GUM (Biuro Informatyki)
D.Luśtyk

Warszawa 31 grudnia 2015

Instrukcja Rami

wersja 1.00

Wprowadzenie

Współczesne standardy konstrukcji przyrządów pomiarowych obejmują systemy zintegrowane z sieciami otwartymi, działającymi w obszarach Internetu czy chmury obliczeniowej. Rozwiązania techniczne tych przyrządów sprawiają, że ich oprogramowanie może być narażone na niekorzystny wpływ otoczenia, w którym funkcjonują, w szczególności informatycznego. Według oszacowań, **przyrządy pomiarowe uczestniczą w od 4 do 6-ciu procent wartości wszystkich transakcji w krajach Unii Europejskiej**. Między innymi dlatego, przyrządy te przed pojawieniem się na rynku UE podlegają prawnej kontroli. Istotnego znaczenia nabiera zatem zagadnienie zgodności ocen ryzyka użytkowania przyrządów pomiarowych w ramach wspólnego rynku UE, co wiąże się z potrzebą oparcia metod jej oceny na obowiązujących normach międzynarodowych jak **ISO /IEC 27005 i 15408**.

Przesłanką do powstania prac obejmujących metody oceny zagrożenia w przyrządach pomiarowych jest **Dyrektywa Unijna (MID) 2014/32/EU**. Metoda tutaj zaproponowana zawiera elementy wywodzące się z międzynarodowego standardu bezpieczeństwa oprogramowania odwołującego się do oceny ryzyka **ISO / IEC 15408** znanej również jako **Common Criteria**.

Niniejsze opracowanie obejmuje streszczenie metody zaimplementowanej w programie, który może być wykorzystany przez jednostki notyfikujące lub nadzoru rynku. W dalszej części opis koncentruje się na parametryzacji czynników **ryzyka** i funkcji jego obliczeń oraz na zagadnieniu budowania spójnego modelu danych. Następnie poruszane są kwestie obsługi programu w realizacji opisanego modelu oceny **ryzyka**, a na końcu dołączony jest przykład obliczeń **ryzyka**.

Streszczenie metody

Ryzyko trudno poddaje się analizie formalnej. Zasadniczy kłopot polega na opracowaniu sposobu przetwarzania, selekcji i szacowaniu wpływu czynników warunkujących **ryzyko**. Zaproponowana metoda opiera się na sześciu zbiorach komponentów: **regulacjach**, **aktywach**, **zagrożeniach**, **atakach, wykonawcach, czynnikach ryzyka**. Komponenty te są punktem wyjścia do formalnego ujęcia zagadnienia szacowania **ryzyka**.

Regulacje w proponowanym modelu są to przepisy, normy, wymagania, które wyrażają oczekiwania co do spełnienia przez przyrząd pomiarowy pewnych właściwości. Najwyższą rangę **regulacji** mają przepisy prawa.

Aktywom w przyrządzie pomiarowym przypisuje się atrybut wartości podlegającej ochronie. Każdy przyrząd pomiarowy ma **aktywa** wynikające z przeznaczenia, budowy i funkcjonalności. W przypadku przyrządu, który wykorzystuje program do realizacji pomiaru, przykładem **aktywa** może być „niedopuszczalny wpływ na oprogramowanie". Określony przyrząd, na ogół zawiera kilka **aktywów**. Źródłem identyfikacji **aktywów** są **regulacje** prawne i wszelkiego rodzaju przepisy. Przykładem może być wymaganie **MID [1] Aneks I 7.6** „Jeżeli przyrząd pomiarowy wyposażony jest w oprogramowanie realizujące inne funkcje, niż pomiarowe, oprogramowanie, które jest istotne dla charakterystyk metrologicznych, powinno być identyfikowalne i powinno być odporne na niedozwolony wpływ oprogramowania powiązanego." Przytoczony przepis odwołuje się do **aktywów** A1 „identyfikacja oprogramowania" i A2 „niedopuszczalny wpływ na oprogramowanie". Identyfikacja **aktywów** związana jest z ustaleniem **własności ochrony aktywa**, przykładowo: **dostępność**, **integralność**,

niedostępność, **autentyczność**. Ustalenie związku: **aktywa – własność ochrony** kwalifikuje określone **aktywa** do zbioru danych uczestniczących w modelu obliczeń **ryzyka**. W powyższym przykładzie **aktywa** posiadają następujące **własności ochrony**: A1: **dostępność**, **integralność**, A2: **niedostępność**.

Zagrożenie - niechciane zdarzenie, które w negatywny sposób wpływa na **aktywa**. **Zagrożenia** są funkcją celów, którymi w tym kontekście są **aktywa** w powiązaniu z niekorzystnym na nie oddziaływaniem.

Atak jest to celowe działanie **agresora** wykorzystującego swój potencjał do negatywnego wpływu na **aktywa**. Oznacza to, że istnieje związek **ataku** z naruszeniem **własności ochrony aktywa**. Potencjalne **ataki** należy formułować z uwzględnieniem specyfiki konstrukcyjnej przyrządu pomiarowego, co wymaga wnikliwej analizy jego dokumentacji oraz wiedzy na temat technicznych możliwości przeprowadzenia niepożądanej ingerencji. Wyprowadzenie **ataków** jest najmniej sformalizowaną procedurą gromadzenia danych do modelu obliczeń **ryzyka**. Przykładem **ataku** może być: „Agresor podrabia klucz autoryzacji na USB mając w ten sposób dostęp do systemu operacyjnego”.

Ryzyko jest funkcją **wpływu** (rangi) przepisu, z którego wyprowadzane są **aktywa**, sposobu realizacji **ataku** i potencjału **agresora**. Potencjał **agresora** uwzględnia w modelu następujące czynniki:

- ✓ **Czas** – potrzebny do realizacji **ataku**,
- ✓ **Kwalifikacje** – merytoryczne **agresora** w dziedzinach wiedzy wymaganej do realizacji **ataku**,
- ✓ **Wiedza** – jaką dysponuje **agresor** na temat przyrządu pomiarowego,
- ✓ **Wyposażenie** – środki techniczne konieczne do realizacji **ataku**,
- ✓ **Dostęp** – wskaźnik osiągalności przyrządu przez **agresora**.

Powyższe parametry oraz **wpływ** są bezpośrednimi argumentami funkcji szacowania **ryzyka,** przyjmują wartości naturalne w ustalonym zakresie zmienności i mogą być wyrażone słowami.

Model danych

Model danych obejmuje zbiór **regulacji**, które warunkują identyfikację **aktywów**. **Aktywa** mogą się powtarzać jeśli uwzględniane w modelu przepisy odwołują się do tych samych **aktywów**. Istotnym tutaj jest identyfikacja **aktywów** dla każdej **regulacji** uczestniczącej w modelu. Na tym etapie można przeprowadzić wstępną selekcję przepisów prawnych ze względu na ich powiązanie z istotnymi dla kontekstu szacowania **ryzyka, własnościami ochrony**. W odniesieniu do przyrządów pomiarowych nie można odwoływać się bezpośrednio do takich wartości jak zdrowie ludzkie, czy wartość materialna (choć mogłyby one być zagrożone w przypadku zafałszowania pomiaru) – można jedynie odnieść się do wartości wyrażonych **własnościami ochrony**. Przykładowo w przyrządach, które swoje działanie opierają na oprogramowaniu, można mówić o **niedostępności** oprogramowania przez urządzenie współpracujące z przyrządem pomiarowym lub **dostępności** identyfikacji pomiaru. Inne możliwe **własności ochrony** to **integralność** wartości pomiaru lub **autentyczność** oprogramowania. Istnieje związek między **aktywem,** a **własnością ochrony**, który ułatwia identyfikację **aktywów** przy ograniczanym zbiorze elementów **własności ochrony** – w przypadku przyrządów zawierających oprogramowanie, cztery **własności ochrony** wyczerpują wszystkie przypadki.

Kolejnym aspektem modelu są **zagrożenia** rozumiane jako sytuacje, które potencjalnie stwarzają warunki przeprowadzenia **ataku**. Przykładowe **zagrożenie**: „Lokalny administrator sprawdza integralność lub autentyczność oprogramowania metrologicznego” zawiera odwołanie do **aktywa**

jakim jest oprogramowanie metrologiczne poprzez związek z dwoma **własnościami ochrony**: **integralność** lub **autentyczność** oraz określa **wykonawcę ataku** - lokalnego administratora. Można powiedzieć, że warunkiem wystąpienia **zagrożenia** są składowe: **aktywa**, **własności ochrony** i **wykonawcy**. **Zagrożenie** warunkuje **atak**, który realizuje **wykonawca**, zainteresowany naruszeniem **własności ochrony** przypisanej do jakiegoś **aktywa**.

W modelu, **atak** jest realizacją **zagrożenia** i mógłby przykładowo brzmieć: „Atakujący podrabia klucz autoryzacji na USB mając w ten sposób dostęp do systemu operacyjnego". Z powyższego zapisu można wyprowadzić **zagrożenie**: Lokalny administrator sprawdza **integralność** lub **autentyczność** oprogramowania metrologicznego. Spójność modelu danych w tym kontekście wyraża zasada: nie istnieje **atak**, który może być uwzględniany w modelu, jeśli nie realizuje co najmniej jednego **zagrożenia**.

Relacyjny model danych szacowania **ryzyka** można przedstawić jako:

- ✓ **regulacja** ma 1 lub więcej **aktywów**,
- ✓ **aktywa** ma 1 lub więcej **własności ochrony**,
- ✓ **atak** ma 1 lub więcej **aktywów**,
- ✓ **atak** ma 1 lub więcej **zagrożeń**,
- ✓ **atak** ma 1 lub więcej **wykonawców**,
- ✓ **atak** niesie jedno **ryzyko**.

Parametryzacja czynników ryzyka

Model obliczeń uwzględnia kilka czynników **ryzyka**. Pierwszym jest **czas** określany w zakresie **od 1 dnia do powyżej 6 miesięcy**. Odpowiada to wartości parametru w zakresie **0…19**. Im wyższa wartość, tym wymagany jest większy **czas** potrzebny na realizację **agresji**. Podobna zasada, obowiązuje dla pozostałych składowych potencjału **agresora** uwzględnianych w modelu **ataku**. Można powiedzieć, że wartości te są swoistego rodzaju „oporem" jaki stawia przyrząd potencjalnemu **agresorowi**.

Kwalifikacje, obejmują zakres, słownie wyrażany **od laika (wartość 0)** do osoby będącej **ekspertem kilku dziedzin (wartość 8)**.

Kolejnym czynnikiem jest **wiedza** na temat przyrządu, gdzie najniższa wartość to **0 dla wiedzy publicznie dostępnej** (np. w Internecie) i **najwyższa wartość 11** dla tzw. **wiedzy krytycznej**, dostępnej dla przedstawicieli zespołów produkcyjnych lub projektowych przyrządu pomiarowego.

Wyposażenie w dyspozycji **agresora** to następny parametr. Wyróżnia się tutaj najniższą **wartość 0 – wyposażenie standardowe i najwyższą 9 dla specjalistycznego wyposażenia wykonywanego na kilkakrotne zamówienie**.

Ostaniem czynnikiem jest **dostęp,** przyjmujący wartości **od 0 do 10**, gdzie granice zmienności stanowią odpowiednio dostęp **nieograniczony** i **trudny**.

Funkcja **ryzyka** uwzględnia, o czym wcześniej wspomniano, **wpływ** regulacji, z której wyprowadzono **aktywa,** w zakresie wartości **od 1 do 5**.

Funkcja ryzyka

Ryzyko jest prostą funkcją czynników**,** skonstruowaną w taki sposób, że jego wartość zawierają się w zakresie w **od 1 do 5. Ryzyko r** oblicza się z formuły: **r = w * p / 5**, gdzie:

w – wartość **wpływu regulacji** w zakresie **od 1 do 5**. Jeśli regulacja wynika z przepisu prawa, **wpływ** przyjmuje największą wartość **5**, a najmniejszą **1**, gdy **atak** odnosi się do pojedynczego pomiaru i może być wykryty przez nadzór metrologiczny.

p – prawdopodobieństwo **ataku** uzyskane jest z mapowania sumy wartości czynników **ryzyka** w zakresie **od 0 do 57** na wartość **prawdopodobieństwa w zakresie 1 – 5**.

O ile funkcja nie jest trudna w obliczeniach, to pewne problemy użycia metody wynikać mogą z szacowania wartości czynników wpływających na **ryzyko**. Wymaga to dogłębnej znajomości badanego przyrządu, jak również szerszej wiedzy na temat technologii produkcji, zastosowanych rozwiązań technicznych, dostępnych narzędzi umożliwiających ingerencję w strukturę techniczką oraz informacyjną (związaną z oprogramowaniem) przyrządów.

Rozwiązanie informatyczne

Zaproponowany sposób szacowania **ryzyka** może znaleźć swoją implementację w programie, który w założeniach powinien wspierać ekspertów problematyki w ocenie **zagrożenia** naruszenia autentyczności pomiaru przyrządu. Głównym celem utworzenia tego programu jest zbudowanie narzędzia, które w systematyczny i sformalizowany sposób wspiera analityków w wypracowaniu wiarygodnych i powtarzalnych wskaźników bezpieczeństwa pomiarów wszelkich przyrządów. Należy mieć na uwadze, że o ile przyrządy pomiarowe opierające swoje działanie na oprogramowaniu i wymagają większego wsparcia informatycznego (ze względu na potencjalnie większą liczbę składowych modelu), to opracowany program może znaleźć zastosowanie również w analizie ryzyka zafałszowania pomiaru innych przyrządów. **Rami** (The **R**isk **A**ssessment of **M**easurement **I**nstrument) oferuje:

- ✓ odwołanie się do wiarygodnego formalizmu szacowania **ryzyka**,
- ✓ weryfikację poprawności i spójności danych,
- ✓ powtarzalność wyników analizy,
- ✓ przyjazny interfejs,
- ✓ graficzną i wspartą opisem interpretację parametrów wejściowych oraz wyniku obliczeń,
- ✓ zapis danych i wyników obliczeń w pliku XML.

Rami umożliwia szybką analizę ryzyka podczas zmian parametrów wejściowych, przeprowadzaną w celu uzgodnienia modelu docelowego. Mowa tutaj o swoistej interakcji między ekspertem, a programem – obliczone **ryzyko** może wpłynąć na korektę parametrów zadawanych przez eksperta w celu uzyskania lepszego szacowania. Oczywiście taka interakcja uwarunkowana jest wiedzą i doświadczeniem w badaniu przyrządów pomiarowych oraz znajomością użytej w programie metody szacowania ryzyka - szczegóły można znaleźć w pozycjach [1] i [2] literatury.

Program nie ogranicza złożoności modelu do liczby jego komponentów. W podstawowym zastosowaniu, analiza opierać się może na maksymalnie dziesięciu pozycjach każdej grupy komponentów: **regulacjach prawnych**, **aktywach**, **własnościach ochrony**, **zagrożeniach**, **atakach**, **wykonawcach**, **ryzykach**, które związane są z jednym dokumentem XML przechowującym dane i

wyniki obliczeń. Bardziej złożone zagadnienia mogą być podzielone na odrębne pliki rejestrujące dane badanego przyrządu.

Interfejs użytkownika

Rami oferuje interfejs, który w menu między innymi zawiera grupę klawiszy służących do zarządzania rejestrami danych i kontrolą ich spójności. Obszar interfejsu związany z wypełnianiem danych wejściowych i obliczenia ryzyka obejmuje trzy główne zakładki:

- ✓ **Przyrząd** – zawiera nazwę i opis, gdzie wprowadzane są istotne charakterystyki urządzenia pomiarowego.
- ✓ **Słowniki** – grupa zakładek obejmujących: **regulacje prawne**, **aktywa**, **własności ochrony**, **zagrożenia**, **ataki** i ich **wykonawców**.
- ✓ **Relacje** – wspierające budowanie spójnego modelu danych w wyniku uzgadniania powiązań z jego komponentami. Znajdują się tu związki: **regulacja – aktywa**, **aktywa – własności ochrony**, **atak – aktywa**, **atak – zagrożenie**, **atak – wykonawca** i **atak – ryzyko**.

Dane

Dane wprowadza się w zakładce **Słowniki**, zawierającej **regulacje i aktywa**, **własności ochrony**, **zagrożenia**, **ataki**, **wykonawców**.

Zakładka **Regulacje / Aktywa** prezentuje cztery grupy formantów przy czym każda grupa zawiera po dziesięć pozycji: pól tekstowych do wpisywania treści **regulacji** prawnych, oznaczeń **regulacji** R1,…,R10, wskaźniki **wpływu,** oraz pola tekstowe **aktywów**, oznaczonych A1,…,A10. **Regulacja** prawna i **aktywa** uczestniczą w modelu jeśli są niepustym zbiorem znaków. Każda **regulacja** ma powiązany ze sobą **wpływ,** wyrażający wagę w skali **od 1 do 5** przepisu – wartość **5** odnosi się do przepisu prawa, a **1** dla norm i ustaleń najniższej rangi lub gdy **atak** dotyczy jednego pomiaru i może być wykryty przez nadzór metrologiczny.

Własności ochrony oznaczone odpowiednio O1,…,O10, **zagrożenia** od Z1 do Z10, **ataki** M1,…,M10 i **wykonawcy** W1,…,W10 to dane tekstowe, które wprowadzane są w odpowiednich zakładkach. Z formalnego punktu widzenia, każda z tych grup danych powinna być wypełniona dla co najmniej jednej pozycji przy czym nie spełnienie tego wymogu i użycie funkcji **Sprawdź,** skutkuje komunikatem błędu o braku jakiegoś komponentu. Funkcja kontroluje ponadto przypisanie:

- ✓ **aktywów** do **regulacji** prawnych,
- ✓ **aktywów** do **własności ochrony**,
- ✓ **ataków** do **aktywów**,
- ✓ **ataków** do **zagrożeń**,
- ✓ **ataków** do **wykonawców**.

Relacje

Poprawność związków pomiędzy komponentami stanowi o zgodności modelu danych z formalizmem metody z jednej strony, z drugiej jest pośrednim wskaźnikiem braku nadmiarowości ustalonych komponentów. Ten etap pracy wpływać może na redefinicję znaczenia i liczebności komponentów przy wsparciu mechanizmu kontroli spójności danych - **Sprawdź**. Użycie tej funkcji skutkować może komunikatem błędu zawierającym typ i pozycję składowej wprowadzającej niespójność. Jeśli dane i wzajemne relacje są poprawne, kontrola spójności kończy się komunikatem: **Dane są spójne**.

Sprawdzenie to, w przypadku wystąpienia błędu, nie niesie sobą żadnych konsekwencji, jest tylko wskazówką, że model danych wymaga korekty przed określeniem parametrów warunkujących **ryzyko**.

W zakładce **Atak-Ryzyko** można wybrać każdy z wcześniej zdefiniowanych **ataków** i w interakcji z **Rami** uzgodnić czynniki wpływające na **ryzyko**. Interfejs udostępnia pięć suwaków, z których każdy pozwala na zmianę wartości czynników: **czas**, **kwalifikacje**, **wiedza**, **wyposażenie**, **dostęp**. Suwaki te umożliwiają wprowadzenie wartości w dopuszczalnym dla danego parametru zakresie zmienności. Wartość parametru wyrażona jest dodatkowo opisem słownym aktualizowanym podczas wywoływania zmiany wartości tego parametru. Wpływ zmiany wartości każdego czynnika, natychmiast jest widoczny na suwaku **Ryzyko** z podaniem jego wartości. Wskazanie suwaka **Ryzyko** nie może być zmienione bezpośrednio – zależy od pozycji suwaków określających wartości czynników **ryzyka**.

Rejestr danych i wyników

Rami zapisuje dane i wyniki obliczeń w plikach XML o strukturze uwzględniającej dopuszczalną maksymalnej liczbę składowych w jednym dokumencie. Program kontroluje wprowadzone zmiany i w przypadku ich wykrycia komunikuje o możliwości zapisu w momencie zamykania dokumentu lub aplikacji.

W przypadku złożonego zagadnienia, rejestr danych może być podzielony na odrębne pliki XML.

Dane i wyniki obliczeń w dokumencie XML można zidentyfikować po nazwach węzłów odwołujących się do słów kluczowych, których znaczenie jest kilkakrotnie przywoływane w niniejszym dokumencie – nie wymagają więc wyjaśnień. Struktura danych w pliku jest następująca:

```
<?xml version="1.0" encoding="utf-8"?>
<Rami>
 <nazwa>Pompa paliwowa</nazwa>
 <opis>Urządzenie komunikuje się z otoczeniem ...</opis>
 <regulacja1>Jeżeli przyrząd pomiarowy wyposażony jest w oprogramowanie ….</regulacja1>
 <wplyw1>5</wplyw1>
…
<regulacja10>Jeżeli przyrząd pomiarowy wyposażony jest w oprogramowanie ….</regulacja10>
 <wplyw10>5</wplyw10>
<aktywa1>Identyfikacja software’u R1, R3.</aktywa1>
…
 <aktywa10>
<wlasnosc1>dostępność</wlasnosc1>
…
<wlasnosc4>niedostępność</wlasnosc4>
<zagrozenie1>Lokalny administrator (W1) sprawdza integralność lub autentyczność oprogramowania metrologicznego.</ zagrozenie 1>
```

…

<zagrozenie10>Lokalny administrator (W1) sprawdza integralność parametrów metrologicznych.</ zagrozenie10>

<atak1>Atakujący podrabia klucz autoryzacji na USB mając w ten sposób dostęp do systemu operacyjnego.</atak1>

…

<atak10>...</atak10>

<wykonawca1>Administrator (W1)</wykonawca1>

…

<wykonawca10/>

<regulacja1_aktywa1>True</regulacja1_aktywa1>

<regulacja1_aktywa2>True</regulacja1_aktywa2>

…

<regulacja1_aktywa10>True</regulacja1_aktywa10>

…

<aktywa1_wlasnosc1>True</aktywa1_wlasnosc1>

…

<aktywa1_wlasnosc10>True</aktywa1_wlasnosc10>

…

<atak1_aktywa1>False</atak1_aktywa1>

…

<atak1_aktywa10>False</atak1_aktywa10>

<atak1_wykonawca1>True</atak1_wykonawca1>

…

<atak1_wykonawca10>False</atak1_wykonawca10>

…

<czas1>19</czas1>

<kwalifikacje1>8</kwalifikacje1>

<wiedza1>11</wiedza1>

<wyposazenie1>9</wyposazenie1>

<dostep1>0</dostep1>

<ryzyko1>1</ryzyko1>

…

Środowisko pracy

Rami może być uruchomiony na komputerze PC pod kontrolą systemu **Windows XP** lub nowszym. Aktualna wersja 1.00 programu skompilowana jest w środowisku **Microsoft Visual Studio 2010**. Program instalacyjny uzupełnia system (w przypadku braku) w komponenty **Microsoft .NET Framework wersja 4.0**.

Instalacja

Program instalowany jest z płyty CD i wymaga przeprowadzenia standardowych czynności dotyczących miejsca instalacji, wersji dla jednego / wielu użytkowników. W przypadku potrzeby instalacji komponentów **Microsoft .NET Framework wersja 4.0**, program realizuje to automatycznie przed właściwą instalacją **Rami**.

Scenariusz analizy ryzyka

Analiza rozpoczyna się od założenia nowego dokumentu - funkcja **Nowy**. W zakładce **Przyrząd** wprowadzane są podstawowe dane: nazwa i opis w kontekście szacowania ryzyka. Następnie w zakładce **Słowniki** wypełnia się pola **regulacji** i **aktywów** w zakładce **Regulacje / Aktywa**, treści dotyczące **własności ochrony** (zakładka **Wł. Ochrony**), **zagrożenia**, **ataków** i **wykonawców** w pozostałych zakładkach. Kolejnym etapem to ustalenie relacji na danych, w zakładce **Relacje**, które odnoszą się do:

- ✓ **regulacji** z **aktywami**,
- ✓ **aktywów** z **własnościami ochrony**,
- ✓ **ataków** z **aktywami**,
- ✓ **ataków** z **zagrożeniami**,
- ✓ **ataków** z **wykonawcami**,
- ✓ **ataków** z **ryzykami**.

Wszystkie wymienione wyżej relacje, z wyjątkiem ostatniej, są defilowane na listach, zgodnie z prezentowanymi treściami. Przykładowo, relacja **Regulacja – Aktywa** dla przepisu o brzmieniu: „Jeżeli przyrząd pomiarowy wyposażony jest w oprogramowanie realizujące inne funkcje, niż pomiarowe, oprogramowanie, które jest istotne dla charakterystyk metrologicznych, powinno być identyfikowane i powinno być odporne na niedozwolony wpływ oprogramowania powiązanego.” ma trzy **aktywa**:

- ✓ Identyfikacja software’u,
- ✓ Niedopuszczalny wpływ na oprogramowanie,
- ✓ Istotne parametry metrologiczne.

Uzgodnienie ww. relacji może zakończyć sprawdzenie spójności danych (funkcja **Sprawdź**) i ewentualna korekta danych jeśli **Rami** wykrył jakieś błędy.

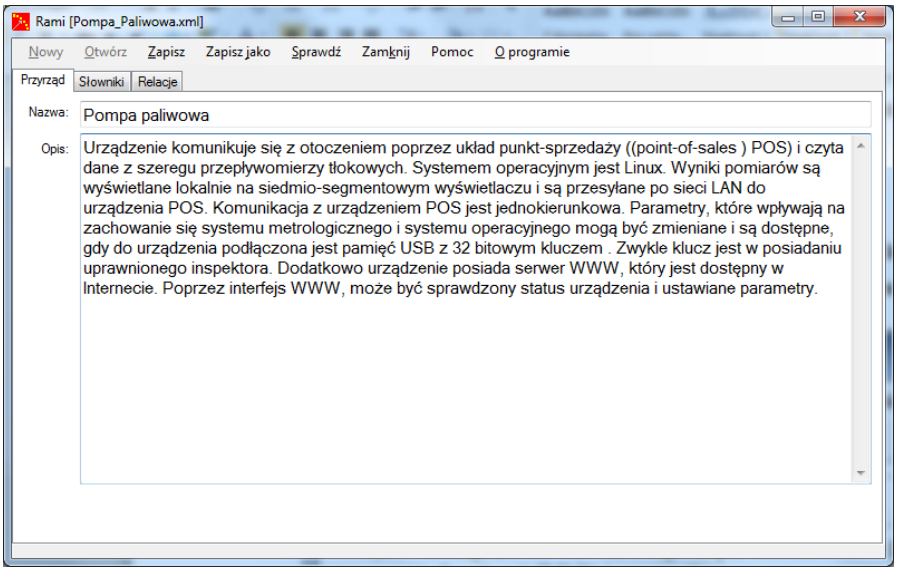
Relacja **Atak – ryzyko** wymaga określenia wartości czynników **ryzyka** na odpowiednich suwakach. Użytkownik podczas tych czynności informowany jest o znaczeniu wybranej przez siebie wartości parametru wraz z podaniem wyniku obliczeń **ryzyka**.

Wprowadzone dane mogą być zapisane w pliku XML funkcjami **Zapisz** lub **Zapisz jako**.

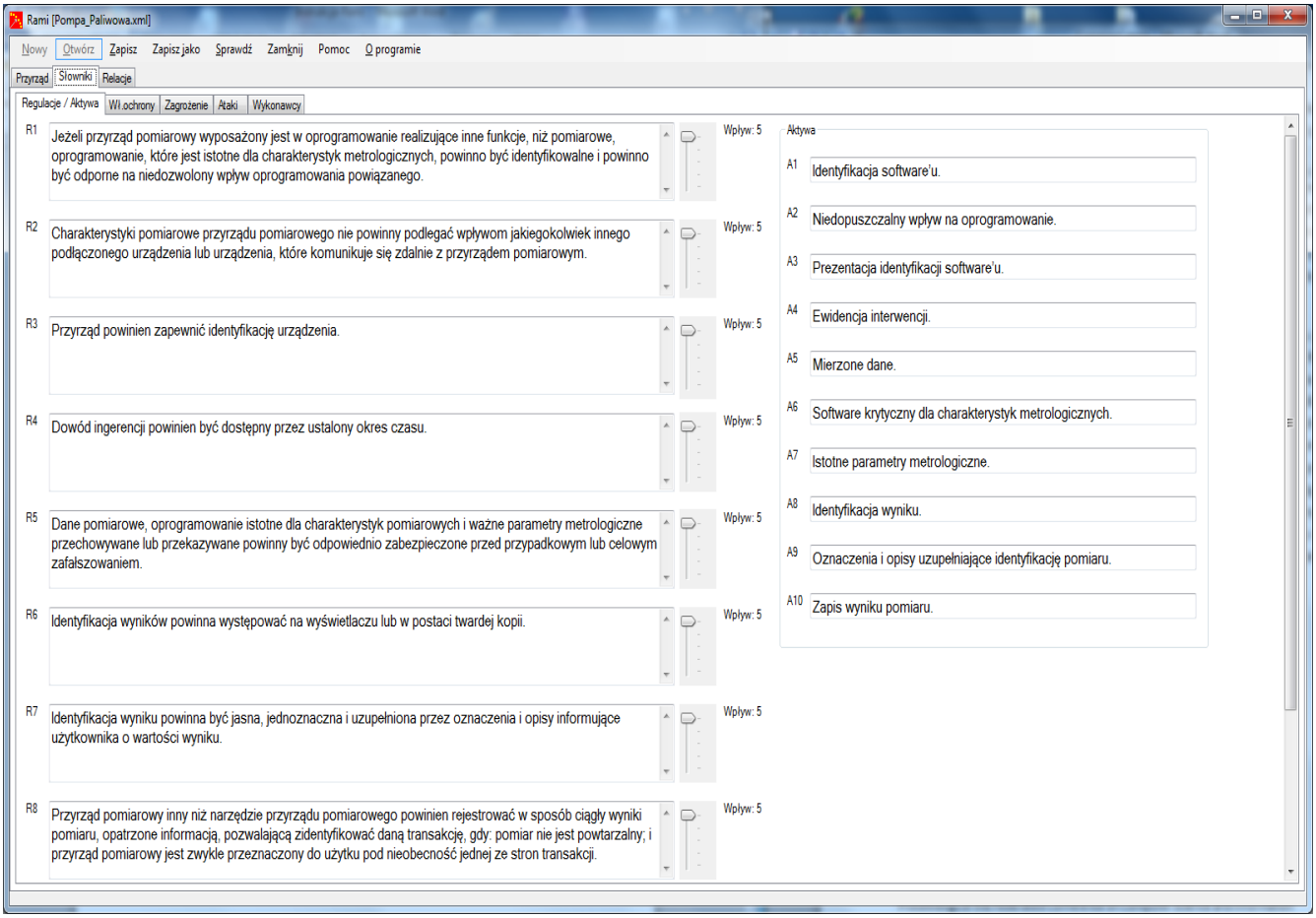
Jeśli nastąpiły zmiany danych, aktywacja funkcji **Zamknij** i pozytywna odpowiedź na pytanie: „Czy zapisać zmiany?” kończy pracę z dokumentem z rejestracją zmian.

Przykład

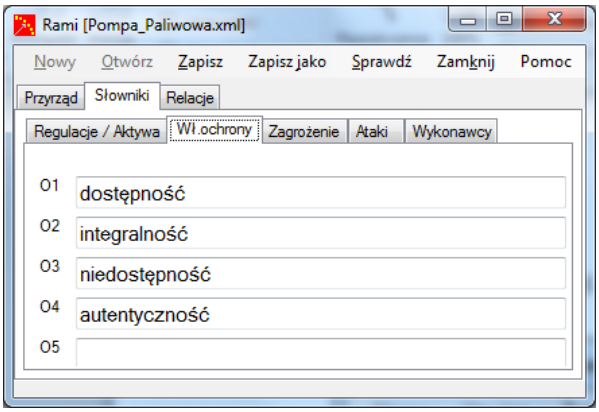
Zamieszczony w pozycji [1] literatury przykład został wykorzystany do testów **Rami**. Fazy definicji i określania relacji pomiędzy składowymi oraz wyniki oceny **ryzyka** zafałszowania pomiaru przedstawiają poniższe kopie ekranów programu użytego do dla analizy pompy paliwowej.



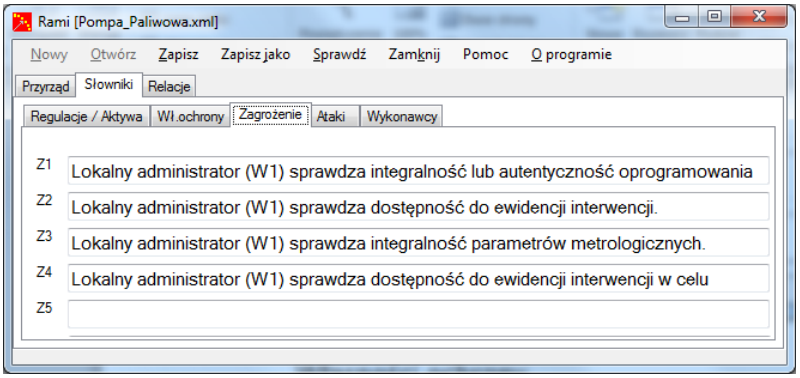
Rys. 1 Opis przyrządu pomiarowego.



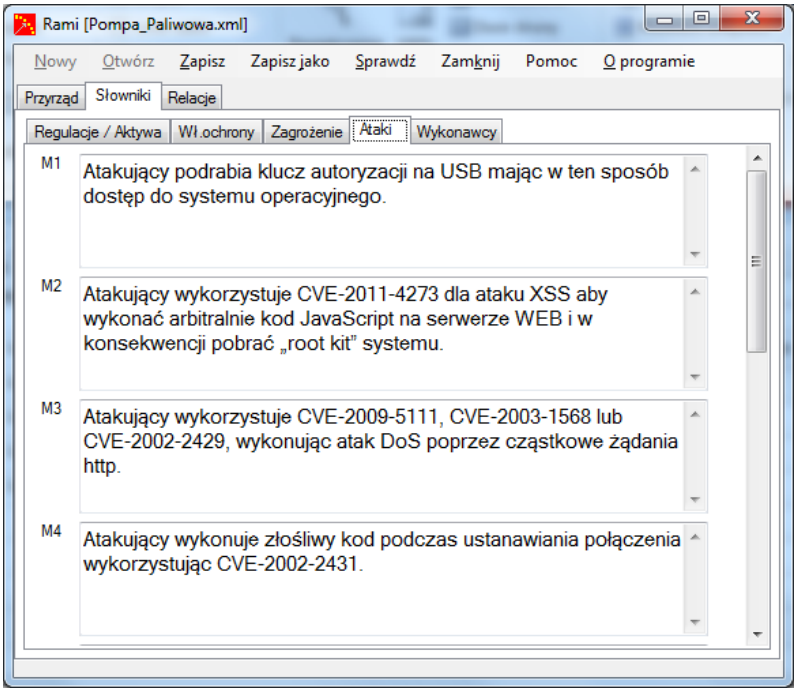
Rys. 2 Zbiór regulacji i wyprowadzenie aktywów.



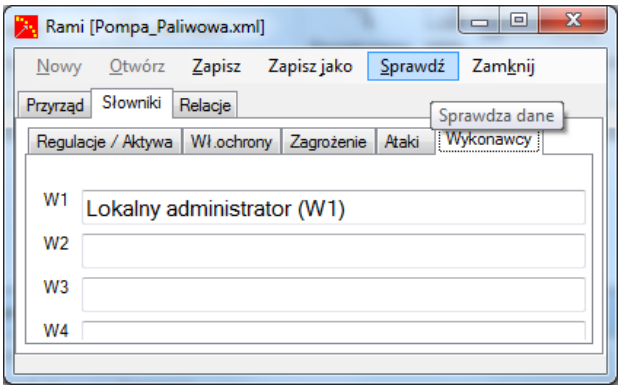
Rys. 3 Własności ochrony.



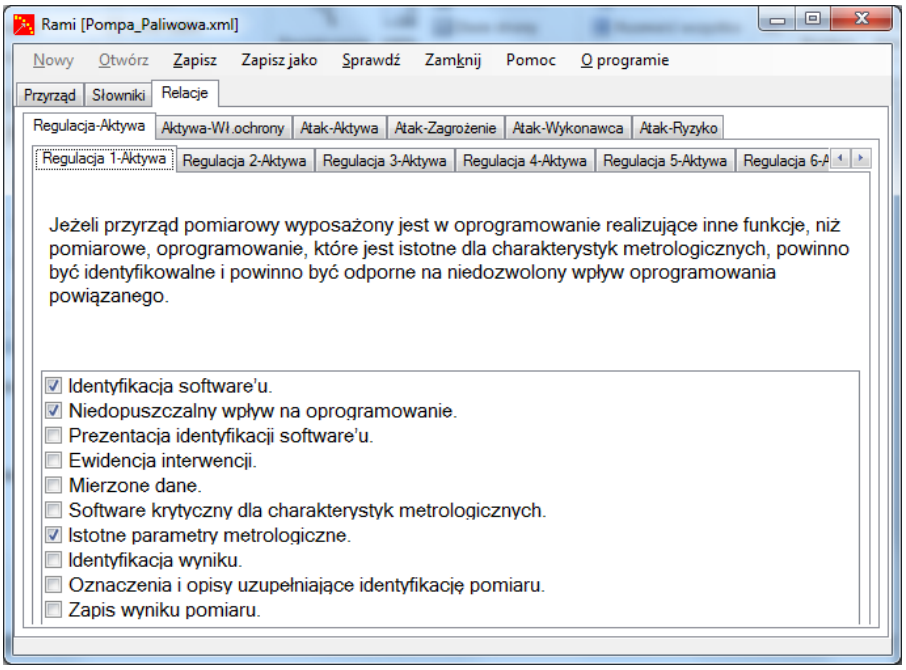
Rys. 4 Zagrożenia.



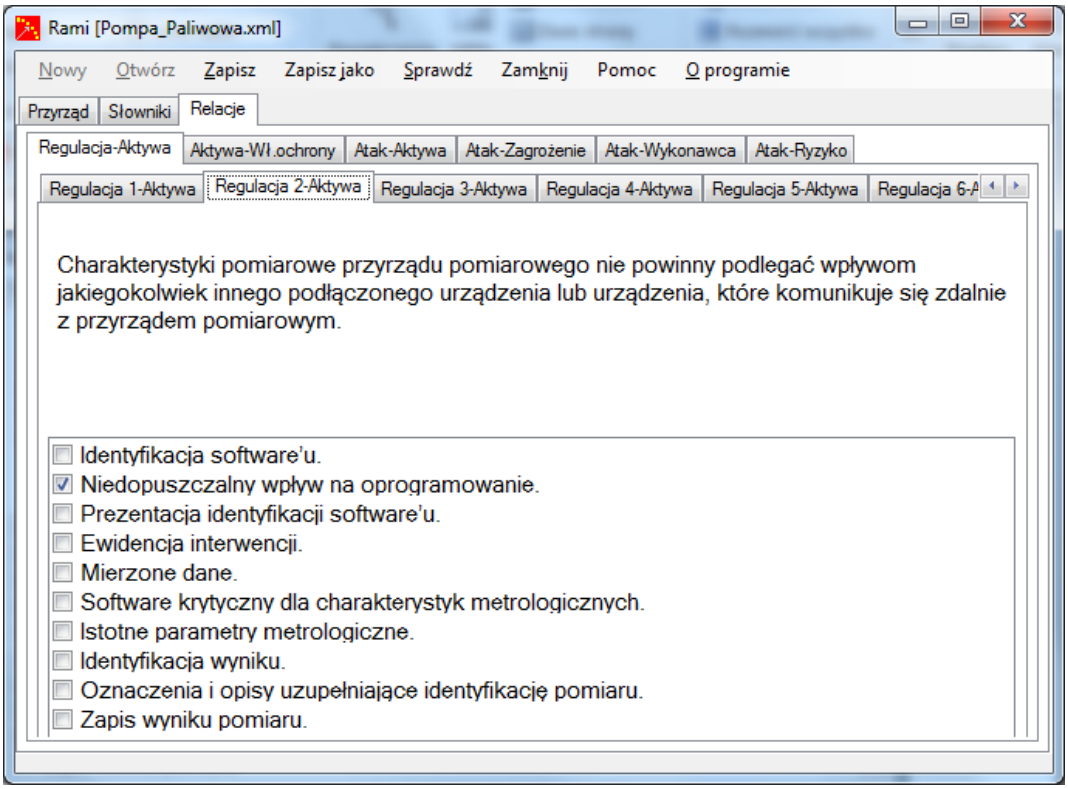
Rys. 5 Ataki.



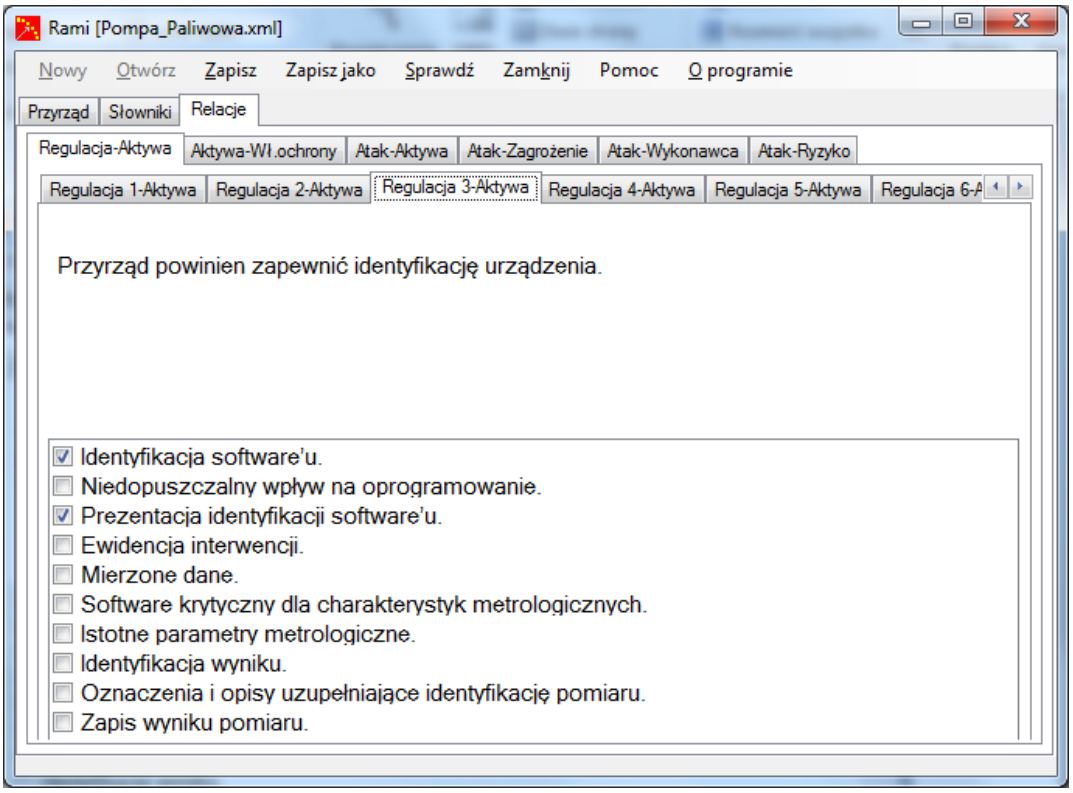
Rys. 6 Wykonawcy.



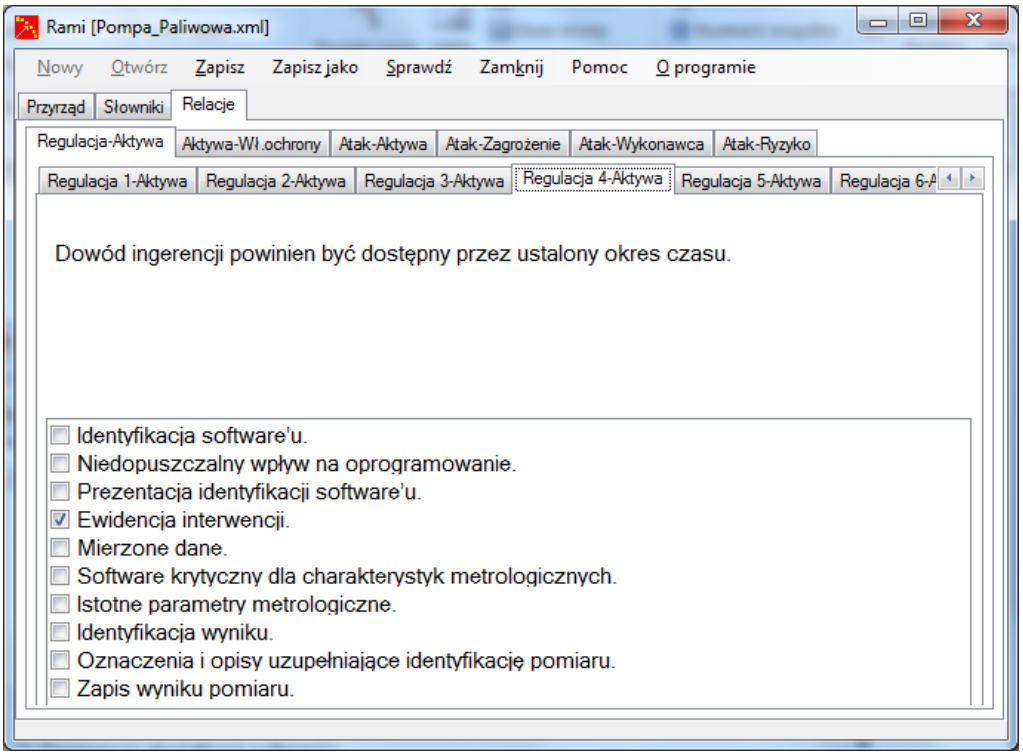
Rys. 7 Relacja Regulacja 1 – Aktywa.



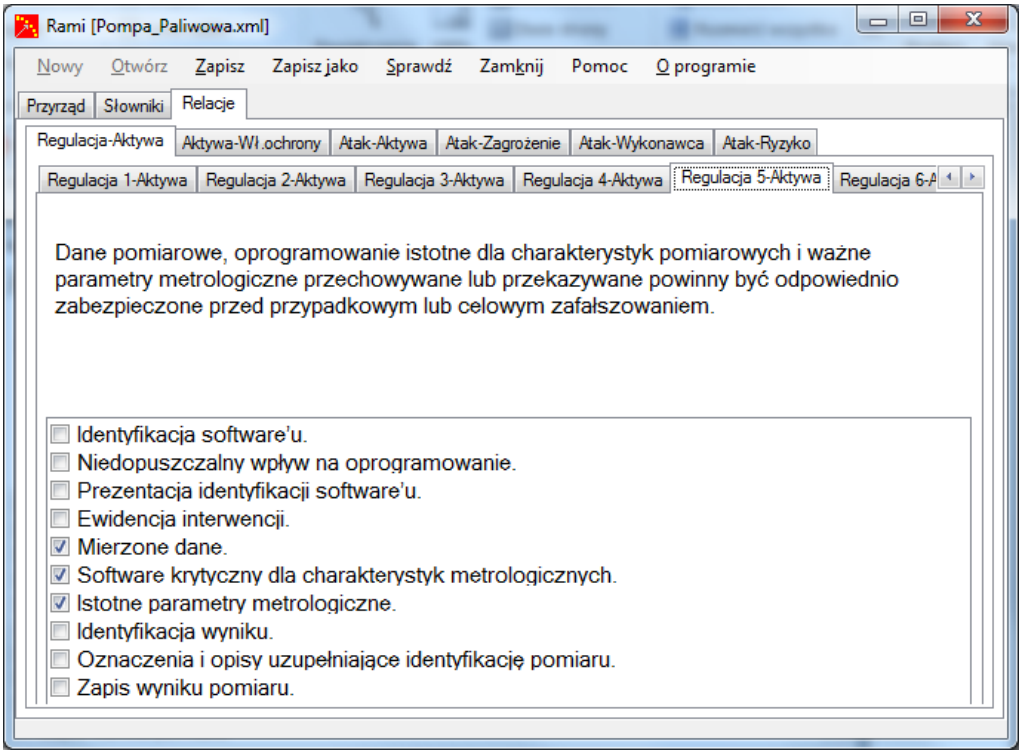
Rys. 8 Relacja Regulacja 2 – Aktywa.



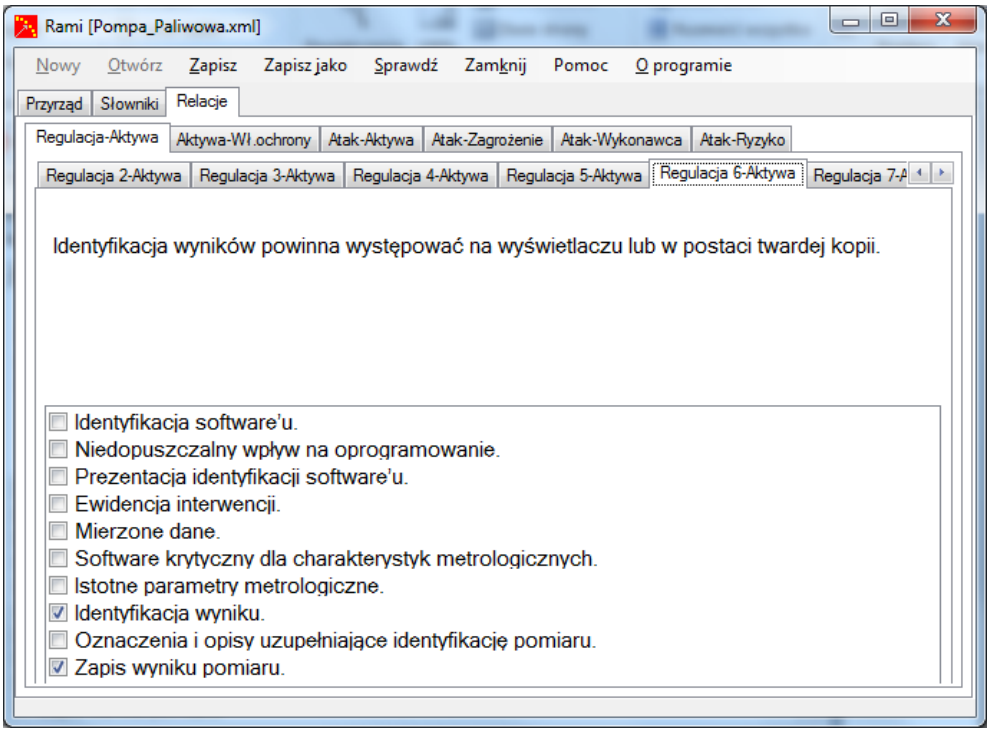
Rys. 9 Relacja Regulacja 3 – Aktywa.



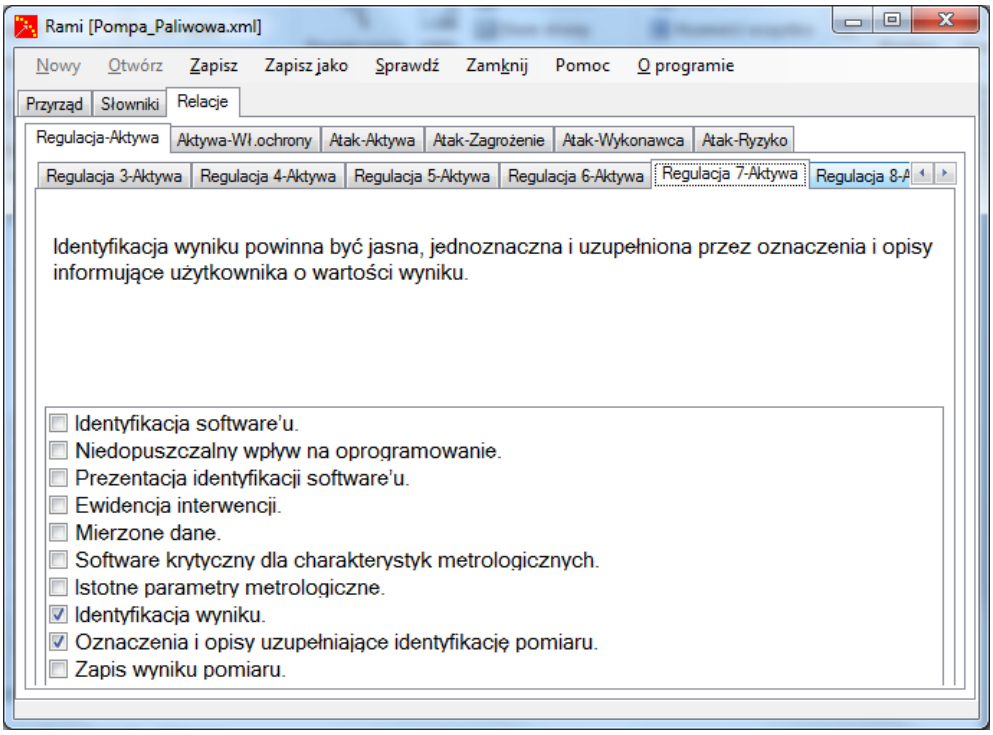
Rys. 10 Relacja Regulacja 4 – Aktywa.



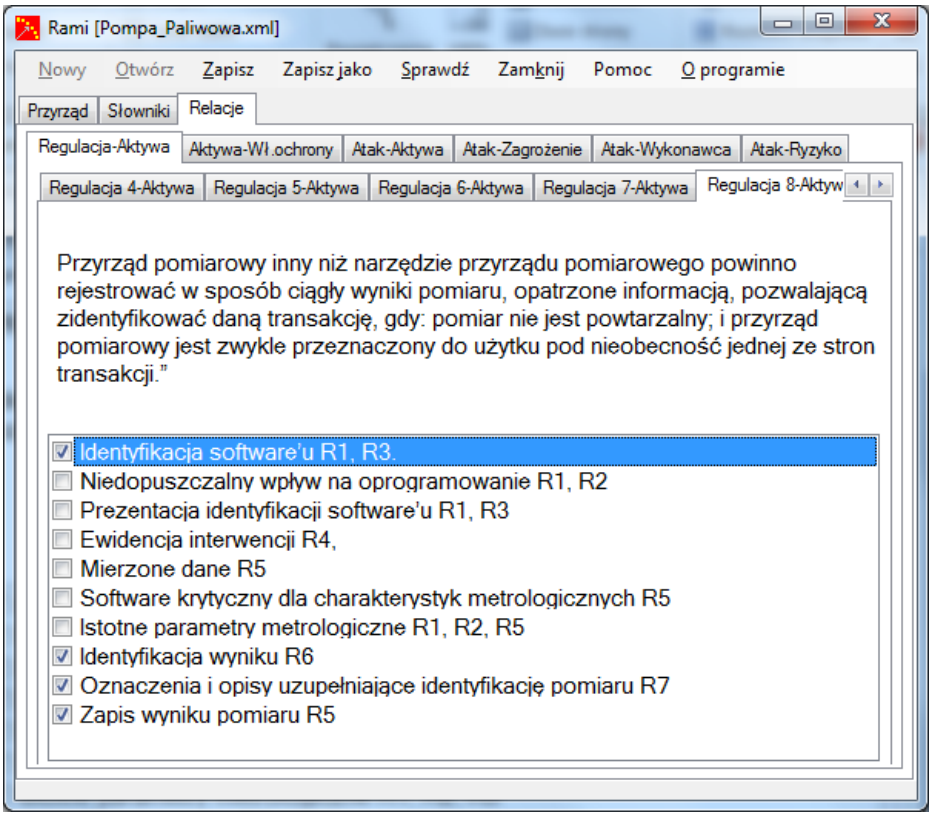
Rys. 11 Relacja Regulacja 5 – Aktywa.



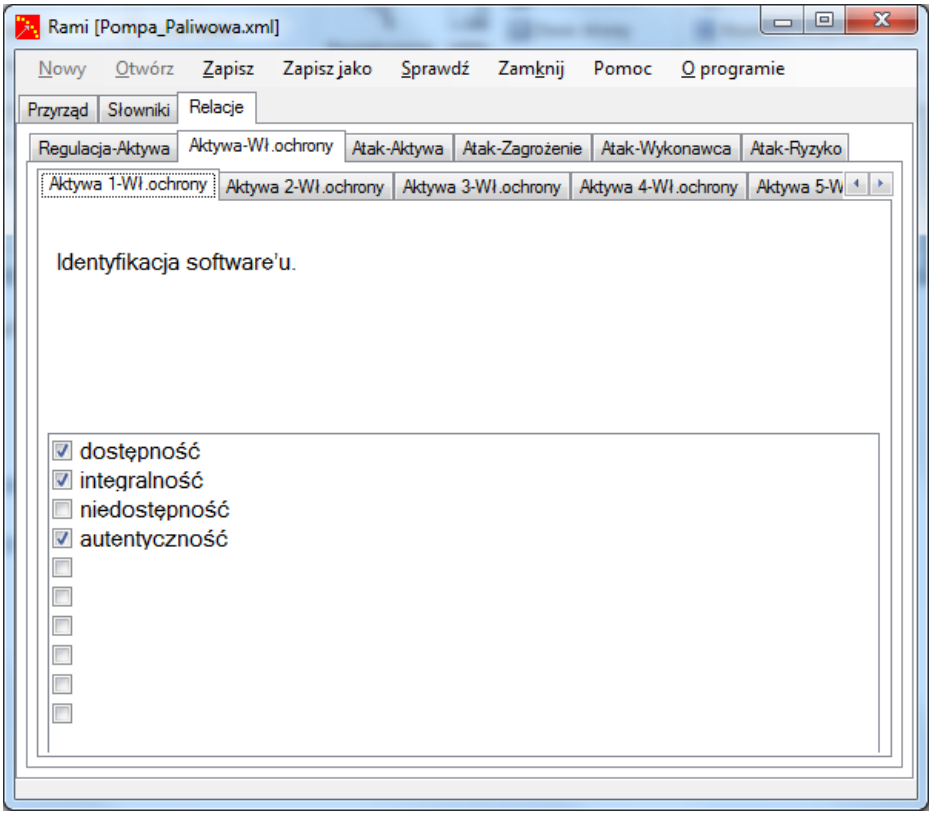
Rys. 12 Relacja Regulacja 6 – Aktywa.



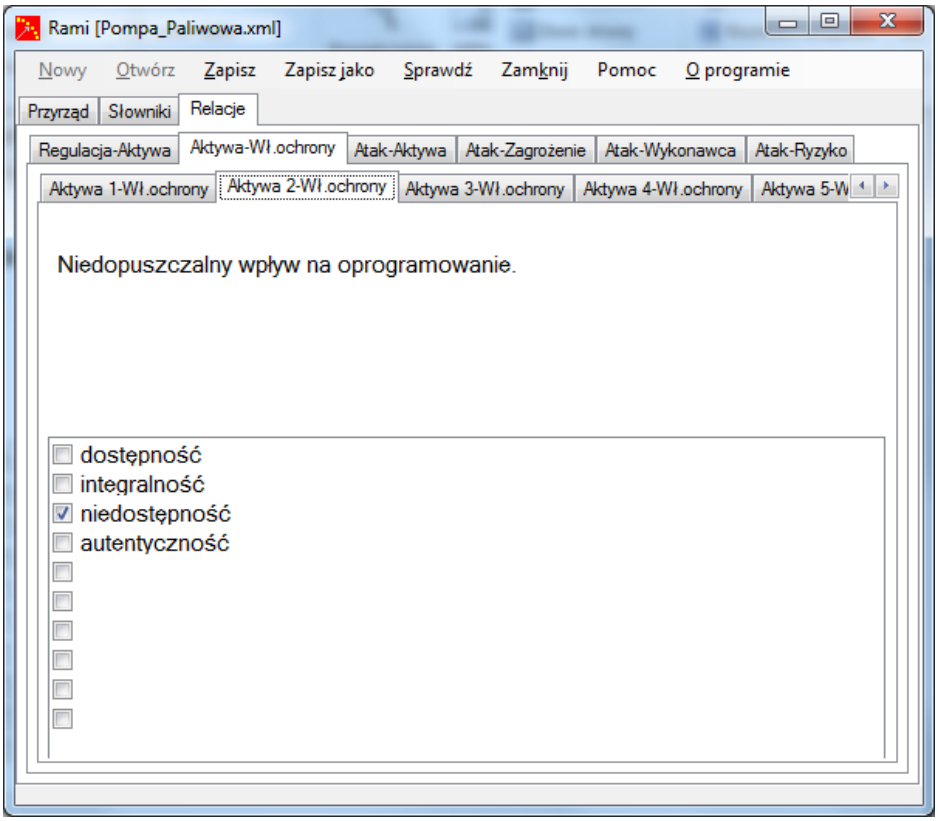
Rys. 13 Relacja Regulacja 7 – Aktywa.



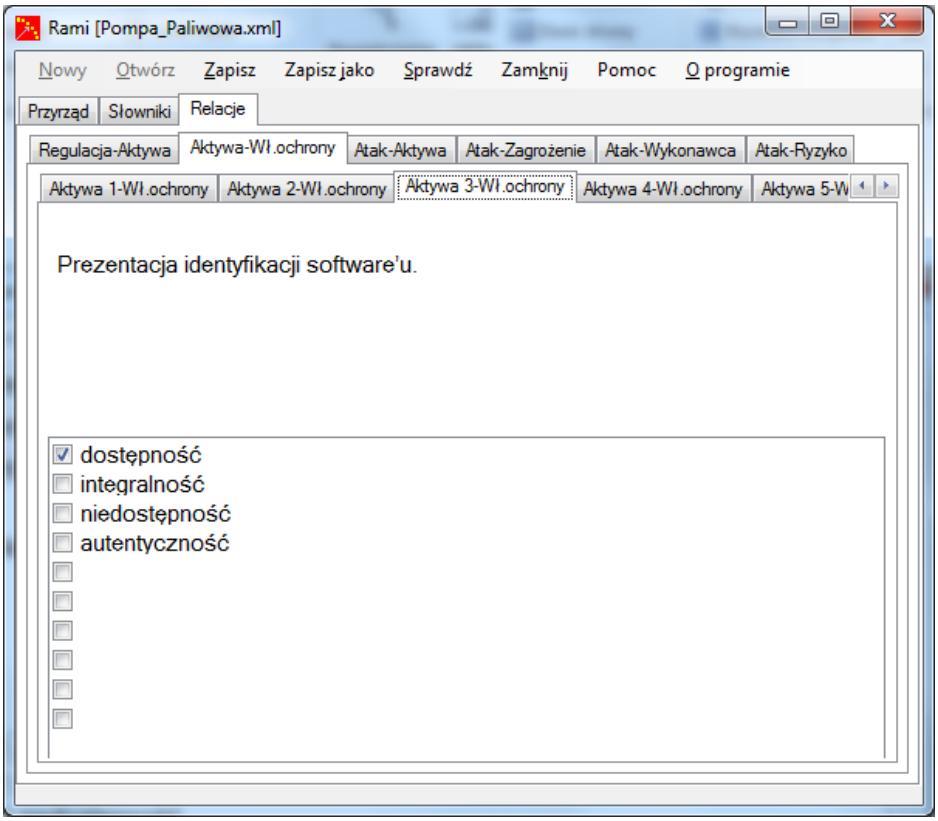
Rys. 14 Relacja Regulacja 8 – Aktywa.



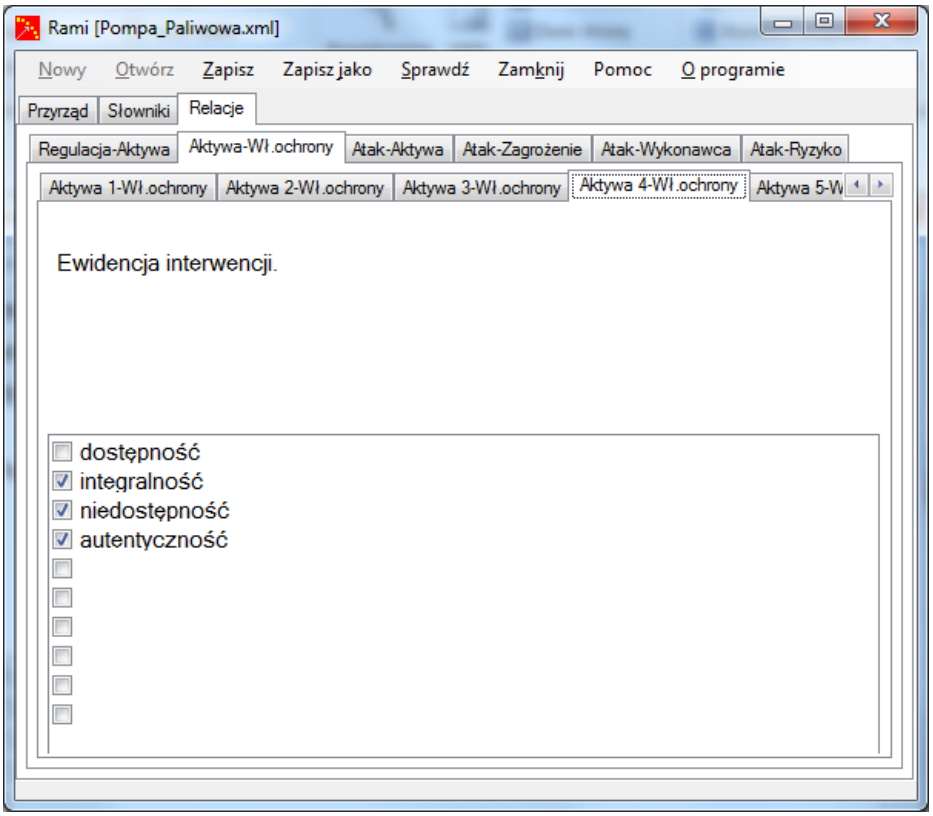
Rys. 16 Relacja Aktywa 1 – własności ochrony.



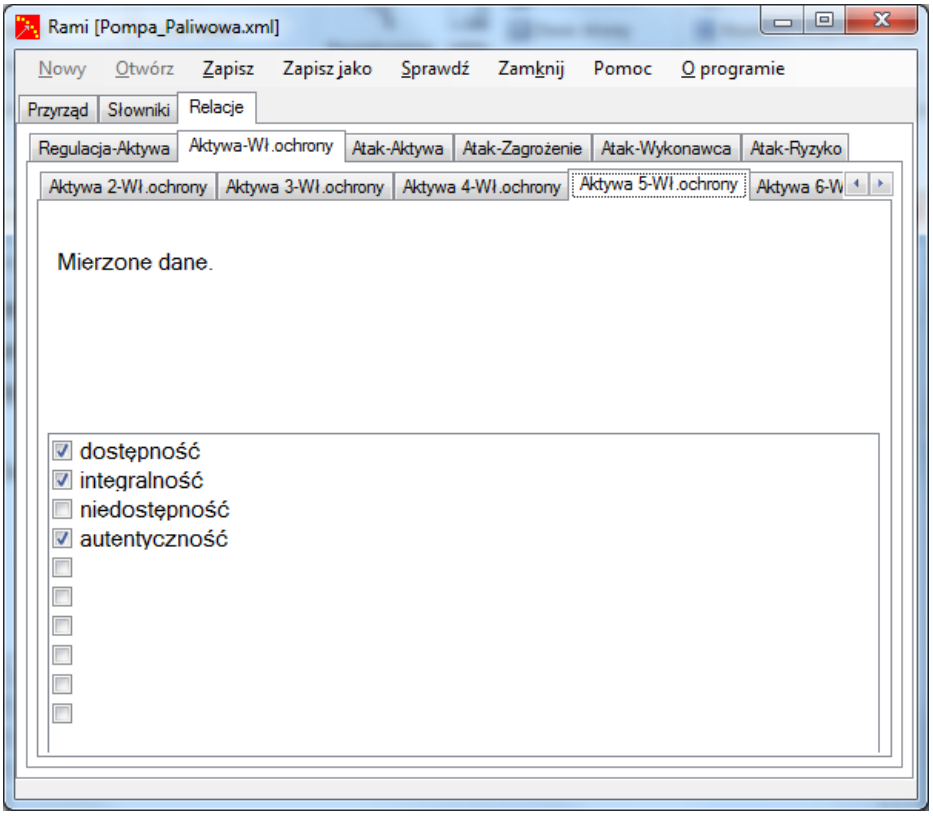
Rys. 16 Relacja Aktywa 2 – własności ochrony.



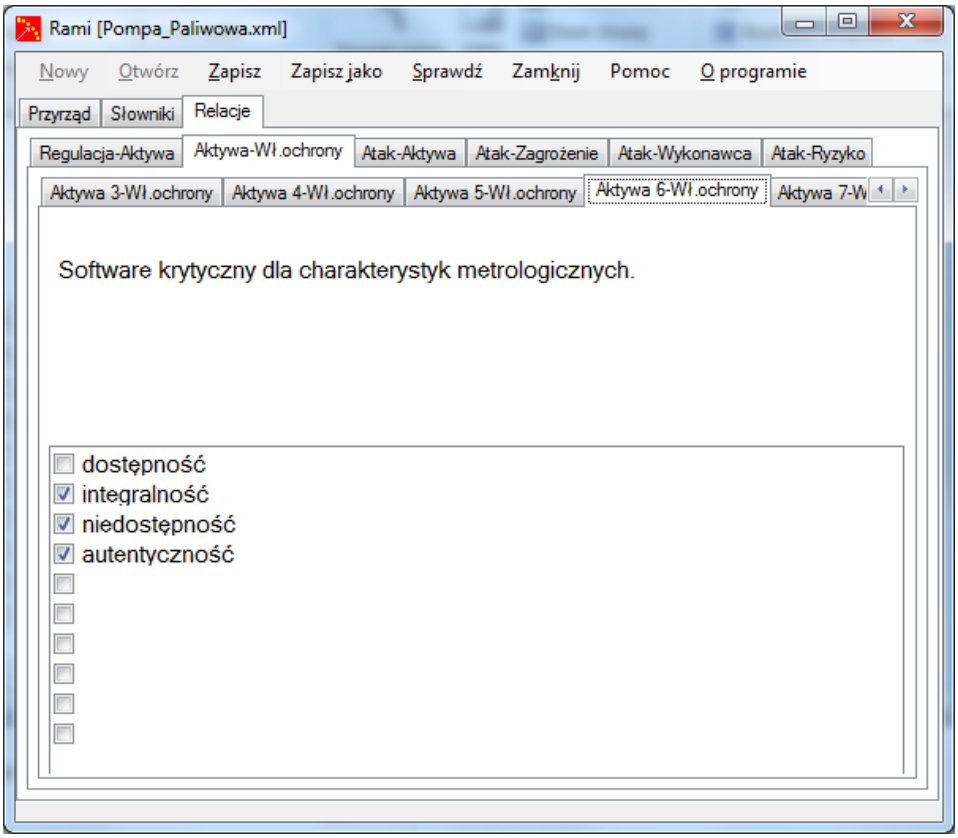
Rys. 16 Relacja Aktywa 3 – własności ochrony.



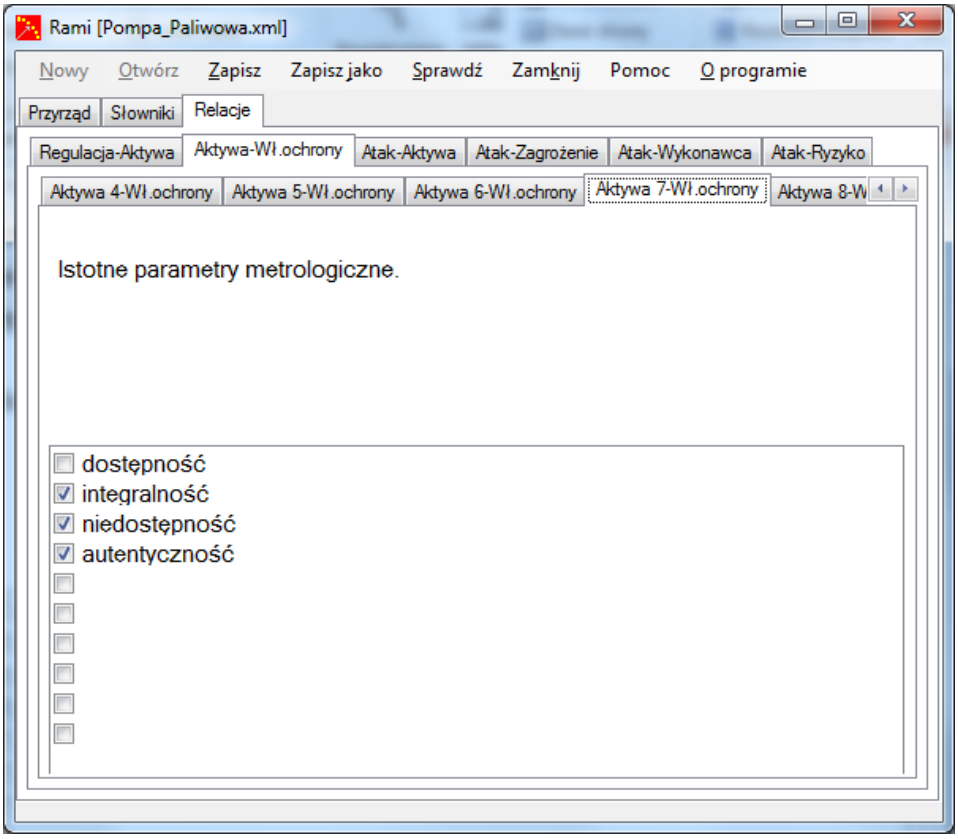
Rys. 18 Relacja Aktywa 4 – własności ochrony.



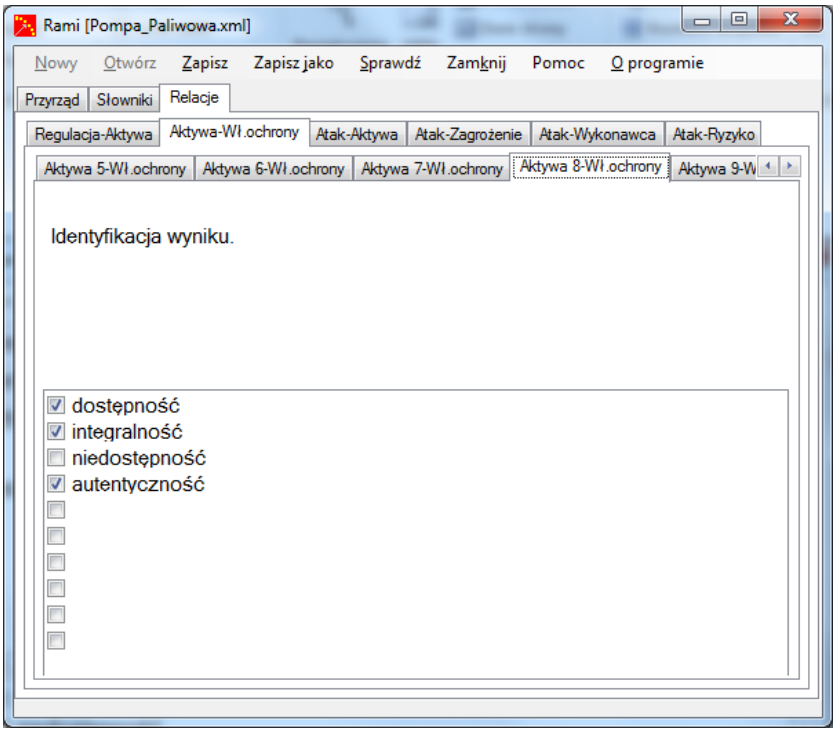
Rys. 19 Relacja Aktywa 5 – własności ochrony.



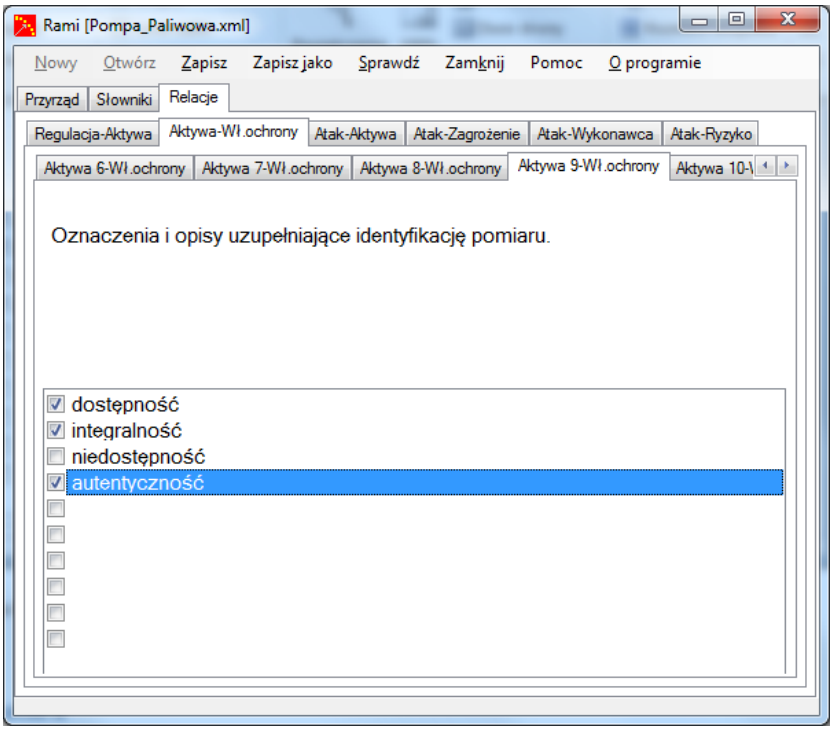
Rys. 20 Relacja Aktywa 6 – własności ochrony.



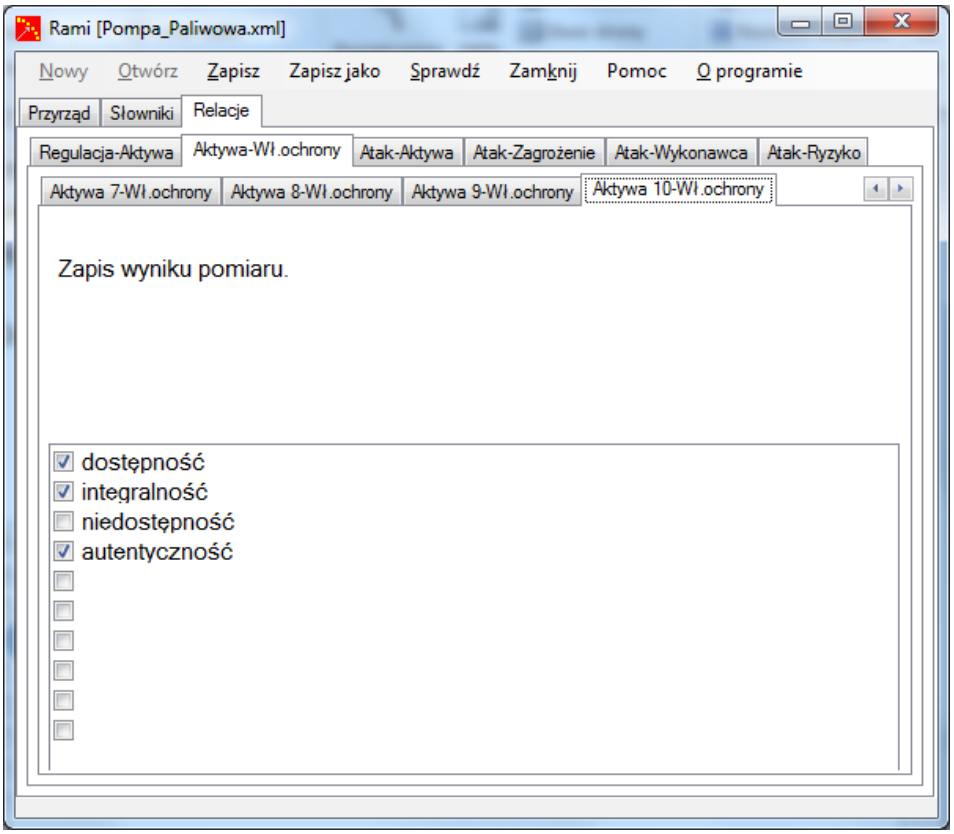
Rys. 21 Relacja Aktywa 7 – własności ochrony.



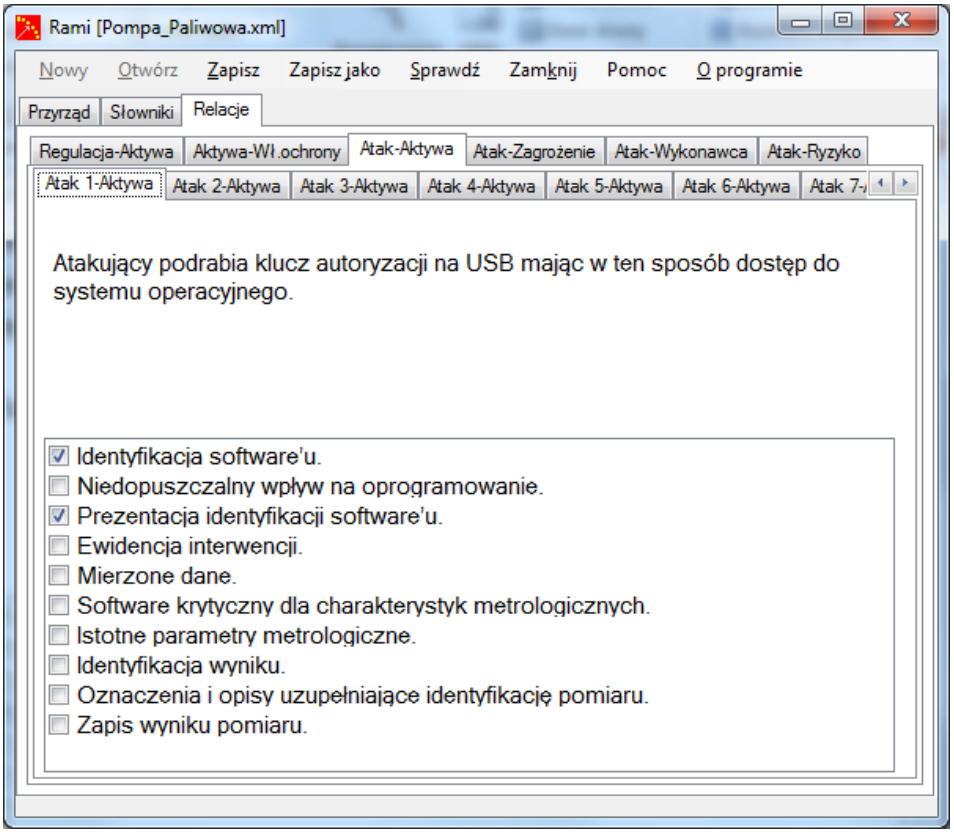
Rys. 22 Relacja Aktywa 8 – własności ochrony.



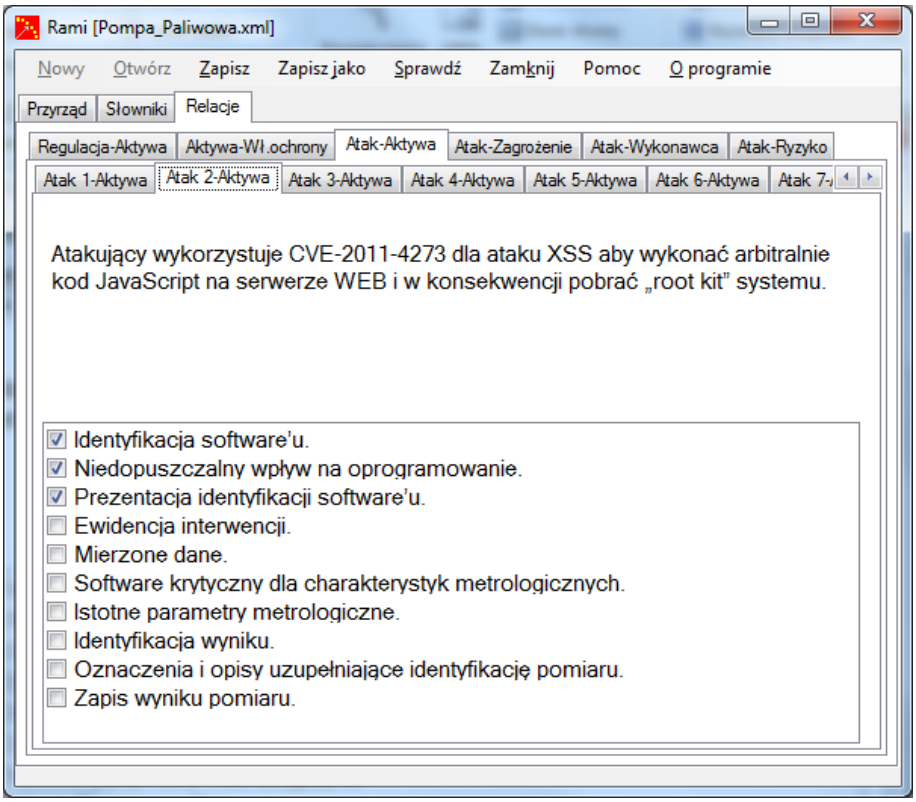
Rys. 23 Relacja Aktywa 9 – własności ochrony.



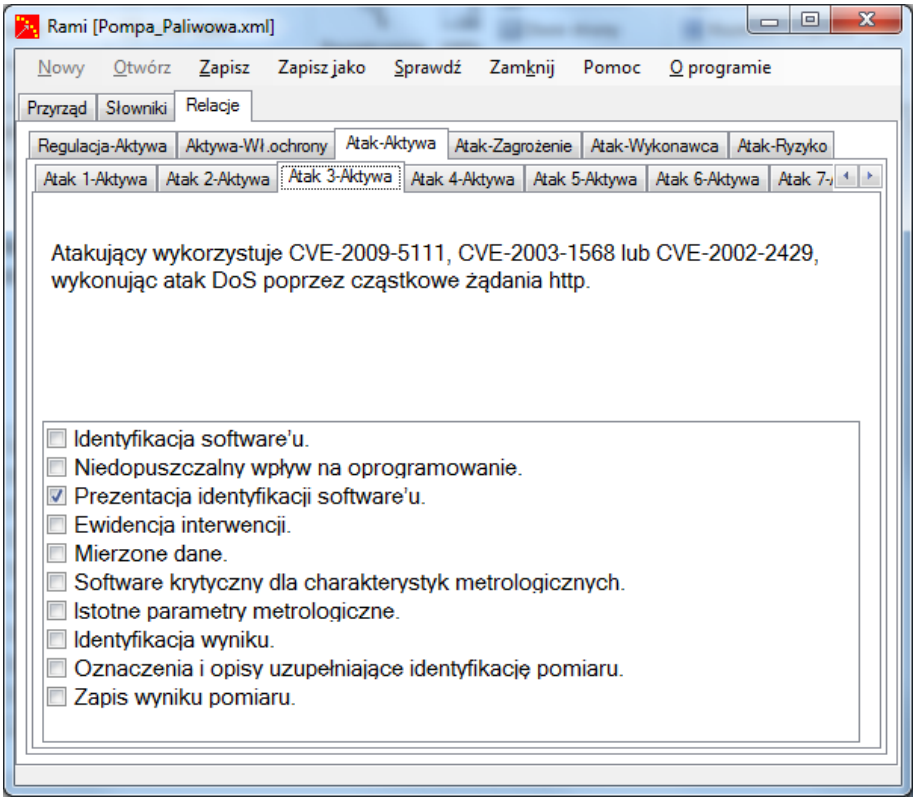
Rys. 24 Relacja Aktywa 10 – własności ochrony.



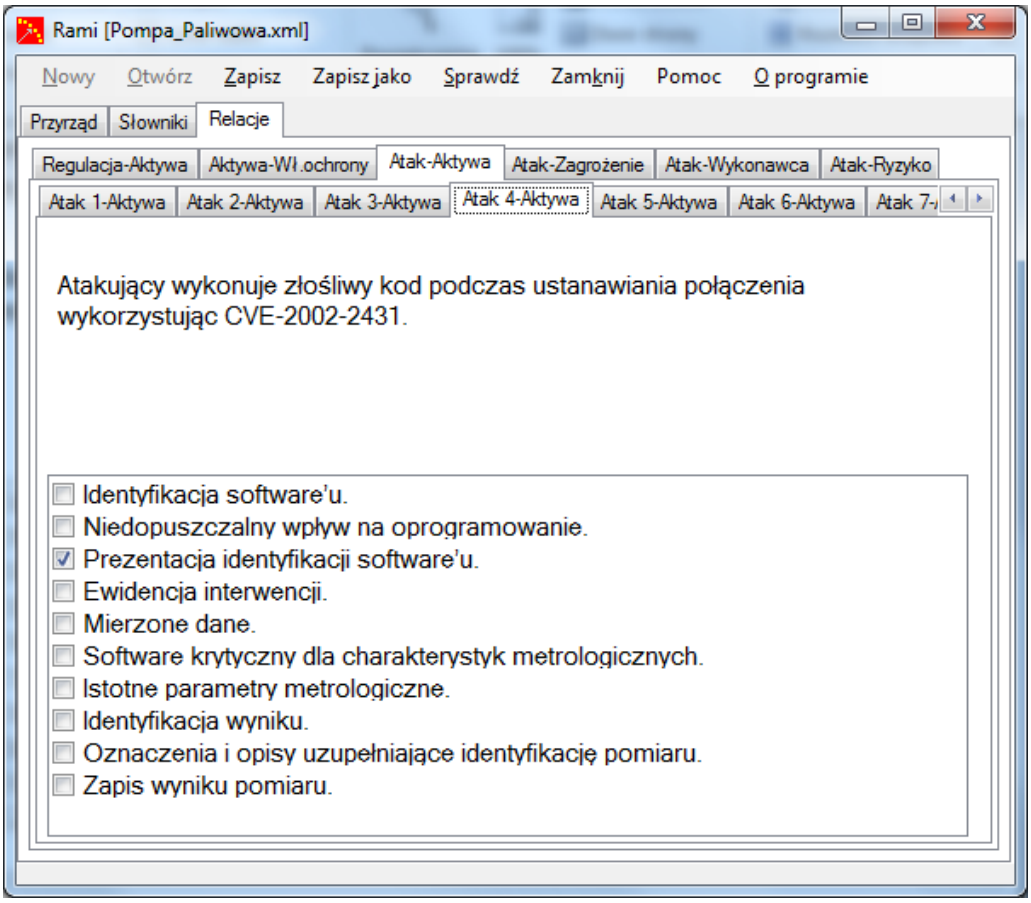
Rys. 25 Relacja Atak 1 – Aktywa.



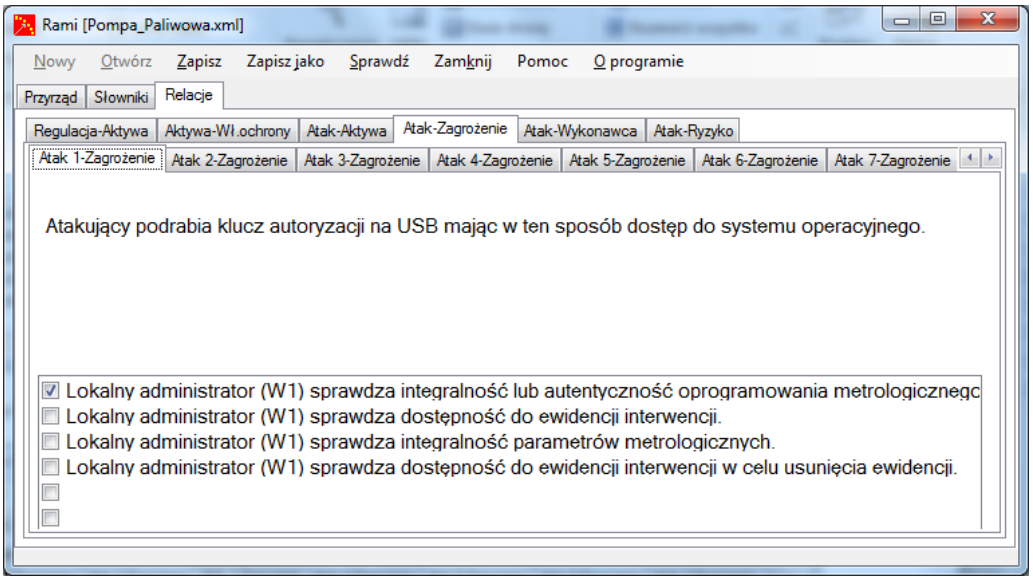
Rys. 26 Relacja Atak 2 – Aktywa.



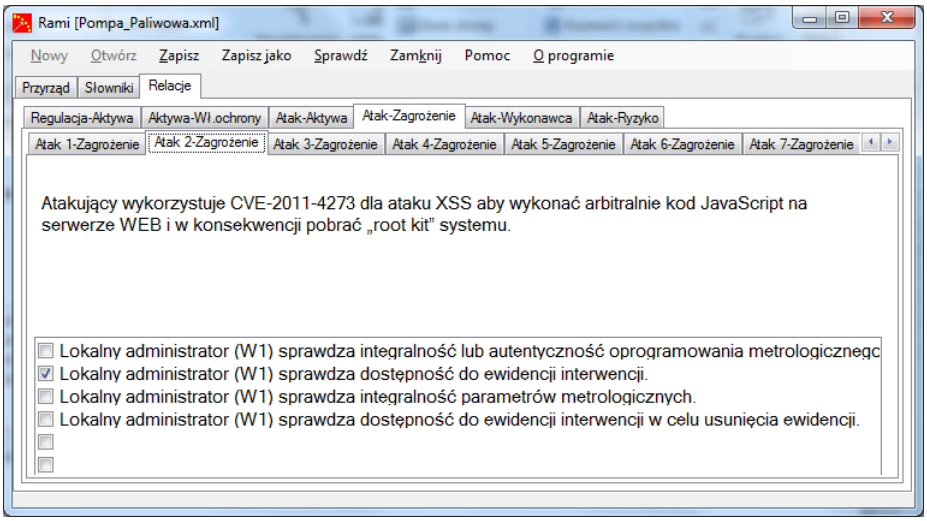
Rys. 27 Relacja Atak 3 – Aktywa.



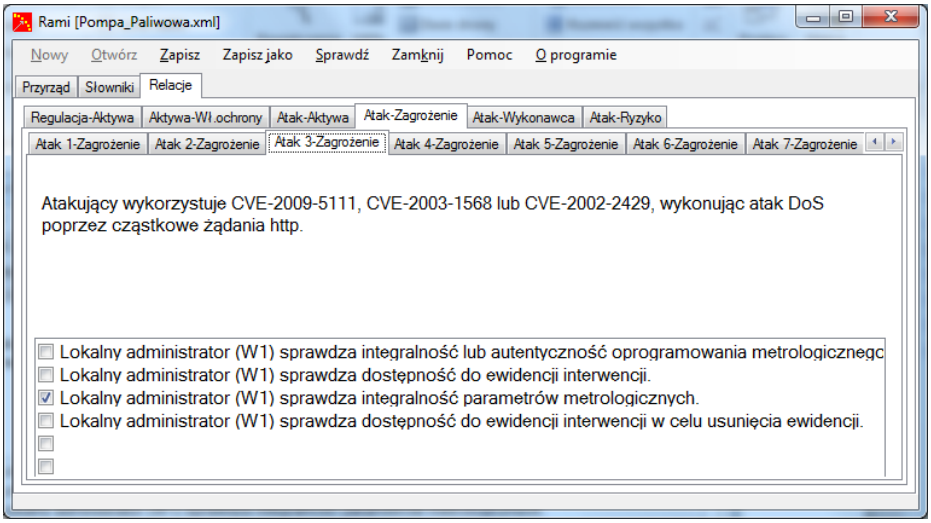
Rys. 28 Relacja Atak 4 – Aktywa.



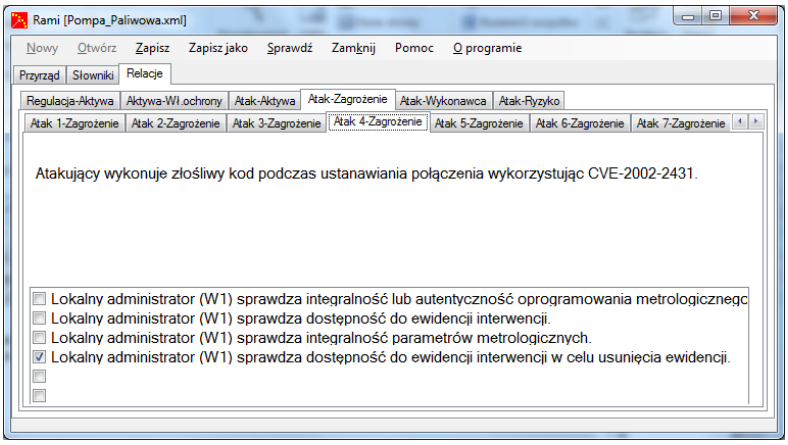
Rys. 29 Relacja Atak 1 – Zagrożenie.



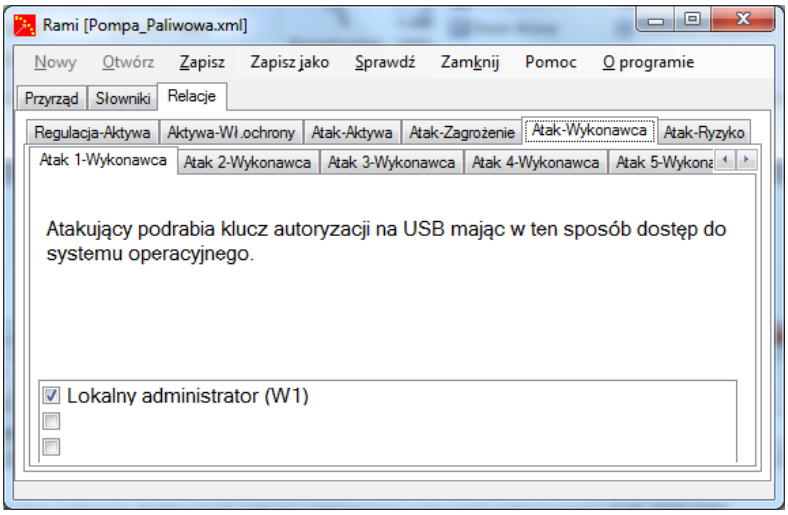
Rys. 30 Relacja Atak 2 – Zagrożenie.



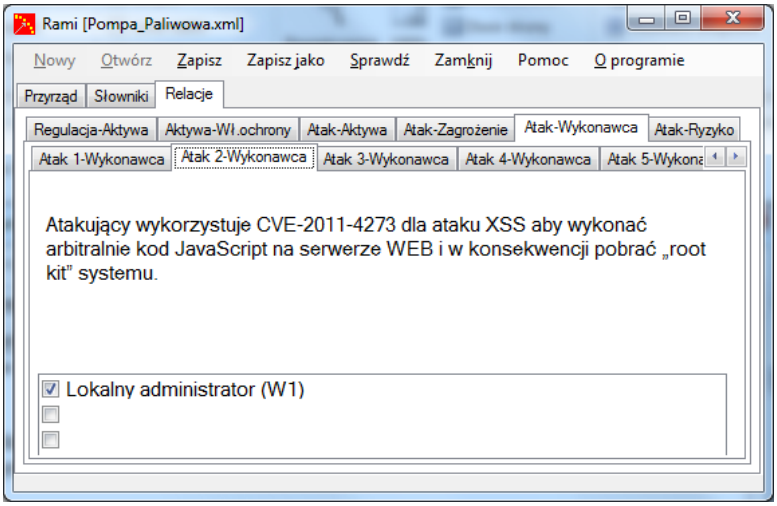
Rys. 31 Relacja Atak 3 – Zagrożenie.



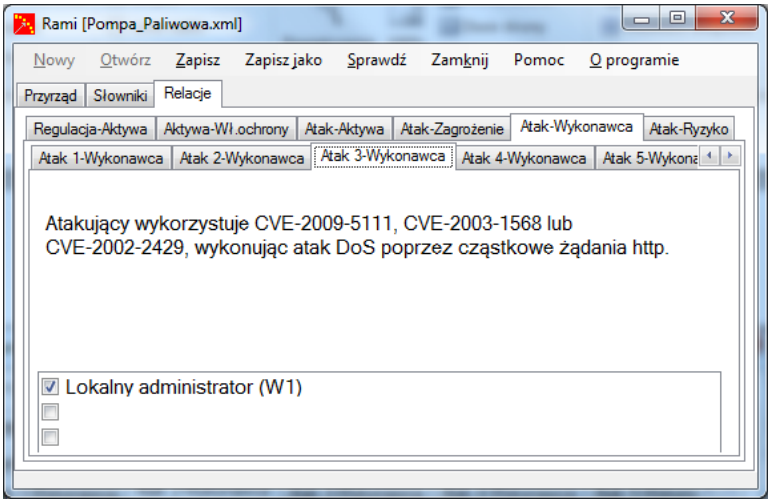
Rys. 32 Relacja Atak 4 – Zagrożenie.



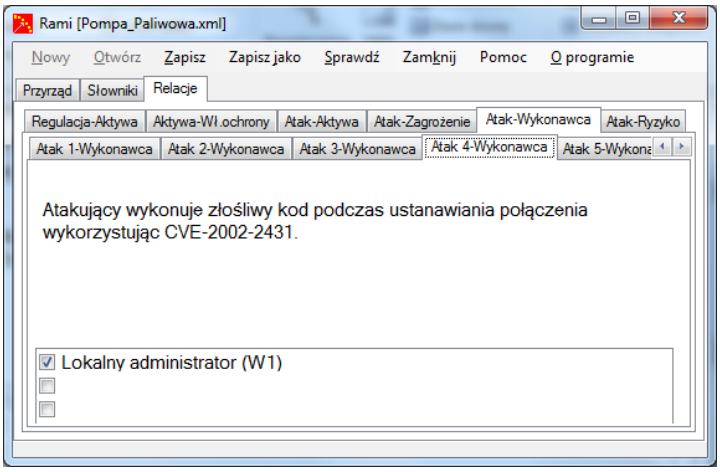
Rys. 33 Relacja Atak 1 – Wykonawca.



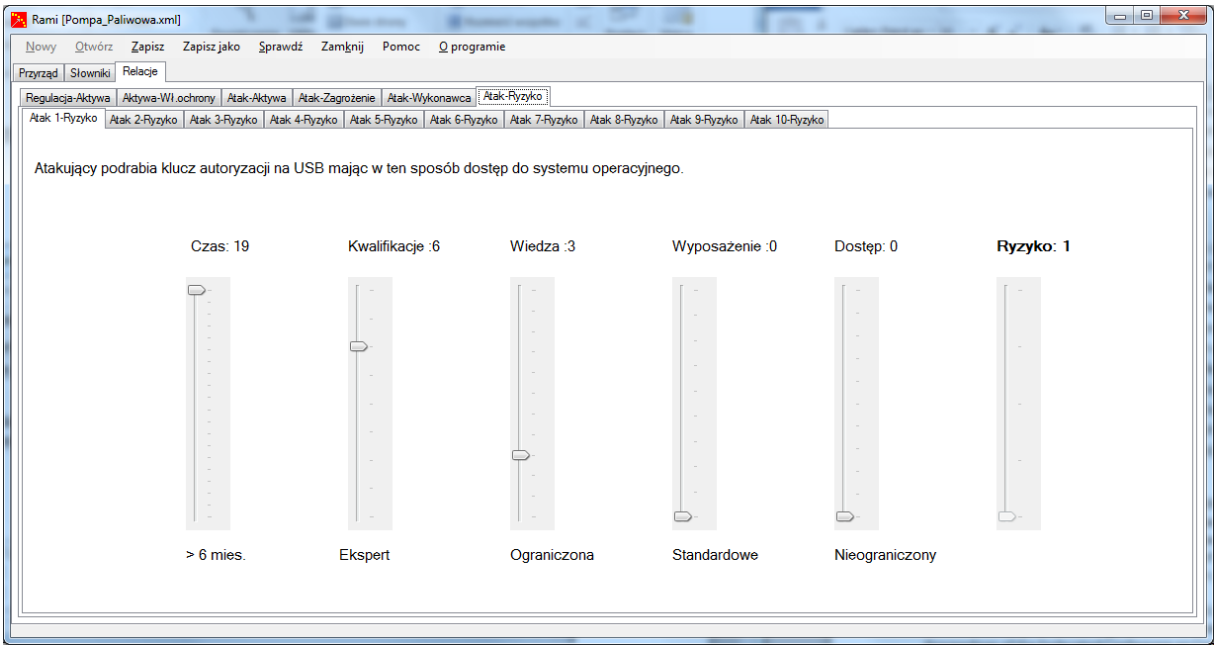
Rys. 34 Relacja Atak 2 – Wykonawca.



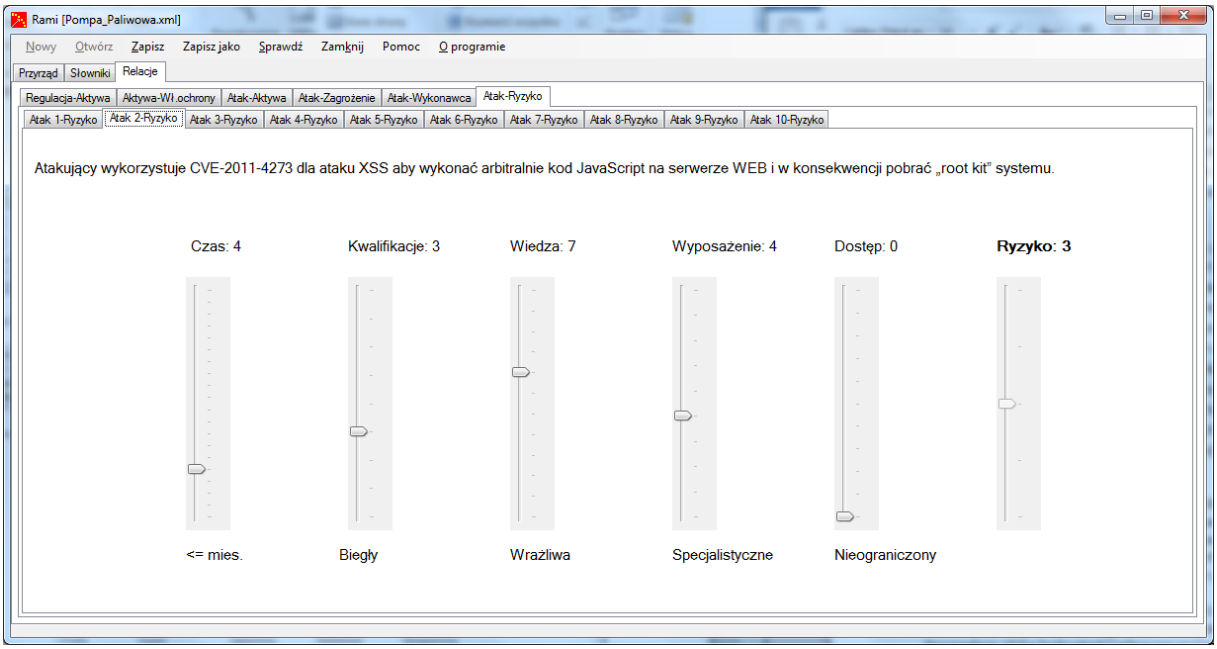
Rys. 35 Relacja Atak 3 – Wykonawca.



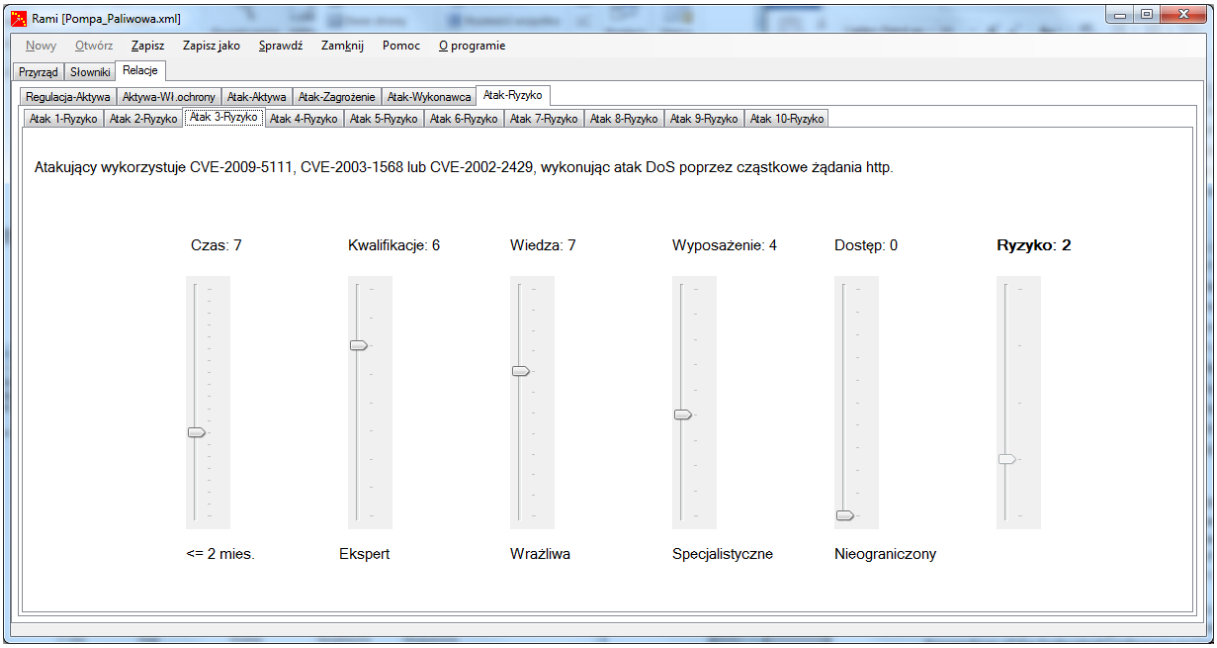
Rys. 36 Relacja Atak 4 – Wykonawca.



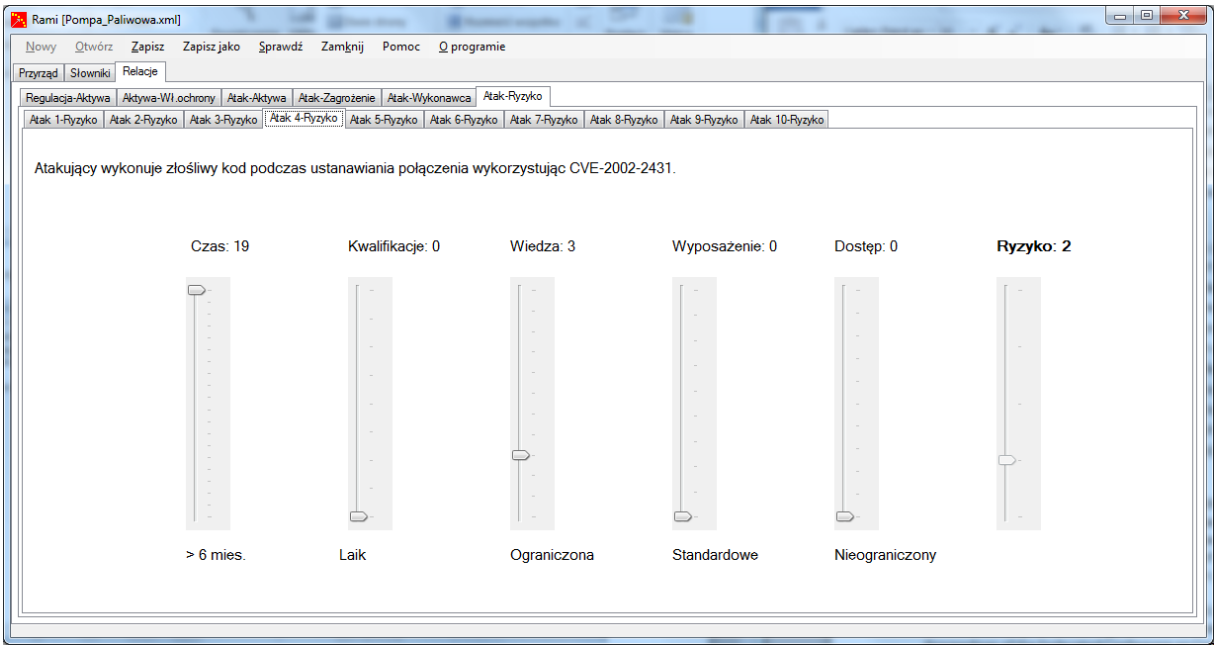
Rys. 37 Ocena ryzyka – atak 1.



Rys. 38 Ocena ryzyka – atak 2.



Rys. 39 Ocena ryzyka – atak 3.



Rys. 40 Ocena ryzyka – atak 4.

Wynik analizy doprowadza do wniosku, że najwyższe ryzyko o wartości 3 związane jest z atakiem 2 - wykonania kodu Java Script na serwerze WWW. Decydują o tym umiarkowany „opór” jaki musi pokonać agresor w ataku na przyrząd i nieograniczony (poprzez Internet) dostęp do przyrządu.

Literatura

[1] Software Risk Assessment for Measuring Instruments in Legal Metrology

Marko Esche, Florian Thiel

Physikalisch-Technische Bundesanstalt

Abbestr. 2-12

10587 Berlin, Germany

[2] Common Methodology for Information Technology Security Evaluation

Evaluation methodology; September 2012; Version 3.1; Revision 4; CCMB-2012-09-004

Spis treści