ო. შონია, კ. ოდიშარია, გ. მაისურაძე

ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფა

რეზიუმე

ნაშრომში დეტალურადაა გაანალიზებული ინფორმაციის, როგორც ადამიანის, საზოგადოების და სახელმწიფოს ძირითადი რესურსების დაცვის პრობლემები. მოცემულია ამ პრობლემათა გადაწყვეტის ძირითადი მიმართულებები და დასაბუთებულია ინფორმაციული რესურსების დაცვის სისტემის შექმნის აუცილებლობა.

საკვანძო სიტყვები: ინფორმაციული უსაფრთხოება, ინფორმაციული ომი, ინფორმაციის დაცვა, დაცვის სისტემა, კრიპტოგრაფია.

ინტერნეტმა საფუძველი დაუდო გლობალური ინფორმაციული საზოგადოების ჩამოყალიბებას და ფაქტიურად „ახალი ინფორმაციული“ საუკუნის დადგომის მაუწყებელი გახდა.

დღეისათვის შეუძლებელია იმის განჭვრეტა, თუ რა სოციალური შედეგები შეიძლება მოიტანოს გლობალური ინფორმაციული სისტემის ფართოდ გავრცელებამ. ერთი რამ კი ცხადია, ინფორმაციული ტექნოლოგიების პროგრესმა წინა პლანზე წამოწია ინფორმაციის, ენერგიასთან და მატერიასთან ერთად, როგორც ნებისმიერი ადამიანის, საზოგადოებისა და სახელმწიფოს სასიცოცხლოდ მნიშვნელოვანი რესურსის დაცვის აუცილებლობა და პარალელურად – პიროვნების, საზოგადოების და სახელმწიფოს ინფორმაციული უსაფრთხოების პრობლემა (მხედველობაში გვაქვს წინასწარგანზრახული ინფორმაციული ზემოქმედებისაგან დაცვა).

სახელმწიფოს მხრიდან ყურადღებას და ხელშეწყობას საჭიროებს არა მარტო სახელმწიფო საიდუმლოებას მიკუთვნებული ინფორმაციის დაცვა, არამედ საერთოდ ქვეყანაში არსებული ინფორმაციული რესურსების (მიუხედავად მათი კუთვნილებისა), როგორც ნაციონალური რესურსების დაცვის უზრუნველყოფა. მსოფლიო ბევრი ქვეყნის გამოცდილება გვიჩვენებს, რომ ერთიანი ინფორმაციული სივრცის ფორმირება უნდა ხდებოდეს ინფორმაციული ინფრასტრუქტურის შექმნის, უსაფრთხოების მეთოდებისა და საშუალებების დანერგვის და შესაბამისი საკანონმდებლო-ნორმატიული ბაზის, მეცნიერული და საჭირო სპეციალისტთა კადრების მომზადებასთან ერთად. აღნიშნულიდან გამომდინარე, აუცილებელია მეცნიერი ექსპერტების მონაწილეობით შეიქმნას სახელმწიფოს, საზოგადოების და პიროვნების ინფორმაციული უსაფრთხოების დაცვის სისტემის კონცეფცია, რომლის ძირითადი მიზანია ხელი შეუწყოს:

ა) ელექტრონული დაცვის საშუალებების განსაზღვრას, შექმნას და დანერგვას;
ბ) ქვეყნის შიგნით გლობალური ფინანსური და ტელესაკომუნიკაციო სისტემების დაცვას;
გ) კომპიუტერული ქსელების დაცვას ინფორმაციული შეტევებისაგან;
დ) ცნობიერებით მანიპულირების წინააღმდეგ ბრძოლას;
ე) საგანგებო დაგეგმვას ინფორმაციულ ომში;
ვ) ინფორმაციული ომის ეთიკური პრობლემების გარკვევას; და ა. შ.

გამოცდილება გვიჩვენებს, რომ:

- ინფორმაციის დაცის უზრუნველყოფა არ შეიძლება იყოს ერთჯერადი აქტი.
- ინფორმაციის დაცვა შეიძლება უზრუნველყოფილ იქნას მხოლოდ დაცვის არსებული ყველა მეთოდებისა და საშუალებების კომპლექსური გამოყენებით საწარმოო სისტემის ყველა სტრუქტურულ ელემენტებში და ინფორმაციის დამუშავების მთელი ტექნოლოგიური ციკლის განმავლობაში.

მაქსიმალური ეფექტი მიიღწევა მაშინ, როცა გამოყენებული საშუალებები, მეთოდები და ზომები ქმნიან ერთიან მექანიზმს – **ინფორმაციის დაცვის სისტემას (იდს).** ამასთან ერთად, სისტემის ფუნქციონირება უნდა კონტროლირდებოდეს, ხდებოდეს მისი განახლება და სრულყოფა შიდა და გარეშე პირობების შეცვლასთან ერთად.

- ვერავითარი იდს ვერ უზრუნველყოფს ინფორმაციის საჭირო დონის დაცვას მომხმარებლის სათანადოდ მომზადებისა და მათ მიერ მისი დაცვის ყველა წესების შესრულების გარეშე.

ინფორმაციის დაცვის სისტემა შეიძლება განვსაზღვროთ, როგორც ორგანიზებული ერთობლიობა სპეციალური ორგანოების, საშუალებების, მეთოდებისა და ღონისძიებებისა, რომლებიც უზრუნველყოფენ ინფორმაციის დაცვას გარეშე და შიდა საფრთხეებისაგან.

ზოგადად ინფორმაციული უსაფრთხოების კონცეფციის ძირითადი კომპონენტები შეიძლება იყოს:

* საფრთხეების, მუქარების ობიექტები – ცნობები დაცვის ობიექტის შემადგენლობის, მდგომარეობის და მოღვაწეობის შესახებ. საკუთრივ დაცვის ობიექტი შეიძლება იყოს: პერსონალი, მატერიალური და ფინანსური ღირებულებები, ინფორმაციული რესურსები.

* საფრთხეები, მუქარები – ესაა ინფორმაციის მთლიანობის, კონფიდენციალობის, სისრულის და შეღწევადობის დარღვევის შესაძლებლობა.

* საფრთხეების, მუქარების წყაროები – ესაა კონკურენტები, ბოროტგანმზრახველები, კორუფციონერები, ადმინისტრაციულ-მმართველობითი ორგანოები და ა. შ.

* მუქარათა მიზნები ბოროტგანმზრახველების მხრიდან – ეს მიზნები შეიძლება იყოს დაცული ცნობების გაცნობა, მათი მოდიფიკაცია ანგარებისათვის და განადგურება პირდაპირი ზარალის მიყენების მიზნით.

* ინფორმაციის წყაროები – ესენია ადამიანები, დოკუმენტები, პუბლიკაციები, ინფორმაციის ტექნიკური მატარებლები, საწარმოო და შრომითი მოღვაწეობის უზრუნველყოფის ტექნიკური საშუალებები, პროდუქცია და საწარმოო ნარჩენები.

* კონფიდენციალური ინფორმაციის არამართლზომიერი დაუფლება (შეღწევის მეთოდები). კონფიდენციალური ინფორმაციის არამართლზომიერი დაუფლება შესაძლებელია მისი გათქმით ინფორმაციის წყაროს მიერ, ინფორმაციის გაჟონვით ტექნიკური საშუალებებიდან და დასაცავ ცნობებთან არასანქცირებულად შეღწევით.

* ინფორმაციის დაცვის მიმართულებები – ინფორმაციის დაცვის ძირითადი მიმართულებებია: სამართლებრივი დაცვა, ორგანიზაციული დაცვა და საინჟინრო-ტექნიკური დაცვა, რომლებიც ერთობლიობაში გამოხატავენ ინფორმაციის დაცულობის კომპლექსურობას.

* ინფორმაციის დაცვის საშუალებები – ესენია ინფორმაციის დაცვის ფიზიკური საშუალებები, აპარატურული საშუალებები, პროგრამული საშუალებები და მათემატიკური (კრიპტოგრაფიული) მეთოდები. კრიპტოგრაფიული მეთოდები შეიძლება რეალიზებული იყოს აპარატურულად, პროგრამულად და პროგრამულ-აპარატურულად.

* ინფორმაციის დაცვის ხერხები – დაცვის ხერხებად გამოიყენება ზომები, წესები და მოქმედებები, რომლებიც საშუალებას იძლევიან დავასწროთ კანონსაწინააღმდეგო ქმედებებისა, თავიდან იქნას ისინი აცილებული, არ მოხდეს არასანქცირებული შეღწევა ინფორმაციასთან.

ინფორმაციის დაცვის სისტემის ერთ-ერთი უმთავრეს კომპონენტს სამართლებრივ და ორგანიზაციულთან ერთად წარმოადგენს საინჟინრო-ტექნიკური დაცვა.

საინჟინრო-ტექნიკური დაცვა – ესაა ერთობლიობა ორგანოების, ტექნიკური საშუალებებისა და მათი გამოყენების ღონისძიებების კონფიდენციალური ინფორმაციის დაცვის ინტერესებისათვის.

საინჟინრო-ტექნიკური დაცვის კლასიფიკაცია შეიძლება მოხდეს: ა) ზემოქმედების ობიექტის მიხედვით; ბ) ღონისძიებების ხასიათის მიხედვით; გ) რეალიზაციის ხერხების მიხედვით; დ) მოცვის მასშტაბების მიხედვით; ე) დაცვის ტექნიკური საშუალებების კლასის მიხედვით; ვ) ბოროტგანმზრახველის მიერ გამოყენებული საშუალებების კლასის მიხედვით.

ფუნქციური დანიშნულების მიხედვით საინჟინრო-ტექნიკური დაცვის საშუალებები შეიძლება დაიყოს შემდეგ ჯგუფებად:

1. **ფიზიკური საშუალებები**, რომლებიც მოიცავენ სხვადასხვა საშუალებებს და ნაგებობებს, რომლებიც დაბრკოლებებს უქმნიან ბოროტგანმზრახველს ფიზიკურად შეაღწიოს დასაცავ ობიექტზე და კონფიდენციალური ინფორმაციის მატერიალურ მატარებლებთან, და ახორციელებს პერსონალის, მატერიალური საშუალებების, ფინანსების და ინფორმაციის დაცვას კანონსაწინააღმდეგო ზემოქმედებებისაგან.

2. **აპარატურული საშუალებები**. ამ საშუალებებს განეკუთვნებიან სრულიად სხვადასხვა პრინციპებზე მომუშავე მოწყობილობები, რომლებიც უზრუნველყოფენ კონფიდენციალური ინფორმაციის გათქმის თავიდან აცილებას,გაჟონვისაგან დაცვას და მასთან არასანქცირებულად შეღწევის აღკვეთას. ინფორმაციის დაცვის აპარატურული საშუალებები გამოიყენება შემდეგი ამოცანების გადასაწყვეტად:

- დასაცავი ობიექტების სპეციალური შესწავლა ინფორმაციის გაჟონვის არხების არსებობაზე;
- ინფორმაციის გაჟონვის არხების ლოკალიზაცია;
- საწარმოო შპიონაჟის საშუალებების ძებნა და აღმოჩენა;
- წინააღმდეგობის გაწევა კონფიდენციალური ინფორმაციის წყაროსთან არასანქცირებულად შეღწევისა და სხვა ქმედებებისადმი.

3. **დაცვის პროგრამული საშუალებები.** კომპიუტერის დაცვა სხვის მხრიდან შემოჭრისაგან ძალზე მრავალფეროვანია და მისი კლასიფიკაცია შეიძლება იყოს ასეთი:

- საკუთარი დაცვის საშუალებები, რომლებიც გათვალისწინებულია საერთო პროგრამულ უზრუნველყოფაში;
- დაცვის საშუალებები გამოთვლითი სისტემის შემადგენლობაში;
- დაცვის საშუალებები ინფორმაციის მოთხოვნით. აღნიშნული საშუალებები საჭიროებენ დამატებითი ინფორმაციის შეტანას მომხმარებელთა უფლებამოსილების დასადგენად.
- აქტიური დაცვის საშუალებები, მათი ინციირება ხდება მაშინ, როცა წარმოიშობა საგანგებო მდგომარეობები: არასწორი პაროლის შეტანისას; არასწორი რიცხვისა და დროის მითითება პროგრამის გაშვებისას; ნებართვის გარეშე ინფორმაციასთან შეღწევის მცდელობისას და ა. შ.
- დაცვის პასიური საშუალებები.

შეიძლება გამოიყოს კონფიდენციალური ინფორმაციის დაცვის მიზნით პროგრამების გამოყენების შემდეგი ძირითადი მიმართულებები:

- ინფორმაციის დაცვა არასანქცირებული შეღწევისაგან;
- ინფორმაციის დაცვა კოპირებისაგან;
- პროგრამების დაცვა კოპირებისაგან;

- პროგრამების დაცვა ვირუსებისაგან;
- კავშირგაბმულობის არხების პროგრამული დაცვა.

დაცვის პროგრამულ საშუალებებს გააჩნია სპეც-პროგრამების შემდეგი მრავალსახეობები:

- ტექნიკური საშუალებების, ფაილების იდენტიფიკაცია და მომხმარებლის აუდენტიფიკაცია;
- რეგისტრაცია და კონტროლი ტექნიკური საშუალებების და მომხმარებლების მუშაობის;
- შეზღუდული მოხმარების ინფორმაციის დამუშავების რეჟიმების მომსახურება;
- კომპიუტერის ოპერაციული საშუალებების და გამოყენებითი პროგრამების დაცვა;
- დაცვის მოწყობილობებში ინფორმაციის განადგურება დამუშავების შემდეგ;
- რესურსების გამოყენების დარღვევის სიგნალიზაცია;
- სხვადასხვა დანიშნულების დამხმარე დაცვის პროგრამები.

4. **კრიპტოგრაფიული საშუალებები** – ესაა სპეციალური მათემატიკური და ალგორითმული საშუალებები ინფორმაციის დაცვისა, რომელიც გადაიცემა კავშირის სისტემებისა და არხების მეშვეობით მუშავდება და ინახება კომპიუტერში დაშიფვრის სხვადასხვა მეთოდების გამოყენებით.

დასკვნა

ამრიგად, ინფორმაციული ტექნოლოგიების სწრაფმა განვითარებამ, მათი ცხოვრებაში ფართოდ დანერგვამ, „ახალი ინფორმაციული“ საზოგადოების ჩამოყალიბებამ წარმოშვა გლობალური პრობლემა ადამიანის, საზოგადოებისა და სახელმწიფოს უსაფრთხოების უზრუნველყოფის თვალსაზრისით. აუცილებელია აღნიშნული პრობლემა წყდებოდეს სისტემურად, ახალი ტექნოლოგიების შექმნისა და დანერგვის პარალელურად.

ლიტერატურა

1. ჩოგოვაძე გ. ინფორნაცია: ინფორმაცია, საზოგადოება, ადამიანი. თბილისი, 2003.
2. შონია ო. სახელმწიფო უსაფრთხოების უზრუნველყოფის გადაწყვეტილებათა მიღების მხარდამჭერი ავტომატიზებული სისტემა. თბილისი, 2004.
3. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. М.,МИФИ,1995.

О. Шония, К. Одишария, Г. Маисурадзе

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Резюме

В работе детально представлен анализ информации, как основной ресурс по проблеме защиты человека, общества и государства. Даны основные направления по решению этих проблем и обоснована необходимость создания информационных ресурсов по защите системы.

Summary

The article represents us information analysis in details, as the basic resource on a problem for protecting human, society and state. It does given the mainstream for determine this problems as the necessity of creation this information resources for protecting system.