ლევან ჟუთათელაძე

ინფორმაციული უსაფრთხოების სისტემის აგების პრინციპები

ლევან ჟუთათელაძე
სტუ-ს დოქტორანტი

საფინანსო-საბანკო დაწესებულების ინფორმაციული უსაფრთხოების სისტემა – ეს არის მთელი რიგი ანტიქმედებების ერთობლიობა, რომელთა მხოლოდ ნაწილი ხვდება დაწესებულების მენეჯმენტის კონტროლის ქვეშ. კომპიუტერული სისტემების უსაფრთხოების უზრუნველყოფის ყველა მოქმედება იყოფა: საკანონმდებლო, მორალურ-ეთიკურ, ადმინისტრაციულ, ფიზიკურ და ტექნიკურ (აპარატულ-პროგრამულ) მეთოდებად.

დაცვის საკანონმდებლო ღონისძიებებს მიეკუთვნება ქვეყანაში მოქმედი კანონები, მითითებები და სხვა ნორმატიული აქტები, შეზღუდული გამოყენების ინფორმაციასთან რეგლამენტირებული წესების გამოყენება და პასუხისმგებლობა ამ წესების დარღვევაზე. ამით ისინი ეწინააღმდეგებან ინფორმაციის არასანქცირებულ გამოყენებას და წარმოადგენენ პოტენციური დამრღვევისათვის შემაჩერებელ ფაქტორს.

ინფორმაციული უსაფრთხოების უზრუნველყოფის *მორალურ-ეთიკურ ღონისძიებებს* მიეკუთვნება ქცევის ნორმები, რომლებიც ტრადიციულად დამკვიდრდა ან მკვიდრდება ქვეყანაში ან საზოგადოებაში კომპიუტერების გავრცელების მოცულობის მიხედვით. მორალურ-ეთიკური ნორმები არის, როგორც დაუწერელი ნორმები (პატიოსნების საყოველთაო ნორმები, პატრიოტიზმი და სხვა), ასევე ისეთი წესების ჩამონათვალი, რომელთა შორის ერთერთი დამახასიათებელი მაგალითია "აშშ-ის კომპიუტერის მომხმარებელთა ასოციაციის წევრთა პროფესიონალური მოქმედების კოდექსი".

დაცვის ადმინისტრაციული ღონისძიებები – ეს არის ორგანიზებული ხასიათის მოქმედებები, რომლებშიც რეგლამენტირებულია სისტემის ფუნქციონირებისას ინფორმაციის დამუშავების პროცესები, მისი რესურსების გამოყენება, პერსონალის მოქმედება. ასევე სისტემასთან მომხმარებელთა მოქმედების თანმიმდევრობა ისე, რომ გაართულოს ან სრულიად გამორიცხოს უსაფრთხოებაზე ზემოქმედების მუქარა.

დაცვის ფიზიკური ღონისძიებები – ეს სხვადასხვა სახის მექანიკური, ელექტრო ან ელექტრო-მექანიკური მოწყობილობები და აღჭურვილობაა, რომლებიც ემსახურება სისტემის სხვადასხვა კომპონენტებსა და დაცულ ინფორმაციაში პოტენციური დამრღვევებისათვის ფიზიკური წინააღმდეგობის შექმნას.

დაცვის ტექნიკური (აპარატულ-პროგრამული) საშუალებები ეწოდებათ სხვადასხვა ელექტრონულ მოწყობილობებს და სპეციალურ პროგრამებს, რომლებიც ასრულებენ (დამოუკიდებლად ან სხვა საშუალებებთან ერთად) დაცვის ფუნქციას (მომხმარებელთა იდენტიფიკაცია და აუნტენტიფიკაცია, რესურსებთან შეღწევის შეზღუდვა, მოვლენათა რეგისტრაცია და სტატისტიკა, ინფორმაციის კრიპტოგრაფიული დაცვა და სხვა).

ნათელია, რომ დაბალი დონის დისციპლინის, ეთიკისა და სამართლებრივ სტრუქტურებში ინფორმაციის დაცვის საკითხის დაყენებას აზრი არა აქვს. ამიტომ პირველ რიგში უნდა გადაწყდეს სამართლებრივი და ორგანიზაციულ-ადმინისტრაციული საკითხები.

ადმინისტრაციულ ზომებს ასევე დიდი მნიშვნელობა აქვთ ინფორმაციული სისტემის უსაფრთხოების უზრუნველყოფაში. ეს ზომები აუცილებელია გამოვიყენოთ მაშინ, როცა დაცვის სხვა მეთოდები და საშუალებები მიუღწეველია (არ არსებობენ ან ძალიან ძვირია). მაგრამ ეს არ ნიშნავს, რომ დაცვის სისტემა უნდა ავაგოთ აუცილებლად ადმინისტრაციულ მეთოდებზე, რასაც ხშირად აკეთებენ ჩინოვნიკები, რომლებიც შორს არიან ტექნიკური პროგრესისგან.

ადმინსტრაციული ღონისძებები, სადაც კი აუცილებელია, ყველგან შეიძლება შეიცვლოს ფიზიკური და ტექნიკური საშუალებებით. მათ უნდა უზრუნველყონ სხვადასხვა მეთოდებისა და დაცვის საშუალებების ეფექტიანი გამოყენება იმ ნაწილში, რომელიც ეხება ადამიანთა მოქმედების რეგლამენტირებას.

თანამედროვე ბიზნესის ძირითადი საკითხი – ეს არის ინფორმაციულ უსაფრთხოებაში დაბანდებების საჭირო დონის შეფასება, რაც

უზრუნველყოფს მოცემულ სფეროში ინვესტიციის მაქსიმალურ ეფექტიანობას. ამ საკითხის გადასაწყვეტად არსებობს მხოლოდ ერთი მეთოდი - რისკების ანალიზის სისტემა, რომელიც საშუალებას იძლევა შევაფასოთ სისტემაში არსებული რისკები და ავირჩიოთ ინფორმაციის დაცვის ვარიანტებიდან ოპტიმალურად ეფექტიანი. სტატისტიკის მიხედვით, საფინანსო-საბანკო ორგანიზაციის ინფორმაციული უსაფრთხოების უზრუნველყოფის საკითხის განხილვისას არის დიდი წინააღმდეგობები. მათგან მთავარია ორი:

- შეზღუდული ბიუჯეტი.
- ხელმძღვანელობის არასაკმარისი მხარდაჭერა.

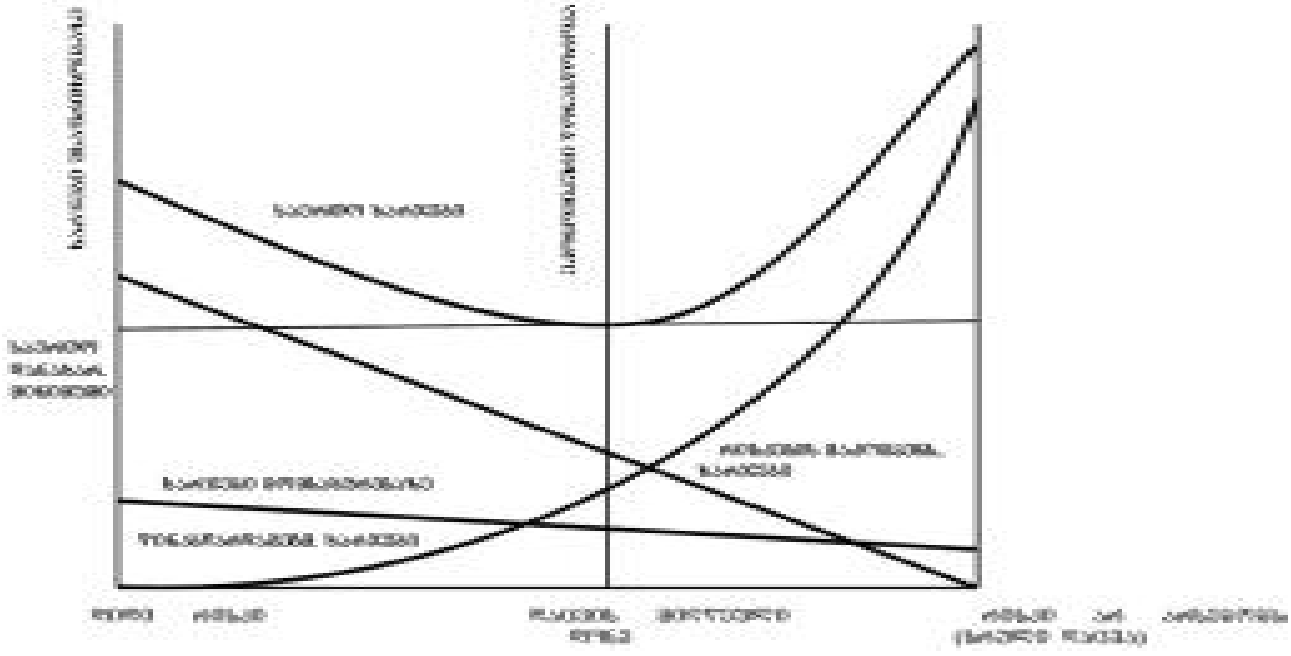
ორივე მიზეზი ჩნდება მაშინ, როცა ხელმძღვანელობას არ ესმის საკითხის სერიოზულობა და სირთულე, თუ რატომ უნდა ჩადონ თანხები ინფორმაციულ უსაფრთხოებაში. თუ საინფორმაციო განყოფილებას შესწავლილი აქვს საკითხი, რამდენს დაკარგავს კომპანია საფრთხის რეალიზაციისას. თუ დაადასტურებს დოკუმენტალურად რამდენი თანხა უნდა დაიხარჯოს და რა სამუშაო უნდა იქნეს ჩატარებული დაცვის დონის ამაღლებისთვის, მაშინ ხელმძღვანელობის დარწმუნება ინფორმაციული უსაფრთხოებისთვის საჭირო თანხის გამოყოფაზე უფრო რეალური გახდება. საფინანსო-საბანკო დაწესებულებაში ინფორმაციული უსაფრთხოების დაცვის ეფექტიანი ორგანიზების განსაზღვრა გულისხმობს ინფორმაციულ უსაფრთხოებაზე დანახარჯების ერთგვარ შეფასებას.

ნახ.1.-ზე მოცემული გრაფიკიდან ჩანს, რომ დაცვის დონე განისაზღვრება ინტერვალში "დიდი რისკი" და "რისკი არ არსებობს (სრული დაცვა)". გრაფიკის მარცხენა მხარის განხილვისას (დიდი რისკი) ჩვენ ვხედავთ, რომ საერთო დანახარჯები უსაფრთხოებაზე ძირითადად იმის გამოა მაღალი, რომ დიდია დანახარჯები უსაფრთხოების დარღვევისას რისკების კომპენსაციაზე. უსაფრთხოების სისტემის მომსახურების ხარჯები ძალიან მცირეა. გრაფიკის მიხედვით მარჯვნივ მოძრაობისას დაცულობის დონე იზრდება (ინფორმაციული რისკი მცირდება). ეს ხდება დაცვის სისტემის მომსახურებასთან დაკავშირებული წინასწარდაგეგმილი ღონისძიებების ზრდის ხარჯზე.

წინასწარდაგეგმილ ღონისძიებებზე ხარჯების ზრდის პარალელურად უსაფრთხოების პოლიტიკის დარღვევის კომპენსაციის ხარჯები მცირდება. როგორც გრაფიკზე ჩანს, ამ სტადიაზე ხარჯები დანაკარგებზე ეცემა უფრო სწრაფად, ვიდრე იზრდება წინასწარდაგეგმილი ხარჯები. ამის შედეგად უსაფრთხოებაზე საერთო დანახარჯები მცირდება.

ეკონომიკური წონასწორობის წერტილის შემდეგ მარჯვენა მიმართულებით მოძრაობისას, (ე.ი. ინტერვალში, სადაც მიღწეული დაცულობის დონე იზრდება) სიტუაცია იცვლება. ჩვენ ვხედავთ, რომ უსაფრთხოების პოლიტიკის დარღვევის კომპენსაციაზე ხარჯების შემცირებისკენ სწრაფვას მივყავართ წინასწარდაგეგმილი ღონისძიებებისათვის ხარჯების სწრაფ ზრდასთან. გამოდის, რომ მნიშვნელოვანი მოცუ-

ნახ. 1



ლობის ხარჯების საფასურად შეიძლება მივაღწიოთ რისკის შედარებით ნაკლებ შემცირებას.

ზემოთ ხსენებულის საფუძველზე შეიძლება გამოვიტანოთ დასკვნა: ინფორმაციული უსაფრთხოების უზრუნველყოფა მხოლოდ პროგრამული და ტექნიკური საშუალებებით შეუძლებელია. ეკონომიკური თვალსაზრისით, მაღალეფექტიანი, ოპტიმალური ინფორმაციული უსაფრთხოების სისტემა – ეს არის მონაცემთა დაცვის კლასიკური საშუალებების ეკონომიკურ მეთოდებთან შერწყმა.

ინფორმაციის დაცვის სფეროში მრავალი გადაწყვეტილება ხშირად იგეგმება ინტუიციურ დონეზე, ყოველგვარი ეკონომიკური გამოთვლების და დასაბუთების გარეშე. მხოლოდ ბიზნესის თანამედროვე მოთხოვნები, რომლებიც წაეყენება ორგანიზაციის ინფორმაციული უსაფრთხოების რეჟიმს, განსაკუთრებულად უწევენ რეკომენდაციას გაცილებით უფრო საფუძვლიან ტექნიკურ-ეკონომიკურ მეთოდებს და საშუალებებს, რომლებითაც შესაძლებელი ხდება კომპანიის დაცულობის დონის რაოდენობრივი შეფასება.

პრაქტიკაში ფართოდაა გავრცელებული ინფორმაციული უსაფრთხოების სისტემის ეფექტიანობის შეფასების მეთოდები, რომლებიც დაფუძნებულია ისეთი ფინანსური მახასიათებლების შეფასებაზე, როგორიცაა – ROI. ROI – ეს არის ინტეგრალური კრიტერიუმი, რომელიც საშუალებას იძლევა შეფასდეს, რამდენად ეფექტიანად მუშაობს კომპანიაში დაბანდებული ფული. სხვა სიტყვებით, რამდენ ფულს "ქმნის" კომპანიაში დაბანდებული 1 ლარი ერთ წელიწადში.

გამოყენებული ლიტერატურა

1. ცაავა გ., აბრამია თ., ცაავა დ., რისკოლოგია. თბილისი, გამომცემლობა "აფხაზეთის მეცნიერებათა აკადემია", 2007.
2. Ярочкин В., И., Безопасность банковских систем. Издательство «Ось – 89», Москва, 2009.

ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЛЕВАН КУТАТЕЛАДЗЕ - докторант ГТУ

Система информационной безопасности финансого-банковского учреждения – это совокурность целого ряда мер противодействия, при этом только часть из них находится в сфере влияния менеджмента компании. По способам осуществления все меры обеспечения безопасности компьютерных систем подразделяются: на правовые (законодательные), морально-этические, административные, физические и технические (аппаратные и програмные).

Очевидно, что в структурах с низким уровнем правопорядка, дисциплины и этики ставить вопрос о защите информации просто бессмисленно. В связи с этим прежде всего надо решать правовые и организационные вопросы. Основной вопрос современного бизнеса – как оценить необходимый уровень вложений в информационную безопасность, чгобы обеспечить максимальную эффективность инвестиций в данную сферу. Для решения этого вопроса существует только один способ – применять систему анализа рисков, позволяющую оценить существующие в системе риски и выбрать оптимальный по эффективности вариант защиты.

PRINCIPLES OF INFORMATION SECURITY SYSTEM CONSTRUCTION

LEVAN QUTATELADZE - PhD student of GTU

Information security system in financing-banking organizations – is an unity of anti-activities only the part of which flows under control of the management of the organization. All activities concerning computer system security provision are divided to as: legislation, moral-ethics, administrative, physical and technical (equipment-program) methods.

It is useless to raise a question of information security in organizations with the low level of discipline, ethics and legislation. As a result, legislation and organizational-administrative issues should be solved first.

The basic issue of modern business is to evaluate necessary level of investments in information security that provides the highest level of investments' effectiveness in the given sector. There is only one method to solve this issue – risk analysis system that provides opportunity to evaluate risks existing in the system and select the most effective way from information security options.