მართვის ავტომატიზებული სისტემების ინფორმაციული უსაფრთხოება

გულბაათ ნარეშელაშვილი[1], თამაზ შეროზია[1], იბრაიმ დიდმანიძე[2],
ვალერი კეკელია[1]

1-საქართველოს ტექნიკური უნივერსიტეტი,
2- ბათუმის სახელმწიფო უნივერსიტეტი

რეზიუმე

სხვადასხვა ორგანიზაციების და კომპანიების წარმატებული მუშაობა, რომლებიც გამოიყენებენ თანამედროვე IT ინფრასტრუქტურებს, დამოკიდებელია საინფორმაციო რესურსების საიმედოობასა და უსაფრთხოებაზე. საინფორმაციო შეტევები, რომლებიც ხორციელდება ავტომატიზებული სისტემების ფუნქციონირებისას, მიმართულია ინფორმაციის კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დარღვევაზე. განიხილება ინფორმაციული შეტევების სახეები და ინფორმაციის დაცვის მეთოდები და საშუალებები, რომლებიც გვაძლევს საშუალებას კომპლექსურად გადავჭრათ ავტომატიზებული სისტემების საინფორმაციო რესურსებზე მავნე ზემოქმედების პრობლემები.

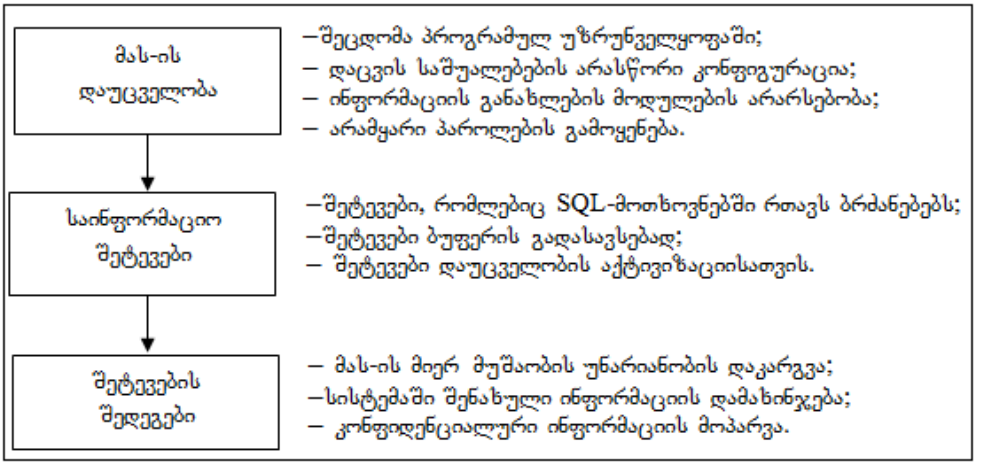
საკვანძო სიტყვები: საინფორმაციო შეტევა. პაროლი. კრიპტოგრაფიული დაცვა. სერვერი. ქსელებშორისო ეკრანი. ანტივირუსი. კონტენტური ანალიზი. სპამი.

1. შესავალი

მართვის ავტომატიზებული სისტემები (**მას**) უდიდეს როლს თამაშობენ ბიზნეს-პროცესების ეფექტურ შესრულებაში, როგორც კომერციულ, ასევე საბიუჯეტო ორგანიზაციებში. ამასთან, **მას**-ის გამოყენება სხვადასხვა სფეროში იწვევს იმ პრობლემების აქტუალიზაციას, რომლებიც დაკავშირებულა ინფორმაციის დაცვასთან. პრაქტიკულად, ნებისმიერი **მას** შეიძლება იყოს ინფორმაციული შეტევის ობიექტი, რის შედეგადაც ირღვევა ინფორმაციის თვისებები: კონფიდენციალობა, მთლიანობა, სისწორე ან ხელმისაწვდომება [1]. ბოროტმოქმედის მიერ ამ თვისებებზე ზემოქმედება იწვევს ორგანიზაციების ბიზნეს პროცესების მიმდინარეობის დარღვევას, ვინაიდან ეს პროცესები იყენებს არსებულ საინფორმაციო რესურსებს. საინფორმაციო შეტევის განსახორციელებლად ბოროტმოქმედმა უნდა გამოიყენოს **მას**-ის სუსტი ადგილები. მაგალითად, **მას**-ის პროგრამულ უზრუნველყოფაში იმ მოდულების არარსებობა, რომელბიც აახლებენ ინფორმაციას, არამყარი პაროლების გამოყენება, **მას**-ის ქსელური სამსახურების არასწორი კონფიგურაცია, ინფორმაციის დაცვის საშუალებების არარსებობა და ა.შ. ამიტომ საჭირო ხდება კომპლექსური მიდგომა ინფორმაციის დაცვისათვის.

2. ძირითადი ნაწილი

მას-ის დაუცველობა, საინფორმაციო შეტევა და სავარაუდო შედეგები ლოგიკურადაა ერთმანეთთან დაკავშირებული (ნახ.1).



ნახ.1

ინფორმაციული შეტევების ძირითადი მიზანია **მას**-ის სუსტი წერტილებიდან შეღწევა და ზარალის მიყენება. ასეთ წერტილებს შეიძლება შეიცავდეს როგორც პროგრამულ-აპარატურული, ასევე ორგანიზაციულ-სამართლებრივი უზრუნველყოფები. პირველი სახის უზრუნველყოფის სამუშაო სადგურები, სერვერები, კავშირის არხები და საკომუნიკაციო მოწყობილობები.

ორგანიზაციულ-სამართლებრივი უზრუნველყოფის სუსტი წერტილების არსებობის ძირითად მიზეზს წარმოადგენს ინფორმაციული უსაფრთხოების ნორმატიული დოკუმენტების არარსებობა, მაგალითად, უსაფრთხოების კონცეპცია, რომელიც განსაზღვრავს მას-ის დაცვის მოთხოვნებს და კონკრეტულ გზებს მათი რეალიზაციისათვის. ინფორმაციული შეტევა შეიძლება დაიყოს ოთხ სტადიად:

1. რეკოგნოსტირების სტადია. ამ ეტაპზე ბოროტმოქმედი აგროვებს ინფორმაციას, რომელიც ახასიათებს შეტევის ობიექტს. მაგალითად, გამოყენებული ოპერაციული სისტემის ტიპი, დარეგისტრირებული მომხმარებლების სია, პროგრამული უზრუნველყოფა და ა. შ. შეტევის ობიექტებს შეიძლება წარმოადგენდეს სამუშაო ადგილები, სერვერები და მას-ის საკომუნიკაციო საშუალებები;

2. მას-ში შეჭრის სტადია. ამ ეტაპზე ბოროტმოქმედი იყენებს არასანქცირებულ შეღწევას მას-ის რესურსებისადმი, რომელთა წინააღმდეგაც ხორციელდება შეტევა;

3. მას-ზე შემოქმედების სტადია. ამ ეტაპზე ბოროტმოქმედი ცდილობს იმ შედეგების მიღწევას, რომელთათვისაც ახორციელებს შეტევას. მაგალითად, მას-ის მწყობრიდან გამოყვანა, კონფიდენციალური ინფორმაციის ხელში ჩაგდება, სისტემაში შენახული მონაცემების შეცვლა, ან წაშლა და სხვ.;

4. შეტევის შემდგომი განვითარების სტადია. ამ ეტაპზე სრულდება მოქმედებები, რომლებიც აგრძელებენ შეტევას მას-ის კვაძების რესურსებზე.

შეტევები შეიძლება დავყოთ შიგა და გარე შეტევებად. გარე შეტევები სრულდებიან იმ კვანძებიდან, რომლებიც არ შედის მას-ის შემგადგენლობაში. მაგალითად, ქსელური შეტევა, როცა ბოროტმოქმედი ახორციელებს შეჭრას ორგანიზაციის ლოკალურ ქსელში ინტერნეტ ქსელიდან. შიგა შეტევები ხორციელდება მას-ის შიგნით, მისი სერვერიდან, ან სამუშაო ადგილიდან. მაგალითად, თანამშრომელმა შეიძლება გადასცეს ბოროტმოქმედს კონფიდენციალური ინფორმაცია [2].

დღეისათვის არსებობს ინფორმაციის დაცვის ორგქანიზაციული და ტექნიკური საშუალებები. საორგანიზაციო საშუალებების გამოყენება დაკავშირებულია ორგანიზაციაში ნორმატიულ-სამართლებრივი დოკუმენტების დამუშავებასა და დანერგვასთან, რომლებიც განსაზღვრავს მოთხოვნებს მას-ის ინფორმაციული უსაფრთხოებისადმი, მაგალითად მას-თან მუსაობის თანამდებობრივი ინსტრუქციები და სხვ.

ტექნიკური საშუალებების რეალიზაცია მას-ში სრულდება შესაბამისი პროგრამული, აპარატურული ან პროგრამულ-აპარატურული კომპლექსების საშუალებებით.

არსებობს ტექნიკური დაცვის შემდეგი საშუალებები: ინფორმაციის დაცვის კრიპტოგრაფიული საშუალებები; მას-ის რესურსებისადმი არასანქცირებული შეღწევისგან დაცვის საშუალებები; მას-ის დაცულობის ანალიზის საშუალებები; შეტევების აღმოჩენის და თავიდან აცილების საშუალებები; ანტივირუსული დაცვის საშუალებები; კონტენტური ანალიზის საშუალებები; სპამისაგან დაცვის საშუალებები.

დაცვის კრიპტოგრაფიული საშუალებები ასრულებს ინფორმაციის გარდაქმნას მისი კონფიდენციალურობის და მთლიანობის კონტროლის უზრუნველსაყოფად. ინფორმაციის დაცვა შესაძლებელია როგორც მისი გადაცემისას, ასევე მას-ში შენახვისა და დამუშავებისას, რომელიც შეიძლება განხორციელდეს სიმეტრიული და ღია გასაღებით [3].

შეღწევის შეზღუდვის საშუალებების დანიშნულებაა მას-ის საინფორმაციო რესურსების დაცვა. ეს ძირითადად ხორციელდება მომხმარებლის იდენტიფიცირებით, აუტენტიფიცირებით და ავტორიზებით.

ქსელებშორის ეკრანები (Firewall) აკონტროლებენ მას-ში შემოსულ და გასულ ინფორმაციას ფილტრაციის საშუალებით, იმ კრიტერიუმების მიხედვით, რომელსაც მიუთითებს ადმინისტრატორი.

დაცულობის ანალიზის საშუალებებით, ე.წ. უსაფრთხოების სკანერებით (security scanners), შეიძლება გამოვავლინოთ მას-ის კვანძებში სუსტი წერტილების არსებობა და დროულად აღმოფხვრათ ისინი. სკანირება იწყება სისტემაზე საწყისი ინფორმაციის მიღებით გამოყენებულ ოქმებზე და ა. შ. და შეიძლება დასრულდეს იმიტაციის ცდით ცნობილი შეტევის გამოყენებით, მაგალითად „პაროლის შერჩევა (brute force)“. სკანირებისათვის შესაძლებელია შემდეგი პროგრამული პროდუქტების გამოყენება: Nessus Security Scanner, Internet Scanner, SAIN და სხვ.

შეტევის აღმოჩენის და თავიდან აცილების საშუალებები წარმოადგენს სპეციალიზებულ პროგრამულ ან აპარატულ-პროგრამულ კომპლექსებს, რომელთა დანიშნულებაა მას-ის რესურსებზე ინფორმაციული შეტევის გამოვლენა და არიდება.

ქსელთაშორისო ეკრანების და შეღწევის აღმოჩენის სისტემებისაგან (IDS) განსხვავებით, შეტევის თავიდან აცილების სისტემებს (IPS) შეუძლია არა მარტო გაანალიზონ გადასაცემი მონაცემები, არამედ დაბლოკონ შეტევებიც. თანამედროვე IPS უზრუნველყოფს: ფუნქციონირებას მონაცემების გადაცემის სიჩქარით (in-line რეჟიმი); მონაცემთა პაკეტების აწყობის სწორ თანმიმდევრობას და მათ ანალიზს არასანქცირებული აქტიურობის გამოსავლენად; შეტევის აღმოჩენის სიგნატურულ და ქცევითი მეთოდების გამოყენებას, ოქმებში ანომალიების იდენტიფიცირებას; მონაცემთა მავნე ტრაფიკის ბლოკირებას.

დღეისათვის ფართოდ გამოიყენება შეღწევების აღმოჩენის და თავიდან აცილების თანამედროვე სისტემა Stone Gate IPS.

კომპიუტერის ანტივირუსული დაცვა, როგორც წესი, შეიცავს მთელ რიგ საშუალებებს, სხვადასხვა მავნე მოქმედებების შესაზღუდავად. არსებობს მრავალი ანტივირუსული პროგრამა, რომლებიც განსხვავდება მოქმედების სისწრაფით, ანტივირუსული ბაზების ხარისხით და სხვა პარამეტრებით. ფართო გამოყენება ჰპოვა Kaspersky Internet Security, ESET NOD32, Norton Antivirus, Dr. Web, Avast ანტივირუსულმა პროგრამებმა. კონტენტური ანალიზის საშუალებების დანიშნულებაა ქსელური ტრაფიკის მონიტორინგის განხორციელება, უსაფრთხოების დარღვევების გამოსავლენად. ანალიზი სრულდება წინასწარ მომზადებული კონტენტური ფილტრაციის ბაზის (კფბ) საფუძველზე. კფბ არა მარტო აღწერს ინფორმაციის კატეგორიებს, რომელიც მოძრაობს მას-ში, არამედ ითვალისწინებს მისი კონფიდენციალობის სხვადასხვა ატრიბუტს. კონტენტური ანალიზის სისტემა Info Watch Data Control ახორციელებს საფოსტო შეტყობინებების აუდიტს და ინტერნეტ-ტრაფიკის მონიტორინგს. სისტემას აქვს საშუალება გამოავლინოს და დაბლოკოს კონფიდენციალური ინფორმაციის გაჟონვის არხები, საფოსტო სისტემების გამოყენებისას. ინტერნეტ-ტრაფიკის მონიტორინგი იძლევა საშუალებას დაიბლოკოს მომხმარებლის მიერ აკრძალული ინტერნეტ-რესურსების გამოყენება და აგრეთვე გამოავლინოს კონფიდენციალური ინფორმაციის გადაცემის მცდელობა HTTP ოქმით [4]. სპამისაგან დაცვის საშუალებები უზრუნველყოფს იმ რეკლამური ხასიათის საფოსტო შეტყობინებების გამოვლენას და ფილტრაციას, რომლებიც არაა მომხმარებლის მიერ მოთხოვნილი. ბრძოლის ეფექტური პროგრამული საშუალებაა Symantec Brightmail Message Filter, რომელიც ხასიათდება მაღალი სიზუსტით და ფართო გამტარუნარიანობის მოქნილი ალგორითმით [5].

3. დასკვნა

დღესდღეობით ორგანიზაციების და კომპანიების შედეგიანი მუშაობა ბევრადაა დამოკიდებული იმაზე, თუ რამდენად კარგად არის დაცული მათში მომუშავე კომპიუტერული მართვის სისტემები შესაძლო საინფორმაციო შეტევებისაგან, რაც განაპირობებს ამ პრობლემის აქტუალობას. განხილულია ინფორმაციის უსაფრთხოების ძირითადი ცნებები, შესაძლო ინფორმაციული შეტევები და არსებული თანამედროვე დაცვის მეთოდები და საშუალებები. ინფორმაციის უსაფრთხოებისათვის საჭიროა მისი დაცვისადმი კომპლექსური მიდგომა.

ლიტერატურა:

1. Мейволд Эрик. Безопасность сетей. Практ. пособие. Пер. с англ. – М., СП ЭКОМб, 2005
2. Касперски Крис. Техника и философия хакерских атак. – М.: Солон – Р, 1999
3. Рябко Б. Я., Фионов А. Н.. Криптографические методы зщиты информации. Уч пособие – М.: Горячая линия – телеком, 2005
4. DLP–Технология предотвращения утечек конфиденциальной информации. www.tadviser.ru/index.php.
5. Владимир Горбунов. Спам и борьба с ним. www.antivirus-navigator.com.

MANAGEMENT SYSTEMS INFORMATIONAL SECURITY

Nareshelashvili G.G.[1], Sherozia T.A.[1], Didmanidze I.Sh.[2], Kekelia V.I.[1]
1-Georgian Technical University, 2-State University of Batumi

Summary

Successful work of the organizations and companies, which are using modern IT technologies largely depends on the reliability and security of ACS information resources. Informational attacks take place with the purpose of violating properties as confidentiality, integrity and accessibility. To implement a vulnerability attack hackers are using the weakness of ACS, which might take place in both: institutional and program-hardware. Modern methods and tools to protect information allow solving an information security problem.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Нарешелашвили Г.Г.[1], Шерозия Т.А.[1], Дидманидзе И.Ш.[2], Кекелия В.И.[1]
1-Грузинский Технический Университет, 2-Батумский Государственный Университет,

Резюме

Успехи работ организаций и компаний, использующих современные IT технологии, во многом зависят от надежности и безопасности информационных ресурсов АСУ. Информационные атаки осуществляются с целью нарушения таких свойств ресурсов, как конфиденциальность, целостность и доступность. Для реализации атаки нарушитель использует определенную уязвимость АСУ, имеющую место как в организационно-правовом, так и в программно-аппаратном обеспечении. Рассматриваются современные методы и средства защиты информации, позволяющие комплексно решить проблему информационной безопасности АСУ.