# Szkic rozwiązania oceny ryzyka

Zasadniczo oprogramowanie powinno składać się z trzech modułów:

* identyfikacji aktywów,
* identyfikacji wektora ataku,
* obliczeń ryzyka.

**Moduł identyfikacji aktywów**

Źródłem danych dla identyfikacji aktywów powinny być definicje uzyskane z regulacji prawnych dotyczących przyrządów pomiarowych. Definicje te mogą być zarejestrowane przez program i dostępne w trakcie uzgadniania aktywów. Cenne może być rejestrowanie związków pomiędzy aktywami z określonym zapisem regulacji prawnej. Każda pozycja aktywa powinna mieć zdefiniowany co najmniej jeden model ataku, co oznacza, że może występować związek (realizowany programowo i pokazywany użytkownikowi) pomiędzy aktywem i jakimś modelem ataku. Tutaj też można kontrolować spójność modelowania aktywa z występującymi agresorami. Ze względu na różny poziom praw dostępu użytkowników może mieć sens podział i identyfikowanie użytkowników o różnych prawach. Kolejnym działaniem może być gromadzenie możliwych szkód, które związane są z aktywem. Innym słowy każdy modelowany agresor może uszkodzić jakieś zidentyfikowane aktywa poprzez unieważnienie jednej lub większej liczby ich własności ochrony dotyczących, przykładowo dostępności, integralności, autentyczności. Wiąże się to także z koniecznością zdefiniowania zbioru własności ochrony i przypisania każdemu aktywu elementów tego zbioru.

Regulacja 1

Regulacja …

Aktywa 1

Szkoda 1

Własność ochrony 1

Szkoda 2

Własność ochrony …

Aktywa 2

Szkoda n

…

Aktywa n

Własność ochrony n

Czas 1,

Rzeczoznawstwo 1,

Wiedza o TOE 1,

Okno możliwości 1,

Wyposażenie 1

Model ataku 1

Ryzyko 1

Model ataku …

Ryzyko …

Model ataku n

Ryzyko n

…

n

**Interfejs:**

o Regulacja (RE) o RE 1 Treść (pole testowe)

o Aktywa (AK) o RE 2

o Wł. Ochrony (WO) o RE… *Wpływ*

o Wykonawca (WY) o RE N Akceptacja

o Szkoda (SZ)

o Atak (AT)

o Regulacja – Aktywa (RE-AK) x AK1

o Regulacja – Szkoda (RE-SZ) x AK2

o Regulacja – Wł. Ochrony (RE-WO) x AK…

o Regulacja – Atak (RE-AT) x AK N

o Atak – Aktywa (AT-AK)

o Atak – Wykonawca (AT-WY)

o Atak – Szkoda (AT-SZ)

v Atak – Ryzyko (AT-RY)

x Ryzyko o AT1 Czas |\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_|

o AT2 Rzeczoznawstwo |\_\_\_\_\_\_|

o AT … Wiedza |\_\_\_\_\_\_\_\_\_\_\_\_\_|

o AT N Możliwości |\_\_\_\_\_\_\_\_\_\_|

Wyposażenie |\_\_\_\_\_\_\_\_|

Ryzyko |\_\_\_\_\_\_\_\_|

**Moduł identyfikacji wektora ataku**

Realizowany na podstawie dokumentacji gromadzi możliwe wektory ataku skojarzone z wcześniej określonymi zagrożeniami.

**Moduł obliczeń ryzyka**

Przypisuje danemu wektorowi ataku wartości źródeł potrzebnych dla jego realizacji w każdym z pięciu obszarów TOE. Następnie sumowane są zgromadzone punkty, które stanowią tzw. „Opór TOE”, który może też być wyrażony słownie. Im opór TOE jest mniejszy tym prawdopodobieństwo wystąpienia ataku (Pr) jest większe. Suma punktów występuje w zakresie od 0 do 57, a odpowiednio prawdopodobieństwo (Pr) w zakresie <5, 1>. Do obliczeń potrzebne są jeszcze tzw. punkty wpływu (Pw) danego zagrożenia występujące w skali od 1 do 5. Jeśli zagrożenie wynika z regulacji prawnej to punkty wpływu przyjmują największą wartość 5, a najniższa wartość wpływu 1 występuje, gdy atak odnosi się do pojedynczego pomiaru i może być wykryty przez nadzór metrologiczny. Ryzyko (R) oblicza się z formuły: R = Pw \* Pr / 5.

**Interfejs użytkownika**

Program oceny ryzyka dla przyrządu pomiarowego (Risk Assessment of a Measuring Instrument) Rami szacuje ryzyko celowego lub przypadkowego zafałszowania pomiaru. Wszelkie rejestry związane z danymi wejściowymi dla obliczeń i wynikami ryzyka dla określonego przyrządu pomiarowego znajdują się w jednym pliku XML o stałej co do liczby i rodzaju elementów tego pliku. Interfejs w szczególności zawiera:

Pola opcji Riadobuttony odpowiadające za wybór zakresu edycji jakiegoś aspektu metody. Przykładowo słownikowa struktura Regulacje zawiera założoną liczbę przepisów prawnych, które mają identyfikator, treść i parametr „wpływ”. Zakłada się, że określony przepis występuje w grupie nie większej niż countRE i ma znaczenie, jeśli jego zapis nie jest pusty – zapisy puste są pomijane w analizie. Usunięcie treści zapisu jest równoznaczne z wyłączeniem regulacji w obliczeniach. Edycja regulacji polega na wybraniu radiobuttona i wprowadzeniu treści, uzgodnieniu wartości wpływu i zaakceptowaniu zmian. Powyższy schemat definiowania innych danych słownikowych jak: Aktywa, Wykonawcy, Szkody itd. Relacje wiążą dane słownikowe i pokazane są w drugiej grupie formantów „Relacje”. Definicja relacji wymaga wyboru pierwszego elementu – radiobutton i wyborów checkbox’ów oznaczających relacje 1 do N. Wybór radiobuttona wywołuje opis pierwszego obiektu relacji w grupie definicji. CheckBox’y pozwalają na określenie relacji.

- opis przyrządu - TextBox,

- regulacje prawne w liczbie N - TextBox,

- wpływ regulacji prawnych w liczbie N – TrackBar w zakresie <1, 5>,

- aktywa w liczbie N,

- własność ochrony w liczbie N – Radio Button – ustalone elementy wyboru,

- szkody w liczbie N – TextBox,

- model ataku w liczbie N – TextBox,

- N grup po N etykiet o ustalonych nazwach,

- N grup po N TrackBar w określonych zakresach wartości dla każdej pozycji,

- ryzyko – TrackBar – nie podlega edycji.