ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფის სამდონიანი მოდელი

ზურაბ ბოსიკაშვილი, ლოლიტა ბეჟანიშვილი, ზურაბ გოგიშვილი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

შემოთავაზებულია ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფის ერთიანი სამდონიანი მოდელის და პროგრამული ბაზის აგების კონცეფცია, რომელიც უზრუნველყოფს უსაფრხოების ამოცანების ეფექტურ მოდელირებას და ანალიზს. შესაბამისად მოდელი უნდა ასახავდეს როგორც ფორმალურ, ასევე არაფორმალურ ასპექტებს. მოდელის ასაგებად განიხილება სემანტიკური ვების მრავალშრიანი არქიტექტურა: **XML → RDF →Ontology (OWL) → Logic → Proof.** მოცემულია ფორმალიზმის საფუძველზე დასახულია შემუშავდეს ინფორმაციული სისტემის სისუსტეების ანალიზის პროგრამული ბაზა (ფრეიმვორკი), რომელიც უნდა წარმოადგენდეს უსაფრთხოების უზრუნველყოფის ერთიანი სისტემის ნაწილს. წარმოდგენილია მთლიანი სისტემის არქიტექტურა, საერთო სალტით დაკავშირებული პროგრამული ქვესისტემების სახით. საერთო სალტე რეალიზდება ვებ-სერვისებით და უზრუნველყოფს მონაცემების გაცვლას კანონიკურ, უნივერსალურ ფორმატში. შექმნილი პროგრამული ბაზით შესაძლებელი იქნება, როგორც სისტემების სისუსტეების ანალიზის მოდელირება, ასევე უსაფრთხოების უზრუნველყოფის სფეროში ცოდნის სტრუქტურიზაცია და ფაქტობრივი ცოდნის დაგროვება.

საკვანძო სიტყვები: ინფორმაციული უსაფრთხოება. სამდონიანი მოდელი. სემანტიკური ქსელი. სემანტიკური ვები. framework. digital asset. ინფორმაციული სისტემები.

1. შესავალი

ინფორმაციული და კომპიუტერული ტექნოლოგიების განვითარების თანამედროვე ეტაპზე, ენერგეტიკულ და გარემოს დაცვის პრობლემებთან ერთად, ერთერთ მნიშვნელოვან პრობლემას ინფორმაციული უსაფრთხოება წარმოადგენს. ეს განპირობებულია კომპიუტერული და ქსელური ტექნოლოგიების ადამიანის საქმიანობის ყველა სფეროში შეჭრით და აგრეთვე, დაგროვილი და გენერირებული ციფრული ინფორმაციის მოცულობის ექსპონენციალური ზრდით. უფრო მეტიც, ჩვენს სამყაროს შეიძლება ვუწოდოთ „გაფართოებადი ციფრული სამყარო“. კერძოდ, 2007 წელს შეიქმნა 282 ექსაბაიტი ინფორმაცია (1 ექსაბაიტი $=10^{18}$ ბაიტს), ანუ 10%-ით მეტი წინა წლის პროგნოზთან შედარებით. ახალი პროგნოზებით, 2012 წელს შეიქმნება 4,000-დე ექსაბაიტის მოცულობის ინფორმაცია — ეს ასტრონომიული რიცხვია.

ადამიანის საქმიანობა სულ უფრო დამოკიდებული ხდება ციფრულ გარემოზე და ამ სფეროში ნებისმიერმა შეფერხებამ შეიძლება მნიშვნელოვანი ზარალი მიაყენოს მას. ციფრული ინფორმაციის მოცულობის ზრდასთან ერთად იზრდება ინფორმაციის დატაცების, არასანქცირებული წვდომის, გამიზნული შეცვლის რისკები და მათი დანაშაულებრივი მიზნებით გამოყენების ცდუნებები. ეს პრობლემები კიდევ უფრო აქტუალური ხდება გლობალური ქსელების და ტექნოლოგიების არსებობის პირობებში. საფრთხეები მოსალოდნელია როგორც ქვეყნის შიგნიდან, ასევე გარედან. საქართველოში ინტერნეტში ჩართული მომხმარებლების რიცხვი 2012 წელს მილიონს გადააჭარბებს. აქედან გამომდინარე, კიდევ უფრო აქტუალურია მოქალაქეების საკუთრების ახალი ფორმის (ციფრული ინფორმაციის) დასაცავად სახელმწიფოს მიერ მნიშვნელოვანი ღონისძიებების ჩატარების ამოცანის ანალიზი და გადაწყვეტა.

ბოლო ხანებში, როგორც ჩვენს ქვეყანაში, ასევე საზღვარგარეთ, მნიშვნელოვანი სამუშაოები ტარდება კიბერუსაფრთხოების გაზრდის თვალსაზრისით, თუმცა პრობლემის სრულად გადაჭრამდე ჯერ კიდევ დიდი მანძილია გასავლელი, რადგანაც რთულდება სისტემები, იხვეწება შეტევების მეთოდები და მექანიზმები. შიდა თუ გარე კიბერ შეტევების ძირითად სამიზნეებს წარმოადგენენ სისტემის სისუსტეები, რომელთა საშუალებითაც ზეგავლენას ახდენენ სისტემების და მათი შემადგენელი კომპონენტების შეუფერხებელ მუშაობაზე, კონფიდენციალობაზე, მთლიანობაზე, უტყუარობაზე, ხელმისაწვდომობაზე და სხვა ასპექტებზე.

ნახ.1

ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფა პირველ რიგში მოიცავს სისუსტეების გამოვლენის და აღმოფხვრის ღონისძიებებს, შეტევების აღმოჩენის და აღკვეთის სამუშაოებს, რომელიც ციკლურ პროცესს წარმოადგენს (ნახ.1).

ზემოთ წარმოდგენილი პროცესი რთული და დინამიურია. ინფორმაციული სისტემების სისუსტეებზე და საფრთხეებზე ანალიზი კვალიფიციურ სპეციალისტებს და დიდ რესურსებს მოითხოვს. ამასთან სასურველია თუ აიგებოდა მოდელი და ავტომატიზირებული სისტემა, რომელიც ასეთ საქმიანობას გააადვილებდა. იმისთვის, რომ განხორციელდეს ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფის პროცესის სრულყოფა, საჭიროა მისი ადექვატური და ეფექტური მოდელის შექმნა. წარმოდგენილი პროცესი ძნელად ფორმალიზებადია, რადგანაც მასში გასათვალისწინებელია როგორც აპარატურულ-პროგრამული ასპექტები, ასევე ადამიანური ფაქტორები. შესაბამისად მოდელი უნდა ასახავდეს როგორც ფორმალურ, ასევე არაფორმალურ ასპექტებს. წარმოდგენილ სტატიაში ამ მიმართულებით შემოთავაზებულია იმ გამოცდილების გამოყენება, რაც დაგროვებულია ხელოვნური ინტელექტის სფეროში.

2. ძირითადი ნაწილი

ხელოვნურ ინტელექტში კარგად არის ცნობილი რთული ამოცანების ამოხსნის რედუქციული მეთოდი, როდესაც საწყისი ამოცანა დაიყვანება სხვა ცნობილ ამოცანათა მიმდევრობაზე, რომელთა ამოხსნა შესაძლებელია, ხოლო შემდეგ ცალკეულ ამონახსნთა სიმრავლეზე ხორციელდება მთლიანი ამოცანის ამოხსნა. წარმოდგენილ სტატიაში შემოთავაზებულ მნიშვნელოვან სიახლეს წარმოადგენს ინფორმაციული სისტემის უსაფრთხოების მოდელის რედუქცია ტესტური კონტროლის ზოგად მოდელში [1,5]. სისტემის გამართული მუშაობის კონტროლს. ტექნიკური სისტემების დიაგნოსტირების შემთხვევაში სისტემაში არსებული ხარვეზების გამოვლენა ხორციელდება სისტემის შემავალი ზემოქმედებების შერჩევით. შესაბამისად ტესტური კონტროლის ამოცანა შეიძლება გაიგივებული იქნეს სისუსტეების ანალიზის ამოცანასთან, ხოლო შემოჭრათა აღმოჩენის და ანალიზის ამოცანა - ტექნიკური დიაგნოსტირების ამოცანასთან. შესამაბისად ტესტური კონტროლის მეთოდოლოგია, მეთოდები და ალგორითმები შეიძლება გამოყენებული იქნას ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფის ამოცანებში. კერძოდ, აიგოს ცალკეული კომპონენტების და მთლიანად სისტემის მოდელები ბულის ფუნქციების ბაზაზე, რაც საშუალებას იძლევა უსაფრთხოების რიცხვითი მოდელირებისა.

სიახლეს წარმოადგენს ინფორმაციული სისტემის უსაფრთხოების უზრუნველყოფის ერთიანი პროცესის წარმოდგენა მოდელების იერარქიის სახით (ნახ.2). პირველი საფეხურის წარმოდგენა შესაძლებელია შემდეგი სახის ფორმალური მოდელით:

$$IS_1 = < S_0, S, F, G >,$$

სადაც S — ინფორმაციული სისტემის მდგომარეობის სივრცეა $S = X \times U \times Y$. ამ გამოსახულებაში U — შემავალი ზემოქმედებების სიმრავლეა, X — სისტემის შიდა მდგომარეობათა ამსახველი სიმრავლეა, Y — სისტემის რეაქციის ამსახველი სიმრავლეა, S_0 — სისტემის მდგომარეობათა სივრცის საწყისი მდგომარეობაა, F წარმოადგენს ოპერატორთა სიმრავლეს, რომელიც სისტემის მდგომარეობათა სივრცის ცვლილებებს ასახავს $F : X \times U \times Y \to U \times Y$, ანუ F არის მოდელირების ოპერატორი. G — მიზნობრივ მდგომარეობათა სიმრავლეა და იგი შეიძლება წარმოდგინდეს $G = \{s | B(s), s \in S\}$, სადაც B — პრედიკატია, რომელიც აიგება შემავალი ზემოქმედებებიდან და ამოცანებიდან გამომდინარე.

მეორე საფეხური ასახავს ინფორმაციული უსაფრთხოების სფეროში ცოდნის სტრუქტურიზაციას (ცნებებს, ცნებებს შორის კავშირებს, ობიექტების აღწერებს, ობიექტებს შორის კავშირებს, მიზეზ-შედეგობრივ დამოკიდებულებებს, გამოყვანის წესებს და კონკრეტულ ფაქტებს).

$$IS_2 = < B, C, R, W >,$$

სადაც $B = (O, A, V)$ ცნებების სიმრავლეა, რომელიც წარმოდგება „ობიექტი-ატრიბუტი ნიშვნელობა“ სამეულის სახით, $C = (B \times B \times ... \times B)$ მიმართებების სიმრავლეა, R დასკვნების კეთების წესების სიმრავლეა, ხოლო W ფაქტების სიმრავლეა. ზოგადი ინფორმაცია წარმოდგება სემანტიკური ქსელების სახით, ხოლო ფაქტები ინახება მონაცემთა ბაზაში.

მესამე საფეხური ასახავს უსაფრთხოების პროცესის უზრუნველყოფის ოპერაციულ სემანტიკას, რომლის საშუალებითაც რიცხობრივად აღიწერება სისტემის კომპონენტების ფუნქციონირება ლოგიკური ფუნქციების

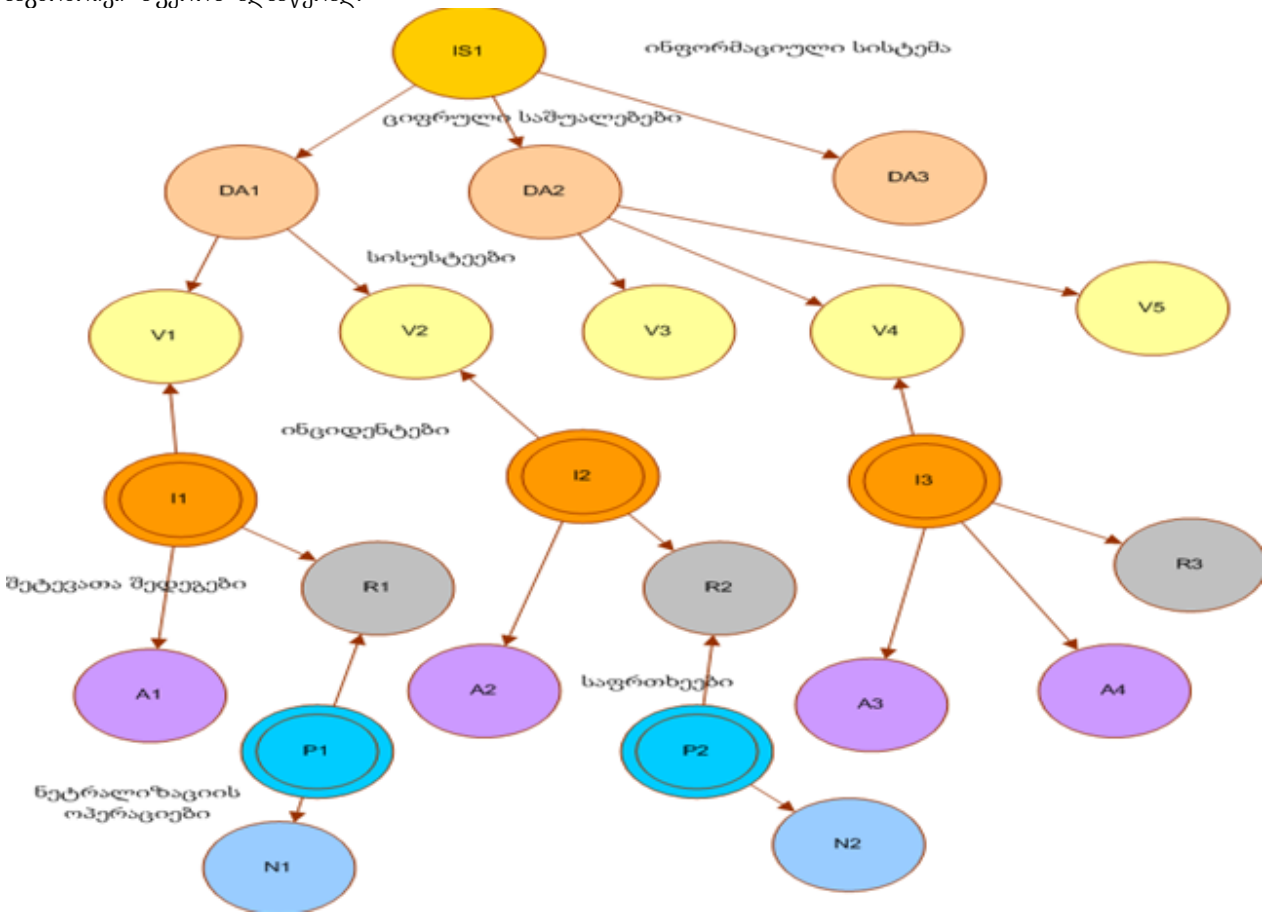
საშუალებით, რომელიც საშუალებას იძლევა განხორციელდეს სისტემის იმიტაციური მოდელირება და სისტემის მახასიათებლების რიცხობრივი დათვლა. შემოთავაზებულია აგებული მოდელების საფუძველზე შემუშავდეს პროგრამული ბაზა (framework), ინფორმაციული სისტემების სისუსტეების ანალიზის პროცესების მოდელირებისთვის. კვლევის ობიექტებს წარმოადგენს ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფის და მასში შემავალი სისუსტეების ანალიზის პროცესები, მათი ერთიანი იერარქიული მოდელების აგების მეთოდოლოგია, მეთოდები და ალგორითმები, რომელიც გულისხმობს ფორმალური, ონთოლოგიური და ოპერაციული მოდელების შექმნას, სისტემის უსაფრთხოების ანალიზის პროგრამული ბაზის აგების პრინციპები და მეთოდები.

3. უსაფრთხოების ონთოლოგიური მოდელი

ეს მოდელი გულისხმობს უსაფრთხოების უზრუნველყოფის პროცესის სემანტიკური ქსელების საშუალებით წარმოდგენას. მოდელის ასაგებად შემოთავაზებულია სემანტიკური ვების მრავალშრიანი არქიტექტურის გამოყენება:

XML→RDF→Ontology (OWL) →Logic →Proof.

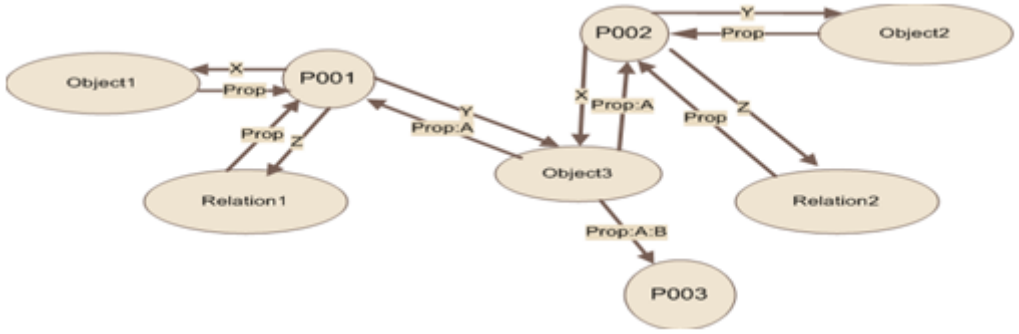
RDF წარმოადგენს რესურსების აღწერის ფორმატს Subject-Predicat-Object (არსი-პრედიკატი-ობიექტი) სამეულის სახით. ონთოლოგიის საშუალებით აღიწერება ცნებები და მათთან დაკავშირებული პროცესები. Logic და Proof უზრუნველყოფს ინფორმაციის ლოგიკურ წარმოდგენას და ლოგიკური დასკვნების კეთების მექანიზმებს. ეს ფორმალიზმი უნივერსალურია და შეიძლება გამოყენებული იყოს ნებისმიერი საგნობრივი სფეროს აღსაწერად.



ნახ.3

ცოდნის გამომსახველობითი უნარის და ძებნის მექანიზმების სიმძლავრის გაზრდისთვის სტატიაში შემოთავაზებულია კონტექსტურად მართვადი სემანტიკური ქსელების გამოყენება (ნახ.4). მისი რეალიზაცია ადვილად ხორციელდება RDF-სქემების საშუალებით. დავუშვათ, გვსურს A:B კონტექსტში მოიძებნოს

ინფორმაციული სისტემის კომპონენტი, რომელიც Object1 კომპონენტთან იმყოფება Relation1 მიმართებაში. ობიექტზე მიმართვა ჩაიწერება შემდეგი ბუნებრივ ენასთან მიახლოებული ფორმით (A:B/Relation1(Object1,?X)). ინფორმაციის მოძებნა სემანტიკურ ქსელში ხორციელდება შემდეგნაირად: პირველად მოცემული კონტექსტისთვის მოიძებნება Relation1 და Object1-თან დაკავშირებული P00? წვეროების სიმრავლეების თანაკვეთა და მოძებნილი წვეროებისთვის Z მიმართებით იძებნება მიზნობრივი.



ნახ.4

თუ მოცემულ კონტექსტში ვერ მოხდა ინფორმაციის მოძებნა, მაშინ ფართოვდება კონტექსტი (მაგ: A/) და ინფორმაცია იძებნება ხელმეორედ. კონტექსტზე შეიძლება დაიდოს ნებისმიერი ხისებრი სტრუქტურა. შემოთავაზებული სემანტიკური წარმოდგენით შეიძლება აღიწეროს, როგორც ფაქტობრივი ცოდნა, ასევე პროცესები.

4. სისტემის არქიტექტურა

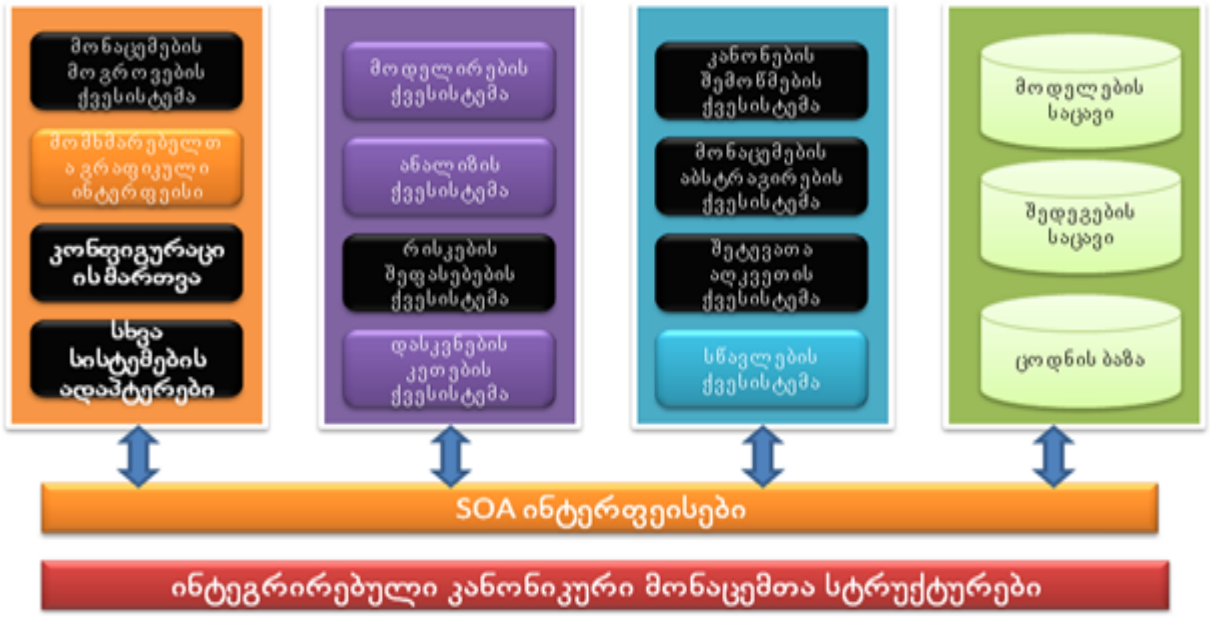
სტატიაში შემოთავაზებული ფორმალიზმის საფუძველზე დასახულია ინფორმაციული სისტემის სისუსტეების ანალიზის პროგრამული ბაზის (ფრეიმვორკი) შემუშავება, რომელიც უნდა წარმოადგენდეს უსაფრთხოების უზრუნველყოფის ერთიანი სისტემის ნაწილს. ამიტომ სტატიაში წარმოდგენილია მთლიანი სისტემის არქიტექტურა, შემოთავაზებული ბაზის ადგილის მითითებით.

არსებული უსაფრთხოების სისტემები ძირითადად ორიენტირებულია ერთ ფუნქციონალზე: შეღწევათა აღმოჩენაზე, სისუსტეების ანალიზზე, ან საფრთხეების განეიტრალებაზე. რადგანაც ასეთ სისტემებს საერთო პრაგმატიკა, საერთო მონაცემთა ბაზები აქვთ, ამიტომ შემოთავაზებულია ინტეგრირებული პროგრამული ბაზის (ფრეიმვორკი) შეიქმნა, რომელიც დამატებით აღიჭურვება მე-5 ნახაზზე ნაჩვენები ფუნქციონალობებით.

ნახ.5

მე-6 ნახაზზე მოყვანილია შემოთავაზებული ფრეიმოვარკის არქიტექტურა. სისტემა აიგება საერთო სალტით დაკავშირებული ქვესისტემების სახით. სერთო სალტე რეალიზირდება ვებ სერვისების სახით და უზრუნველყოფს მონაცემების გაცვლას კანონიკურ, უნივერსალურ ფორმატში. მთლიანი სისტემის რეალიზაცია დიდ რესურსებს მოითხოვს და შეიცავს მისი განხორციელების დიდ რისკებს. ამიტომ შემოთავაზებულია აიგოს

სისტემის მხოლოდ ნაწილი, რომელიც ნახატზე ფერებითაა ნაჩვენები, ხოლო სისტემის სრული რეალიზაცია განხორციელდეს შემდგომ ეტაპზე.



ნახ. 6

3. დასკვნა

კვლევის მოსალოდნელი შედეგები:

- დამუშავდება ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფის პროცესების მოდელირების საფუძვლები, რომელზედაც შეიძლება დაშენება შემდგომი კვლევებისა ამ მიმართულებით;
- შეიქმნება პროგრამული ბაზა სისუსტეების გამოვლენის და ანალიზის პროცესების მოდელირებისა, რომელიც იქნება გაფართოებადი (შესაძლებელი იქნება ახალი ფუნქციონალობების დამატება);
- შექმნილი პროგრამული ფრეიმვორკი შეიძლება გამოყენებული იქნეს ინფორმაციული ტექნოლოგიებში მომუშავე ნებისმიერი ორგანიზაციების მიერ, როგორც უსაფრთხოების პროცესების მოდელირებისთვის, ასევე პერსონალის სწავლებისთვის;
- შექმნილი პროგრამული ბაზით შესაძლებელი იქნება, როგორც ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფის სფეროში ცოდნის სტრუქტურიზაცია, ასევე ფაქტობრივი ცოდნის დაგროვება;

ლიტერატურა:

1. Bosikashvili Z., Kapanadze D., Zhvania T. “About Unified Model of Safety of Information Systems”. Reacent Advances in Computational Intelligance Proceedings of the 4yh WSEAS International Conference on COMPUTATIONAL INTELLIGENCE (CI’10). Universitataea Politehnica, Bucharest, Romania, April 20-22, 2010. Pg. 35-38;

2. Bosikashvili Z , The blocking meta-heuristics for combinatorial problems solving, The ACM Digital Library, World Scientific and Engineering Academy and Society (WSEAS) Stevens Point, Wisconsin, USA ©2010 ISBN: 978-960-474-179-3

3. Bosikashvili Z , Lominadze.T,Factorization of combinatorial problems with blocking meta-heuristics, The ACM Digital Library, World Scientific and Engineering Academy and Society (WSEAS) Stevens Point, Wisconsin, USA ©2009 ISBN: 978-960-474-088-8

4. Bosikashvili Z., Kapanadze D., Zhvania T., About formalization of the problem of the test control, Transactions Automated Control Systems #1(2), GTU, Tbilisi, 2007.

5. Karibskiy V.V., Etc., Technical diagnostics of objects of the control, M.: Energya, 1967;

6. Peter. R. Stephenson, A Formal Model for Information Risk Analysis Using Colored Petri Nets, http://www.daimi.au.dk/CPnets/workshop04/cpn/papers/stephenson.pdf;

THE THREE-TIER MODEL FOR THE INFORMATION SYSTEMS SECURING

Bosikashvili Zurab, Bejanishvili Lolita, Gogishvili Zurab
Georgian Technical University

Summary

At the present stage of development of information and computer technologies the humankind activity increasingly becomes dependent on the digital environment and any delay in this area can cause significant damage to it. In the conditions of global networks and technologies the risk of theft, unauthorized access, single-minded modifying information and attempts of its use with criminal purpose grows.

The primary objective of cyber attacks are vulnerabilities in the systems through which have an impact on the smooth operation of the system and its constituent components, to impact on the confidentiality, integrity, authenticity and reliability of data and other aspects. Maintenance of safety of information systems, first of all, includes arrangements on detection of weaknesses and their elimination, cyclic works on detection and suppression of attacks. The article proposed an approach that helps professionals in solving the problem, because the presented process is difficultly formalizable.

The article proposed a unified three-tier model and framework to ensure the security of information systems. Accordingly, the model should display both formal and informal aspects. To build the model we suggest to use multi-layer architecture for Semantic Web:

XML → RDF →Ontology (OWL) → Logic → Proof

Using formalism the article proposed to define a basic software development (the so-called framework) for information systems vulnerability analysis, which should be a part of the unified security management system. The article represented a system architecture, showing the location of the proposed framework in the system. The framework will make it possible to use as the simulation of system vulnerabilities analysis, and structuring and accumulation of factual knowledge in the area of the information systems security.

ТРЕХУРОВНЕВАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Босикашвили З., Бежанишвили Л., Гогишвили З.
Грузинский Технический Университет

Резюме

На современном этапе развития информационных и компьютерных технологий деятельность человечества все больше становится зависимой от цифровой среды, и любые помехи в этой области могут нанести значительный ущерб. В условиях глобальных сетей и технологий растет риск краж, несанкционированного доступа, целеустремленного изменения информации и попытки её использования в преступных целях.

Основная целью кибератак являются уязвимости систем. Обеспечение безопасности информационных систем, прежде всего, включает в себя механизмы обнаружения недостатков и их ликвидации, циклические работы по выявлению и пресечению нападений. Эта статья предлагает такой подход, который поможет специалистам в решении этой проблемы. Предложено создание единой трехуровневой модели и framework-а для обеспечения безопасности информационных систем. Для построения модели предлагается использование многоуровневой архитектуры семантического Web-а:

XML → RDF →Ontology (OWL) → Logic → Proof

Используя формализм в статье предлагается разработка базового программного обеспечения (так наз. framework) для анализа уязвимости информационных систем, которое должно быть частью объединенной системы обеспечения безопасности.