ინფორმაცია და კიბერუსაფრთხოების სტრატეგია

დავით ბურჭულაძე, თამარ ქიტიაშვილი

საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

გარკვეული პერიოდის განმავლობაში, საზოგადოებრივი კეთილდღეობა და ეკონომიკური სტაბილურობა ეყრდნობოდა გადაცემის ქსელების მონაცემებისა და გამოთვლითი მომსახურების გამართულ მუშაობას, რომლის სანდოობის მაჩვენებელი საკმაოდ დიდი იყო. საერთო მოხმარების ინფორმაციული სისტემების ფუნქციონირებაზე დიდი გავლენა აქვს ისეთ ფაქტორებს, როგორებიც არის ინტერნეტზე შეტევა (attack), ფიზიკური ზემოქმედების შედეგად მიყენებული დარღვევები, პროგრამული და აპარატული უზრუნველყოფის მწყობრიდან გამოსვლა, ადამიანის, როგორც მომხმარებლის მიერ მუშაობის პროცესში დაშვებული შეცდომები. ჩამოთვლილი ფაქტორები ნათლად აჩვენებს იმ გარემოებას, თუ რამდენად არის დამოკიდებული თანამედროვე საზოგადოება ინფორმაციული სისტემების სტაბილურ მუშაობაზე. მოცემულს ნათლად ასახავს კიბერუსაფრთხოების გერმანული სტრატეგია, კერძოდ: ,,კიბერსივრცეზე დაშვების უზრუნველყოფა, ასევე ინფორმაციის კონფიდენციალობა და სანდოობა კიბერსივრცეში გახდა ერთერთი მნიშვნელოვანი პრობლემა 21-ე საუკუნეში. ამიტომ კიბერსივრცის დაცვა ხდება მთავარი ამოცანა სახელმწიფოს, ეკონომიკისა და საზოგადოების, როგორც ქვეყნის, ისე საერთაშორისო დონეზე.

საკვანძო სიტყვები: ინფორმაცია. კიბერუსაფრთხოება. ინფორმაციული სისტემა. პოგრამული უზრუნველყოფა. აპარატურული უზრუნველყოფა.

1. შესავალი

დღეისთვის ქვეყნის ერთ–ერთ მნიშვნელოვან პრიორიტეტულ მიმართულებას წარმოადგენს სახელმწიფო ხელისუფლების განხორციელებისას ელექტრონული მმართველობის პრინციპებზე დაფუძნებული ერთიანი სისტემის შექმნა, ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი განხორციელების ხელშეწყობა. ელექტრონული სერვისები წარმოადგენს სახელმწიფოს მიერ განხორციელებული მომსახურების ყველაზე უფრო იაფ, მოსახერხებელ და სწრაფ მომსახურებას. ელექტრონული მომსახურების განვითარებასთან ერთად კრიტიკულ მნიშვნელობას იძენს ინფორმაციული უსაფრთხოების საკითხები, რაც სახელმწიფო უსაფრთხოების საკითხებს განეკუთვნება.

იბერუსაფრთხოება ხშირად განიხილება როგორც სახელმწიფო მნიშვნელობის სტრატეგიული პრობლემა, რომელიც ეხება საზოგადოების ყველა ფენას. კიბერუსაფრთხოების სახელმწიფო პოლიტიკა (NCSS - National Cyber Security Strategy) არის საშუალება, რომელიც ემსახურება სახელმწიფოს ინფორმაციული სისტემებისა და მთლიანად ინფრასტრუქტურის უსაფრთხოებისა და სანდოობის გაზრდის შესაძლებლობას, რომელიც ამავდროულად მაქსიმალურად ამცირებს რისკებს.

კიბერუსაფრთხოების სტრატეგიაში გამოიყენება პრობლემისადმი მაღალი დონის მიდგომა, კერძოდ: გამოიყოფა სახელმწიფოს მთელი რიგი მიზნები, ამოცანები და პრიორიტეტები, რომლებიც აუცილებელია მოცემული დროის მონაკვეთში მისაღწევად. ფაქტიურად, სტრატეგია ეს

არის მოდელი, რომელიც საშუალებას იძლევა კიბერუსაფრთხოების საკითხების მოგვარებას ქვეყნის შიგნით.

2. ძირითადი ნაწილი

თანამედროვე მსოფლიოს კიბერსივრცეში არსებული და პოტენციური რისკები/საფრთხეები საზოგადოებრივი ცხოვრების რეალობად იქცა. ტექნოლოგიების განვითარებასთან ერთად უფრო რთული ხდება აღნიშნული საფრთხეების პრევენცია და დაძლევა. საერთაშორისო სტატისტიკის მიხედვით, წარმატებული კიბერინციდენტების რიცხვი ყოველწლიურად მატულობს და შესაბამისად იზრდება კიბერინციდენტებით გამოწვეული ზარალი.

რუსეთ - საქართველოს ომის დროს, რუსეთის ფედერაციამ საქართველოს წინააღმდეგ სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, განახორციელა მიზანმიმართული და მასირებული კიბერშეტევები. აღნიშნულმა კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სახმელეთო, საზღვაო და საჰაერო სივრცეების დაცვა". ეს კიბერშეტევა ბევრი საერთაშორისო ექსპერტის მიერ შეფასდა როგორც „ინფორმაციული/კიბერ ომი" საქართველოს წინააღმდეგ, რასაც ქვეყანა მოუმზადებელი შეხვდა, არ არსებობდა საჭირო რესურსები, გამოცდილება და შესაბამისად საქართველომ კიბერშეტევის მოგერიება ვერ შეძლო. შედეგად ქვეყანა აღმოჩნდა სერიოზული საერთაშორისო ინფორმაციული ვაკუუმის წინაშე. პრობლემა გადაიჭრა ქვეყნის უცხოელი სტრატეგიული პარტნიორების, ჩარევის შემდეგ, რის შედეგადაც შეჩერებული და თავიდან აცილებული იქნა მთლიანი ინფრასტრუქტურის განადგურება.

2008 წლის აგვისტოს ომისა და მისი შედეგების გათვალისწინებით, რაც უკავშირდებოდა ქვეყნის დაუცველ კიბერსივრცეს, საქართველოს ხელისუფლებამ დაიწყო სამართლებრივ - ნორმატიულ ბაზაზე მუშაობა მოცემული მიმართულებით, რის შედეგად 2013 წლის მაისში გამოქვეყნდა საქართველოს კიბერუსაფრთხოების სტრატეგია, რომელიც „წარმოადგენს „ეროვნული უსაფრთხოების მიმოხილვის" პროცესის ფარგლებში შექმნილი კონცეპტუალური და სტრატეგიული დოკუმენტების პაკეტის ნაწილს. შესაბამისად, აღნიშნული სტრატეგია ეფუძნება „საქართველოს საფრთხეების შეფასების 2010 – 2013 წ.წ. დოკუმენტს" და „საქართველოს ეროვნული უსაფრთხოების კონცეფციას".

საქართველოს კიბერუსაფრთხოების სტრატეგია არის გარდამავალი დოკუმენტი და მისი განხორციელების ვადებია 2013 – 2015 წლები, რისთვისაც შექმნილი არის სპეციალური სამოქმედო გეგმა 42 და მის განხორციელებაზე თავისი კომპეტენციის ფარგლებში პასუხისმგებელი უწყებები: საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო და საქართველოს ჩ ღთ; საქართველოს შინაგან საქმეთა, იუსტიციისა და საგარეო საქმეთა სამინისტროები; საქართველოს ეროვნული უშიშროების საბჭოს აპარატი. სტრატეგიის სამოქმედო გეგმაში ასევე გათვალისწინებულია საერთაშორისო დახმარება კვლევითი ლაბორატორიის შექმნასა და ელექტრონული მტკიცებულებების (კიბერკრიმინალისტიკის) სფეროში, კიბერდანაშაულის ექსპერტების სპეციალიზებული ტრენინგების ორგანიზებაში.

საერთაშორისო სისტემაში არსებული საფრთხეებისა და გამოწვევების გათვალისწინებით, საქართველოს უსაფრთხოების პოლიტიკის დაგეგმვა და განხორციელება განიხილავს კიბერუსაფრთხოების სფეროში შემდეგ საფრთხეებსა და გამოწვევებს:

კიბერუსაფრთხოების სტრატეგიის გამოქვეყნებას წინ უძღოდა 2012 წლის ივნისში კანონის „ინფორმაციული უსაფრთხოების შესახებ“ გამოქვეყნება. მოცემული კანონის მიზანია „ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, დააწესოს საჯარო და კერძო სექტორების უფლება - მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში, აგრეთვე განსაზღვროს ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები“ [1]

კერძოდ, იქიდან გამომდინარე, რომ კანონი შემუშავებული საერთაშორისო პრაქტიკის გათვალისწინებით, ვფიქრობთ, რომ კრიტიკული ინფრასტრუქტურის სუბიექტებში იგულისხმება:

- საფინანსო სექტორი;
- კომუნიკაციების სექტორი;
- ინფორმაციული ტექნოლოგიების სექტორი;
- ენერგეტიკისა და წყალმომარაგების სექტორი;
- სატრანსპორტო სისტემების სექტორი;
- ჯანმრთელობის დაცვისა სექტორი;
- ინდუსტრიული, მათ შორის სამშენებლო და ქიმიური მრეწველობის სექტორი;
- თავდაცვისა და უსაფრთხოების სექტორი და ა.შ.

თავისთავად, აღნიშნული სექტორები მოიცავს მიმართულებების საკმაოდ ფართო სპექტრს, რომელიც შესაძლებელია მიჩნეულ იქნეს კრიტიკული ინფრასტრუქტურის სუბიექტებად.

აღნიშნული ჩამონათვალი ფართოვდება შემდეგი ჩანაწერით: „ამ კანონის მოქმედება ვრცელდება ყველა იურიდიულ პირზე და სახელმწიფო ორგანოზე, რომელიც წარმოადგენს კრიტიკული ინფრასტრუქტურის სუბიექტს“.

კანონის მოქმედება ასევე ვრცელდება ისეთ ორგანიზაციაზე ან უწყებაზე, რომელიც შედის კრიტიკული ინფრასტრუქტურის სუბიექტის დაქვემდებარებაში ან დაკავშირებულია სუბიექტთან დასაქმების, სტაჟირების, სახელშეკრულებო ან სხვა ურთიერთობით, რომელიც უზრუნველყოფს წვდომას ინფორმაციულ აქტივზე ასეთი ურთიერთობის ფარგლებში.

მაგალითად, ამერიკის შეერთებული შტატებში კრიტიკულ ინფრასტრუქტურად ითვლება მასობრივი საზოგადოებრივი თავშეყრის ადგილები. თუმცა, პარლამენტში ინიცირებულ კანონპროექტში ზუსტდება, რომ კრიტიკული ინფრასტრუქტურის სუბიექტია – „სახელმწიფო ორგანო, იურიდიული პირი, რომლის ინფორმაციული სისტემების უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის, ეკონომიკური უსაფრთხოების, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის.“

შესაბამისად, საქართველოს შემთხვევაში იგულისხმება ზემოჩამოთვლილ სექტორებში მოქმედი ის სუბიექტები, რომელთა საქმიანობაც მჭიდროდ არის დაკავშირებული ინფორმაციული სისტემების ფუნქციონირებასთან. მაგალითად,

- საფინანსო სექტორში - ბანკები და სხვა ფინანსური ინსტიტუტები;
- კომუნიკაციების სექტორში - სამაუწყებლო და საკომუნიკაციო კომპანიები;
- ინფორმაციული ტექნოლოგიების სექტორში - ინტერნეტ პროვაიდერი კომპანიები და ა.შ.

უნდა დადგინდეს და დაცული იქნას ინფორმაციული უსაფრთხოების რისკების მართვის პროცესისთვის საჭირო ორგანიზაციული სტრუქტურა და პასუხისმგებლობები [2]. ძირითადი როლები და პასუხისმგებლობები გახლავთ:

- ორგანიზაციაზე მორგებული ინფორმაციული უსაფრთხოების რისკების მართვის პორცესის შემუშავება;
- დაინტერესებული პირების გამოვლენა და ანალიზი;
- ყველა მხარის (როგორც შიგა, ასევე გარე) როლებისა და პასუხისმგებლობების განსაზღვრა ორგანიზაციისათვის;
- ორგანიზაციასა და დაინტერესებულ პირებს შორის საჭირო ურთიერთობის დამტკიცება, ასევე ორგანიზაციის მაღალი დონის რისკების მართვის ფუნქციებისთვის ინტერფეისების დადგენა (მაგალითად, ოპერაციული რისკების მართვა), ასევე სხვა პროექტების და ქმედებებისთვის საჭირო ინტერფეისები;
- გადაწყვეტილების მიღების წესის განსაზღვრა;
- აღრიცხვიანობის (რეგისტრირების, ჩანაწერების) მახასიათებლები.

მსოფლიოს მასშტაბით კომპიუტერები თითქმის სრულად მოიცავს ყველა მნიშვნელოვან ლეგალურ ოპერაციას. მათ შორის საქართველოში იგი უკვე გამოიყენება არამხოლოდ სოციალური კომუნიკაციებისათვის, არამედ კონტრაქტების გასაფორმებლად, შესყიდვების საწარმოებლად.

ბოლო პერიოდში საქართველოში არაერთი საკანონმდებლო რეფორმა ჩატარდა, მიღებულ იქნა ახალი კანონმდებლობა ,,კიბერ კრიმინალთან“ მიმართებაში, სხვადასხვა სამართალდამცავ უწყებებში შეიქმნა ახალი ორგანიზაციული საშტატო ერთეულები. ადამიანი, რომელიც მოყვება ,,კიბერ კრიმინალთან“ დაკავშირებულ ინციდენტში, სამართლებრივი დავის პროცესს სრულიად უძლურია, რადგან საქართველოში ცოტა ადვოკატი თუ მოიძებნება, რომელიც ერკვევა კიბერ დანაშაულებებსა და თანამედროვე ტექნოლოგიებთან დაკავშირებულ საკითხებში. ეს კი ერთ-ერთ მთავარი პრინციპის, მხარეთა თანასწორობის დარღვევას იწვევს, რაც უფრო ფუნდამენტურ საკითხს, სამართლიან სამართალს ეხება [3].

ნებისმიერ სასამართლო პროცესში დაცული უნდა იქნეს მხარეთა თანასწორობის პრინციპი. როგორც კანტი აღნიშნავს, სამართლიანობა უზრუნველყოფილია არა სამართლის პრინციპებით, არამედ კანონების განხორციელების დემოკრატიული პროცედურით. ანუ, სხვა სიტყვებით რომ ვთქვათ – თუ სახელმწიფომ მიიღო კანონმდებლობა, მოამზადა პროკურორები და მეორე მხარეს არ არსებობს ძალა, რომელიც დაიცავს ბრალდებულს სასამართლო პროცესში, თავად

სახელმწიფოა ვალდებული საგანმანათლებლო პროგრამებითა თუ ნებისმიერი სხვა საშუალებებით მოამზადოს კვალიფიური ადვოკატები, კიბერ-კრიმინალის კუთხით. თუმცა ჩვენ ყოველთვის გვაქვს არჩევანი, ვისაუბროთ მხოლოდ იმაზე თუ რა არის სწორი, ან თავად გადავდგათ კონკრეტული ნაბიჯები სიტუაციის გამოსასწორებლად.

2008-2011 წლებში საქართველოს წინააღმდეგ განხორციელებულმა ფართომასშტაბიანმა კიბერშეტევებმა ნათლად დაგვანახა კიბერუსაფრთხოების პოლიტიკის შემუშავების აუცილებლობა, რათა უზრუნველყოფილ იქნას კრიტიკული ინფორმაციული სისტემების გამართული და უსაფრთხო ფუნქციონირება. აღნიშნულმა გარემოებამ განაპირობა თავდაცვის სამინისტროს მიერ შემუშავებულიყო კიბერუსაფრთხოების პოლიტიკა 2014-2016 წლებისათვის [4].

ქვეყანაში კიბერუსაფრთხოების დანერგვა და განვითარება ნატოსთან ნაკისრი ვალდებულებების ერთ-ერთი შემადგენელი ნაწილია. საქართველოს თავდაცვის სამინისტროს მიერ დასახული მიზნები და გატარებული ღონისძიებები კიბერუსაფრთხოების სფეროში ხელს შეუწყობს საქართველოს ინტეგრაციის პროცესს ევროპულ და ჩრდილო-ატლანტიკურ ორგანიზაციებში.

სახელმწიფოს ინიციატივა - უზრუნველყოს და განავითაროს კიბერუსაფრთხოება, გახლავთ მისი მხრიდან გადადგმული ერთ-ერთი მნიშვნელოვანი ნაბიჯი, რაც უზრუნველყოფს საქართველოს თავდაცვის სფეროსა და მასში შემავალი კრიტიკული ინფორმაციული სისტემების დაცვასა და გაძლიერებას.

კიბერსივრცე ქმნის ერთიან კომპლექსურ გარემოს მასში შემავალი ინფორმაციული და კომუნიკაციების ტექნოლოგიების მოწყობილობებითა და ქსელებით, რაც საშუალებას აძლევს საქართველოს თავდაცვის სამინისტროს სამოქალაქო ოფისს, შეიარაღებული ძალების გენერალური შტაბის სტრუქტურულ ქვედანაყოფებსა და სამინისტროში შემავალ საჯარო სამართლის იურიდიულ პირებს განახორციელონ სხვადასხვა ტიპის კომუნიკაცია, ძალებისა და საშუალებების მართვა.

მომავალში კიბერსივრცე კიდევ უფრო მასშტაბური გახდება, გაიზრდება სახელმწიფო სტრუქტურების დამოკიდებულება ინფორმაციულ ტექნოლოგიებზე, რაც განაპირობებს ახალი რისკებისა და საფრთხეების წარმოქმნას. სწორედ აქედან გამომდინარე, აუცილებელია კიბერუსაფრთხოების ისეთი მოქნილი მექანიზმების შექმნა, რომლებიც ეფექტურად უპასუხებს ახლად წარმოქმნილ გამოწვევებს. კიბერუსაფრთხოების უზრუნველყოფის მნიშვნელოვან ნაწილს, წარმოადგენს აგრეთვე ახალი კიბერშეტევებისადმი ინფორმაციული სისტემების მდგრადობის ამაღლების მიზნით პრევენციული ღონისძიებების შემუშავება და გატარება.

კიბერუსაფრთხოება მოიცავს საქართველოს თავდაცვის სამინისტროს საქმიანობის ყველა იმ სფეროს, სადაც გამოიყენება ინფორმაციული ტექნოლოგიები, იქნება ეს სამხედრო/თავდაცვითი ოპერაციების დაგეგმვა, სამხედრო წვრთნების წარმოება, ლოგისტიკური მხარდაჭერა თუ სხვა,

რათა უზრუნველყოფილ იქნეს ინფორმაციის მთლიანობა, ხელმისაწვდომობა და დროული გაზიარება [5].

კიბერუსაფრთხოება ხშირად განიხილება როგორც სახელმწიფო მნიშვნელობის სტრატეგიული პრობლემა, რომელიც ეხება საზოგადოების ყველა ფენას. კიბერუსაფრთხოების სახელმწიფო პოლიტიკა (NCSS - National Cyber Security Strategy) არის საშუალება, რომელიც ემსახურება სახელმწიფოს ინფორმაციული სისტემებისა და მთლიანად ინფრასტრუქტურის უსაფრთხოებისა და სანდოობის გაზრდის შესაძლებლობას, რომელიც ამავდროულად მაქსიმალურად ამცირებს რისკებს.

კიბერუსაფრთხოების სტრატეგიაში გამოიყენება პრობლემისადმი მაღალი დონის მიდგომა, კერძოდ: გამოიყოფა სახელმწიფოს მთელი რიგი მიზნები, ამოცანები და პრიორიტეტები, რომლებიც აუცილებელია მოცემული დროის მონაკვეთში მისაღწევად. ფაქტობრივად, სტრატეგია ეს არის მოდელი, რომელიც საშუალებას იძლევა კიბერუსაფრთხოების საკითხების მოგვარებას ქვეყნის შიგნით.

როგორც წესი, ყოველი ქვეყნის კიბერუსაფრთხოების სტრატეგიებს მაინც გააჩნიათ საერთო პრინციპები, რომელიც შეიძლება შემდეგნაირად ჩამოყალიბდეს:

- სახელმწიფო მოდელისა და პოლიტიკის შემუშავება, რომელიც მიმართულია კიბერუსაფრთხოების უზრუნველყოფაზე;
- სახელმწიფო პარტნიორობაზე დაფუძნებული შესაბამისი მექანიზმის განსაზღვრა, რომელიც კერძო და სახელმწიფო სექტორის დაინტერესებულ მხარეებს საშუალებას აძლევს განიხილონ და დაამტკიცონ პოლიტიკა დაკავშირებული კიბერუსაფრთხოების პრობლემებთან;
- აუცილებელი პოლიტიკისა და მექანიზმების რეგულაციების დაგეგმვა და განსაზღვრა, როლების, უფლებებისა და პასუხისმგებლობის მკვეთრი გამიჯვნა კერძო და სახელმწიფო სექტორისთვის;
- რისკების სახელმწიფო მართვის მიმართ სისტემური და ინტეგრირებული მიდგომის შემუშავება;
- ინფორმაციული პროგრამების მიზნების განსაზღვრა და აღნიშვნა, რომელიც მიმართულია შესთავაზოს მომხმარებელს ქცევისა და მუშაობის ახალი მოდელები;
- საერთაშორისო თანამშრომლობა არამარტო ევროკავშირის წევრ - ქვეყნებს შორის, არამედ იმ ქვეყნებთანაც, რომლებიც არ შედიან ევროკავშირში;
- კომპლექსური კვლევების ჩატარება და პროგრამების განვითარებაზე მუშაობა, რომელიც მიმართულია კიბერსივრცის უსაფრთხოების პრობლემების გადაჭრაზე. ინტელექტუალური რესურსების განვითარება;

საქართველოს კიბერუსაფრთხოების სტრატეგია გამოქვეყნდა 2013 წლის 20 მაისს, საქართველოს პრეზიდენტის 2013 წლის 17 მაისის №321 ბრძანებულების მიღების თანახმად. მოცემული დოკუმენტი შემუშავდა საქართველოს ეროვნული უშიშროების საბჭოსთან არსებული ეროვნული უსაფრთხოების სტრატეგიული დოკუმენტების შემუშავების მაკოორდინირებელი მუდმივმოქმედი საუწყებათაშორისო კომისიის მიერ და ის წარმოადგენს არამარტო სტრატეგიას, არამედ მასში მოცემულია ასევე ამ სტრატეგიის განხორციელების 2013-2015 წწ. სამოქმედო გეგმაც [6].

„საქართველოს კიბერუსაფრთხოების სტრატეგია არის კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტი, რომელიც ასახავს სტრატეგიულ მიზნებს, ძირითად პრინციპებს, აყალიბებს სამოქმედო გეგმებს და ამოცანებს. სტრატეგიაზე დაყრდნობით, საქართველოს ხელისუფლება გაატარებს ღონისძიებებს, რომლებიც ხელს შეუწყობს სახელმწიფო ორგანოების, კერძო სექტორისა და სამოქალაქო საზოგადოების კიბერსივრცეში დაცულად ფუნქციონირებას, ელექტრონული ოპერაციების უსაფრთხო განხორციელებას და ქვეყანაში ეკონომიკისა და ბიზნესის შეუფერხებლად მოქმედებას“.

საქართველოს ეროვნული უსაფრთხოების კონცეფცია კიბერსივრცის დაცვის უზრუნველყოფასა და, ზოგადად, კიბერუსაფრთხოებას განიხილავს, როგორც ქვეყნის უსაფრთხოების ერთერთ ძირითად შემადგენელ ნაწილს და მის მნიშვნელოვან მიმართულებას. კიბერსივრცის დაცვასა და კიბერუსაფრთხოების უზრუნველყოფაზე ბევრად არის დამოკიდებული ქვეყნის შემდგომი ეკონომიკური სტაბილურობა და სოციალური განვითარება. მოცემული მიზნის მისაღწევად, სტრატეგია განიხილავს შემდეგი თანამშრომლობის მნიშვნელოვან პრინციპებს:

- საქართველოს მთავრობის ერთიანი მიდგომა;
- თანამშრომლობა სახელმწიფო და კერძო სექტორებს შორის;
- აქტიური საერთაშორისო თანამშრომლობა;
- ინდივიდუალური პასუხისმგებლობა;
- ადეკვატური ზომები.

საქართველო აქტიურად მიისწრაფვის ევროინტეგრაციისკენ, ქვეყანა ცდილობს გახდეს ევროკავშირისა და ჩრდილოეთ ალიანსის სრულუფლებიანი წევრი, ხელი მოეწერა ასოცირების ხელშეკრულებას. ყოველივე ეს ნიშნავს, რომ ქვეყანა თავის თავზე იღებს ყველა იმ ვალდებულებას, რაც უზრუნველყოფს არამარტო საქართველოს უსაფრთხოებას, არამედ ევროკავშირის როგორც ცალკეული წევრი ქვეყნებისა, ისე მთლიანად ევროკავშირის უსაფრთხოების შესაბამისი ნორმების დაცვას, სადაც ასევე იგულისხმება კიბერსივრცის მაქსიმალური დაცვის უზრუნველყოფა.

ეს არის ქვეყნისთვის სერიოზული გამოწვევა, რადგან საქართველომ უნდა შექმნას ეროვნული კანონმდებლობა, წესრიგში მოიყვანოს და საერთაშორისო სტანდარტებს შეუსაბამოს ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემისა და ცალკეული სუბიექტების დაცვა, გაზარდოს საერთაშორისო თანამშრომლობა და რისკების შემცირების მიზნით, უნდა მოახდინოს საზოგადოების ცნობიერების ამაღლება და საგანმანათლებლო სისტემის შემუშავება [4].

1. დასკვნა

დღესდღეისობით სახელმწიფოები აქტიურად იყენებენ კიბერშეტევებს პოლიტიკური, გეოპოლიტიკური, სამხედრო და სხვა მიზნების გასახორციელებლად. თანამედროვე კიბერშეტევები საფრთხეს უქმნის ქვეყნის უსაფრთხოებას, განვითარებას და ხელს უშლის საზოგადოების ფუნქციონირებას. შესაბამისად, გლობალური უსაფრთხოების უზრუნველყოფის ერთ-ერთი მთავარი კომპონენტი სწორედ საკუთარი ქვეყნის კიბერთავდაცვაა, რაც ისეთივე მნიშვნელოვანია, როგორც სახმელეთო, საჰაერო და საზღვაო სივრცეების დაცვა. თითოეული სახელმწიფო, რომელიც ტექნოლოგიური განვითარებისკენ მიისწრაფვის, საზოგადოების წინაშე ვალდებულია, დაიცვას საკუთარი კიბერსივრცე.

ლიტერატურა:

1. კიბერუსაფრთხოების ბიუროს გენდერული თანასწორობის სტრატეგია. (2014). საქართველოს თავდაცვის სამინისტრო.

2. სურგულაძე გ., ურუშაძე ბ. (2014). საინფორმაციო სისტემების მენეჯმენტის საერთაშორისო გამოცდილება (BSI, ITIL, COBIT). სტუ. „ტექნიკური უნივერსიტეტი". თბილისი.

3. ჯორბენაძე ს., ბახტაძე უ., მაჭარაძე ზ. (2014). მედიასამართალი. სახელმძღვ., დავით ბატონიშვილის სამართლის ინსტიტუტის გამომცემლობა, „ქოლორი". ISBN 978-9941-0-7062-4 http://lawlibrary.info/books/giz2014-ge-MediaLaw.pdf

4. საჯარო სამართლის იურიდიულ პირის – კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ. (2014). საქართველოს თავდაცვის მინისტრის ბრძანება №27 2014 წლის 7 აპრილი. თბილისი

5. ინფორმაციული უსაფრთხოება (2011). უსაფრთხოების მექანიზმები, ინფომრაციული უსაფრთხოების მართვის წესები და ნორმები. საქართველოს თავდაცვის სამინისტრო. 8.11.2011 წ.

6. კიბერუსაფრთხოების პოლიტიკა. (2014). საქართველოს თავდაცვის სამინისტრო. 2014-2016

CYBER SECURITY STARTEGY OF GEORGIA

Burchuladze David, Kitiashvili Tamar
Georgian Technical University

Summary

For a certain period of time prosperity and economic stability of society were based on the data of transfer networks and proper working of calculation service the trust indicator of which was quite high. Functioning of information systems of common usage is influenced by such factors as internet attack, violations caused by physical impact, software and hardware failure, errors made by man as a customer in the process of working. The listed factors clearly demonstrate the situation of how modern society is depended on stable working of informational systems. the given is clearly reflected by German strategy of cyber security, namely, "ensuring access on cyber space, also information confidentiality and reliability in cyber space have become one of the important problems of the 21st century, that's why protection of cyber space is becoming the core objective of state, economy and society both on the country and international level." current and potential risks/threats of the modern world cyber space have become the reality of modern life. Together with technological development it is harder to prevent the mentioned threats and to overcome them. According to international statistics the number of successful cyber incidents is increasing and accordingly the damage caused by cyber incidents is increasing too.

КИБЕРСТРАТЕГИЯ БЕЗОПАСНОСТИ ГРУЗИИ

Бурчуладзе Д., Китиашвили Т.
Грузинский Технический Университет

Резюме

В течении определенного периода благосостояние общества, его экономическая стабильность основывались на надежной работе сетей передачи данных и их переработке. На работу информационных систем общего пользования большое влияние оказывают такие факторы, как атаки (attack) на интернет, нарушения в работе в следствии физического воздействия, выход из строя программного и аппаратного обеспечения, ошибки, допущенные пользователем в процессе работы. Приведенные факторы наглядно

показывают, насколько зависимо современное общество от стабильной работы информационнх систем. Это наглядно отображает немецкая стратегия кибербезопасности, в частности: “Обеспечение доступа к киберпространству, а также конфиденциальность и надежность информации в киберпространстве стала одной из важнейших проблем 21 века. Поэтому защита киберпространства стала основной задачей государства, экономики и общества как на уровне страны, так и на международном уровне”.