# ინფორმაციული უსაფრთხოების კონცეფცია ორგანიზაციებსა და დაწესებულებებში

კახელი ბექა, ქართველიშვილი იოსები

საქართველოს ტექნიკური უნივერსიტეტი

**რეზიუმე**

ნაშრომში წარმოდგენილია ინფორმაციული უსაფრთხოების ჩამოყალიბების მეთოდოლოგიები. ინფორმაციული უსაფრთხოება აუცილებელია როგორც დიდ ასევე მცირე და საშუალო ორგანიზაციულ დაწესებულებებში. ინფორმაციული უსაფრთხოება თავის მხრივ კომპლექსური მცნებაა, რომელშიც არის თავმოყრილი რამდენიმე საკითხი. იმის გათვალისწინებით, რომ სრულიად დაცული სისტემის ჩამოყალიბება დიდ ძალისხმევასთან და ხარჯებთან არის დაკავშირებული, ნაშრომში წარმოდგენილია ის ფაქტორები, რომლებიც რეალურ საფრთხეს წარმოადგენენ, ასევე წარმოდგენილია მეთოდები და მაგალითები, რომლის შესრულება აუცილებელია, რათა შეიქმნას დაცული ქსელური ინფრასტრუქტურა.

**საკვანძო სიტყვები:** ინფორმაციული უსაფრთხოება, შეტევები, Antivirus, Anti spy, Firewall , Active Directory.

## 1. შესავალი

ოცდამეერთე საუკუნეში მნიშვნელოვნად გაიზარდა კომპიუტერული ტექნოლოგიების როლი. მსოფლიო ორგანიზაციები ცდილობენ მათი საქმიანობის ძირითადი ნაწილის ავტომატიზებას ელექტრონული სისტემების და ტექნოლოგიების დანერგვით. ამ ფაქტმა განაპირობა კონფიდენციალური ინფორმაციის დაცვის აუცილებლობა, რადგანაც ეს ინფორმაცია არ უნდა ყოფილიყო ყველასთვის ხელმისაწვდომი. შეიქმნა სპეციალური სისტემები, რომლებიც განსაზღვრავენ ინფორმაციასთან წვდომის საფეხურებს. ამ ყველაფრის გათვალისწინებით მთელ რიგ ორგანიზაციებში შეიქმნა მონიტორინგისა და ინფორმაციული უსაფრთხოების დეპარტამენტები, რომლებიც იცავენ ორგანიზაციას არასასურველი მომხმარებლებისგან.

საქართველოში, ამ ეტაპზე, ინფორმაციული უსაფრთხოება, როგორც პროფესია, ჩამოყალიბების პროცესშია. ბანკებისა თუ სხვა ორგანიზაციებში ამ სფეროს სპეციალისტებს ექმნებათ დიდი პრობლემები, რადგანაც მათ არ გააჩნიათ შესაბამისი ბერკეტები და გამოცდილება. ჩვენი აზრით, დღესდღეობით ეს არის ყველაზე მოთხოვნადი და აქტუალური საკითხი, განსაკუთრებით საბანკო სექტორისთვის, რადგანაც მათ აქვთ მთელი რიგი ინფორმაციები, რომლის კონფიდენციალურობაც არავითარ შემთხვევაში არ უნდა დაირღვეს.

## 2. ძირითადი ნაწილი

ინფორმაციული უსაფრთხოება, ისევე როგორც ინფორმაციის დაცვა, კომპლექსური და რთული ამოცანაა. იგი მიმართულია უსაფრთხოების უზრუნველყოფისა და სპეციალური უსაფრთხოების

სისტემების დანერგვისაკენ. ინფორმაციის დაცვა მთელი რიგი კომპანიებისთვის საკმაოდ პრობლემატური საკითხია და მოიცავს არაერთ ამოცანას. ინფორმაციის დაცვა უნდა მოხდეს ყველა იმ შემოტევებისგან, რომელსაც ე.წ „Adversaries“ გვიწყობენ, ესენი შეილება იყოს შემდეგი ჯგუფის წარმომადგენლები: Terrorist; Criminals; Hackers; Government და ა.შ.

განვიხილოთ შემოტევების ხუთი ტიპი: Passive; Active; Close-in; insider; Distributed.

- Passive - პასიური შეტევები მოიცავს ქსელის ტრაფიკის ანალიზს, დაუცველი საკომუნიკაციო სისტემის მონიტორინგს, სუსტად დაშიფრული ტრაფიკიდან ავტორიზების ინფორმაციის ამოღებას მაგალითად, როგორიცაა „ User“ , „password“. პასიური შეტევის შედეგი არის ის, რომ მომხმარებლის პირადი ინფორმაცია და ფაილები გამჟღავნდება მისი ნებართვის გარეშე.

- Active - აქტიური შეტევები მოიცავს მცდელობას გააცუროს ან გატეხოს დაცვის სისტემა, რათა „ჰაკერული“ პროგრამული კოდის მეშვეობით მოიპარონ ან შეცვალონ მათთვის სასურველი ინფორმაცია.

- Close –in - შეტევები შედგება რეგულარული ცალკეული პირების შეტევებისგან, სისტემების ან ობიექტების შეცვლის მიზნით.

- Insider - შიდა შეტევები იყოფა ორ ნაწილად. შიდა შეტევები რომლებსაც აქვთ მუქარის ხასიათი, ისინი შეგნებულად იწერენ, იპარავენ ან აზიანებენ ინფორმაციას, რომელსაც შემდგომ თაღლითობისთვის იყენებენ. შიდა შეტევები, რომლებიც არ ატარებენ მუქარის ხასიათს, ისინი ძირითადად ხდება დაუდევრობის, არასაკმარისი ცოდნის ან განზრახ დაშვებული შეცდომის გამო, რომელსაც ვიღაცის დაკვეთით ასრულებენ.

- Distributed - განაწილებული თავდასხმა ფოკუსირებულია მუქარაზე, აპარატურის ან სისტემის პარამეტრების მოდიფიცირებაზე ეს ყველაფერი დამოკიდებულია შეტევის ხანგრძლივობაზე. ამ შეტევების მიზანია „ჰაკერული“ კოდის მეშვეობით სისტემაში დატოვონ ე.წ „Black door“, რომლის მეშვეობითაც შეძლებენ სისტემაში არასანქცირებულ შესვლას, სადაც შეცვლიან ან მოიპარავენ სასურველ ინფორმაციას.

ზემოჩამოთვლილი შეტევების სახეობები წარმოადგენენ ისეთ საფრთხეებს, რომლებიც ხშირად დამღუპველ შედეგს იწვევენ ორგანიზაციებისთვის. სწორედ ამ შემოტევებისგან უნდა დავიცვათ თავი. ამისათვის საჭიროა სპეციალური როგორც აპარატურული ისე პროგრამული პროდუქტები. არსებობს უსაფრთხოების საერთაშორისო სტანდარტები. ეს ის მითითებებია, რომლებიც უნდა შესრულდეს, რათა შესაძლებელი იყოს სისტემის უსაფრთხოების დაცვა.

არსებობს უსაფრთხოების 6 კლასი : C1, C2, B1, B2, B3, A1. იმისათვის რომ, სისტემა სერტიფიკაციის პროცედურის შედეგად რომელიმე კლასს მივაკუთვნოთ, მისი უსაფრთხოების პოლიტიკა და გარანტირების დონე უნდა აკმაყოფილებდეს განსაზღვრულ მოთხოვნებს.

იმისათვის რომ შესაძლებელი იყოს ორგანიზაციის ინფორმაციული უსაფრთხოების დაცვა, აუცილებელია შემდეგი პროგრამული და აპარატურული პროდუქტების დანერგვა:

Antivirus - ანტივირუსი საშუალებას იძლევა მოვახდინოთ კომპიუტერში არსებული „ვირუსული" ფაილების დეტექტირება, ლოკალიზება და იმ შემთხვევაში თუ გექნებათ შესაბამისი მონიტორინგის სისტემები, შესაძლებელი იქნება აკონტროლოთ ცენტრალიზებულად თქვენ ქსელში არსებული კომპიუტერების მდგომარეობა.

Anti spy - ანტი ჯაშუში. სამწუხაროდ ანტივირუსებს არ აქვთ იმის შესაძლებლობა, რომ აღმოაჩინონ სისტემაში დამალული ჯაშუში პროგრამები. იმისათვის, რომ ავამაღლოთ სისტემის უსაფრთხოება და თავიდან ავიცილოთ ინფორმაციის გაჟონვა, საჭიროა გვქონდეს პროგრამული უზრუნველყოფა, რომელიც მოახდენს ჯაშუში პროგრამების დეტექტირებას და ნეიტრალირებას.

Firewall - ყველაზე საჭირო და აუცილებელი ხელსაწყო გახლავთ IT სპეციალისტის ხელში, ჩვენი აზრით ორგანიზაციას, რომელსაც ჯერ კიდევ არ აქვს ჩამოყალიბებული ინფორმაციული უსაფრთხოების ინფრასტრუქტურა, მან უნდა დაიწყოს სწორედ ამ მექანიზმის დანერგვით.

რა არის Firewall ? ეს არის აპარატურული ან პროგრამული უზრუნველყოფა, რომელიც ახორციელებს მასში შემავალი პაკეტების, ტრაფიკის კონტროლს და ფილტრაციას. მის ძირითად დავალებას წარმოადგენს ლოკალური ქსელის ან ცალკეული კვანძების დაცვა არასანქცირებული წვდომისგან, რომელიც კრძალავს არაავტორიზებულ წვდომას და ნებას რთავს მხოლოდ ავტორიზებულ კავშირს, როგორც ქსელიდან გამავალ პაკეტებზე, ასევე ქსელში შემავალ პაკეტებზე.

Firewall-ი როგორც დაცვითი საშუალება, პირველად გამოყენებულ იქნა 1988 წელს, როდესაც Digital Equipment Corporation კორპორაციის თანამშრომლებმა განაცხადეს პაკეტების ფილტრაციის სისტემის შექმნაზე სახელწოდებით Firewall. Bill Cheswick და Steve Bellovin განაგრძობდნენ კვლევას პირველ პაკეტების ფილტრაციის სისტემაზე ამავე კომპანიაში.

კიდევ ერთი და ყველაზე აუცილებელი მექანიზმი, რომელიც აუცილებელია ინფრასტრუქტურის მართვისთვის ე.წ Firewall-ის შემდეგ, სასურველია დანერგილი იყოს Active Airectory. Active Directory (AD) არის კომპანია Microsoft –ის მიერ შემუშავებული ტექნოლოგია, რომელიც შეიქმნა ისეთი ქსელური მოწყობილობების მონიტორინგისა და მართვისთვის, როგორიცაა: LDAP directory services, Kerberos based authentication, DNS naming, უსაფრთხო კავშირი რესურსებთან და მრავალი სხვა. Active Directory იყენებს ერთ საერთო მონაცემთა ბაზას, რომელზე წვდომა და ინფორმაციის შენახვა შეუძლია მრავალ სხვადასხვა პროგრამასა და სერვისს.

AD გამოიყენება სისტემის ადმინისტრატორების მიერ, რათა შეინახონ ინფორმაცია მომხმარებლების შესახებ, უსაფრთხოების პოლიტიკის შესახებ და დანერგონ სხვადასხვა პროგრამული პროდუქტი. განვიხილოთ Active Directory-ის ძირითადი სტრუქტურა, მუშაობის პრინციპები და შემადგენელი კომპონენტები.

Active Directory არის ადგილი, სადაც ინახება ინფორმაცია ხალხის, საგნების (კომპიუტერები, პრინტერები და ა.შ.), პროგრამების, სერვისების და უსაფრთხოების წესების შესახებ. ხოლო პროგრამები და სერვისები შემდეგ იყენებს ამ ინფორმაციას. მაგალითად: Microsoft Windows იყენებს Active Directory-ში არსებულ ინფორმაციას, რათა მომხმარებელს მისცეს სისტემაში შესვლის ნება (login) და მიანიჭოს ის უფლებები, რაც უსაფრთხოების პოლიტიკაშია გაწერილი [1,2]. თუ მომხმარებლის ანგარიში Active Directory-ში გაუქმებულია, მაშინ windows არ აძლევს მას სისტემაში შესვლის უფლებას.

აღსანიშნავია, რომ AD საშუალებით ხდება პროგრამების დანერგვა. ქსელის ადმინისტრატორს შეუძლია შეიტანოს წესების პოლიტიკაში ცვლილებები იმის შესახებ, რომ კონკრეტული პროგრამა დაინერგოს კონკრეტული მომხმარებლისათვის. შემდეგ ამ ინფორმაციის საფუძველზე თავად მომხმარებლის ოპერაციული სისტემა Windows ახორციელებს აღნიშნული პროგრამის ინსტალაციას.

Active Directory შესაძლებლობას გვაძლევს შევქმნათ მოქნილი იერარქია ჩვენი გარემოსათვის. იგი შესაძლებლობას აძლევს მთავარ ადმინისტრატორს, გარკვეული უფლებების დელეგირება მოახდინოს ადგილობრივ ადმინისტრატორებზე, გუნდის წევრებზე ან ჯგუფებზე.

შესაძლებელია აიგოს იერარქია ნებისმიერი სასურველი გზით - გეოგრაფიული ადგილების, ქვეგანყოფილებების, ზოდიაქოს ნიშნების და ა.შ. AD-ის სტრუქტურა იწყება forest და domain-ით და მთავრდება ორგანიზაციული ერთეულებითა და ობიექტებით. მოქნილი იერარქიული დიზაინი არის უპირატესობა ქსელური არქიტექტურისათვის, მაგრამ დასაწყისში არასწორად დაგეგმილი სტრუქტურა მომავალში შეიძლება საფრთხედ გადაიქცეს. აქედან გამომდინარე, აუცილებელია ხანგრძლივი ანალიზი, ვიდრე მის აგებას შევუდგებით.

## 3. დასკვნა

ზემოთაღნიშნული ტექნოლოგიები აუცილებელია იმისათვის, რომ გაგვაჩნდეს მინიმალურად, მაგრამ დაცული ინფორმაციული ინფრასტრაუქტურა. აუცილებელია, რომ არ იქნას დაზოგილი ფული და დრო ამ ცვლილებების გატარებისათვის, რადგანაც ორგანიზაციის განვითარების შემთხვევაში დროთა განმავლობაში საჭირო იქნება ამ მექანიზმების უფრო მეტად ოპტიმიზირება და დახვეწა, რაც შეიძლება შეუძლებელი გახდეს იმის გამო, რომ თავიდანვე შეძენილი იქნა იაფფასიანი პროდუქცია, რომლის შესაძლებლობებიც შეზღუდულია.

ლიტერატურა:

1. Shapiro J.F. Windows Server 2008. Bible, Wiley India Pvt. Ltd. 2008

2. Дэн Холме, Нельсон Рест, Даниэль Рест. Настройка Active Directory. Windows Server 2008, 2011.

## THE CONCEPT OF INFORMATION SECURITY IN ORGANIZATIONS AND ESTABLISHMENTS

Kakheli Beqa, Kartvelishvili Ioseb

**Summary**

The work presents the development of information security methodologies. Information security is essential in both large as well as small and medium-organizational institutions. Information security is a complex commandments which in turn is concentrated in a few issue. Because completely protected system with a lot of effort and costs, I tried to imagine the work the factors that are the real threat to, the methods and examples presented, implementation of necessary in order to create a secure infrastructure.

## КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ И УЧРЕЖДЕНИЙ

Кахели Б., Картвелишвили И.

**Резюме**

В работе предоставлена методология создания информационной безопасной среды. Информационная безопасность объязательна как в больших, так и в малых организационных объектах. Информационная безопасность в свою очередь комлексный вопрос, в котором содержится несколько подпунктов. Учитывая то, что создание полностью безопасной системы связанно с большой тратой времени и средств, в данной работе рассматриваются те факторы, которые представляют реальную опасность, а так же методы и примеры, использование которых необходимо, чтобы создать сравнительно безопасную ифраструктуру.