საინფორმაციო სისტემების უსაფრთხოების ინფრასტრუქტურის დაგეგმარება

კახაბერ ჟამურაშვილი, რომან სამხარაძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განიხილება საინფორმაციო სისტემების უსაფრთხოების ინფრასტრუტურის დაგეგმარების პრობლემები და მათი გადაჭრის საკითხები. კერძოდ, შემოთავაზებულია თანამედროვე პროგრამული გადაწყვეტილებები. შედეგად, შესაძლებელი ხდება ინფორმაციის ელექტრონულად გადაცემა. ეს უკანასკნელი უკვე თავისთავად გულისხმობს იმას რომ რამდენჯერმე იზრდება ინფორმაციის გადაცემის სისწრაფე, პრინტერებისა და სხვა აპარატურული მოწყობილობების ქსელში გაზიარება, რაც ამცირებს არასასურველი აპარატურის რაოდენობას. გარდა ამისა, შესაძლებელი ხდება შეიქმნას ელექტრონული საფოსტო სისტემა, რაც ბევრად ამარტივებს და აჩქარებს კომპანიაში მიმდინარე პროცესებს. ინფორმაციული ინფრასტრუქტურის განვითარების შედეგად მარტივდება კომუნიკაცია თანამშრომლებს შორის, გადაწყვეტილებების მიღების პროცესი ბევრად უფრო ეფექტურად და სწრაფად მიმდინარეობს, გაცილებით ადვილია შექმნილ ელექტრონულ საბუთებთან ურთიერთობა და შემდგომში მათი მოძიება.

საკვანძო სიტყვები:საინფორმაციო სისტემები. უსაფრთხოება. ლოკალური ქსელი. აპარატურული უზრუნველყოფა. პროგრამული უზრუნველყოფა.

1. შესავალი

კომპიუტერული ლოკალური ქსელის არსებობა აუცილებელია თანამედროვე ორგანიზაციებისათვის, სადაც მნიშვნელოვანია, რომ ოპერატიულად და ცენტრალიზებულად მოხდეს ინფორმაციის დამუშავება და შესაბამისად, ინფორმაციას განესაზღვროს გრიფი. იმავდროულად, ლოკალური ქსელი რთული საკაბელო სისტემაა, რომლის გაერთიანებისა და ფუნქციონირებისთვის უამრავი კომპონენტია საჭირო. აქედან გამომდინარე, აუცილებელია კვალიფიციური და სწორი მიდგომა ინფორმაციული ინფრასტრუქტურის დაპროექტებისა და შემდგომ, მისი მონტაჟის დროს.

2. ძირითადი ნაწილი

ლოკალური გამომთვლელი ქსელი(LAN) აპარატურებისა და პროგრამული მომსახურების ერთობლიობაა, რომელიც კომპიუტერებს აერთიანებს ერთიან გამანაწილებელ სისტემად, ინფორმაციის დამუშავებისა და შენახვის საშუალებად. აპარატურულ უზრუნველყოფად შეიძლება ჩაითვალოს კომპიუტერები, რომლებსაც აქვთ ქსელური ადაპტერები, სვიჩები, როუტერები, IP ტელეფონები, სერვერები და ყველა ის მოწყობილობა, რომელსაც ამა თუ იმ გზით აქვს ქსელში წვდომა და შეუძლია ინფორმაციის დამუშავებაში გარკვეული მონაწილეობის მიღება [1].

პროგრამულ უზრუნველყოფას წარმოადგენს ყველა ის პროგრამა, რომელიც გამოიყენება ინფორმაციის დამუშავების, გადაცემის, შიფრაციისა და სხვა სამუშაოებისთვის. მაგალითისთვის შეიძლება მოვიყვანოთ:VPN (ვირტუალური კერძო ქსელი) – პროგრამული უზრუნველყოფა, რომელიც მოშორებული კომპიუტერისთვის ინფორმაციის უსაფრთხოდ გადაცემის საშუალებას იძლევა. ამ ტიპის ქსელი სპეციალური შიფრაციის მეთოდებითაა დაცული.

Microsoft SQL Server – პროგრამული პროდუქტი, რომელიც ცენტრალიზებულად და ონლაინ რეჟიმში ინფორმაციის დამუშავების საშუალებას იძლევა. ინფორმაციის დამუშავების და შენახვის

ეს პროგრამული პროდუქტი ძალზე ეფექტურად გამოიყენება მცირე და საშუალო ზომის დაწესებულებებში.

დღეისათვის ინფორმაციული ტექნოლოგიები აქტიურად გამოიყენება თითქმის ყველა სფეროში. ყველა ორგანიზაციასა და დაწესებულებას გააჩნია გარკვეული საინფორმაციო ბაზა, რომლითაც ისინი ხელმძღვანელობენ და იღებენ გადაწყვეტილებებს. ხშირ შემთხვევებში ეს ინფორმაცია კონფიდენციალურია, რომელზეც მხოლოდ გარკვეულ პირებს აქვთ წვდომა. ეფექტური, უსაფრთხო და დაცული ინფორმაციული ინფრასტრუქტურის შესაქმნელად აუცილებელია თანამედროვე ორგანიზაციებში შესაბამისი ინფორმაციული სისტემების დანერგვა.

ინფორმაციის დამუშავების ავტომატიზება, ინფორმაციის დამუშავების მეთოდებისა და ფორმების გართულება პირდაპირპროპორციულად არის დამოკიდებული მომხმარებლის მიერ მოთხოვნილ უსაფრთხოების საიმედოობაზე. რაც უფრო საიმედოა ინფორმაციის დაცვის სისტემა, მით უფრო რთულია დაცვის მეთოდები და ფორმები. ყოველგვარი ინფორმაციული უსაფრთხოების მხარდაჭერა პირდაპირ არის დაკავშირებული ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკასთან [2].

ჩატარებულმა კვლევებმა აჩვენა, რომ ჯერ კიდევ ბოლომდე არ არის შესწავლილი და დადგენილი ის სტანდარტები, რომლებიც სრულად უზრუნველყოფს ინფორმაციის უსაფრთხოებას. ინფორმაციის უსაფრთხოების საკითხები სულ უფრო და უფრო აქტუალური ხდება თითქმის ყველა თანამედროვე ორგანიზაციისთვის. ამის გამო, ორგანიზაციები ხშირად ქირაობენ სპეციალურ კომპანიებს/სპეციალისტებს თავიანთი ორგანიზაციების უსაფრთხოების შემოწმების მიზნით.

გარკვეული ტიპის დაწესებულებებს, მაგალითად, სააქციო საზოგადოებებს, ხშირ შემთხვევაში, აქვთ მთელი რიგი განყოფილებები, დაკომპლექტებული პროფესიონალებით, რომლებიც უზრუნველყოფენ უსაფრთხოების ნორმების, ჩარჩოების გამართვას და მათ სრულფასოვან ფუნქციონირებას.

დღეისათვის ეს სფერო ჯერ კიდევ განვითარების ეტაპზეა და საგრძნობი პოპულარობით განსაკუთრებით დიდ ორგანიზაციებში სარგებლობს. იმისათვის რომ შესაძლებელი იყოს ინფორმაციაზე წვდომის კონტროლი, აუცილებელია როგორც აპარატურული, ისე პროგრამული საშუალებების ეფექტურად ფუნქციონირება.

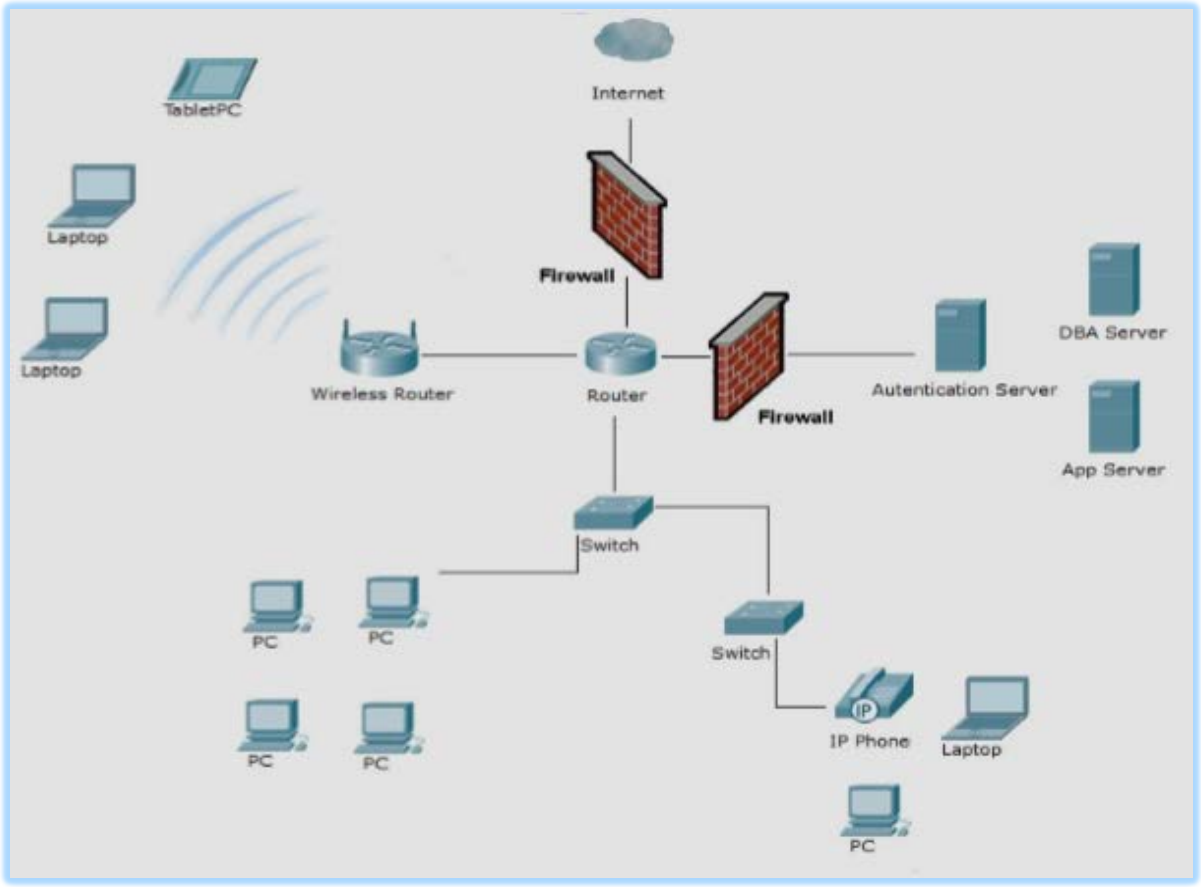
1-ელ ნახაზზე ნაჩვენებია, როგორ უნდა იყოს გამართულიინფორმაციული ინფრასტრუქტურა მცირე ორგანიზაციებში, აპარატურული და პროგრამული საშუალებების მინიმალური ნაკრების გამოყენებით.

ასეთი სისტემა იდეალურია მცირე ზომის ობიექტისთვის, რომელსაც სავსებით დააკმაყოფილებს გამოყენებული აპარატურის წარმადობა.

დავახასიათოთ მოკლედ თითოეული მათგანი [3]:

- **Firewall**(ბრანდმაუერი) – აპარატურული ან პროგრამული უზრუნველყოფაა, რომელიც ახორციელებს მასში შემავალი პაკეტების ტრაფიკის კონტროლს და ფილტრაციას. მისი ძირითადი ამოცანა ლოკალური ქსელის ან მისი ცალკეული კვანძების არასანქცირებული წვდომისგან დაცვაა. ის კრძალავს არაავტორიზირებულ წვდომას და ნებას რთავს მხოლოდ ავტორიზებულ კავშირს როგორც ქსელიდან გამავალ პაკეტებზე, ასევე ქსელში შემავალ პაკეტებზე. ორგანიზაციამ, რომელსაც ჯერ კიდევ არა აქვს ჩამოყალიბებული ინფორმაციული უსაფრთხოების ინფრასტრუქტურა, სწორედ ამ მექანიზმის დანერგვით უნდა დაიწყოს;

- **Authentication server** (აუთენტიფიკაციის სერვერი) – შესაძლებლობას გვაძლევს შევქმნათ მოქნილი იერარქია ჩვენი გარემოსათვის.



ნახ.1. საინფორმაციო სისტემების უსაფრთხოების ინფრასტრუქტურა.

მთავარ ადმინისტრატორს, მისი გამოყენებით, შეუძლია გარკვეული უფლებების დელეგირება მოახდინოს ადგილობრივ ადმინისტრატორებზე, გუნდის წევრებზე ან ჯგუფებზე;შესაძლებელია იერარქია აიგოს ნებისმიერი სასურველი გზით - გეოგრაფიული ადგილების, ქვეგანყოფილებების, ზოდიაქოს ნიშნების და ა.შ. მიხედვით; აგრეთვე უზრუნველყოფს ქსელში კომპიუტერებისა და მომხმარებლების კონტროლს;

- **Switch** (სვიჩი) –სხვადასხვა ქსელური მოწყობილობის ქსელში ჩართვის საშუალებას იძლევა. გარდა ამისა, მისი ერთ-ერთი ფუნქციაა დეტექტირება მოახდინოს და ქსელში შეუშვას მხოლოდ საჭირო აპარატურა;

- **Router**(როუტერი) –უზრუნველყოფს ქსელში არსებული პაკეტების მარშრუტიზებას, რაც მთელი სისტემისთვის უმთავრესი ამოცანაა. ის უნდა იყოს მაქსიმალურად ძლიერი იმისათვის, რომ შეძლოს მასთან მისული ინფორმაციის სრულად დამუშავება;

- **DBA სერვერზე** ინახება ყველა ის ინფორმაცია, რომელიც გააჩნია დაწესებულებას;
- **App სერვერის** არსებობა მნიშვნელოვანია ინფორმაციის შეგროვება – დამუშავებისთვის.

3. დასკვნა

ზემოთ განხილული კომპონენტების გარეშე ინფორმაციული ინფრასტრუქტურის აგების დაწყება შეუძლებელია. ამ კომპონენტებზე უნდა მოხდეს რესურსის კონცენტრირება და შეირჩეს მაქსიმალურად სწორად, რათა შემდგომი ინფრასტრუქტურული განვითარება წარმატებით

დასრულდეს. თანამედროვე ორგანიზაციებისათვის ინფორმაციული ინფრასტრუქტურის განვითარება ხელს უწყობს ინფორმაციის ეფექტურ დამუშავებას, ოპტიმალურს ხდის ორგანიზაციის მმართველობას, ფინანსური დანახარჯებისა და დროის ეფექტურად გამოყენების საშუალებით.

ლიტერატურა - References - Литература:

1. Serova E. (2012). Enterprise Information Sytems in New Generation. The el-Journal "Information Systems Evaluation",vol. 15, Issue 1. pp. 116 -126. http:\\www.ejise.com.

2. She W., Thuraisingham B. (2007). Security for Enterprise Resource Planning Systems. Information Systems Security. 16:pp. 152–163. Copyright © Taylor & Francis Group, LLC .

3. Weider B., Booth P., Matolcsy P.Z., Ossimitz Maria-Luise. The impact of ERP systems on firm and business process performance. www.emeraldinsight.com/1741-0398.htm.

DEVELOPMENT OF SECURITY INFRASTRUCTURE OF INFORMATION SYSTEMS

Jamurashvili Kakhaber, Samkharadze Roman

Georgian Technical University

Summary

Article discusses information system security infrastructure planning problems and respective solution issues. In particular, modern software solutions are discussed. As a result, it becomes possible to transmit information electronically. The latter implies that the transmission speed is increased several times; It becomes possible to share printers and other hardware devices in the network, thus reducing the number of unwanted equipment. In addition, it is possible to set up an electronic mailing system that makes it much easier and accelerates the processes occurring in the company. Information infrastructure simplifies communication among employees, the decision-making process is much more efficient and quicker, much easier to communicate by electronic documents and their subsequent retrieval.

РАЗРАБОТКА ИНФРАСТРУКТУРЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Жамурашвили К., Самхарадзе Р.

Грузинский Технический Университет

Резюме

Становиться возможным эффективная электронная передача информации. Это подразумевает, что в несколько раз возрастает скорость передачи информации, становится возможным поделится принтерами и другими сетевыми устройствами в сети, что уменьшает количество нежелаемой аппаратуры. Кроме этого, становиться возможным создание электронной почтовой системы, что намного упрощает и ускоряет все процессы, протекающие в компании. В результате развития инфраструктуры упрощается коммуникация между сотрудниками, процесс принятия решений становиться более эффективным и быстрым, резко упрощается использование и поиск электронных документов.