STUDIA INFORMATICA 2002
Volume 23 Number 2B (49)

Andrzej BIAŁAS
Wyższa Szkoła Informatyki i Zarządzania

WPROWADZENIE DO MODELOWANIA PROCESÓW ANALIZY RYZYKA W SYSTEMACH TELEINFORMATYCZNYCH

Streszczenie. Artykuł dotyczy problematyki modelowania podstawowego procesu zarządzania bezpieczeństwem informacji, jakim jest analiza ryzyka systemów teleinformatycznych. Ujęcie istoty tych procesów pozwala na opis formalny, a ten z kolei umożliwia tworzenie efektywnych narzędzi do komputerowego wspomagania. W artykule przedstawiono poszczególne fazy analizy ryzyka i możliwość ich formalnego opisu: identyfikację zasobów i ich podatności, opis środowiska zagrożeń oraz oszacowanie samego ryzyka. Zwrócono uwagę na trudności opisu, takie jak: subiektywność i trudnomierzalność ocen, zmienność w czasie czy złożoność relacji między elementami analizy ryzyka. Wszystko to utrudnia tworzenie komputerowych narzędzi wspomagających prowadzenie analizy ryzyka i stanowi ciągłe wyzwanie dla twórców tego typu analizatorów.

INTRODUCTION TO RISK ANALYSIS PROCESS MODELLING

Summary. The paper deals with IT security risk assessment modelling, allowing creation of effectiveness computer assistance risk analysis tools. Reviewing processes like identification and valuation of assets, vulnerability and threats assessment and summary risk assessments, basic modelling problems were identified, i.e. complexity, unmeasureability, changing in time and subjectivity of assessments.

1. Wprowadzenie

Artykuł stanowi wprowadzenie do problematyki analizy ryzyka w systemach teleinformatycznych. Właściwie przeprowadzona analiza ryzyka pozwala efektywnie zarządzać ryzykiem poprzez dobór właściwych zabezpieczeń, to znaczy adekwatnych do zagrożeń i do wartości chronionych zasobów. Występuje tu aspekt techniczny (skuteczność zabezpieczeń), organizacyjny (łatwość zarządzania nimi) i ekonomiczny (relacja kosztów do

wartości zasobów). W systemach bardzo złożonych i przeznaczonych do odpowiedzialnych zastosowań, analizy ryzyka pominąć się nie da, zaś jej przeprowadzenie wymaga posiadania odpowiednich metod, *know-how* oraz precyzyjnych narzędzi wspomagających. Są one pilnie strzeżone przez przodujące firmy konsultingowe oraz instytucje koordynujące zabiegi wokół bezpieczeństwa informacji w poszczególnych krajach. Dokładność ocen zależy od precyzji danych wejściowych i inteligencji samych narzędzi. Podstawowym warunkiem spełnienia tych wymagań jest odpowiednie zamodelowanie procesów i zależności zachodzących podczas analizy ryzyka.

W artykule przedstawiono określenie pojęcia ryzyka i jego miejsce w procesach zarządzania bezpieczeństwem informacji, podstawowe strategie zarządzania ryzykiem i wreszcie naszkicowano przebieg formalnej analizy ryzyka. Ponadto zwrócono uwagę na podstawowe problemy, które należy rozwiązać przy budowie modelu ryzyka, stanowiącego bazę do tworzenia narzędzi wspomagających jego analizę.

2. Analiza ryzyka i jej miejsce w zarządzaniu bezpieczeństwem informacji

Podstawowe pojęcia dotyczące analizy ryzyka przedstawiono w [6, 11]. Przypomnijmy tylko, że ryzyko (ang. *risk*) to prawdopodobieństwo (czasem tylko mniej formalnie - możliwość), że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować zniszczenie zasobów lub inne straty, czyli następstwa.

Wartości liczbowej prawdopodobieństwa towarzyszą zwykle pewne informacje opisowe:

- scenariusz ryzyka, tj. opis, w jaki sposób dane zagrożenie wykorzystuje podatność zasobu prowadząc do następstw,
- charakterystyka ewentualnych następstw.

Analiza ryzyka (ang. *risk analysis*) to proces identyfikacji ryzyka, określania jego wielkości i wyodrębnienia obszarów wymagających zabezpieczeń. Wynikiem tej analizy jest lista niebezpieczeństw, jakie zagrażają systemom z podaniem ich prawdopodobieństw, scenariuszy i skutków wystąpienia niekorzystnych zdarzeń.

Zarządzanie ryzykiem (ang. *risk management*) sprowadza się do ciągłych działań ograniczających zidentyfikowane ryzyko, ale należy pamiętać, że odbywa się to pewnym kosztem (koszt zabezpieczeń, ich wdrożenia i utrzymywania). Analiza ryzyka ma raczej charakter statyczny, gdyż prowadzona jest w określonych sytuacjach, np. przy projektowaniu lub przebudowie systemu, co pewien czas, po incydencie, itp., zaś zarządzanie ryzykiem to proces permanentny.

Zarządzanie ryzykiem, zarządzanie konfiguracją i zarządzanie zmianami składają się na jeszcze bardziej ogólny proces, jakim jest zarządzanie bezpieczeństwem informacji.

Procesy analizy ryzyka wkomponowane są w trójpoziomowy model hierarchii celów, strategii i polityk. Rozważając bezpieczeństwo na poziomie instytucji, prowadzi się ogólną analizę ryzyka (ang. *high level risk analysis*), w której toku określa się możliwość zakłócenia realizacji zadań statutowych instytucji z przyczyn, które tkwią w użytkowanych systemach teleinformatycznych. Wyniki tej analizy służą do przyjęcia dla instytucji jednej z czterech podstawowych strategii zmierzających do redukcji ryzyka [3]:

- zastosowanie zabezpieczeń typowych dla określonych warunków, często skatalogowanych - ochrona podstawowa (ang. *baseline approach*),
- przyjęcie zabezpieczeń po przeprowadzeniu nieformalnej, często uproszczonej analizy ryzyka (ang. *informal approach*),
- przyjęcie zabezpieczeń wynikających z dokładnej, formalnej analizy ryzyka (ang. *detailed risk analysis*),
- w wyniku ogólnej analizy ryzyka wyznacza się szczególnie wrażliwe obszary systemu, dla których zabezpieczenia dobiera się na podstawie formalnej analizy ryzyka, zaś dla reszty systemu wystarcza ochrona podstawowa (ang. *combined approach*).

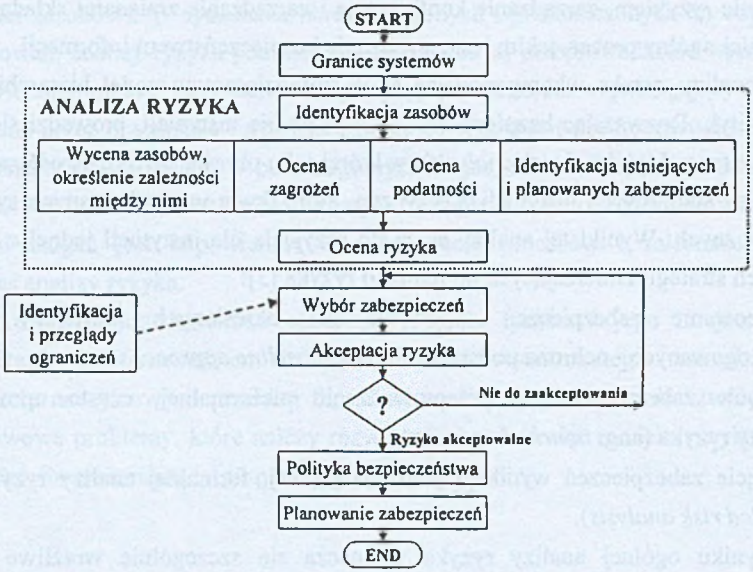
Przeprowadzenie dokładnej analizy ryzyka wymaga posiadania narzędzi wspomagających, opartych na formalnych modelach ryzyka.

3. Procesy analizy ryzyka i ich opis formalny

Proces zarządzania ryzykiem wspomagany formalną analizą ryzyka [3] przedstawia rys 1. Na wstępie należy określić granice systemów instytucji - obszarów, w obrębie których będzie prowadzone zarządzanie ryzykiem. Uwzględnia się przy tym takie elementy, jak:

- zasoby teleinformatyczne: informacje wrażliwe, sprzęt i oprogramowanie,
- zasoby kadrowe: personel, podwykonawcy i inne osoby z zewnątrz,
- otoczenie: budynki, pomieszczenia, infrastruktura,
- działanie: funkcje i usługi oferowane za pomocą systemów.

Analiza ryzyka obejmuje identyfikację zasobów (aktywów) instytucji, ustalenie wzajemnych relacji między nimi i ich podatności, analizę środowiska zagrożeń, w którym wyeksponowano podatne zasoby, wyposażonego już zwykle w pewne zabezpieczenia i wreszcie oszacowanie ryzyka wystąpienia incydentów, prowadzących do następstw.



Rys. 1. Zarządzanie ryzykiem wspierane formalną analizą ryzyka
Fig. 1. Risk management supported by detailed risk analysis

3.1. Analiza zasobów

Zasoby (aktywa) mają wartość dla instytucji i warunkują prowadzenie przez nią działalności, stąd powinny one podlegać ochronie. Do przykładowych należą:

- dane i informacje wrażliwe: tajemnice przedsiębiorstwa oraz prawnie chronione – w postaci plików, wiadomości, dokumentów elektronicznych, baz danych,
- usługi udostępniania informacji, obliczeniowe, płatnicze, transakcyjne i związane z nimi poufność oraz zaufanie,
- sprzęt teleinformatyczny: komputery, drukarki, środki łączności, okablowanie, urządzenia i linie zasilające,
- oprogramowanie systemowe, komunikacyjne i użytkowe,
- dokumentacja papierowa (kontrakty, projekty, kartoteki, procedury),
- firmware i nośniki z danymi lub oprogramowaniem instalacyjnym lub tworzonym w instytucji,
- personel - jego wiedza i doświadczenie,
- infrastruktura produkcyjno–usługowa, maszyny, linie technologiczne, bankomaty, stanowiska obsługi, zapasy materiałowe,
- infrastruktura techniczna – budynki, pomieszczenia, środowisko instytucji,
- wizerunek instytucji, w tym zaufanie klientów.

Zasoby mają różnorodny charakter, wymagają klasyfikacji i wyceny prowadzonej w kontekście ich utraty. Bardzo trudno jest to wyrazić za pomocą konkretnych kwot, stąd stosuje się umowne skale wartości, np.: pomijalna, niska, średnia, wysoka, bardzo wysoka, które jednak powinny zostać oszacowane w kontekście danej instytucji. Wycenę prowadzi się w myśl zasady „co się stanie, jeśli...?", uwzględniając przy tym wielkość i różnorodność potencjalnych następstw, takich jak:

- zakłócenie ciągłości procesów biznesowych, składających się na misję instytucji,
- zagrożenie dla zdrowia lub życia,
- zakłócenie porządku publicznego,
- możliwość naruszenia prawa lub zobowiązań,
- starty finansowe,
- utrata reputacji instytucji,
- zagrożenie dla środowiska naturalnego,
- ujawnienie lub zniszczenie danych osobowych, danych o tożsamości instytucji czy też tajemnic handlowych.

Osobnym problemem jest wyrażenie relacji między zasobami – utrata jednego zasobu pociąga zwykle za sobą utratę kilku innych. Badając zależności między zasobami, należy uwzględnić efekt propagacji ich wartości, to znaczy, jeśli zasób podrzędny ma wartość wyższą od nadrzędnego, to musi być ona również przypisana do nadrzędnego.

Wynika stąd, że model zasobów powinien uwzględniać co najmniej:

- identyfikator i nazwę zasobu,
- kategorię w przyjętej klasyfikacji zasobów,
- szereg atrybutów i przyporządkowanych im umownych wartości,
- listy powiązań, wyrażających zależności między zasobami,
- listy powiązań z rekordami opisującymi inne elementy modelu (podatności, zagrożenia, itp.).

W rezultacie analiz uzyskuje się uporządkowaną listę zasobów i ich wartości w kontekście utraty poufności, integralności i dostępności. Na potrzeby polityki bezpieczeństwa wymagane są dodatkowe atrybuty zasobów, m.in., ich umiejscowienie, zasady eksploatacji, kto jest właścicielem, a kto odpowiedzialnym za dany zasób.

3.2. Środowisko zagrożeń

Zagrożenia są potencjalnymi przyczynami incydentów prowadzącymi do następstw, na przykład: błędy i uchybienia, oszustwo i kradzież, sabotaż, utrata lub zniszczenie elementów infrastruktury, działania intruzów, zawirusowanie, czy też szpiegostwo przemysłowe. Ich realność ocenia się na podstawie statystyk, opinii ekspertów, użytkowników lub właścicieli

zasobów. Różnorodność form zagrożeń wymaga ich klasyfikacji, ułatwiającej prowadzenie analiz. Funkcjonują więc podziały zagrożeń na przypadkowe i rozmyślne, na mające źródło w środowisku bądź powodowane przez człowieka. Należy pamiętać, że żadna wzorcowa lista zagrożeń nie może być zamknięta – ciągle bowiem pojawiają się nowe formy zagrożeń. W katalogach zagrożeń [10] przedstawionych jest kilkaset ich przykładów.

Model zagrożeń powinien uwzględniać:

- identyfikator i nazwę zagrożenia,
- kategorię w klasyfikacji zagrożeń,
- źródło, czyli określać, co lub kto go powoduje,
- obiekt zagrożenia - które elementy systemu są zagrożone,
- prawdopodobieństwo (w sensie matematycznym) lub tylko możliwość wystąpienia (w skali umownej), oceniane na podstawie:
    - częstości występowania, określonej na podstawie statystyk i doświadczeń, jeśli takowe są dostępne,
    - motywacji sprawcy,
    - wymaganych zdolności, wiedzy i zasobów sprawcy,
    - atrakcyjności i podatności celu ataku,
    - czynników geograficznych i środowiskowych, takich jak: bliskość strategicznych obiektów czy też warunki psychofizyczne sprzyjające błędom ludzkim lub awariom urządzeń,
- powiązanie z podatnymi zasobami, do których zagrożenie się odnosi.

Rezultatem tej analizy jest lista zidentyfikowanych zagrożeń powiązana z zasobami lub ich grupami, których one dotyczą oraz możliwość ich wystąpienia, wyrażona w skali umownej lub za pomocą prawdopodobieństwa.

3.3. Ocena podatności

Analiza podatności polega na zidentyfikowaniu słabości dotyczących: infrastruktury, środowiska, sprzętu, oprogramowania, informacji, środków łączności, dokumentacji, personelu, organizacji i administracji, które mogą być wykorzystane przez zagrożenia w celu spowodowania szkód, na przykład: nie zabezpieczone połączenia, niewyszkolony personel, brak klasyfikacji informacji, brak kopii zapasowych, brak polityki bezpieczeństwa, nieświadomość zagrożeń w sferach kierowniczych, brak kontroli dostępu, brak rozliczalności. Podatność jest pewnym atrybutem każdego zasobu. Model podatności powinien uwzględniać co najmniej:

- identyfikator i nazwę podatności,
- kategorię w stosowanej klasyfikacji podatności,

- wskaźnik do zasobów, których ona dotyczy,
- wskaźnik do zagrożeń, które ją wykorzystują,
- stopień konsekwencji (surowość), którą ona z sobą niesie, wyrażony w kilkustopniowej skali umownej (niski, średni, wysoki), czyli łatwość, z jaką podatność jest wykorzystywana przez zagrożenie.

Wynikiem analizy podatności jest lista zidentyfikowanych i oszacowanych w skali umownej podatności zasobów, powiązana z konkretnymi zagrożeniami.

3.4. Identyfikacja istniejących lub planowanych zabezpieczeń

Analiza ryzyka wymaga uprzedniej identyfikacji zabezpieczeń już istniejących w systemach. Ma to aspekt ekonomiczny, zmierzający do uniknięcia dublowania zabezpieczeń. Część z tych zabezpieczeń zostanie usunięta, część wymieniona lub uzupełniona – ogólnie dopasowana do tworzonego planu zabezpieczeń. Dobór zabezpieczeń jest procesem zarządzania ryzykiem, znajdującym się poza zakresem rozważań niniejszego artykułu, jednak na potrzeby analizy ryzyka przyjąć należy pewien uproszczony model zabezpieczeń, uwzględniający co najmniej następujące elementy:

- identyfikator i nazwę zabezpieczenia,
- kategorię w stosowanej klasyfikacji zabezpieczeń,
- funkcje zabezpieczenia (przed czym ono zabezpiecza i w jakim stopniu),
- koszt zabezpieczenia,
- status (wdrożony, planowany).

Wynikiem analizy istniejących i planowanych zabezpieczeń jest ich lista.

3.5. Ocena ryzyka

Celem tego etapu analizy ryzyka, jest identyfikacja i oszacowanie ryzyka dla zasobów częściowo zabezpieczonych, ale nadal podatnych, wyeksponowanych w środowisku zagrożeń. Ryzyko jest funkcją:

- wartości zasobów,
- prawdopodobieństwa wystąpienia zagrożenia,
- łatwości, z jaką zagrożenie wykorzystuje podatność,
- skuteczności istniejących lub planowanych zabezpieczeń.

Każdy z tych argumentów wyrażony jest zwykle w predefiniowanej skali umownej (miara jakościowa), również oszacowane ryzyko wyrażone w skali umownej. Liczba poziomów tych skal i ich wycena wartościowa zależą od potrzeb danej instytucji. Stosowane są różne metody szacowania ryzyka, których przykłady zamieszczono w poniższych tabelach.

3.5.1. Macierz predefiniowanych wartości

Przyjmując, że zagrożenia i podatności można wyrazić w skali trójstopniowej (tabela 1), zaś wartość zasobów w skali 6-stopniowej, to wówczas oszacowane ryzyko uzyskuje się w skali 10-stopniowej.

Tabela 1

Macierz predefiniowanych wartości

	Zagrożenie	Niskie			Średnie			Wysokie		
	Podatność	niska	średnia	wysoka	niska	średnia	wysoka	niska	średnia	wysoka
Wartość zasobu	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

3.5.2. Ranking zagrożeń

W tym przypadku (tabela 2) należy wyznaczyć listę rankingową zagrożeń, wyrażającą ich powagę i wskazującą na kolejność (priorytet), jaką należy się kierować w toku zarządzania ryzykiem. Przyjmując, że następstwa (wartość zasobu) oraz możliwość wystąpienia zagrożenia (łatwość, z jaką zagrożenie wykorzystuje podatność) można wyrazić w skali od 1 do 5, to ryzyko umowne będące ich iloczynem wyrażone jest w skali od 1 do 25. Wyznaczenie wartości tego ryzyka pozwala ustalić listę rankingową zagrożeń, czyli pożądaną kolejność ich eliminowania.

Tabela 2

Ranking zagrożeń

Zagrożenie	Następstwo (wartość zasobu)	Możliwość wystąpienia zagrożenia	Ryzyko	Powaga zagrożenia (miejsce w rankingu)
Zagrożenie #1	1	2	2	6
Zagrożenie #2	4	3	12	3
Zagrożenie #3	3	5	15	2
Zagrożenie #4	5	5	25	1
Zagrożenie #5	5	1	5	4
Zagrożenie #6	2	2	4	5

3.5.3. Częstość zagrożeń

Metoda jest dwustopniowa. Najpierw na podstawie zagrożeń i podatności tworzona jest skala pomiarowa częstości zagrożeń (tabela 3). W przykładzie założono 3-poziomową skalę dla podatności i 4-poziomową skalę dla zagrożeń. Uzyskano 6-stopniową skalę pomiaru częstości zagrożeń.

Tabela 3

Ustalenie skali częstości zagrożeń

Zagrożenie	Niskie			Średnie			Wysokie			Bardzo wysokie		
Podatność	niska	średnia	wysoka	niska	średnia	wysoka	niska	średnia	wysoka	niska	średnia	wysoka
Częstość zagrożeń	0	1	2	1	2	3	2	3	4	3	4	5

W drugim kroku (tabela 4), na podstawie częstości zagrożeń oraz wartości zasobów (potencjalnych szkód), ustalana jest szacunkowa wartość ryzyka.

Tabela 4

Szacunkowa wartość ryzyka

	Następstwo (wartość zasobu)	0	1	2	3	4	5
Częstość zagrożeń							
0		0	1	2	3	4	5
1		1	2	3	4	5	6
2		2	3	4	5	6	7
3		3	4	5	6	7	8
4		4	5	6	7	8	9
5		5	6	7	8	9	10

3.5.4. Ryzyko tolerowane

W niektórych przypadkach wystarcza tylko uzyskanie odpowiedzi na pytanie, czy dane ryzyko ma być w instytucji tolerowane (T), czy też nie (NT). Przyjmując częstości zagrożeń z tabeli 4, tabela ryzyka tolerowanego (tabela 5) pozwala uzyskać odpowiedź na tak postawione pytanie. Przyjęto założenie, że ryzyko umowne do wartości 5 będzie w instytucji tolerowane.

Tabela 5

Ryzyko tolerowane

	Następstwo (wartość zasobu)	0	1	2	3	4	5
Częstość zagrożeń							
0		T	T	T	T	T	T
1		T	T	T	T	T	NT
2		T	T	T	T	NT	NT
3		T	T	T	NT	NT	NT
4		T	T	NT	NT	NT	NT
5		T	NT	NT	NT	NT	NT

4. Wnioski i uwagi końcowe

Artykuł stanowi wprowadzenie do analizy ryzyka, która stanowi podstawę doboru zabezpieczeń podczas zarządzania ryzykiem. Przedstawione modele są dość ogólne i oparte na oszacowaniach elementów analizy w predefiniowanych skalach umownych.

Modele tu przedstawione nie wyrażają zależności logicznych i korelacji między zdarzeniami związanymi z bezpieczeństwem. Modele te nie wyrażają również dynamiki procesów bezpieczeństwa, zwłaszcza zapewnienia odpowiedniej reakcji na naruszenia, a także samokontroli skuteczności zabezpieczeń. Każde z tych zagadnień jest godne uwagi, gdyż tylko modele zdolne do wyrażenia tych własności mogą być podstawą do tworzenia narzędzi wspomagających.

LITERATURA

1. ISO/IEC TR 13335-1: 1996, Information technology – Guidelines for the management of IT Security, Part1: Concepts and models for IT Security.
2. ISO/IEC TR 13335-2: 1997, Information technology – Guidelines for the management of IT Security, Part2: Managing and planning IT Security.
3. ISO/IEC TR 13335-3: 1998, Information technology – Guidelines for the management of IT Security, Part3: Techniques for the management of IT Security.
4. ISO/IEC TR 13335-4: 2000, Information technology – Guidelines for the management of IT Security, Part4: Selection of safeguards.
5. ISO/IEC WD 13335-5: 1999, Information technology – Guidelines for the management of IT Security, Part5: Management guidance on Network security.
6. PN-I-13335-1: Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, styczeń 1999.
7. BS7799 Part 1: Code of practice for Information Security Management, British Standard Institute, 1999.
8. BS7799 Part 2: The Specification for Information Security Management, British Standard Institute, 1999.
9. ISO/IEC 17799 Information technology - Code of practice for information security management, 2000.
10. IT Baseline Protection Manual (IT-Grundschutz Handbuch), Bundesamt fuer Sicherheit in der Informationstechnik.

11. Białas A.: Zarządzanie bezpieczeństwem informacji w systemach gospodarki elektronicznej, VIII Konferencja SIECI KOMPUTEROWE – Krynica 2001, Studia Informatica vol. 22, Number 2(44), Silesian University of Technology Press, Gliwice 2001.
12. Pańkowska M.: Istota ryzyka ochrony zasobów informatycznych, http:/netsecurity.pl/articles/polskie/Istota_ryzyka_ochrony_zasobów_informatycznych.htm
13. Liderman K.: Analiza ryzyka dla potrzeb bezpieczeństwa teleinformatycznego, WinSecurity Magazine Nr 2, grudzień 2001.
14. Mąka D.: Elementy analizy zagrożeń i zarządzania ryzykiem w świetle polityki bezpieczeństwa informacyjnego, IT Security Magazine 8-9 (24-25)/2001.

Recenzent: Prof. dr hab. inż. Andrzej Grzywak

Wpłynęło do Redakcji 26 marca 2002 r.

Abstract

The paper deals with IT security risk assessment. Basic terminology and all stages of risk analysis were presented like identification of assets, vulnerability and threats assessments, identification of existing or planned safeguards and finally assessment of the risk. Risk management supported by detailed risk analysis was shown on the Fig 1. Contents of the data structure of the model and its relations were mentioned. Risk assessment methods were presented: matrix with predefined values (table 1), ranking of threats by measures of risk (table 2), assessing a value for the frequency and the possible damage of risks (table 3) and distinction between tolerable and intolerable risks (table 4).