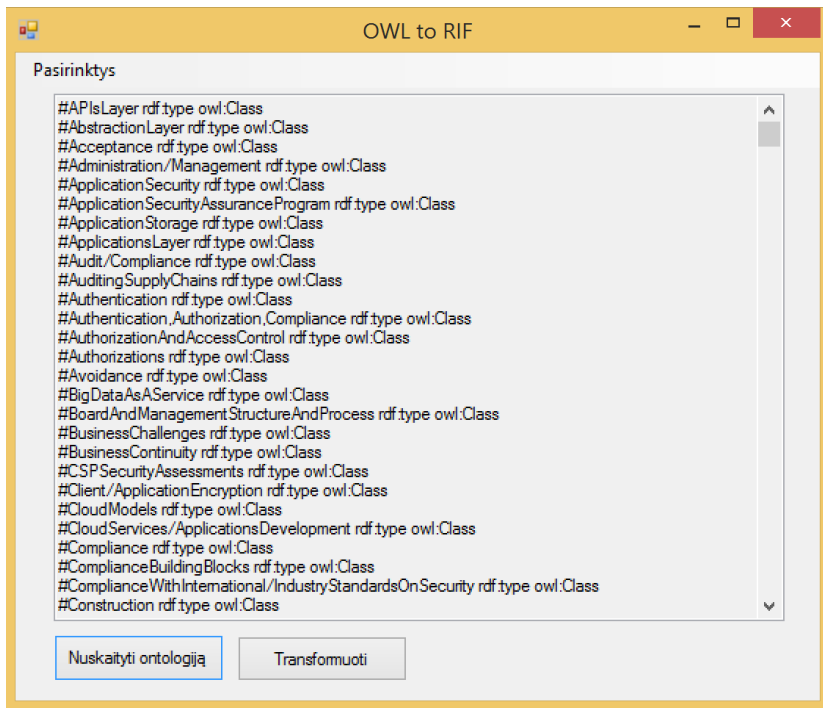


## Annex B. Examples of the developed tools



**Fig. B.1.** Example of software for ontology transforming into RIF

```

es:clp  /read_xml.clp
(
  (deftemplate question
    (slot id)
    (slot nr)
    (slot country)
    (slot type)
    (slot date)
    (slot name)
    (slot value)
    (slot class)
    (slot platform)
    (multislot description)
  )

  (load-facts book.xml)
  (facts)
)

Problems  Javadoc  Declaration  Console
<terminated> read_xml.clp [less Application] C:\Program Files\Java\jre1.8.0_191\bin\javaw.exe (Jan 22, 2019 8:37:21 PM)
f-134 (MAIN:question (id 637) (nr 10) (country "Lithuania") (type "Local infections") (date "2019-01-22") (name "Trojan.Win32.Hosts2.gen") (value "28") (class "TrojWare") (platform "Trojan-Spy") (description "
f-135 (MAIN:question (id 638) (nr 1) (country "Lithuania") (type "On-Demand Scan") (date "2019-01-22") (name "DangerousObject.Multi.Generic") (value "7.954") (class "DangerousObject") (platform "Multi") (d
f-136 (MAIN:question (id 639) (nr 2) (country "Lithuania") (type "On-Demand Scan") (date "2019-01-22") (name "HackTool.MSIL.KMSAuto.d") (value "4.88") (class "HackTool") (platform "MSIL") (description "App
f-137 (MAIN:question (id 640) (nr 3) (country "Lithuania") (type "On-Demand Scan") (date "2019-01-22") (name "HackTool.MSIL.KMSAuto.a") (value "4.344") (class "HackTool") (platform "MSIL") (description "Ap
f-138 (MAIN:question (id 641) (nr 4) (country "Lithuania") (type "On-Demand Scan") (date "2019-01-22") (name "HackTool.Win64.HackKMS.b") (value "2.578") (class "HackTool") (platform "Win64") (description "
f-139 (MAIN:question (id 642) (nr 5) (country "Lithuania") (type "On-Demand Scan") (date "2019-01-22") (name "Trojan.Win32.SHEER.gen") (value "1.801") (class "Trojan") (platform "Win32") (description "This
f-140 (MAIN:question (id 643) (nr 6) (country "Lithuania") (type "On-Demand Scan") (date "2019-01-22") (name "Trojan.Multi.Accessstr.a.sh") (value "1.928") (class "Trojan") (platform "Multi") (description "
f-141 (MAIN:question (id 644) (nr 7) (country "Lithuania") (type "On-Demand Scan") (date "2019-01-22") (name "Trojan.Multi.GenBadur.gen") (value "1.784") (class "Trojan") (platform "Multi") (description "T
f-142 (MAIN:question (id 645) (nr 8) (country "Lithuania") (type "On-Demand Scan") (date "2019-01-22") (name "Trojan.Multi.Accessstr.a.um") (value "1.674") (class "Trojan") (platform "Multi") (description "
f-143 (MAIN:question (id 646) (nr 9) (country "Lithuania") (type "On-Demand Scan") (date "2019-01-22") (name "Trojan.Script.Generic") (value "1.488") (class "Trojan") (platform "Script") (description "This
f-144 (MAIN:question (id 647) (nr 10) (country "Lithuania") (type "On-Demand Scan") (date "2019-01-22") (name "HackTool.Win32.KMSAuto.er") (value "1.468") (class "HackTool") (platform "Win32") (description
f-145 (MAIN:question (id 648) (nr 1) (country "Lithuania") (type "Spam") (date "2019-01-22") (name "Shikari") (value "47.918") (class "nil") (platform "nil") (description "nil"))
f-146 (MAIN:question (id 649) (nr 2) (country "Lithuania") (type "Spam") (date "2019-01-22") (name "Linguistic Analysis") (value "43.024") (class "nil") (platform "nil") (description "nil"))
f-147 (MAIN:question (id 650) (nr 3) (country "Lithuania") (type "Spam") (date "2019-01-22") (name "Analysis of Formal Attributes") (value "8.698") (class "nil") (platform "nil") (description "nil"))
f-148 (MAIN:question (id 651) (nr 4) (country "Lithuania") (type "Spam") (date "2019-01-22") (name "Signature Analysis") (value "0.338") (class "nil") (platform "nil") (description "nil"))
f-149 (MAIN:question (id 652) (nr 5) (country "Lithuania") (type "Spam") (date "2019-01-22") (name "Enforced Anti-Spam Update Service") (value "0.024") (class "nil") (platform "nil") (description "nil"))
f-150 (MAIN:question (id 653) (nr 6) (country "Lithuania") (type "Spam") (date "2019-01-22") (name "Other") (value "0.028") (class "nil") (platform "nil") (description "nil"))
f-151 (MAIN:question (id 654) (nr 1) (country "Lithuania") (type "Vulnerabilities") (date "2019-01-22") (name "Exploit.MSOffice.CVE-2017-11882.gen") (value "85.718") (class "Malware") (platform "DoS") (des
f-152 (MAIN:question (id 655) (nr 2) (country "Lithuania") (type "Vulnerabilities") (date "2019-01-22") (name "Exploit.Script.Generic") (value "2.868") (class "Exploit") (platform "Script") (description "A
f-153 (MAIN:question (id 656) (nr 3) (country "Lithuania") (type "Vulnerabilities") (date "2019-01-22") (name "Exploit.SMF.Agent.a") (value "2.864") (class "Malware") (platform "DoS") (description "Exploit
f-154 (MAIN:question (id 657) (nr 4) (country "Lithuania") (type "Vulnerabilities") (date "2019-01-22") (name "Exploit.Win32.BypassUAC") (value "2.864") (class "Malware") (platform "DoS") (description "Exp
f-155 (MAIN:question (id 658) (nr 5) (country "Lithuania") (type "Vulnerabilities") (date "2019-01-22") (name "Exploit.HTML.IframeBof") (value "1.438") (class "Malware") (platform "DoS") (description "Expl
f-156 (MAIN:question (id 659) (nr 6) (country "Lithuania") (type "Vulnerabilities") (date "2019-01-22") (name "Exploit.Java.CVE-2012-1723.gen") (value "1.438") (class "Malware") (platform "DoS") (descripti
f-157 (MAIN:question (id 660) (nr 7) (country "Lithuania") (type "Vulnerabilities") (date "2019-01-22") (name "Exploit.Java.CVE-2013-0431.gen") (value "1.438") (class "Malware") (platform "DoS") (descripti
f-158 (MAIN:question (id 661) (nr 8) (country "Lithuania") (type "Vulnerabilities") (date "2019-01-22") (name "Exploit.AndroidOS.Lootor.cc") (value "1.438") (class "Exploit") (platform "AndroidOS") (descri
f-159 (MAIN:question (id 662) (nr 1) (country "Lithuania") (type "Web threats") (date "2019-01-22") (name "Trojan.Script.Miner.gen") (value "54.558") (class "Trojan") (platform "Script") (description "This
f-160 (MAIN:question (id 663) (nr 2) (country "Lithuania") (type "Web threats") (date "2019-01-22") (name "Trojan.Script.Generic") (value "25.894") (class "Trojan") (platform "Script") (description "This f
f-161 (MAIN:question (id 664) (nr 3) (country "Lithuania") (type "Web threats") (date "2019-01-22") (name "Trojan-Downloader.JS.Inor.a") (value "4.558") (class "Trojan-Downloader") (platform "JS") (descrip
f-162 (MAIN:question (id 665) (nr 4) (country "Lithuania") (type "Web threats") (date "2019-01-22") (name "Trojan-Clicker.HTML.Iframe.dg") (value "2.558") (class "Trojan-Clicker") (platform "HTML") (descri
f-163 (MAIN:question (id 666) (nr 5) (country "Lithuania") (type "Web threats") (date "2019-01-22") (name "Hoax.HTML.FraudLoad.m") (value "1.798") (class "Hoax") (platform "HTML") (description "This family
f-164 (MAIN:question (id 667) (nr 6) (country "Lithuania") (type "Web threats") (date "2019-01-22") (name "DangerousObject.Multi.Generic") (value "1.588") (class "DangerousObject") (platform "Multi") (desc
f-165 (MAIN:question (id 668) (nr 7) (country "Lithuania") (type "Web threats") (date "2019-01-22") (name "Trojan.Win32.Agent.vho") (value "1.438") (class "Trojan") (platform "Win32") (description "Malicio
f-166 (MAIN:question (id 669) (nr 8) (country "Lithuania") (type "Web threats") (date "2019-01-22") (name "Trojan.JS.Redirector.afx") (value "1.238") (class "TrojWare") (platform "Trojan-Spy") (description
f-167 (MAIN:question (id 670) (nr 9) (country "Lithuania") (type "Web threats") (date "2019-01-22") (name "Trojan.JS.Miner.y") (value "1.128") (class "Trojan") (platform "JS") (description "This family inc
f-168 (MAIN:question (id 671) (nr 10) (country "Lithuania") (type "Web threats") (date "2019-01-22") (name "Trojan.MSIL.Crypton.gen") (value "0.828") (class "Trojan") (platform "MSIL") (description "Malwar
For a total of 169 facts in module MAIN.

```

Fig. B.2. Example of the knowledge base import to the JESS expert system

```

JESS> (batch "Attack_Trees/JESS/RFID_Comm_Block_UATSV2.clp")
f-0 (MAIN::initial-fact)
f-1 (MAIN::program (phase initialization))
f-2 (MAIN::question (ident node-select) (text "Which node ID would you like to select?"))
f-3 (MAIN::question (ident slot-select) (text "Which slot would you like to modify? "))
f-4 (MAIN::question (ident modify-value) (text "What should the value be? ")) (answer nil)
f-5 (MAIN::question (ident main-menu) (text "What would you like to do? (l)ookup name, (m)odify data, (v)iew AT, (q)uit:"))
f-6 (MAIN::tree (tname "RFID Comm Block UATSV2") (rootnode "Block Communication"))
f-7 (MAIN::node (id 0) (name "Block Communication") (parent nil) (connector OR) (cost 0) (time 0) (measure FALSE) (children 1 14))
f-8 (MAIN::node (id 1) (name "Block Tag Reader") (parent 0) (connector OR) (cost 0) (time 0) (measure FALSE) (children 2 8 9 10))
f-9 (MAIN::node (id 2) (name "Shield Tag") (parent 1) (connector AND) (cost 0) (time 0) (measure FALSE) (children 3 5))
f-10 (MAIN::node (id 3) (name "Be in Vicinity of Tag") (parent 2) (connector OR) (cost 0) (time 0) (measure FALSE) (children 4))
f-11 (MAIN::node (id 4) (name "Secure Warehouse") (parent 3) (connector nil) (cost 0) (time 0) (measure TRUE) (children nil))
f-12 (MAIN::node (id 5) (name "Faraday Cage") (parent 2) (connector OR) (cost 0) (time 0) (measure FALSE) (children 6 7))
f-13 (MAIN::node (id 6) (name "Cage Around Reader") (parent 5) (connector nil) (cost 0) (time 0) (measure FALSE) (children nil))
f-14 (MAIN::node (id 7) (name "Cage Around Tag") (parent 5) (connector nil) (cost 0) (time 0) (measure FALSE) (children nil))
f-15 (MAIN::node (id 8) (name "Blocker Reader") (parent 1) (connector nil) (cost 0) (time 0) (measure FALSE) (children nil))
f-16 (MAIN::node (id 9) (name "Blocker Tag") (parent 1) (connector nil) (cost 0) (time 0) (measure FALSE) (children nil))
f-17 (MAIN::node (id 10) (name "Jam Signal") (parent 1) (connector OR) (cost 0) (time 0) (measure FALSE) (children 11))
f-18 (MAIN::node (id 11) (name "Isolate Network") (parent 10) (connector OR) (cost 0) (time 0) (measure TRUE) (children 12 13))
f-19 (MAIN::node (id 12) (name "Secure Warehouse") (parent 11) (connector nil) (cost 0) (time 0) (measure TRUE) (children nil))
f-20 (MAIN::node (id 13) (name "Faraday Around Tag and Reader") (parent 11) (connector nil) (cost 0) (time 0) (measure FALSE) (countermeasure TRUE) (children nil))
f-21 (MAIN::node (id 14) (name "Block Reader Backend") (parent 0) (connector OR) (cost 0) (time 0) (measure FALSE) (children 15))
f-22 (MAIN::node (id 15) (name "Dos in Network") (parent 14) (connector nil) (cost 0) (time 0) (measure FALSE) (children nil))
For a total of 23 facts in module MAIN.
What would you like to do? (l)ookup name, (m)odify data, (v)iew AT, (q)uit:

```

**Fig. B.3.** Example of automatically generated rules from attack trees successful import into JESS

```

/home/jess61p4
#Ar yra imoneje programines irangos kompiuteriams? (skaicius) 8
#Ar yra imoneje monitoringo sistema? (skaicius) 20
#Ar imoneje yra saugos specialistas/u? Kiek? (skaicius) 11
#Ar galimas KPK paplitimas irangoje? (taip ar ne) taip
#Ar yra imoneje atsarginio maitinimo saltiniu? (skaicius) 5
#Kiek imoneje darbuotoju? (skaicius) 9
#Ar gali buti sukciavimo atvejy(phishing)? (taip ar ne) ne
#Ar imone yra turejusi saugumo incidentu? (taip ar ne) taip
#Ar gali buti pavogta iranga? (taip ar ne) ne
#Ar yra imoneje serveriu? (taip ar ne) taip
#Ar gali kas nors atskleisti informacija? (taip ar ne) ne
#Ar yra imoneje multifunkciniu kopijavimo aparatu? (skaicius) 12
@@@Prasome atreipti demesi: Imone maza 13
#Ar imoneje atlikta rizikos analize? (taip ar ne) ne
#Ar gali nutikti aparatinis irangos gedimas? (taip ar ne) taip
#Kokia tikimybe tokiam ivykiui ivykti ? (Nurodykite tarpe 0-10,skaicius - t
)? (skaicius) 9
#Ar yra imoneje smulkios tinklo irangos? (skaicius) 16
#Ar gali nutikti nesankcionuota prieiga prie tinklo resursu? (taip ar ne)
#Ar yra imoneje specialios patalpos irangai? (skaicius) 10
#Ar imonei gali gresti saugumo incidentai? (taip ar ne) ne
#Ar yra imoneje kitokiu prietaisui? (skaicius) 11
#Ar yra imoneje daugiau nei vienas interneto tiekijas? (skaicius) 5
#Ar yra imoneje ugniasieniui? (skaicius) 15
#Ar yra imoneje nesiojamu irenginiu? (skaicius) 20
#Ar imoneje informacia klasifikuoti taikomos gaires? (taip ar ne) tai
#Ivertinkite desimtbaleje sistemoje imones atsparuma saugumo incidentams? (
)
#Ar yra imoneje irangos talpinimo sistemos? (skaicius) 10
#Ar yra imoneje valdymo irenginiu? (skaicius) 4
#Ar yra imoneje kompiuteriu? (taip ar ne) taip
***** 13
@@@Rekomendacijos pagrindas: Saugos specialistas turi taikyti mazai imonei
ugos politika.Saugos politika turi buti pritaikyta mazai imonei.$$$$ ne
waste_0000Corsair /home/jess61p4
$ ./b.sh
Iveskite ataskaitos pavadinima
ataskaita
Ataskaitos failas ataskaita.txt
Testas baigtas
waste_0000Corsair /home/jess61p4
$

```

```

EditPad Lite 7 - [C:\cygwin64\home\jess61p4\at
File Edit Search Go Block Extra Convert Options View Help
ataskaita.txt ESv3.clp
@@@Rekomendacijos pagrindas: Reikalinga saugumo politika ir part-time specialistas sa
7
#Ar yra vykdoma nuodugni riziku identifikacija susijusi su isoriniu saliu teikiamomis
@@@Rekomendacijos pagrindas: Reikalinga saugumo politika ir part-time specialistas sa
#Ar imoneje taikoma fiziniu iejimu kontrole? (taip ar ne)
#Ar imoneje aprasyta turto valdymo politika? (taip ar ne) taip
#Ar yra imoneje specialios patalpos irangai? (skaicius) ne
#Ar priejimo teisiu nuraukimas su nutraukiamais asmenimis yra valdomos lygiagrečiai nu
#Ar imoneje yra patvirtinta ir taikoma saugos politika? (taip ar ne) taip
#Ar imoneje kiekvienam darbuotojui yra priskirtos roles ir atsakomybes? (taip ar ne)
#Ar visi atsakingi asmenys turi valdytoju kontaktus? (taip ar ne) 9
#Ar imoneje egzistuoja koofidencialumo sutartys? (taip ar ne) 10
#Ar imoneje visas turtas inventorizuotas? (taip ar ne) taip
#Ar yra imoneje monitoringo sistema? (skaicius) 19
#Ar imones patalpos isskirtos i vidinius ir viesus segmentus? (taip ar ne) ne
#Ar apibreztos SLA,RPO,RTO reiksmes sutartyse? (taip ar ne) 13
#Ar imoneje yra atsakingas asmuo uz saugumo politikos kooordinavima imones viduje? (ta
#Ar imoneje yra saugos specialistas/u? Kiek? (skaicius) ne
#Ar irangai priziureti taikomos proceduros ir jos atliekamos reguliariai? (taip ar ne)
#Ar imonei gali gresti saugumo incidentai? (taip ar ne) taip
@@@Prasome atreipti demesi: Imone vidutine taip
#Ar prasizenge darbuotojai apmokomi is naujo? (taip ar ne) ne
#Ar imoneje taikoma fizine perimetro apsauga? (taip ar ne) taip
#Ar reguliariai atliekama treciu saliu teikiamu paslaugu prieziura? (taip ar ne)
#Ar imone yra turejusi saugumo incidentu? (taip ar ne) 8
#Ar imoneje vykdoma informacijos klasifikacija? (taip ar ne) 11
#Ar taikomies saugumo procesams reikalingas valdytoju leidimas? (taip ar ne) taip
#Ar darbuotoju/treciu saliu sutarciai nutraukimui taikomos konkretios proceduros? (taip
#Kiek imoneje darbuotoju? (skaicius) 17
#Ar saugumo atsakomybes yra aiskiai ir tiksliai apibreztos kiekvienam darbuotojui? (ta

```

Fig. B.4. Example of automated testing of the expert system prototype