ინფორმაციული უსაფრთხოება
(მიმოხილვა)

კახაბერ ჟამურაშვილი, დოქტორანტი

რეზიუმე

ინფორმაციული ტექნოლოგიებით სარგებლობა მის განვითარებასთან ერთად კიდევ უფრო აქტუალური გახდა, სწორედ ამიტომ კრიტიკულ მნიშვნელობას იძენს მისი ეფექტური და უსაფრთხო გამოყენება, სტანდატების ჩამოყალიბება მისი მნიშვნელობისა და გავრცელების სფეროს განსაზღვრა, სტატიაში განხილული საკითხები ხელს უწყობს ინფორმაციული უსაფრთხოების სამი ძირითადი კომპონენტის უზრუნველყოფას როგორიც არის ინფორმაციის: მთლიანობა, კონფიდენციალურობა და ხელმისაწვდომობა.

Information security review

Kakhaber Jamurashvili

Summary

Information technology for use in its development with even more urgency, the amitimom critical importance of effective and safe to use, standards in light of its importance and scope define discussed issues contributes to information security are three main components to support such as information: integrity, confidentiality and availability.

* * * * *

ინფორმაციული უსაფრთხოების მიზანია ყველა სახის და წარმომავლობის ინფორმაციის დაცვა. ეს ინფორმაცია შეიძლება ინახებოდეს როგორც ქაღალდზე, ასევე კომპიუტერულ სისტემებში, ან თუნდაც მომხმარებელთა გონებაში. IT უსაფრთხოება დაკავებულია პირველ რიგში ელექტრონულად შენახული ინფორმაციის უსაფრთხოებაზე და მის დამუშავებაზე. ინფორმაციული უსაფრთხოების კლასიკური საბაზო ფასეულობებია კონფიდენციალობა, მთლიანობა და წვდომა. „საინფორმაციო სისტემების მენეჯმენტის საერთაშორისო გამოცდილება“ ინფორმაციული უსაფრთხოების სხვა გენერირებული ზოგადი ტერმინებია, მაგალითად, აუთენთიციტეტი, პასუხისმგებლობა, საიმედოობა და უმტყუნობა. ინფორმაციის უსაფრთხოებას ემუქრება არა მხოლოდ განზრახ ქმედებები (მაგალითად, კომპიუტერული ვირუსები, ინფორმაციის წართმევა/მოსმენა, კომპიუტერის ქურდობა). შემდეგი მაგალითები იძლევა ამის ილუსტრაციას: დაუძლეველი ძალის მიერ (როგორიცაა ცეცხლი, წყალი, ქარიშხალი, მიწისძვრა) მედია–მატარებლები და IT-სისტემები დაზარალებულია ან ჩაშლილია ხელმისაწვდომობა მონაცემთა ცენტრში. დოკუმენტები, Iთ-სისტემები ან სამსახურები აღარაა სურვილისამებრ ხელმისაწვდომები; მას შემდეგ, რაც მოხდა წარუმატებელი პროგრამული განახლება, აპლიკაციები აღარ ფუნქციონირებს ან მონაცემები შეუმჩნევლად შეიცვალა; მნიშვნელოვანი ბიზნეს პროცესი ჭიანურდება, რადგან ერთადერთი ადამიანი, ვინც იცნობს პროგრამებს, ავადაა; კონფიდენციალური ინფორმაცია შემთხვევით გადაეცა არასანქცირებული პირს, რადგან დოკუმენტები ან ფაილი არ იყო მონიშნული, როგორც „საიდუმლო”. „საინფორმაციო სისტემების მენეჯმენტის საერთაშორისო გამოცდილება“ ელექტრონული დამუშავება გავრცელებულია ცხოვრების თითქმის ყველა სფეროში, აღარ აქვს მნიშვნელობა განსხვავებას, ინფორმაცია მუშავდება ინფორმაციული ტექნოლოგით, საკომუნიკაციო ტექნოლოგიით თუ ქაღალდზე. ტერმინი საინფორმაციო უსაფრთხოება, ნაცვლად IT უსაფრთხოებისა, ყოვლისმომცველია და ამიტომ უფრო შესაფერისი. თუმცა, ლიტერატურაში გამოიყენება ძირითადად ტერმინი „IT უსაფრთხოება” (რადგან ეს მოკლეა). წინამდებარე ნაშრომშიც იქნება გამოყენებული ეს ტერმინი, ან შესაბამისი ტერმინი „IT საბაზო დაცვა“ [1].

ინფორმაციული უსაფრთხოების სტანდარტების მოკლე მიმოხილვა ინფორმაციული უსაფრთხოების სფერში სხვადასხვა სტანდარტები შემუშავდა, რომლებშიც ნაწილობრივ სხვადასხვა მიზნობრივი ჯგუფები ან თემატური სფეროები არის წინა პლანზე წამოწეული. უსაფრთხოების სტანდარტების გამოყენება ბიზნესში ან ხელისუფლებაში არა მხოლოდ აუმჯობესებს უსაფრთხოების დონეს, ის ასევე ხელს უწყობს სხვადასხვა დაწესებულებებს შორის კოორდინაციას, რომლებშიც უსაფრთხოების ზომები უნდა განხორციელდეს ნებისმიერი ფორმით. ქვემოთ, შემდეგი მიმოხილვა გვიჩვენებს ყველაზე მნიშვნელოვანი სტანდარტების მიმართულებებს.

ISO–სტანდარტები ინფორმაციული უსაფრთხოებისთვის ISO და IEC საერთაშორისო ნორმების ორგანიზაციებში გადწყდა, რომ ინფორმაციული უსაფრთხოების სტანდარტები გაერთიანებულიყო 2700x სერიაში, რომელიც მუდმივად იზრდება. მნიშვნელოვანი სტანდარტებია: „საინფორმაციო სისტემების მენეჯმენტის საერთაშორისო

გამოცდილება“ ISO 2700x ეს სტანდარტი იძლევა ზოგად მიმოხილვას ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემების (ISMS) და მათი ურთიერთდამოკიდებულების შესახებ ISO 2700 x –ოჯახის სხვადასხვა სტანდარტებს შორის. აქვე გადმოცემულია ISMS–ის ძირითადი პრინციპები, კონცეფციები, ტერმინები და განსაზღვრებანი. ISO 27001 საინფორმაციო ტექნოლოგიების სირთულისა და სერთიფიკატებზე მოთხოვნების გამო მრავალი ინსტრუქცია, სტანდარტი და ინფორმაციული უსაფრთხოების ეროვნული სტანდარტები წარმოიშვა ბოლო წლებში. სტანდარტი ISO 27001 – “ინფორმაციული ტექნოლოგია - უსაფრთხოების ტექნიკა - ინფორმაციული უსაფრთხოების მართვის სისტემის მოთხოვნების სპეციფიკაცია” არის პირველი საერთაშორისო სტანდარტი ინფორმაციული უსაფრთხოების მართვაში, რომელიც ასევე სერტიფიცირების საშუალებას იძლევა. ISO 27001 იძლევა 10 გვერდიან ზოგად რეკომენდაციებს, მათ შორის შესავლის (დანერგვის), ექსპლუატაციის და დოკუმენტირებული ინფორმაციის უსაფრთხოების მართვის სისტემის სრულყოფისთვის, ასევე რისკების გათვალისწინებით. ნორმატიულ დანართში მოხსენიებულია კონტროლი ISO / IEC 27002 –დან. თუმცა, მკითხველი არ იღებს დახმარებას პრაქტიკული განხორციელებისთვის. ISO 27002 ISO 27002–ის (ყოფილი ISO 17799:2005) “ინფორმაციული ტექნოლოგიები - ინფორმაციული უსაფრთხოების მენეჯმენტის საპროცესო კოდექსი” მიზანია ინფორმაციული უსაფრთხოების მენეჯმენტის ჩარჩოს განსაზღვრა. ფუნქციონირებადი უსაფრთხოების მენეჯმენტის ასაგებად და ორგანიზაციაში მიმაგრებას. აუცილებელი უსაფრთხოების ზომები მოკლედაა აღწერილი ISO-სტანდარტის ISO/IEC 27002–ში, დაახლოებით 100 გვერდზე. რეკომენდაციები, რომელიც განკუთვნილია მართვის დონისთვის და, შესაბამისად, შეიცავს მცირე კონკრეტულ ტექნიკურ შენიშვნებს. უსაფრთხოებისის რეკომენდაციების რეალიზაცია არის ერთ–ერთი გზა მრავალი შესაძლებლობიდან, რომლებიც აკმაყოფილებსის რეკომენდაციების რეალიზაცია არის ერთ–ერთი გზა მრავალი შესაძლებლობიდან, რომლებიც აკმაყოფილებს ISO 27002–ის რეკომენდაციების რეალიზაცია არის ერთ–ერთი გზა მრავალი შესაძლებლობიდან, რომლებიც აკმაყოფილებს ISO სტანდარტის 27001–ის მოთხოვნებს. შენიშვნა: ISO 17799 სტანდარტი 2007 წლის დასაწყისში გადაეცა არსებითი ცვლილებების გარეშე ISO 27002–ს, იმისათვის, რომ ხაზი გაესვათ მის მიკუთვნებაზე ISO 2700x სერიისთვის. ISO 27005 ეს ISO–სტანდარტი „ინფორმაციული უსაფრთხოების რისკების მენეჯმენტი“ შეიცავს ძრითად რეკომენდაციებს რისკების მართვის შესახებ ინფორმაციული უსაფრთხოებისთვის. მათ შორის იგი მხარს უჭერს ISO/IEC 27001 სტანდარტის მოთხოვნების რეალიზაციას. ოღონდ აქ არავითარი მეთოდი რისკების მართვისთვის არაა მოცემული. ISO/IEC 27005 ცვლის ISO 13335-2 სტანდარტს. ეს სტანდარტი ISO 13335-2 „უსაფრთხოების ინფორმაციულ–კომუნიკაციური ტექნოლოგიები, ნაწ.2: რისკების მენეჯმენტის მეთოდები ინფორმაციულ უსაფრთხოებაში“, იძლეოდა ინსტრუქციებს ინფორმაციული უსაფრთხოების მენეჯმენტისთვის. ISO 27006 ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემებში“, განსაზღვრავს აკრედიტაციის მოთხოვნებს სერტიფიცირების ორგანოებისთვის ISMS–ში და განიხილება ამ სერტიფიცირების პროცესების თავისებურებანი. ISO-2700x- რიგის სხვა სტანდარტები ISO 2700x სტანდარტული სერია სავარაუდოდ გრძელვადიან პერსპექტივაში ISO სტანდარტების 27000-27019 27030-27044 სახით დაკომპლექტდება. ამ სერიის ყველა სტანდარტი მოიცავს უსაფრთხოების მართვის სხვადასხვა ასპექტებს და ეფუძნება ISO 27001–მოთხოვნებს. სხვა სტანდარტების მიზანია გააუმჯობესოს გაგება და პრაქტიკული გამოყენების ISO 27001–ის. ეს შეთანხმებაა, მაგალითად, ISO 27001– ის პრაქტიკული განხორციელებისთვის, ანუ რისკების შეფასება ან რისკების მართვის მეთოდებია [2-3].

ბრიტანეთის სტანდარტიზაციის ინსტიტუტის მიერ დამტკიცებული სტანდარტები ინფორმაციული უსაფრთხოებისთვის: თემა IS მენეჯმენტი 100-1 ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემები (ISMS) ეს სტანდარტი განსაზღვრავს ISMS–ის ზოგად მოთხოვნებს. ეს არის სრულად თავსებადი ISO სტანდარტის 27001 და კვლავაც გაითვალისწინებს რეკომენდაციებს ISO სტანდარტების 27000 და 27002. იგი სთავაზობს მკითხველს ადვილად გასაგებ და სისტემატურ ინსტრუქციებს, მიუხედავად იმისა, თუ რომელი მეთოდის საშუალებით სურთ მათ მოთხოვნების განახორციელება. BSI წარმოადგენს ISO სტანდარტის შინაარსს საკუთარ BSI სტანდარტში, გარკვეული საკითხების უფრო დეტალურად აღსაწერად, და ამით შინაარსის დიდაქტიკური წარმოდგენის საშუალება მიეცეს. გარდა ამისა, სტრუქტურა იყო ისე დამუშავებული, რომ იგი თავსებადია IT-საბაზო დაცვის მეთოდებთან. უნიფიცირებული სათაურების საშუალებით აღნიშნულ დოკუმენტებში მკითხველისთვის ძალიან მარტივია ორიენტაირება. 100-2 IT- საბაზო დაცვა–მეთოდიკა IT–საბაზო–დაცვა–მეთოდიკა აღწერს ეტაპობრივად, ნაბიჯ– ნაბიჯ, თუ როგორ უნდა აიგოს ინფორმაციული უსაფრთხოების „საინფორმაციო სისტემების მენეჯმენტის საერთაშორისო გამოცდილება“ მენეჯმენტის სისტემა პრაქტიკულად და როგორ მოხდეს მისი ექსპლუატაცია. ინფორმაციული უსაფრთხოების მენეჯმენტის ამოცანები და ორგანიზაციული სტრუქტურის აგება ინფორმაციული უსაფრთხოებისთვის ძალზე მნიშვნელოვანი თემებია. IT–საბაზო–დაცვა–მეთოდიკა დეტალურად განიხილავს იმას, თუ როგორ შეიძლება უსაფრთხოების კონცეფ-

ციის (პოლიტიკის) დამუშავება პრაქტიკაში, როგორ აირჩევა შესაბამისი უსაფრთხოების ზომები და რა შეიძლება ჩაითვალოს უსაფრთხოების კონცეფციის რეალიზაციად. ასევე საკითხი, როგორ ხდება ინფორმაციული უსაფრთხოების მხარდაჭერა და სრულყოფა ექსპლუატაციის პირობებში, არის ამომწურავად პასუხგაცემული. IT–საბაზო-დაცვა BSI-Standard 100-2 სტანდარტთან კავშირში, ახდენს აქამდე დასახელებული 27000, 27001 და 27002 ISO-სტანდარტების ძალზე ზოგადად მიღებული მოთხოვნების ინტერპრეტირებას და ეხმარება მომხმარებლებს პრაქტიკაში რეალიზაციის დროს, მრავალი შენიშვნით, საცნობარო ინფორმაციით და მაგალითით. IT–საბაზო–დაცვის–კატალოგები ხსნიან არა მხოლოდ იმას, თუ რა უნდა გაკეთდეს, არამედ იძლევა ძალიან კონკრეტულ შენიშვნას, თუ როგორ უნდა გამოიყურებოდეს რეალიზაცია (ასევე ტექნიკურ დონეზე). პროცესი IT–საბაზო–დაცვის მიხედვით არის აპრობირებული და ეფექტური შესაძლებლობა, ზემოჩამოთვლილ ISO-სტანდარტის ყველა მოთხოვნის შესასრულებლად. 100-3 რისკების ანალიზი IT–საბაზო–დაცვის საფუძველზე BSI–მ დაამუშავა რისკების ანალიზის მეთოდიკა IT–საბაზო– დაცვის საფუძველზე. მის გამოყენებას აზრი აქვს მაშინ, როცა კომპანიები ან სახელმწიფო დაწესებულებები მუშაობენ წარმატებით IT–საბაზო–დაცვასთან და უჩნდებათ სურვილი დამატებითი უსაფრთხოების ანალიზის ჩასატარებლად, „საინფორმაციო სისტემების მენეჯმენტის საერთაშორისო გამოცდილება“ 100-4 საგანგებო სიტუაციათა მენეჯმენტი BSI Standard 100-4 სტანდარტში ახსნილია სახელმწიფო დაწესებულებათა ან კომპანიების მასშტაბებში საგანგებო სიტუაციათა მენეჯმენტის აგების და ექსპლუატაციის მეთოდიკა. აქ აღწერილი მეთოდიკა ეფუძნება BSI-Standard 100-2 სტანდარტის IT–საბაზო–დაცვის–მეთოდიკას და აფართოვებს მას სასარგებლოდ. ISO 27001 სერტიფიცირება IT–საბაზო–დაცვის საფუძველზე BSI ახდენს საინფორმაციო ქსელების სერტიფიცირებას, ანუ ინფრასტრუქტურული, ორგანიზაციული, პერსონალური და ტექნიკური კომპონენტების ურთიერთმოქმედებას, რომლებიც გამოიყენება ბიზნეს–პროცესების და ტაქნიკური დავალებების სარეალიზაციოდ. BSI სერტიფიცირება მოიცავს როგორც გამოცდას ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემებში, ასევე გამოცდას კონკრეტულ უსაფრთხოებიზ ზომებში IT–საბაზო– დაცვის საფუძველზე. BSI სერტიფიცირება ამასთანავე ყოველთვის მოიცავს ოფიციალურ ISO–სერტიფიცირებას ISO 27001–ის მიხედვით, მაგრამ ბევრად მნიშვნელოვანია, ვიდრე უბრალოდ ISO–სერტიფიცირება, დამატებითი კვლევით–ტექნიკური ასპექტების გამო. უსაფრთხოების მენეჯმენტის გამოცდის ძირითადი მოთხოვნები აუდიტის ჩარჩოებში (კონტექსტში) აღმოცენდება უსაფრთხოების მენეჯმენტის საბაზო დაცვის ბლოკის (B 1.0) ღონისძიებებიდან. ამ ბლოკის ეს ზომები ისეა დაწერილი, რომ ISMS-ის BSI–სტანდარტის მნიშვნელოვანი მოთხოვნები სწრაფად იყოს იდენტიფიცირებული განსაზღრული.

გამოყენებული ლიტერატურა:

1. http://en.wikipedia.org/wiki/BSI_GrouZertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Prüfschema für ISO 27001-Audits, BSI, Version

2. www.bsi.bund.de/gshb/zert

3. COBIT Overview ISACA. http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx.

4. surgulaZe g., gulua d., uruSaZe b., kaSibaZe m. organizaciis sainformacio infrastruqturis avtomatizebis Tanamedrove meTodebi.

5. sainformacio sistemebis menejmentis saerTaSoriso gamocdileba (BSI, ITIL, COBIT) gia surgulaZe, beqar uruSaZe