się zdarzenia takie** (nazywane dalej elementarnymi)**, dla których prawdopodobieństwa są znane na podstawie doświadczenia lub które można uzyskać od ekspertów z danej dziedziny**.

W szczególności, możliwe są następujące sposoby uzyskania prawdopodobieństw zdarzeń elementarnych:

- z prawdopodobieństwa zajścia konkretnych zdarzeń otrzymanego na podstawie danych statystycznych o pracy określonego systemu teleinformatycznego. Warunkiem jest tutaj znalezienie takiego systemu teleinformatycznego, dla którego jest prowadzony dziennik eksploatacji obejmujący m.in. takie fakty jak: sprzętowe awarie systemu, nieudane próby logowania do systemu, awarie systemu na skutek wniknięcia wirusów, włamania do systemu itd.;
- z prawdopodobieństwa otrzymanego na podstawie danych ogólnych (gromadzonych przez niektóre organizacje dla celów statystycznych) dotyczących konkretnych zjawisk, np. Komenda Główna Straży Pożarnej może dysponować danymi dotyczącymi ilości pożarów w Ośrodkach Komputerowych i strat poniesionych w ich wyniku w ciągu roku, Komenda Główna Policja powinna dysponować uogólnionymi danymi na temat kradzieży sprzętu komputerowego, korporacja przemysłowa może posiadać dane dotyczące przewidywanego czasu eksploatacji swoich urządzeń, CERT może udostępnić dane o różnych typach włamań do systemów komputerowych itp.;
- z oszacowania dokonanego przez eksperta liczby interesujących nas zdarzeń, które mogą zajść w ciągu pewnego okresu czasu;
- z przypisania przez eksperta współczynnika możliwości zajścia danego zdarzenia (w skali np. 1-10) w ciągu pewnego okresu czasu, np. roku;
- na podstawie metody delfickiej.

W większości przypadków w analizie ryzyka mamy do czynienia z oceną prawdopodobieństwa zdarzeń rzadkich (jak często zdarza się pożar lub trzęsienie ziemi zagrażające ośrodkowi komputerowemu?). W przypadku braku danych empirycznych, korzystamy (jak wynika z przytoczonej wcześniej listy) z ocen ekspertów.

Praktyka wskazuje, ze oceny ekspertów, czyli subiektywne szacowanie prawdopodobieństw zdarzeń rzadkich, może być obciążone dużymi błędami. Przyczyn takiego stanu rzeczy można się doszukiwać m.in. w dramatyzowaniu niektórych zdarzeń w środkach masowego przekazu, jak np. ujawnienie okolicznościowego wirusa lub włamanie do systemu komputerowego. Z tego powodu te zagrożenia (wirusy i hackerzy) są uważane za najgroźniejsze dla systemu komputerowego i przetwarzanej w nim informacji, chociaż w praktyce okazuje się, że znacznie częstsze i groźniejsze w skutkach mogą być np. ubytki wykwalifikowanego personelu.

W [1] przytacza się kilkuetapową procedurę określania subiektywnych ocen prawdopodobieństwa zdarzeń rzadkich:

1) przedstawia się ekspertowi listę takich zdarzeń i prosi o wskazanie najbardziej prawdopodobnego i najmniej prawdopodobnego zdarzenia na liście oraz o uszeregowanie wszystkich zdarzeń według rosnącego prawdopodobieństwa;
2) prosi się eksperta o podanie jego własnej oceny relacji między prawdopodobieństwami różnych zdarzeń (np. czy prawdopodobieństwo zdarzenia A jest trzy czy dziesięć razy większe od prawdopodobieństwa zajścia zdarzenia B);
3) pyta się eksperta, czy poszczególne zdarzenia przedstawione na liście są mniej czy bardziej prawdopodobne niż pewne zdarzenie lub zdarzenia odniesienia (zdarzenia rzadkie o znanych prawdopodobieństwach);
4) każdemu zdarzeniu przypisuje się wartość liczbową.

Inną, wymienioną wcześniej metodą określania prawdopodobieństw zdarzeń rzadkich, jest *metoda delficka*. W jednym z wariantów tej metody, zbiera się szacunkowe prawdopodobieństwa wystąpienia interesujących nas zdarzeń od ekspertów, uśrednia zebrane wartości, powiela otrzymane dane i taki zbiór rozprowadza się wśród tych samych ekspertów z zapytaniem, czy po zapoznaniu się z tymi ocenami nie są skłonni zmodyfikować swojej.

Po takiej „rundzie modyfikacyjnej" dane są zbierane ponownie. Jeżeli otrzymuje się spójne wartości, obliczane są na ich podstawie ostateczne wartości prawdopodobieństw. Jeżeli wartości są niespójne, eksperci powinni zostać zebrani w jednym miejscu w celu przedyskutowania przyczyn niespójności i wypracowania wartości końcowych prawdopodobieństw ocenianych zdarzeń rzadkich.

4. Metody oceny akceptowalności ryzyka

W analizie ryzyka przy ocenie akceptowalności ryzyka, można stosować następujące formalne metody [1]:

- *preferencje ujawnione* - miarą akceptowalności nowego ryzyka związanego z danym przedsięwzięciem jest ryzyko już istniejące w społeczeństwie, tzn. trzeba posiadać informacje z nim związane i porównać z badanym ryzykiem;
- *preferencje wyra#one* - różne osoby są pytane wprost o akceptowalność konkretnego ryzyka (musza być świadome zarówno ryzyka jak i korzyści przedsięwzięcia);

- *analiza ryzyka i korzy$ci*.

Akceptowalność ryzyka (w szczególności w trzeciej z metod) napotyka na poważne trudności, gdy w grę wchodzi życie ludzkie (a więc głównie w systemach komputerowych wspomagających intensywną terapię, nawigację w samolotach, pracę reaktora jądrowego itp.)[6], ponieważ **nie ma akceptowanych powszechnie metod oceniania wartości życia ludzkiego**.

W literaturze [1] można spotkać następujące podejścia do wyceny wartości życia ludzkiego[7]:

- życie ludzkie jako kapitał - *wersja netto*: wartość osoby jako wartość straty dla reszty społeczeństwa - od dyskontowanych zarobków tej osoby odejmuje się dyskontowaną kwotę zarobków przeznaczonych przez nią w przyszłości na konsumpcję; *wersja brutto*: ocena wartości życia obejmuje również kwotę zarobków przeznaczonych przez daną osobę w przyszłości na konsumpcję, której nie odejmuje się od dyskontowanej sumy przyszłych zarobków;
- orzeczenia sądowe w sprawach odszkodowań za utratę życia;
- ogólna suma odszkodowania, której zażądaliby członkowie grupy narażonej na ryzyko za zgodę na dodatkowe prawdopodobieństwo utraty życia wynikające z ocenianego przedsięwzięcia;
- metoda „wojskowa" - ilość strat własnych w „sile żywej" w stosunku do osiągniętych celów.

5. Podsumowanie

W artykule zaproponowano definicję ryzyka ukierunkowaną na bezpieczeństwo informacji. Definicja ta wiąże podstawowe atrybuty związane z bezpieczeństwem informacji (tajność, integralność i dostępność) z miarą stopnia zagrożenia (wyrażaną najczęściej za pomocą prawdopodobieństwa) oraz stratami poniesionymi w wyniku zrealizowania się zagrożenia. Powiązanie definicji ryzyka z definicją bezpieczeństwa teleinformatycznego (podaną na początku niniejszego artykułu) pozwala sprecyzować proces analizy ryzyka dla

[6] Jak widać z przytoczonych przykładów, są to systemy czasu rzeczywistego, związane ze sterowaniem różnego typu procesami, realizowane często jako systemy wbudowane. Dotyczy ich zwykle wspomniane w rozdz.2 „bezpieczeństwo na zewnątrz" ujęte normą IEC 61508.

[7] Trzeba jednak pamiętać, że również podatność na włamanie systemu bazodanowego może nieść śmiertelne zagrożenie dla człowieka (np. w bazie danych mamy informacje o świadkach incognito lub naszych agentach służb specjalnych działających wewnątrz mafii).

potrzeb bezpieczeństwa teleinformatycznego w sposób opisany w kolejnych rozdziałach.

Do podstawowych wad *analizy ryzyka* jako metody należy zaliczyć:

- częsty brak danych do wyznaczenia prawdopodobieństwa zdarzeń elementarnych;
- trudności w ustaleniu pełnego zbioru zagrożeń i podatności;
- niezdolność do badania skutków negatywnych o wspólnej przyczynie;
- nieuwzględniane ryzyka wtórnego[8];
- nieuwzględniane zagrożenia spowodowanego rozmyślnie;
- trudności w interpretacji wyników.

Za podstawowe zalety metod analizy ryzyka można uznać:

- dane i oceny ekspertów z różnych dziedzin mogą być ujęte we wspólne ramy logiczne;
- można jawnie formułować założenia;
- wagę poszczególnych założeń można ocenić przy pomocy analizy wrażliwości.

Odnosząc przeprowadzoną ocenę do *analizy ryzyka jako pewnego kompletnego procesu*, można wypunktować następujące jego **zalety**:

- pomaga precyzyjniej identyfikować zagrożenia oraz ich przyczyny;
- stanowi podstawę do podejmowania decyzji administracyjnych i managerskich;
- systematyzuje proces oceny bezpieczeństwa teleinformatycznego

oraz **wady**:

- może być mało precyzyjna, zarówno w odniesieniu do samego ryzyka, jak i w analizie kosztów i zysków (jak oceniać zagrożenie życia ludzkiego?);
- może dawać złudne poczucie bezpieczeństwa w przypadku braku systematycznego ponawiania analizy ryzyka dla konkretnego systemu komputerowego (nowe zagrożenia mogą fałszować wyniki wcześniej przeprowadzonej analizy ryzyka). Ze względu na koszty takiego procesu, często się o tym aspekcie oceny bezpieczeństwa teleinformatycznego „zapomina".

Literatura:

[8] Np. awaria systemu nawigacji w samolocie bojowym może kosztować nie tylko życie pilota, ale w przypadku, gdy samolot spadnie na tereny zamieszkane również wielu innych ludzi.

[1] Findeisen W. (red): *Analiza systemowa - podstawy i metodologia*,. PWN, Warszawa,1985
[2] Liderman K.: *Bezpiecze&stwo informacji w systemach komputerowych*, IAiR WAT, Warszawa, 1999
[3] PN-I-02000: *Technika informatyczna. Zabezpieczenia w systemach informatycznych*, 1998
[4] PN-I-13335-1: *Technika informatyczna. Wytyczne do zarz"dzania bezpiecze&stwem systemów informatycznych. Poj'cia i modele bezpiecze&stwa systemów informatycznych*, 1999.

Recenzent: dr hab. in#. W!odzimierz Kwiatkowski
Praca wp!yn'!a do redakcji (*0.*(*0.200*(