STUDIA INFORMATICA 2001
Volume 22 Number 4 (46)

Dobrosław MĄKA
Wojskowe Służby Informacyjne

PRZECIWDZIAŁANIE ZAGROŻENIOM BEZPIECZEŃSTWA INFORMACYJNEGO – ZARZĄDZANIE RYZYKIEM W ŚWIETLE POLITYKI BEZPIECZEŃSTWA

Streszczenie. Stałym elementem polityki bezpieczeństwa jest prowadzenie bieżących analiz związanych z podatnością systemów informatycznych na zagrożenia, tzw. analiza zagrożeń. Z pojęciem tym wiąże się zarządzanie ryzykiem, obejmujące system metod i działań zmierzających do obniżenia stopnia oddziaływania ryzyka na funkcjonowanie systemu, pozwalających na podejmowanie decyzji optymalnych. W niniejszej artykule przedstawiono stosowane metody zarządzania ryzykiem w systemach i sieciach teleinformatycznych.

COUNTERACTION AGAINST INFORMATION SECURITY THREATS – RISK MANAGEMENT IN THE LIGHT OF SECURITY POLICY

Summary. The constant element of security policy is conducting of current analyses, connected with vulnerability IT systems to threats, so called threats analysis. This includes risk management, comprising methods and activities towards decreasing influence of risk level on system functionality, which allow an optimal decision taking. This publication shows suitable methods of risk management in IT systems and networks.

1. Wprowadzenie

We współczesnym świecie, w warunkach postępującej globalizacji informacyjnej, gdzie informacja jest podstawą biznesu i rozwoju gospodarki, konieczna staje się znajomość środków jej ochrony. Dołączenie polskiej gospodarki do gospodarki europejskiej spowoduje dalsze rozpowszechnienie standardów stosowanych w krajach rozwiniętych, a stosowanie

środków ochrony informacji stanie się podstawowym wymogiem stawianym przed nowoczesną firmą.

Jesteśmy społeczeństwem uzależnionym od informacji. Nowoczesne techniki przekazu umożliwiają nam łatwe jej przenoszenie na praktycznie dowolną odległość. Działalność niemal każdej instytucji związana jest z przetwarzaniem informacji. Problemem jest jedynie zapewnienie, aby trafiała ona do ludzi, dla których jest przeznaczona oraz aby nie była wykorzystywana przez organizacje i instytucje przestępcze do działań szkodzących bezpieczeństwu państwa, instytucji czy też obywateli.

Od połowy lat 80 nastąpił gwałtowny rozwój technik informatycznych, a w latach 90 dodatkowo telekomunikacji oraz technik przekazywania danych. Rozwój technologiczny końca XX wieku spowodował też powstanie szeregu nowych zjawisk patologicznych, w tym szeroko rozumianą przestępczość teleinformatyczną (oszustwa komputerowe, manipulacje bilansowe, szpiegostwo komputerowe, hackerstwo) - w literaturze fachowej określane jako "cyberterroryzm".

Ochrona informacji ściśle związana jest z tzw. pojęciem polityki bezpieczeństwa informacyjnego. Zgodnie z polską normą PN-I-13335-1, przez pojęcie polityka bezpieczeństwa instytucji w zakresie systemów informatycznych (ang. *IT security policy*) rozumiane są: zasady, procedury zarządzania, które określają, jakie zasoby (włącznie z informacjami wrażliwymi) są zarządzane, chronione i dystrybuowane w danej instytucji i jej systemach informatycznych.

Wyżej wspominana polska norma PN-I-13335-1 definiuje również zagrożenia, na jakie narażona jest informacja. Ochrona informacji jest elementem kluczowym, znajduje to odzwierciedlenie w kolejnych nowelizacjach ustawy o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. Przepisy ustawy znacznie rozszerzają krąg zainteresowania. Szczególną uwagę zwraca się w niej na ochronę informacji niejawnych w odniesieniu do przedsiębiorstw, jednostek naukowych, badawczo-wdrożeniowych. Istotnym elementem, na który położono nacisk, jest posiadanie poświadczenia bezpieczeństwa przez osoby mające bezpośredni dostęp do informacji niejawnych, wydanego przez właściwe służby ochrony państwa. Zostały również uściślone procedury sprawdzające postępowanie odwoławcze i skargowe. Dużym zmianom uległy rozdziały 10 (bezpieczeństwo systemów i sieci teleinformatycznych) oraz 11 (bezpieczeństwo przemysłowe), gdzie baczną uwagę zwrócono na techniki kryptograficzne i certyfikację urządzeń.

Ochrona informacji ściśle jest powiązana z polityką bezpieczeństwa poszczególnych organizacji. Celem polityki bezpieczeństwa jest stworzenie podstaw dla metod zarządzania, procedur i wymagań niezbędnych dla zminimalizowania zagrożeń niekontrolowanego ujawnienia informacji wrażliwej. Niemałe znaczenie ma tutaj analiza i zarządzanie ryzykiem, jako

element podlegający ustawicznym badaniom, w szczególności w krajach członkowskich NATO.

2. Analiza ryzyka a analiza zagrożeń

Stałym elementem polityki bezpieczeństwa jest prowadzenie analiz związanych z podatnością systemów informatycznych na zagrożenia, tzw. analiza zagrożeń. Analiza ta polega na gromadzeniu informacji o możliwych zagrożeniach systemu przetwarzania informacji w taki sposób, aby nie pominąć żadnego z zagrożeń istotnych. Stąd też istotna staje się właściwa klasyfikacja zagrożeń oraz dobór stosownego kryterium klasyfikacji.

Poniżej przedstawiono przykładowe klasyfikacje wg różnych kryteriów podziału:

Podział 1:

- **bierne** – nieuprawnione ujawnienie informacji bez oddziaływania na pracę systemu (podsłuch, analiza ruchu w sieci, emisja ujawniająca);
- **czynne** – aktywne oddziaływanie na system (nieuprawniony dostęp do systemu, nieautoryzowane dokonywanie zmian, niszczenie informacji, dezinformacja, nieuprawnione nadanie praw dostępu do zasobów); działania te zwykle poprzedzone są działaniami biernymi;

Podział 2:

- **wewnętrzne** – dokonywane ze strony legalnych użytkowników sieci;
- **zewnętrzne** – dokonywane przez osoby postronne z zewnętrz (intruzów), zainteresowanie danymi posiadanymi przez daną instytucję;

Podział 3:

- **losowe** – wynikające z błędów obsługi ze strony administratorów czy też operatorów, jak również uszkodzeń sprzętu, błędów w oprogramowaniu itp.;
- **celowe** – świadome (złośliwe) działania mające na celu zniszczenie lub unieruchomianie systemu.

Możliwy jest również także 4 podział zagrożeń:

- **sprzętowe** – powodowane przez sprzęt;
- **programowe** – powodowane poprzez oprogramowanie,
- **osobowe** – powodowane przez ludzi.

Przedstawiona klasyfikacja zagrożeń nie wyklucza wzajemnego przenikania i nakładania się na siebie poszczególnych elementów, co oznacza iż zagrożenie może być np. jednocześnie czynne, wewnętrzne, celowe programowe lub jednocześnie przypadkowe i sprzętowe.

Skuteczny atak na system wymaga przełamania bariery, którą stanowią zasady dostępu do systemu. Wbrew powszechnemu mniemaniu, podkreślić należy, że największego zagrożenia należy spodziewać się ze strony legalnych użytkowników systemu, przy czym zagrożenie to wzrasta wraz z liczbą użytkowników i zróżnicowania ich uprawnień.

Zagrożenia zewnętrzne mogą być całkowicie niezależne od działania ludzkiego (np. katastrofy żywiołowe) albo mogą powstać na skutek awarii innych systemów (np. pożar lub zalanie). Do kategorii zagrożeń zewnętrznych należy zaliczyć:

- wypadki i katastrofy spowodowane czynnikami naturalnymi (woda, ogień, wyładowania atmosferyczne, trzęsieniem ziemi itp.),
- wpływy środowiskowe (zmiany temperatury i wilgotności, zanieczyszczenie powietrza, zapylenie, silne pola magnetyczne, wibracje mechaniczne itp.),
- utrata możliwości pracy personelu (choroba, śmierć, strajk itp.).

Do zagrożeń przypadkowych zalicza się wszelkiego typu błędy i awarie. Zagrożenia przypadkowe charakteryzują się losowym rozkładem prawdopodobieństwa wystąpienia. Ryzyko związane z tymi zagrożeniami może być mierzone metodami ilościowymi i określane np. na podstawie. średniej ilości błędów operatora w roku lub średniego czasu pomiędzy awariami.

Zagrożenia rozmyślne dotyczą wyłącznie działań ludzkich. Często w literaturze są one określane jako ataki. Kategoria ta obejmuje zarówno aktywność intruza znajdującego się na zewnątrz, jak i wewnątrz systemu informacyjnego. Cechą charakterystyczną tej kategorii zagrożeń jest intencja wyrządzenia szkody. Do zagrożeń rozmyślnych zalicza się: włamanie, kradzież, przechwycenie, manipulacja, oszustwo, podszycie się (maskarada), uszkodzenie lub zniszczenie.

Każdy istotny element aktywów systemu powinien być analizowany pod kątem zagrożeń, które mogą przyczynić się do jego uszkodzenia lub utraty. Szczególną uwagę należy zwrócić na identyfikację sposobów, jakimi dane zagrożenie może się objawić. Przykładowo, działaniami, które mogą prowadzić do uzyskania nieupoważnionego dostępu, może być podsłuch i odtworzenie (*playback)* zarejestrowanej sesji użytkownika, złamanie hasła, dołączenie nieautoryzowanych elementów do sieci itp.

3. Zarządzanie ryzykiem

Kierownicy jednostek organizacyjnych oraz administratorzy muszą mieć stałą świadomość istnienia zagrożeń. Są sytuacje, w których nawet duże inwestycje i tak będą za małe i nie pozwolą na uniknięcie mało prawdopodobnych zagrożeń. Dlatego osoby funkcyjne muszą znaleźć odpowiedź na takie pytania, jak:

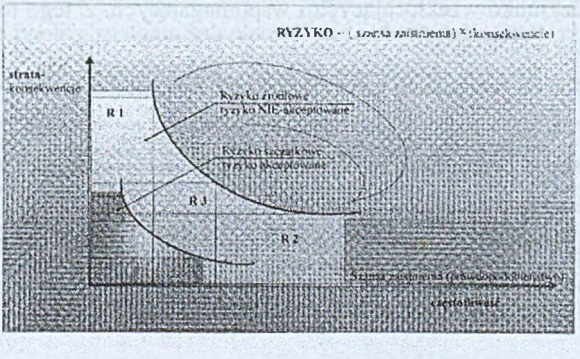
- Co złego może się zdarzyć i z jakim prawdopodobieństwem?
- Jakie będą konsekwencje zagrożenia, i w jaki sposób można je zminimalizować?
- Jak duże ryzyko jest akceptowalne, i w jaki sposób można je zminimalizować?
- Jakie będą koszty wprowadzenia zabezpieczeń?
- Jakie mogą być straty w przypadku wystąpienia zagrożenia oraz czy koszty strat nie będą większe niż koszty zabezpieczeń?

Zasadniczym celem zarządzania ryzykiem jest obniżenie ryzyka, gdyż całkowite jego wyeliminowanie nie jest możliwe. Istnieją różne definicje ryzyka. Polska norma PN-I-13335-1 – "*Wytyczne do zarządzania bezpieczeństwem systemów informatycznych*" definiuje tzw. pojęcie zarządzania ryzykiem (ang. *risk management*). Polega ono na "porównywaniu określonego ryzyka z zyskami i/lub kosztami zabezpieczeń oraz tworzeniu strategii wdrożenia polityki bezpieczeństwa w zakresie systemów informatycznych zgodnej z celami działania danej instytucji". Zgodnie z tą normą "należy rozważyć różne rodzaje zabezpieczeń oraz wykonać analizę kosztów i/lub zysków. Zabezpieczenia są dobierane dla odpowiedniego ryzyka i potencjalnych następstw. Należy także wziąć pod uwagę poziom akceptowalnego ryzyka szczątkowego".

Matematycznie można to określić jako iloczyn szansy zaistnienia danego zagrożenia i konsekwencji, jakie z tego mogą wyniknąć:

$$Ryzyko = (szansa\ zaistnienia) \times konsekwencje \quad (1)$$

Obniżenie ryzyka można uzyskać poprzez zastosowanie środków zabezpieczających, a obniżone w ten sposób ryzyko stanowi ryzyko szczątkowe (ang. *residual risk*). Istotnym problemem jest, do jakiego poziomu należy obniżać ryzyko, aby instytucja była zdolna ponieść koszty zabezpieczeń, a ryzyko szczątkowe było akceptowalne. występujące tutaj współzależności dobitnie obrazuje poniższy rysunek:



Rys. 1. Zależności ryzyka
Fig. 1. Risk Dependencies

Przy rozgraniczaniu ryzyka akceptowalnego od nieakceptowalnego niezbędna jest analiza maksymalnego dopuszczalnego ryzyka - MDR. Dopuszczalne maksymalne ryzyko rozumiane jest jako część środków własnych, jaką dana instytucja gotowa jest ponieść w przypadku "katastrofy", jak również tzw. zyski operacyjne ("cash-flow") czy też gwarancje w formie odszkodowań uzyskane od firm ubezpieczeniowych. Matematycznie można to zapisać:

$$MDR = \alpha \cdot S_w + \beta \cdot Zysk + \gamma \cdot Gwarancje \qquad (2)$$

gdzie:

S_w – część środków własnych,

α – część (procent) przeznaczona na środki własne,

β – część (procent) rocznego zysku operacyjnego brutto,

γ – szacunkowy wskaźnik odszkodowań.

Analiza ryzyka obejmuje cztery podstawowe etapy:

1) określenie wszystkich możliwych i prawdopodobnych niepożądanych skutków działania (bliższych i dalszych) dla każdego alternatywnego wariantu działania;
2) oszacowanie prawdopodobieństwa wystąpienia tych skutków;
3) obliczenie strat, jakie mogą wystąpić;
4) obliczenie strat związanych z możliwymi wariantami działania jako sumy iloczynów strat oszacowanych dla poszczególnych skutków przez prawdopodobieństwa ich wystąpienia.

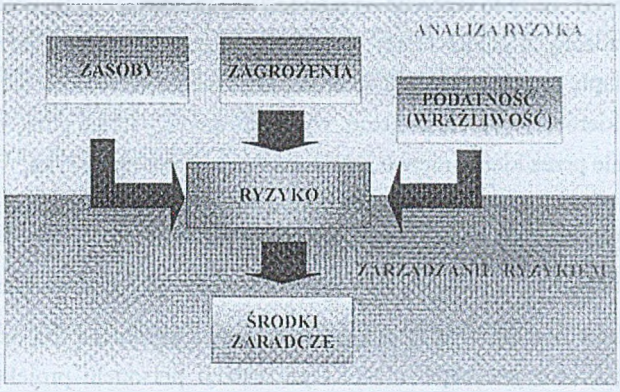
Analiza ryzyka obejmuje procesy identyfikacji, analizy i reagowania na ryzyko w systemie. Związana jest nierozłącznie z podejmowaniem decyzji w sytuacji braku całkowitej pewności, na podstawie zebranych niezbędnych informacji pozwalających na przewidywanie przyszłych skutków. W większości przypadków wiąże się to z obliczeniem prawdopodobieństwa wystąpienia czynników zakłócających i wspomagających. Z tego też powodu podejmowane decyzje można podzielić na:

- podejmowane w warunkach pewności - gdy dysponujemy wszystkimi potrzebnymi informacjami,
- podejmowane w warunkach niepewności - gdy nie dysponujemy informacją o przyszłych stanach systemu i otoczenia,
- podejmowane w warunkach ryzyka - gdy na podstawie posiadanych informacji możemy ocenić prawdopodobieństwo wystąpienia różnych stanów otoczenia oraz systemu.

Ryzyko najczęściej rozumiane jest jako niebezpieczeństwo poniesienia straty, możliwość wystąpienia określonego zagrożenia lub nieosiągnięcia celu. Można je także określić jako taką sytuację, w której nie można przewidzieć przyszłych warunków eksploatacji systemu,

natomiast znany jest rozkład prawdopodobieństwa ich wystąpienia. Ryzyko jest naturalnym zjawiskiem i nie można go wyeliminować. Można je natomiast ograniczać poprzez prowadzenie rozpoznania, kształtowanie, badania, kontrolę realizacji zadań.

4. Analiza ryzyka a zarządzanie ryzykiem



Rys. 2. Analiza ryzyka a zarządzanie ryzykiem
Fig. 2. Risk Analysis and Risk Management

Istnieje kilka definicji analizy ryzyka. Najprościej ujmując, analiza ryzyka ma na celu zidentyfikowanie oraz określenie wielkości ryzyka oraz obszary wymagające ochrony, w tym również działania profilaktyczne. Jest procesem identyfikacji ryzyka bezpieczeństwa, przykładowo zagrożeń słabych punktów systemów lub sieci teleinformatycznych (TI), określania ich ważności i identyfikowania obszarów wymagających ochrony lub środków zapobiegawczych. Ryzyko bezpieczeństwa zdefiniowane jest jako prawdopodobieństwo, z jakim wewnętrzne słabe punkty systemu lub sieci TI mogą być wykorzystane przez zagrożenia dla systemu, prowadząc do narażenia informacji przetwarzanej w systemie, systemów lub sieci TI.

Z analizą ryzyka wiążą się również takie pojęcia, jak szacowanie ryzyka, czy też analiza zagrożeń, która polega na gromadzeniu informacji o wszystkich możliwych zagrożeniach dla aktywów systemu informacyjnego. Ważne jest, aby nie zostało pominięte żadne istotne zagrożenie, bo może to wpłynąć na niewłaściwy dobór mechanizmów zabezpieczeń. Ważnym elementem analizy jest też właściwa klasyfikacja zagrożeń oraz kryterium podziału, które przyjmujemy.

Z analizą ryzyka ściśle wiąże się pojęcie zarządzanie ryzykiem - dotyczy ono identyfikacji, kontrolowania i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia niepewnych zdarzeń, które mogą mieć wpływ na decyzje informacyjne oraz zawierające sku-

teczny program zarządzania, obejmujący ocenę ryzyka, decyzje zarządzające, wdrożenie środków kontroli oraz sprawdzenie (przegląd) skuteczności. Jest to system metod i działań zmierzających do obniżenia stopnia oddziaływania ryzyka na funkcjonowanie systemu i do podejmowania w tym celu optymalnych decyzji. Szczegółowe poznanie charakteru i zakresu potencjalnego ryzyka pozwala na wybór w odpowiednim czasie czynności zapobiegawczych bądź też minimalizujących jego wpływ i skutki.

W procesie zarządzania ryzykiem ważne jest, aby nie zostało pominięte żadne istotne zagrożenie, ponieważ może to wpłynąć na niewłaściwy dobór mechanizmów zabezpieczeń.

Sukces prowadzonych analiz zależy w głównej mierze od udziału zarządu najwyższego szczebla już na etapie projektu systemu teleinformatycznego. W analizie należy uwzględnić:

- wsparcie kierownictwa dla projektu, wyrażone na wszystkich poziomach organizacji;
- wyjaśnienie przez kierownictwo zamiarów i celów analizy ryzyka;
- wybranie przez kierownictwo wykwalifikowanego zespołu oraz formalne przekazanie pełnomocnictwa i odpowiedzialności;
- przegląd i aprobatę wyników pracy zespołu analizy ryzyka przez kierownictwo.

Dobranie składu zespołu analizy ryzyka jest sprawą krytyczną dla osiągnięcia sukcesu projektu. Rzeczą istotną jest zapewnienie reprezentacji personelu projektowego odpowiedzialnego za bezpieczeństwo:

- fizyczne;
- personelu;
- proceduralne;
- obiegu informacji i dokumentów;
- informatyki;
- łączności.

Obszary wymienione powyżej powinny być reprezentowane w zespole analiz ryzyka przez ludzi dobrze poruszających się w obszarze zarówno własnego zadania, jak i jego związkami z ogólnym zadaniem organizacji. Ważne jest, aby kierownik zespołu lub przynajmniej któryś z członków zespołu posiadał doświadczenia w przeprowadzaniu analiz ryzyka.

5. Zautomatyzowane systemy analizy ryzyka

Koszty przeprowadzenia analizy ryzyka są z reguły dosyć wysokie, jednak zautomatyzowana analiza ryzyka z reguły rekompensuje je.

Do szczególnych zalet takiej analizy należą:

- ustalone sposoby wprowadzania danych, a następnie łatwość dostępu i posługiwania się danymi zestawionymi w bazie niezbędnej do prowadzenia analizy;
- możliwość manipulowania danymi w celu zobrazowania wpływu i efektów różnych kombinacji zastosowania środków zabezpieczających i symulacji strat;
- możliwość szybkiego wprowadzania zmian do rozpoznawanego środowiska (aktywa i zasoby) oraz rozpoznanie wielkości ryzyka w organizacji.

Proces wyboru narzędzi może być składową zadania stawianego przy podstawowej analizie potrzeb. Przeprowadzić go można w kilku fazach poprzez:

- zdefiniowanie kryteriów wymagań;
- wybranie zespołu do oceny narzędzi;
- przygotowanie listy ocenianych punktów;
- przedstawienie propozycji oprogramowania wykorzystywanego w analizie ryzyka;
- ocenę i wybór programu.

Automatyczne narzędzie analizy ryzyka powinno zabezpieczyć pracę w następujących trzech obszarach:

- zbierania danych;
- procedur analitycznych;
- generowania (zobrazowania) wyników.

Zbieranie danych ma umożliwić wprowadzenie informacji tekstowych lub graficznych dotyczących wszystkich aspektów analizowanego systemu lub sieci.

Aktywa i zasoby opisane ilościowo, wartościowo lub jakościowo oraz informacje o zagrożeniach, słabych punktach i środkach zaradczych muszą tworzyć korelacyjną bazę danych jako podstawę do dalszej analizy.

Ważne jest, by narzędzie (metodologia) bez względu na to, czy wykorzystuje podejście ilościowe, jakościowe czy mieszane reagowało w sposób interakcyjny na scenariusze zmiany parametrów, np. "co będzie jeżeli...?". Znaczącą rolą narzędzi analizy ryzyka jest opracowywanie wyników. Niezależnie od tego, czy narzędzie posiada opcję typowania środków zaradczych, niezmiernie ważne jest, by program dostarczył wyniki wskazujące miejsca, gdzie należy zastosować te środki, ochraniając zasoby (aktywa) krytyczne.

Od kilku lat w krajach Europy Zachodniej i w USA wyspecjalizowane firmy eksperckie oferują produkty prezentujące najczęściej metodologię i oprogramowanie przydatne do analizy i zarządzania ryzykiem. Produkty te chronione są prawami autorskimi. W niektórych przypadkach oprogramowanie przewidziane dla administracji rządowej objęte jest prawami ochrony tajemnicy państwowej.

Z konieczności więc zostanie przedstawionych tylko kilka wybranych produktów.

5.1. VIR'94 - Holandia

Metodologia VIR'94 - (*Voorschrift Infomatiebeyeiliging Rijksdienst*), łącznie z właściwym oprogramowaniem, zalecana jest przez oficjalne służby ochrony informacji jako dyrektywa działania. Stosować ją można na wszystkich szczeblach zarządzania, od ministerstwa poprzez departamenty, agencje, aż do instytucji czy przedsiębiorstw.

Pakiet składa się z sześciu części:

1) słownictwo i terminologia;
2) przewodnik po zakresie działania i cele;
3) polityka informacyjna i zasady obiegu dokumentacji;
4) środki ochrony informacji;
5) realizacja ITSec;
6) uwagi i zadania końcowe.

Ciekawym rozwiązaniem jest metoda (D&V) podzielenia analizy ryzyka na dwa działy:

D (dependency) – z 5-etapową analizą uzależnienia organizacji od systemów TI;

V (vulnerability) – z 3-etapową analizą podatności.

W dyrektywie wprowadza się oprogramowanie typu CRAMM jako narzędzie automatycznej analizy. Oprogramowanie CRAMM w swoich dwóch pierwszych częściach działania odpowiada metodzie D&V.

5.2. CRAMM – Wielka Brytania

CRAMM - CCTA Risk Analysis and Management Methodology jest pakietem służącym do analizy i zarządzania ryzykiem wyprodukowanym przy współpracy brytyjskich specjalistów rządowych i firmy BIS Applied System Limited.

Podstawą jego działania jest metoda kwalifikacyjna. Pakiet składa się z trzech części opartych w dużej mierze na bibliotece ankiet, kwestionariuszy i zaleceń.

W części pierwszej prowadzona jest według skali 10-punktowej:

1) identyfikacja zasobów (aktywów) i zagrożeń;
2) ocena podatności zasobów na poszczególne rodzaje zagrożeń.

W drugiej części doprowadza się do właściwego szacowania ryzyka powodowanego zagrożeniami. Zgodnie z algorytmem analizy grupuje się odpowiednio zasoby i zagrożenia, których zmaterializowanie mogłoby spowodować utratę ich wartości. Obowiązuje tutaj skala ocen od 1 do 5.

Część trzecia zawiera zbiór rozwiązań, mogących mieć zastosowanie w procesie zarządzania ryzykiem. Pakiet udostępnia dużą liczbę raportów pomagających w implementacji procedur ITSEC, będących podstawą ocen.

Oprogramowanie CRAMM zabezpieczone jest przed nieuprawnionym dostępem oraz przed utratą poufności baz danych, jakie tworzy się w trakcie realizacji zadań.

5.3. MARION - Wielka Brytania

Pakiet służy głównie do analizy ryzyka w organizacjach biznesu. Opiera się na bibliotece aktualnie znanych incydentów. Pakiet zawiera wiele ankiet i kwestionariuszy stosowanych do oceny rozwiązań w zakresie bezpieczeństwa. W analizie ryzyka przyjęto metodę kwalifikacyjno - kwantyfikacyjną.

Oprogramowanie wylicza wyniki analizy dla 27 kategorii zasobów i zagrożeń. Umożliwia także prowadzenie analizy porównawczej wyników oraz utworzenie cenowej bazy danych dla elementów mających wpływ na bezpieczeństwo. Umożliwia to programowe oszacowanie kosztów ponoszonych w związku z poprawą systemu zabezpieczeń.

Prezentacja wyników możliwa jest zarówno w formie numerycznej, jak i graficznej.

5.4. MAGERIT - Hiszpania

Metodologia MAGERIT - Methodology of Risk Analysis and Management of Information Systems of Public Administrations - zalecana jest dla instytucji administracji publicznej. Zajmuje się następującymi 3 dziedzinami:

1. opisem metodologii analizy i zarządzania ryzykiem;
2. przygotowaniem możliwie pełnej informacji i zgrupowaniem jej w bazie danych stanowiącej produkt wyjściowy do właściwej oceny ryzyka;
3. programowaniem narzędziowym wspomagającym implementację metody.

Produkt obejmuje wszystkie fazy przetwarzania, przesyłania i przechowywania informacji w systemach TI.

5.5. MASSIA - Francja

Produkt MASSIA - Methode d'Audit de la Securite des Systemes d'Information de l'Armement - łącznie z oprogramowaniem narzędziowym obejmuje:

- przeprowadzenie badania podatności systemu informatycznego na zagrożenia;
- przeprowadzenie badania procedur operacyjnych, odpowiedzialnych za zapewnienie bezpieczeństwa.

W trakcie badania dokonuje się przeglądu stałej organizacji systemu, podsystemu działań zapobiegawczych, wewnętrznych i zewnętrznych, kontroli itd.

Produkt stosuje przede wszystkim metodę kwantyfikacyjną, prowadzącą do uzyskania pełnych danych dla wypracowania tzw. szczególnych wymagań bezpieczeństwa (SWB). Metoda stosowana jest głównie do prowadzenia procedur kontrolnych ITSEC.

5.6. IST/RAMP - USA

W pakiecie IST/RAMP - International Security Technology / Risk Anałysis Management - zastosowano metodologię kwantyfikacyjną. Wymaga on sprzętu typu "mainframe". Komputery klasy PC stosuje się jedynie do zobrazowania wyników.

W trakcie działania program generuje zestawy potrzebnych ankiet i kwestionariuszy. Po ich uzyskaniu grupowane są one w pięciu kategoriach aktywów i zagrożeń. Pakiet dysponuje dużą biblioteką incydentów i ma możliwość przeprowadzenia analizy porównawczej.

5.7. RISKPAC - USA

Pakiet przygotowany jest do prowadzenia analizy ryzyka w agencjach rządowych. Zastosowano w nim metodę kwalifikacyjno-kwantyfikacyjną.

Zestawy ankiet i kwestionariuszy pogrupowane są w cztery kategorie. Każda z nich tworzy oddzielny zbiór aktywów i zagrożeń, podlegających szczegółowej ocenie. Poziomy ryzyka przedstawiane są i monitorowane dla każdej kategorii oddzielnie. W systemie zawarto osobny moduł korekcji, który na podstawie przeprowadzonej analizy przedstawia zalecenia, których celem jest poprawienie stanu bezpieczeństwa.

6. Podsumowanie

Podsumowując, należy mieć świadomość, że ryzyko można oszacować i zredukować, ale nie da się go wyeliminować całkowicie.

Analiza przewidywanych zagrożeń, prowadzona jako część procesu analizy ryzyka, pozwala przedstawić w sposób kompleksowy przewidywane zagrożenia dla informacji i związane z neutralizacją tych zagrożeń wymagania bezpieczeństwa. Nie daje jednak możliwości opartego na ekonomicznych podstawach wyboru środków ochrony oraz skierowania środków zabezpieczenia przeciw ryzykom przynoszącym największe szkody.

Wbrew powszechnym oczekiwaniom większość potencjalnych zagrożeń pochodzi z niezamierzonych działań z wewnątrz, jest wynikiem braku wiedzy i praktyki lub braku świadomości zagrożeń na poziomie użytkownika lub administratora systemu TI.

Niektóre zagrożenia, takie jak wirusy i włamania przez sieć są bardzo nagłaśniane i są na nie przeznaczane duże środki, podczas gdy to właśnie powtarzalne pomyłki użytkownika

powodują największe straty. Przeprowadzona w sposób profesjonalny analiza ryzyka pomaga dostrzec, że często pożar lub utrata kluczowych osób z personelu są o wiele bardziej prawdopodobne i bardziej brzemienne w skutki niż wirusy i awarie. Właśnie „czynnik ludzki" bywa często najsłabszym ogniwem bezpieczeństwa. Ludzi można przekupić, szantażować, zastraszyć, przekonać do złamania zabezpieczeń systemu za mniejsze pieniądze, niż wynosi koszt zaawansowanych technologicznie urządzeń zabezpieczających.

Korzyścią z zastosowania procesu analizy ryzyka jest wzrost świadomości zagrożeń na wszystkich poziomach jednostki organizacyjnej, od kierownictwa odpowiedzialnego za zarządzanie do użytkowników i personelu pomocniczego. Wzrost świadomości zagrożeń powinien wzmacniać bezpieczeństwo i czynić je bardziej zgodne z potrzebami użytkowników.

Na wyniki analizy ryzyka znaczący wpływ ma wiedza, doświadczenie i zaangażowanie osób ją przeprowadzających. W znacznej mierze wpływają one na jakość, koszt i czas. Jednak niewątpliwą korzyścią przeprowadzonego procesu jest pewność, że zrobiono wszystko, aby przy racjonalnych kosztach zabezpieczyć informację niejawną.

LITERATURA

1. Polska Norma PN-I-13335-1 - "Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych", cz. 1.
2. Wiśniewski A.: Analiza ryzyka. Wytyczne dla administratorów systemów. AZW.
3. Weierbach R.: Vulnerability assessments. INFS 762, 2000.
4. Gallagher B. P.: Software acquisition. Risk management. Key Process Area (KPA) - A guidebook. 1999.

Recenzent: Prof. dr hab. inż. Andrzej Grzywak

Wpłynęło do Redakcji 6 listopada 2001 r.

Abstract

Conducting of current analyses, connected with vulnerability IT systems to threats is the constant element of the Security Policy The Security Policy is inseparably connected with so called Risk Management, encompassing methods and activities towards decreasing influence of risk level on system functionality, which allows to take an optimal decision. Detailed

recognition of character and range of potential risk let choose preventive activities or minimise its impact and result at the right time.

This publication presents classifications of threats, risk management issues, including it four stages:

- determining of all possible and probably undesirable results of activity for everyone variant of activity,
- likelihood assessment of result appearance,
- calculation of loses, which may appear,
- calculation of loses for variants of activity.

Costs of Risk Analysis, as a rule, are usually high, so the major part of presented publication was dedicated to automatic systems, which can compensate them. Automatic assessment tools may provide secure works for following three areas of activity:

- data collecting,
- analytic procedures,
- generation of results.

As a conclusion of these considerations, we should remember that the risk may be assessed and reduced, but it is not possible to eliminate it completely. Most of threats have their origin from unintentional external activities, result from lack of knowledge and experience or lack of threats consciousness both on the user or CIS administrator level.