კომპიუტერულ სისტემებში ინფორმაციის დაცვის პრობლემები

გიორგი მაისურაძე, სტუ-ს დოქტორანტი

რეზიუმე

ინფორმაციის დაცვის პრობლემა: მისი საიმედოდ შენახვის უზრუნველყოფა და გამოყენება თანამედროვეობის ერთ-ერთი მნიშვნელოვანი პრობლემაა.

აპარატურული საშაულებებზე წვდომის შეზღუდვით და დაშიფრვით.

კომპიუტერული ქსელების შექმნამ მნიშვნელოვან პრობლემად აქცია ინფორმაციის დაცვა.

დღეისათვის ინფორმაციის გადაცემის საშუალებას წარმოადგენს კომპიუტერული ქსელები. კონკურენტულ გარემოში ინფორმაცია შეიძლება საინტერსო იყოს კონკურენტული ორგანიზაციებისთვის, ამიტომ იქმნება მისი დაცვის პრობლემა. ინფორმაციის დაცვის ქვეშ იგულისხმება არა მარტო ტექნიკურ-პროგრამული საუალებები არამედ საკანონმდებლოც.

იურიდიულად ფორმულირებულია ინფორმაციული უსაფრთხოების სამი პრინციპი, რომელმაც უნდა უზრუნველყოს:

- მონაცემთა მთლიანობა;
- ინფორმაცის კონფედენციალურობა;
- ყველა დარეგისტრირებული მომხმარებლისთვის ინფორმაციასთან წვდომა;

ყველა კომპიუტერული დანაშაული შეიძლება დაიყოს ორ დიდ ჯგუფად: დანაშაული, რომელიც არღვევს კომპიუტერის მუშაობას და დანაშაული, რომელიც კომპიუტერს იყენებს როგორც აუცილებელ ტექნიკურ საშუალებად.

თანამედროვე სიტუაციისთვის აქტუალურია:

1. კომპიუტერში შენახულ ინფორმაციასთან ინფორმაციასთან არასამართლებრივი წვდომა. მასში იგულისხმება ინფორმაციის მიღება მისი მფლობელის გარეშე.არასამართლებრივი წვდომა როგორც წესი ხორციელდება სხვისი სახელით,ტექნიკური მოწყობილობების ფიზიკური მისამართების შეცვლით, პროგრამული და აპარატურული საშუალებების შეცვლით

2. კომპიუტერის ბოროტმოქმედული პროგრამების შექმნით, გამოყენებით და გავრცელებით.

3. კომპიუტერული ვირუსების დამუშავებიტ დაგავრცელებიით.

4. პროგრამულ-აპარატურული კომპლექსის დამზადებისას და ექსპლუა-ტაციისას დანაშაულებრივი გაუფრთხილებლობით, რომელსაც მივყავართ ინფორმაციის დაკარგვამდე

5. კომპიუტერული ინფორმაციის გაყალბებით;

6. კომპიუტერული ინფორმაციის მოპარვით.

აღნიშნული პრობლემები თანამედროვე საზოგადოებაში ინფორმაციის დაცვის საკითხებს ქმნის აქტუალურს.

საკვანძო სიტყვები: კომპიუტერული ქსელი, ინფორმაციის დაცვა, თავდასხმა

Summary

Giorgi Maisuradze

The Security Problem of Information: Its reliably prevision of storage of and use is one of the most important problem of modern .

Computer Network of creation important problem action information of protection. For today information transfer allow the present of Computer networks. The information may be of interest concrete in environment for concrete organization, it will be the problem. Information of protection under means not only technical-software development tools but of the legislative.

The Law stipulates the information security three principles which should provide:

- Data integrity;
- Confidentiality of information;
- Information access for all registered casers ;

All computer crime can be divided in to two large groups:

The crime which violates the Computer work and the crime, which uses a computer as as a necessary technical means.

For the modern situation is actual:

1.The unfair access to information stored on your computer. It is understood information of receive without the owner's. Illegal to access which procedure is carried out other of name, Technical equipment for physical addresses change, and Software and hardware means of changing.

2. By creation, using and proliferation of Computer Abuse Programs

3. by treatment and proliferation of Computer viruses.

4. Software-hardware complex of the issuance and operation of the criminal negligence, which leads to loss.

5. By fascination of Computer Information.

6. By stolen of Computer Information.

The above mentioned problems modern in society information protection of issues of creating the actual.

The keyword: Computer network, Information of protection, attack.

* * * * * * * *

მსოფლიო საინფორმაციო საზოგადოების ფორმირება თანამედროვე ცივილიზაციის განვითარების გლობალურ ფაქტორად იქცა. მსოფლიო თანამეგობრობის სუბიექტების ურთიერთკავშირების გაძლიერების ფონზე მიმდინარეობს უწყვეტი ბრძოლა ეკონომიკური ინტერესებისა და სხვადასხვა რესურსებისთვის. გარდა ამისა, ბრძოლის მიზანია სამხედრო უპირატესობის მოპოვება და პოლიტი-

კური, იდეოლოგიური თუ კულტურული გავლენების გაძლიერება. აღნიშნული ბრძოლა მწვავდება და მიზნების მისაღწევად გამოიყენება საინფორმაციო უპირატესობები. საინფორმაციო-ტექნოლოგიური თვალსაზრისით მოწინავე ქვეყნების სამხედრო პოტენციალი მკვეთრად იზრდება, რაც იწვევს გლობალური და რეგიონალური ძალთა ბალანსის ცვლილებას.

საინფორმაციო განვითარება მნიშვნელოვანი ფაქტორია, რომელსაც შეუძლია ძალთა ცენტრებს, რეგიონებსა და სახელმწიფოებს შორის ურთიერთობების შეცვლა. დღესდღეობით და უახლოეს მომავალშიც საქართველოს რთულ პრობლემებთან მოუწევს გამკლავება, რაც დაკავშირებულია ეროვნული ინტერესების დაცვასთან.

საქართველო განვითარების რთულ ეტაპზე იმყოფება. ეს ყოველივე განპირობებულია როგორც საერთაშორისო ურთიერთობების არაერთგვაროვნებითა და წინააღმდეგობრიობით, ასევე მცდელობებით, ჩვენი ქვეყნის წინააღმდეგ წარიმართოს საინფორმაციო-ფსიქოლოგიური ომი და შეიქმნას სახელმწიფოთაშორისი ურთიერთობების გლობალური საინფორმაციო სტრუქტურა, რომელიც დაეფუძნება ერთპიროვნულ გადაწყვეტილებებს.

დღეს, ციფრულ ხანაში, ყველაზე აქტუალური საკუთარი სისტემისა და ინფორმაციის დაცვის პრობლემაა. კომპიუტერული ტექნოლოგია საშუალებას იძლევა, ერთი მავნე ფაილის საშუალებით სხვის პირად ცხოვრებაში ჩაერიოთ, ვმართოთ სხვისი მანქანები, მოვიპაროთ ინფორმაცია ან თუნდაც ფული და ა.შ., ამიტომ ბუნებრივად ჩნდება კითხვა — როგორ დავიცვათ თავი?

თავის დაცვა რამდენიმენაირად შეიძლება, ამ საშუალებებში შედის უბრალოდ კომპიუტერის გამორთვა, ინტერნეტის გათიშვა, ყველა საეჭვო ფაილის შემოწმება და ა.შ.,

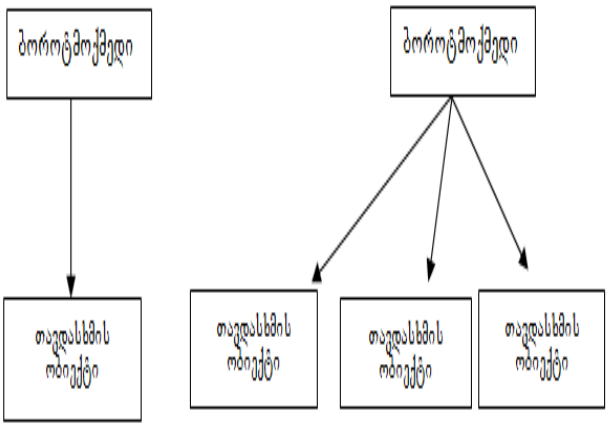
ინფორმაციის დაცვის პრობლემა: მისი საიმედოდ შენახვის უზრუნველყოფა და გამოყენება თანამედროვეობის ერთ-ერთი მნიშვნელოვანი პრობლემაა.

30-35 წლის წინ ინფორმაციის დაცვა ეფექტურად წყდებოდა ორგანიზაციული და ცალკეული აპარატურულ-პროგრამული საშუალებებით —აპარატურული საშაულებებზე წვდომის შეზღუდვით და დაშიფრვით.

ინფორმაციული სისტემის თავდასხმის ქვეშ იგულისხმება ბოროტმოქმედის წინასწარგანზრახული ქმედება რომელიც იყენებს ინფორმაციული სისტემის დაუცველობას და იწვევს დასამუშავებელი ინფორმაციასთან წვდომის, მთლიანობის და კონფედენციალურობის დარღვევას.

თავდასხმის მოდელი

თავდასხმის ტრადიციული მოდელი აგებულია პრინციპზე „ერთი ერთზე“ ან „ერთი ბევრზე“(ნახ.1).



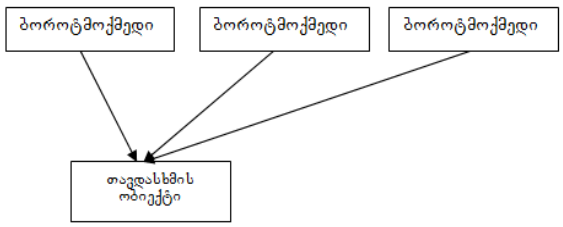
ა) ბ)

ნახ.1 თავდასხმის მოდელები ა) ერთი- ერთზე და ბ) ერთი- ბევრზე

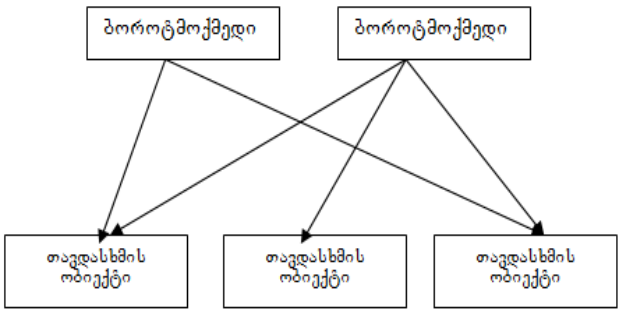
ეს ნიშნავს, რომ თადასხმა ხდება ერთი წყაროს საშუალებით. დაცვის საშუალებების დამმუშავებლები ორიენტირებულნი არიან თავდასხმის ტრადიციულ საშუალებებზე, დასაცავი ქსელის სხვადასხვა ადგილებში ყენდება სისტემის დაცვისთვის აგენტები, რომლებიც გადასცემენ ინფორმაციას მართვის ცენტალურ კონსოლს.

განაწილებული თავდასხმების მოდელში (ნახ.2) გამოიყენება სხვა პრინციპი. ტრადიციული მოდელებისგან განსხვავებით გამოიყენება დამოკიდებულება „ბევრი ერთთან“ და „ბევრი ბევრთან“

ა)



ბ)



ნახ.2 განაწილებული თავდასხმების მოდელი ა) „ბევრი ერთთან“ და ბ) „ბევრი ბევრთან“

განაწილებული თავდასხმების მოდელი დაფუძნებულია კლასიკურ თავდასხმის ტიპზე „მომსახურებაზე უარი“, უფრო ზუსტად მის ქვესიმრავლეზე, ცნობილი როგორც Flood-თავდასხმა ან შტორმ-თავდასხმა. ამ თავდასხმის აზრი მდგომარეობს იმაში, რომ თავდასხმის კვანძზე იგზავნება ბევრი პაკეტი. თავდასხმის ობიექტი შეიძლება გამოვიდეს მწყობრიდან, რადგან ის ვეღარ შეძლებს ავტორიზებული მომხმარებლების მოთხოვნების დამუშავებას. ამ პრინციპით მუშაობს თავდასხმები -Flood, Smurf, UDP Flood, Targa3 და ა.შ.

თავდასხმის რეალიზაციის ეტაპები:

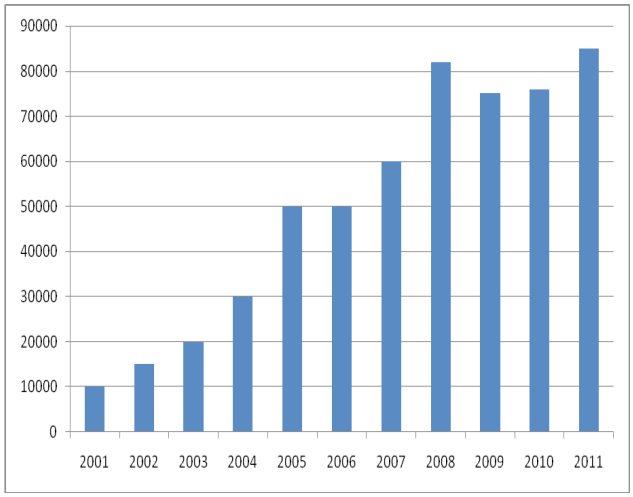
შეიძლება გამოვყოთ თავდასხმის რეალიზაციის შემდეგი ეტაპები:

- თავდასხმის წინასწარი ქმედებები ანუ ინფორმაციის შეკრება;
- თავდასხმის რეალიზაცია;
- თავდასხმის დასრულება.

ჩვეულებრივ როდესაც თავდასხმაზე საუბრობენ გულისხმობენ მეორე ეტაპს. ინფორმაციის შეკრება - ეს არის მნიშვნელოვანი ეტაპი თავდასხმის რეალიზაციაში. თასვდასხმის რეალიზაციის პირველი ეტაპი ესაა თავდასხმის სისტემაზე ან კვანძზე ინფორმაციის შეკრება. ის გულისხმობს ისეთ მოქმედებებს როგორიცაა ქსელური ტოპოლოგიის ტიპის, თავდასასხმელი ობიექტის ოპერაციული სისტემის ვერსიის განსაზღვრას და ა.შ.

თავდაპირველად ირჩევა თავდასხმის მიზანი და შემდეგ ხდება მასზე ინფორმაციის შეგროვება (ოპერაციული სისტემის ტიპი და ვერსია, ღია პორტები და გაშვებული ქსელური სერვისები, დაყენებული სისტემური და გამოყენებითი პროგრამული უზრუნველყოფა და მათი კონფიგურაცია და ა.შ.), შემდეგ ხდება თავდასასხმელი სისტემის სუსტი ადგილების იდენტიფიცირება, რომელზეც ზემოქმედება ბოროტმოქმედს მიიყვანს შედეგამდე. ამ ეტაპზე თავდამსხმელი იკვლევს ქსელურ გარემოს თავდასხმის ობიექტის გარშემო. მას მიეკუთვნება მაგალითად ინტერნეტ პროვაიდერის ან დაშორებული ოფისის კვანძები. ამ ეტაპზე ბოროტმოქმედი შეიძლება შეეცადოს განსაზღვროს მისამართები „ნდობით“ აღჭურვილი სისტემები და კვანძები რომლებიც პირდაპირ არიან შეერთებული თავდასხმის მიზანთან და ა.შ.

თავდასხმების ზრდის ტემპი წლების მიხედვით:



ნახ.3 თავდასხმების ზრდის ტემპი წლების მიხედვით

გამოყენებული ლიტერატურა:

1.Семкин С.Н., Семкин А.Н. Основы информационной безопасности объектов обработки информации. Научно-практическое пособие. – Орел: 2000.- 300с.

2. Анин Б.Ю. Защита компьютерной информации. - СПб.: БХВ- Санкт-Петербург, 2000. - 384с.

3. Смирнова Г.Н. Проектирование экономических информационных систем: Учебник/ Г.Н.Смирнова, А.А.Сорокин, Ю.Ф.Тельнов; Под ред. Ю.Ф.Тельнова.– М.:Финансы и статистика, 2001. – 512с.

4. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с

5. Kotenko et al., Kotenko I.V., Ulanov A.V. The Software Environment for multi-agent Simulation of Defense Mechanisms against DDoS Attacks // The International Conference on Intelligent Agents, Web Technologies and Internet Commerce. IAWTIC’2005. 2005.

6. Mirkovic et al., Mirkovic J., Dietrich S., Dittrich D., Reiher P. Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall PTR. 2004.