ინფორმაციის უსაფრთხოების პრობლემები სპეციალიზებულ კომპიუტერულ ქსელებში

ზურაბ გასიტაშვილი, გიორგი მაისურაძე, ლევან ჯიქიძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია კომპიუტერული ქსელების დაცვის საკითხები, მოყვანილია კომპიუტერული ქსელების საფრთხეთა კლასიფიკაცია. შემუშავებულია ინფორმაციის დაცვის პრიორიტეტებიდან გამომდინარე კლასიფიკაცია. საფრთხეების თავიდან ასაცილებლად განხილულია მისი მოდელის შექმნის საკითხები.

საგასაღებო სიტყვები: კომპიუტერული ქსელის დაცვა. კომპიუტერული ქსელის დაცვის მოდელირება, კომპიუტერული სისტემის დაცულობის ანალიზი.

1. შესავალი

კომპიუტერული ქსელების მომხმარებლების ზრდასთან ერთად შემცირდა მომხმარებლების კვალიფიციურობის დონე, კომპიუტერული ქსელი მისაწვდომი გახდა რიგითი მომხმარებლებისთვის. ამ გარემოებამ კი მნიშვნელოვნად გაუმარტივა საქმე ბოროტმოქმედს, რადგან არაკვლიფიციურ მომხმარებლებს არ შეუძლიათ მუდმივად აკონტროლონ თავისი სისტემის დაცვის ხარისხი, რადგან იგი საჭიროებს შესაბამის ცოდნას და გამოცდილებას ასევე დროს და საშუალებას. შედეგად კი - ორგანიზაციები, მათი ინფორმაციული სისტემები და ქსელები უფრო და უფრო მეტად ეჯახებიან სხვადასხვა სახის საფთხეს. კომპიუტერული ვირუსების გვერდით გაჩნდა ისეთი სახის საფრთხეები, რომლებიც საჭიროებს ბოროტმოქმედის მაღალკვალიფიცირებას.

დღეისათვის ორგანიზაციები სულ უფრო მეტად დამოკიდებული ხდება ინფორმაციულ სისტემებზე და შესაბამისად მეტად დამოკიდებული საფრთხეების გაზრდაზე. ეს შეეხება კლიენტ – სერვერ არქიტექტურასაც, რომელმაც ქსელური არქიტექტურა გადააქცია განაწილებულ გამომთვლელ გარემოდ. ამიტომ ქსელის უსაფრთხოება დამოკიდებული გახდა გამოთვლითი ტექნიკის ყველა ელემენტის უსაფრთხოებაზე.

განსაკუთრებით მკაცრი მოთხოვნები აქვს წაყენებული ყველა სპეციალიზებულ და მათ შორის სამხედრო დანიშნულების კომპიუტერული ქსელის დაცვის საკითხებს.

კომპიუტერული საფრთხეების თავიდან ასაცილებლად საწყის ეტაპზე მნიშვნელოვანია ჩატარდეს ამ საფრთხეთა მოდელირება. დადგინდეს, რა უნდა დაიცვას დაპროექტებულმა სისტემამ, ვისგან და რა დროის განმავლობაში. საფრთხეების მოდელის შექმნის პროცესში აუცილებელია მთელი ქსელის გათვალისწინება და არა მხოლოდ იმ მონაცემების, რომელთა დაცვა აუცილებელია. ჩვენ უნდა ვიცოდეთ, ვინ და როგორ გამოიყენებს სისტემას. რა არის დამრღვევის მოტივი ? აუცილებელია თავდასხმის თავიდან აცილება, თუ საკმარისი იქნება მისი მოგერიება ? თუ კომპიუტერული ქსელის დაზიანება მოხდა, როგორაა შესაძლებელი უსაფრთხოების სისტემის აღდგენა ?

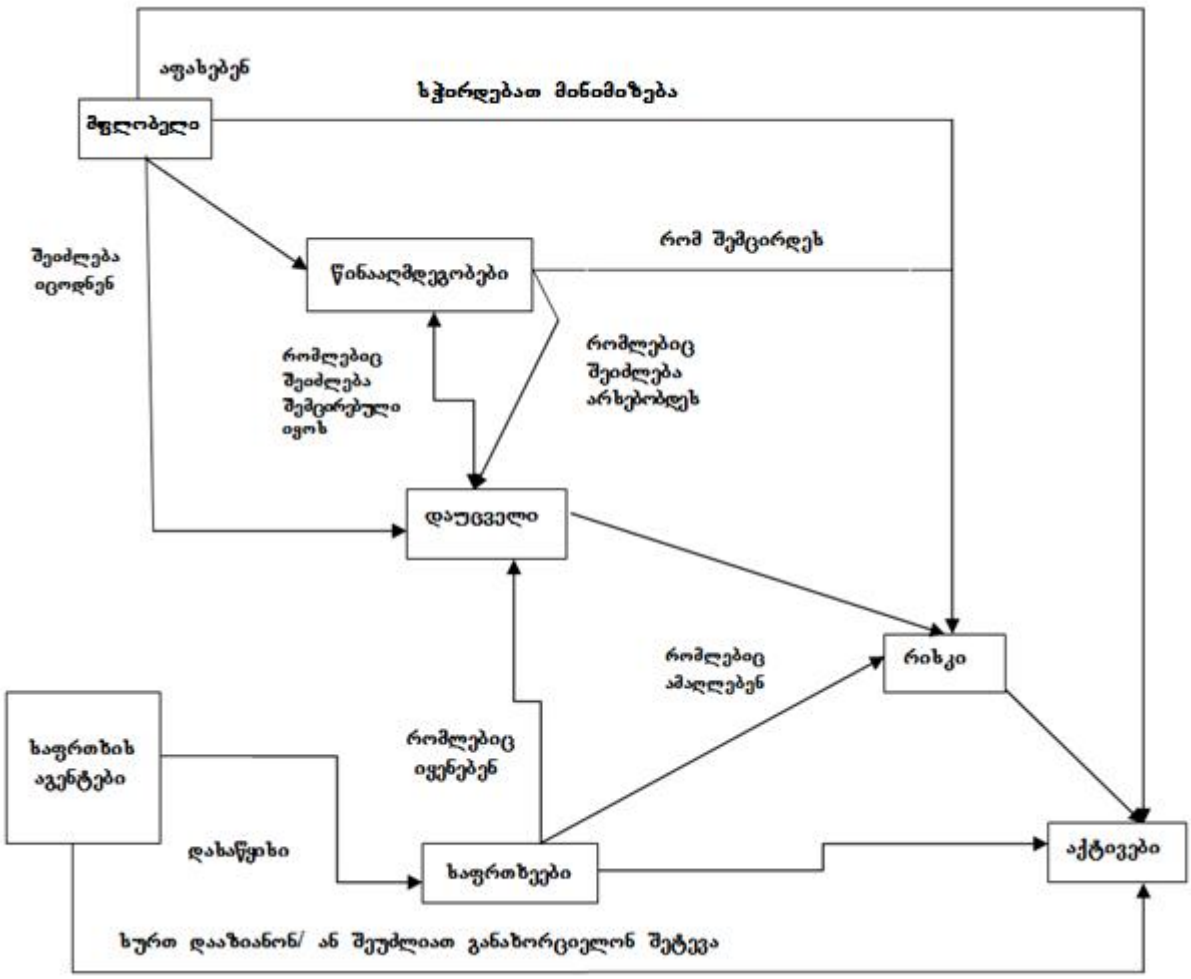
საფრთხეების მოდელირების გარკვეული სტანდარტები მოყვანილია [1,3] წყაროებში. ამასთანავე, საფრთხეთა რეალიზაციის თავისებურებანი თითოეული კომპიუტერული ქსელისთვის უნიკალურია.

2. ძირითადი ნაწილი

საფრთხეების მოდელი, დასაცავი ქსელის (ობიექტის) გამოკვლევის პროცესში მიღებული საწყისი მონაცემების საფუძველზე, საშუალებას აძლევს ინფორმაციის დაცვის სისტემის როგორც დამპროექტებლებს, ასევე მომხმარებლებს, დაადგინონ ინფორმაციული უსაფრთხოების სისტემის მიზნობრივი ფუნქცია და განსაზღვრონ, უსაფრთხოების უზრუნველყოფის რა საშუალებები სჭირდებათ. საფრთხეების მოდელი აუცილებელია აღწერდეს გარკვეული პირობების და

ფაქტორების წარმოშობის შესაძლებლობას, რაც ქმნის სპეციალიზებული კომპიუტერული ქსელის დაცულობაზე დესტრუქციული (არასანქცირებული, შემთხვევითი ან წინასწარ განზრახული) ზემოქმედების საფრთხეს ფუნქციონირების კონკრეტულ პირობებში. მის შემდეგ უსაფრთხოების მოდელი ქმნის ისეთი ღონისძიებების დაგეგმვის და განხორციელების საფუძველს, რომელთა დანიშნულებაა ინფორმაციის უსაფრთხოების უზრუნველყოფა სპეციალიზებულ ინფორმაციულ სისტემაში მისი დამუშავებისას.

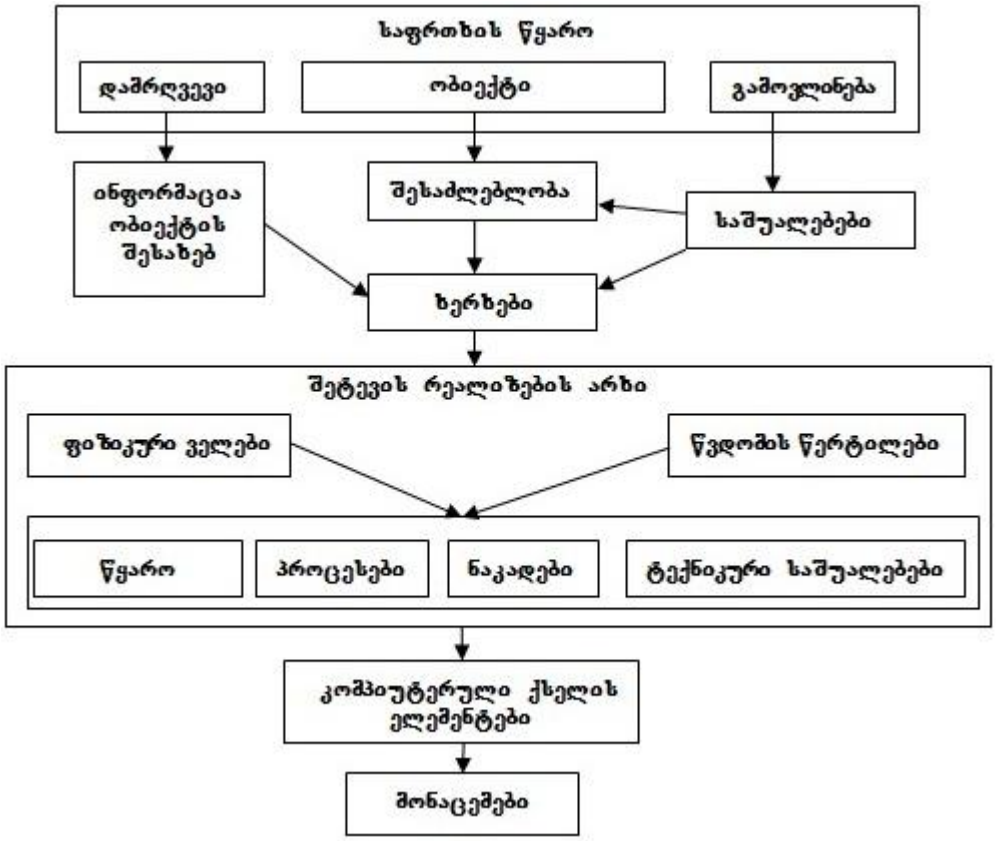
საფრთხეთა კლასიფიკაციისას, მხედველობაში უნდა მივიღოთ სხვადასხვა ხასიათის საფრთხეები, თუმცა როდესაც კომპიუტერულ ქსელში ინფორმაციის დაცვის სისტემის დამუშავება ხდება, ყველაზე მნიშვნელოვანი ადამიანის ქმედებებთან დაკავშირებული საფრთხეების გათვალისწინებაა [3]. უსაფრთხოების და საფრთხეთა ცნებების ურთიერთდამოკიდებულება ნაჩვენებია 1-ელ ნახაზზე.



ნახ.1

საფრთხეების მოდელი ფორმალურად შეიძლება აღიწეროს, როგორც „საფრთხეების წყაროს“, „საფრთხეების განხორციელების პოტენციური შესაძლებლობების“, „შესაბამისი საშუალებების არსებობის“, დაშვების არხის ან შეერთების წერტილის არსებობის თანაფარდობა. საფრთხეთა რეალიზაციის სქემა ნაჩვენებია მე-2 ნახაზზე.

საფრთხის რეალიზების მიზეზი ინფორმაციის უსაფრთხოების წინაშე არსებული საფრთხის რეალიზების არხის გაჩენაა. აღნიშნული არხი საფრთხის წყაროსა და ინფორმაციის მატარებელს (წყაროს) შორის ჩნდება, რაც ქმნის ინფორმაციული უსაფრთხოების დარღვევის (არა-სანქცირებული ან შემთხვევითი წვდომის) აუცილებელ პირობას.



ნახ.2. საფრთხეების რეალიზების სქემა

რეალიზების U არხის ძირითადი ელემენტებია:

- U წყარო –სუბიექტი, მატერიალური ობიექტი ან ფიზიკური მოვლენა, რომელიც ქმნის ui-ის;
- ინფორმაციის გავრცელების ან ზემოქმედების გარემო (გზები და არხები), სადაც ფიზიკური ველი, სიგნალი, მონაცემები ან პროგრამები ვრცელდება და ზემოქმედებს ინფორმაციის დაცულ მახასიათებლებზე (კონფიდენციალურობაზე, მთლიანობაზე, მიღწევადობაზე);
- კომპიუტერული ქსელის ელემენტები – ინფორმაციის მატარებლები, მატერიალური ობიექტები და ამ ობიექტების მიერ შექმნილი ფიზიკური ველი, სადაც ინფორმაცია პოვებს გამოხატულებას სიმბოლოების, სიგნალების, ტექნიკური გადაწყვეტილებების, პროცესების, ხარისხობრივი მახასიათებლების და ფიზიკური სიდიდეების სახით.

საფრთხის ძირითადი კრიტერიუმი მიყენებული ზიანის პოტენციალს წარმოადგენს. ამავდროულად, შეიძლება ითქვას, რომ არ არსებობს საფრთხეთა მოდელის ფორმირების შესახებ ერთიანი ხედვა. საფრთხეების მოდელის ფორმირებისათვის შემდეგი ეტაპები გამოიყოფა:

- საფრთხეების წყაროების იდენტიფიკაცია და დამრღვევის მოდელის შედგენა;
- კომპიუტერული ქსელის სუსტი წერტილების ანალიზი;
- საფრთხეების იდენტიფიკაცია;
- საფრთხის რეალიზების ალბათობის შეფასება;
- საფრთხის პოტენციალის შეფასება;
- საფრთხის აქტუალობის და რისკის მისაღებობის ხარისხის შეფასება.

საფრთხის აღწერას საფრთხის აგენტის (დამრღვევის) იდენტიფიკაციით იწყებენ, ხოლო შემდეგ მოდის თავდასხმის ალბათობის და თავდასხმის ობიექტი აქტივის შეფასება.

3. საფრთხეთა წყაროები და დამრღვევის მოდელი

იდენტიფიკაციას გარემოში არსებული ყველა საფრთხე კი არ ექვემდებარება, არამედ ისინი, რომლებიც გავლენას ახდენს კომპიუტერული ქსელის ექსპლუატაციის უსაფრთხოებაზე. საფრთხეების აღწერისას აუცილებელია აქტივების მიმართ არსებული ყველა საფრთხის გათვალისწინება, რომელთა წინააღმდეგ ხდება კომპიუტერული ქსელის ან მისი გარემოს დაცვის საშუალებების გამოყენება.

როგორც უკვე აღვნიშნეთ, საფრთხის წყარო შეიძლება იყოს სუბიექტი, მატერიალური ობიექტი ან ფიზიკური მოვლენა, რომელსაც შეუძლია ამა თუ იმ საფრთხის შექმნა.

საფრთხის რეალიზაცია რეალიზაციის არხის შექმნის შედეგია. აღნიშნული არხი იქმნება საფრთხის წყაროსა და ინფორმაციის მატარებელს შორის, რაც ქმნის ინფორმაციული უსაფრთხოების პოტენციური დარღვევის (არასანქცირებული ან შემთხვევითი წვდომის) აუცილებელ პირობებს.

საფრთხის რეალიზაციას დამრღვევი ახდენს, რაც იმას ნიშნავს, რომ საფრთხის რეალიზაციის პოტენციალს განაპირობებს U წყაროების შესაძლებლობები. ამ უკანასკნელთა პოტენციალი თავის მხრივ დამოკიდებულია ინფორმაციისადმი არასანქცირებული ან შემთხვევითი წვდომის მეთოდების და საშუალებების არსებობაზე, რის შედეგადაც შესაძლებელია ინფორმაციის კონფიდენციალურობის (ასლის გაკეთება, არამართლზომიერი გავრცელება), მთლიანობის (განადგურება, შეცვლა) და ხელმისაწვდომობის (ბლოკირება) დარღვევა.

საფრთხის აგენტი (დამრღვევი) აუცილებელია აღიწეროს ისეთი ასპექტების გათვალისწინებით, როგორიცაა კომპეტენტურობა, ხელმისაწვდომი რესურსების რაოდენობა და მოტივაცია. განსაკუთრებით მნიშვნელოვანი ამოცანაა დამრღვევის იდენტიფიკაცია. სხვადასხვა წყაროებში ამა თუ იმ ტიპის დამრღვევებს მიაკუთვნებენ სხვადასხვა კატეგორიებს. მათ შორის არიან უცხო სახელმწიფოების სპეციალური სამსახურები, კრიმინალური სტრუქტურები, კონკურენტი ორგანიზაციები, არაკეთილსინდისიერი პარტნიორები და თანამშრომლები, ტერორისტები, ტერორისტული ორგანიზაციები, პროგრამული პროდუქტების ჰაკერები, ყოფილი თანამშრომლები და მომხმარებლები.

ობიექტის მოკვლევის პროცესში დადგენილი დაშვების სისტემის, ფიზიკური პირობების და დაცვის საშუალებების გათვალისწინებით დგინდება პირთა კატეგორია, რომელთაც შეუძლიათ ისარგებლონ სპეციალიზებული კომპიუტერული ქსელის სუსტი წერტილებით. ეს პირები ხვდებიან დამრღვევების ზემოთ დადგენილ კატეგორიებში იმისდა მიხედვით, თუ საფრთხეთა რეალიზების რა პოტენციალი გააჩნიათ.

საშიშროების წყარო	დამრღვევის ტიპი								შენიშვნა
	H1	H2	H 3	H4	H5	H6	H7	H8	
	±	+	+	+	±	+	+	+	

აგრეთვე გამოყოფენ კომპიუტერული ქსელის უსაფრთხოების დარღვევის ძირითად მოტივებს. მათ შორის არის შურისძიება, ფულადი სარგებელი (მიღებული ინფორმაციის გაყიდვის ხარჯზე), ხულიგნობა, ცნობისმოყვარეობა, პროფესიული თვითშეფასების ამაღლება და ა.შ.

ამგვარად, უკვე ამ ეტაპზე შესაძლებელია დამრღვევების დადგენილი ტიპების და საფრთხის წყაროების კატეგორიების ერთმანეთთან დაკავშირება, ეს კი უფრო ობიექტურ წარმოდგენას ქმნის მათ შესაძლებლობებზე, ზემოქმედების მეთოდებზე და დესტრუქციული ქმედების შედეგებზე.

მეთოდურ დოკუმენტებში გათვალისწინებულია პოტენციური დამრღვევების სიიდან სპეციალიზირებული ინფორმაციული სისტემების პრივილეგირებული მომხმარებლების ამოღება. ესენი არიან ადამიანები, ვინც ახორციელებს კომპიუტერული ქსელის ტექნიკური და პროგრამული საშუალებების მომსახურებას, მათ შორის კი კონფიგურირებას და მნიშვნელოვანი დოკუმენტების გადანაწილებას არაპრივილეგირებულ მომხმარებლებს შორის.

ესენი შეიძლება იყოს ლოკალური გამოთვლითი ქსელების ადმინისტრატორები, კომპიუტერული ქსელის სეგმენტების (ფრაგმენტის) უსაფრთხოების ადმინისტრატორები და კომპიუტერული ქსელის უსაფრთხოების ადმინისტრატორები, სისტემური ადმინისტრატორები, დამხმარე პროგრამების დეველოპერები და კომპიუტერული ქსელის ტექნიკურ მომსახურებაზე პასუხისმგებელი პირები.

H4-H9 კატეგორიის პირები, როგორც წესი, პოტენციურ დამრღვევთა სიაში არ შედიან, თუ:

– პოტენციური დამრღვევები მარტო მოქმედებენ, სწავლობენ დარღვევის მეთოდებს, ამზადებენ და ახორციელებენ თავდასხმას, თუმცა არ შეუძლიათ თავდასხმის საშუალებათა და მეთოდების მომზადების შეკვეთა სამეცნიერო-კვლევით ცენტრებზე, რომლებიც სპეციალიზებულია ინფორმაციის კრიპტოგრაფიული დაცვის საშუალებების დამუშავებასა და ანალიზზე;

– პოტენციური დამრღვევი არ ფლობს ინფორმაციას თავდასხმის ობიექტებზე და არ აქვს სრულყოფილი ინფორმაცია კავშირის ქსელებზე; ასევე არ ფლობს ინფორმაციას დამხმარე პროგრამული უზრუნველყოფის საწყის ტექსტებზე; არ გააჩნია დოკუმენტაცია ინფორმაციის კრიპტოგრაფიული დაცვის საშუალებების და მათი ფუნქციონირების გარემოს შესახებ;

– პოტენციურ დამრღვევს საფრთხის შემცველი საშუალებებიდან მხოლოდ თავისუფალ გაყიდვაში არსებული აპარატურული და პროგრამული კომპონენტები გააჩნია. გარდა ამისა, ინფორმაციულ სისტემაში გატარებული ორგანიზაციული და რეჟიმული ღონისძიებების შედეგად არ გააჩნია დამატებითი შესაძლებლობები და არ შეუძლია ინფორმაციის დაცვის კრიპტოგრაფიული საშუალებების ლაბორატორიული გამოკვლევა.

ამასთანავე, ბოლო ორი პირობის შესასრულებლად აუცილებელია შევადგინოთ იმ ცნობების ჩამონათვალი, რომლებიც საჭიროა შესაბამისი საფრთხის განსახორციელებლად. არდა ამისა, აუცილებელია ეს ცნობები შედარდეს შესაბამისი დამრღვევის შესაძლებლობებს, რაც მხოლოდ მას შემდეგ გახდება შესაძლებელი, როდესაც შედგენილ იქნება საფრთხეთა მოდელი.

4. დასკვნა

მოყვანილი მოსაზრებებიდან გამომდინარე, უსაფრთხოების დამრღვევებს საშტატო საშუალებების გამოყენება მხოლოდ კონტროლირებადი ზონიდან შეუძლიათ. გარდა ამისა, დამრღვევს შეიძლება ჰქონდეს ინფორმაციის კრიპტოგრაფიული დაცვის საშუალებების მხოლოდ თავისუფალ გაყიდვაში არსებული აპარატურული და პროგრამული კომპონენტები.

ვინაიდან საფრთხის რეალიზაციის ალბათობის კრიტერიუმი გახლავთ კავშირის არხების ხელმისაწვდომობა (როგორც კონტროლირებადი ზონის ფარგლებში, ასევე მის ფარგლებს გარეთ), რომლებიც არ არის დაცული ორგანიზაციულ-ტექნიკური საშუალებებით, ისევე როგორც საშტატო საშუალებების ხელმისაწვდომობა, მიზანშეწონილია დამრღვევისთვის არსებული ხელმისაწვდომობის ხარისხის შეფასება. სხვაგვარად რომ ვთქვათ, უნდა დავუშვათ, რომ დამრღვევი მხოლოდ საფრთხის შემცველი არხის ან საშტატო საშუალების ხელმისაწვდომობის შედეგად გაჩნდება.

კომპიუტერული ქსელების საფრთხეების შემუშავებული კლასიფიკაცია უნდა იყოს განხილული ინფორმაციის დაცვის პრიორიტეტებიდან გამომდინარე, არა მარტო

კონფედენციალობის, არამედ ინფორმაციის მთლიანობის (როგორიცაა, სიზუსტე, სასრულობა) და წვდომადობის (ოპერატიულობა, უწყვეტობა) მიხედვით.

ლიტერატურა:

1. Schneider B. Why Cryptography Is Harder Than it Looks. Ppersonaluri veb gverdi www. Schneider.com/essay-037.ht6ml

2. Stang D.J., Moon S. Network Security Secrets. IDG Books Worldwide 2009

3. Анин Б.Ю. Защита компьютерной информации. СПБ. Петербург. 2010. ISBN 5-8206-0104-1.

PROBLEMS OF SECURITY OF INFORMATION IN SPECIALIZED COMPUTER NETWORKS

Gasitashvili Zurab, Maisuradze Giorgi, Jiqidze Levan

Georgian Technical University

Summary

The article discusses issues related to the protection of computer networks. There is given the classification of dangers of computer networks. It is developed the classification for information security priorities. The article deals with threats to prevent the creation of the model, the main issues that need to meet the model.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В СПЕЦИАЛИЗИРОВАННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Гаситашвили З., Майсурадзе Г., Джикидзе Л.

Грузинский Технический Университет

Резюме

Рассматриваются вопросы, связанные с защитой компьютерных сетей. Дается классификация опасностей компьютерных сетей. Разработана классификация с учетом приоритетов защиты информации. Рассматриваются вопросы создания модели с целью предотвращения возможных угроз.