Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 53 - 66 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

ISRAEL CYBER SECURITY SYSTEM

Leri Saraidarov, PhD student of the Faculty of Law
and International Relations of Georgian Technical University.

ABSTRACT. There is no doubt that the national security problems exist in any country, regardless of the governors and regime conditions, however in democratic states, especially for the countries in war situations where, along with others the terrorist threats are increased. Ensuring the security of the country is a priority and it is of particular importance.

In the State of Israel, special attention is paid to information security- one of its key areas and components - cyber security and cyber defense. As you know, in the cybernetic age, with the development and availability of technologies, are increasing the number and extent of threats and challenges.

In Israel, a number of public and private sector agencies and organizations provide reliable and sustainable cyber threats and risks including the special services, police and defense units, as well as highly rated startups and information security companies.

To summarize, it has to be said, the foundation for success is a multitude of highly qualified specialists, years of work experience, innovative approaches, the development of modern technologies and the inevitable dilemma of forming an advanced leader and a protected state.

KEYWORDS: Cyber security, security services, fight cyber threats, startups in cyber security, government agencies.

ისრაელის კიბერუსაფრთხოების სისტემა

ლერი სარაიდაროვი, საქართველოს ტექნიკური უნივერსიტეტის სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტის დოქტორანტი.

რეზიუმე. უდავოა, რომ ეროვნული უშიშროების უზრუნველყოფის პრობლემა არსებობს ნებისმიერ ქვეყანაში, მიუხედავად მმართველობისა და რეჟიმის პირობებისა, თუმცა დემოკრატიულ სახელმწიფოებში, მით უმეტეს საომარ მდგომარეობაში მყოფ ქვეყნებში, სადაც სხვა საფრთხეებთან ერთად მომეტებულია ასევე ტერორისტული საფრთხეები, ქვეყნის უშიშროების უზრუნველყოფა პრიორიტეტულია და მას ენიჭება განსაკუთრებული მნიშვნელობა.

ისრაელის სახელმწიფოში განსაკუთრებული ყურადღება ეთმობა საინფორმაციო უსაფრთხოებასა და მის ერთ-ერთ მნიშვნელოვან მიმართულებას და კომპონენტს- კიბერუსაფრთხოებას და კიბერთავდაცვას. მოგეხსენებათ, კიბერნეტიკულ ერაში, ტექნოლოგიების

განვითარებასთან და ხელმისაწვდომობასთან ერთად იზრდება საფრთხეებისა და გამოწვევების რაოდენობა და მოცულობა.

ისრაელში კიბერსაფრთხეებთან და რისკებთან საიმედო და მდგრად გამკლავებას უზრუნველყოფს არაერთი სახელმწიფო და კერძო სექტორში მომუშავე სამსახური თუ ორგანიზაცია. მათ შორის სპეცსამსახურების, პოლიციის და თავდაცვის ძალების დანაყოფები, ასევე მაღალრეიტინგული სტარტაპ და საინფორმაციო უსაფრთხოების სფეროში მომსახურე კომპანიები.

შესაჯამებლად უნდა ითქვას, რომ ისრაელის კიბერუსაფრთხოების სფეროში მიღწეული წარმატების საფუძველს წარმოადგენს მაღალკვალიფიციური სპეციალისტების მრავალრცხოვანი შტატი, მრავალწლიანი სამუშაო გამოცდილება, ნოვატორული მიდგომები, თანამედროვე ტექნოლოგიების განვითარება და მოწინავე-ლიდერ და დაცულ სახელმწიფოდ ჩამოყალიბების გაუნელებელი ჟინი.

საკვანძო სიტყვები: კიბერუსაფრთხეობა, სპეცსამსახურები, კიბერსაფრთხეებთან ბრძოლა, სტარტაპი კიბერუსაფრთხოებაში, სახელმწიფო უწყებები.

უდავოა, რომ ეროვნული უშიშროების[1] უზრუნველყოფის პრობლემა არსებობს ნებისმიერ ქვეყანაში, მიუხედავად მმართველობისა და რეჟიმის პირობებისა, თუმცა დემოკრატიულ სახელმწიფოებში, მით უმეტეს საომარ მდგომარეობაში მყოფ ქვეყნებში, სადაც სხვა საფრთხეებთან ერთად მომეტებულია ასევე ტერორისტული საფრთხეები, ქვეყნის უშიშროების უზრუნველყოფა პრიორიტეტულია და მას ენიჭება განსაკუთრებული მნიშვნელობა. ბალანსის დაცვა ქვეყნის უშიშროების ნიშნულსა და დემოკრატიული პრინციპების რეალიზაციის ხელშეწყობას შორის მსგავსი ტიპის ქვეყნებში დიდ სირთულეებთან არის დაკავშირებული.

ზოგადად, ქვეყნის ეროვნული უშიშროების უზრუნველყოფის სისტემა დაფუძნებულია და აერთიანებს სახელმწიფო ორგანოებს, ძალებს-პოტენციალის სახით, სხვადასხვა სახის რესურსებსა და საშუალებებს, რომელთა გამოყენება და ფუნქციონირება ხორციელდება ქვეყანაში მოქმედი და აღიარებული სამართლებრივი აქტების შესაბამისად. სახელმწიფოში უშიშროების პრიორიტეტულ მიმართულებებს წარმოადგენს პიროვნების, საზოგადოების და სახელმწიფოს პოლიტიკური, სამართლებრივი, ორგანიზაციული, ეკონომიკური, სამხედრო და სხვა მსგავსი ხასიათის უსაფრთხოება. სისტემის ძირითად ფუნქციას განეკუთვნება ეროვნული უშიშროების წინაშე მდგარი საფრთხეების თაობაზე ინფორმაციის მოპოვება, შეფასება, იდენტიფიცირება, მათზე რეაგირება, კონკრეტულ მოქმედებათა ორგანიზება, რათა აღმოფხვრილ, ნეიტრალიზებულ და მინიმუმამდე იქნას დაყვანილი საფრთხეებისა და რისკების რაოდენობა [1, 26-35].

[1] ეროვნული უშიშროება-მდგომარეობა, როდესაც ქვეყანაში უზრუნველყოფილია პიროვნების, საზოგადოების და სახელმწიფოს დაცულობა შიდა და გარე საფრთხეებისაგან, ასევე უზრუნველყოფილია კონსტიტუციური უფლებების რეალიზაცია, მოსახლეობის ცხოვრების მაღალი დონე, ქვეყნის სუვერენიტეტი, ტერიტორიული მთლიანობა, მდგრადი განვითარება, სახელმწიფოსა და მოსახლეობის თავდაცვა და უშიშროება.

ცხადია, რომ ისრაელისთვის, მისი ოფიციალურად დამოუკიდებელ სახელმწიფოდ გამოცხადების დღიდან ეროვნული უშიშროების სისტემის სიმტკიცის უზრუნველყოფა წარმოადგენს სახელმწიფო პოლიტიკის პრიორიტეტულ მიმართულებას. ცალკეული ყურადღება ექცევა ეროვნული უშიშროების უზრუნველსაყოფად სპეცსამსახურებისა და სამართალდამცავი ორგანოების მიერ გამოყენებულ საშუალებებს, მეთოდებსა და ინსტრუმენტებს.

„უშიშროების“ ცნებას სამართლებრივ და სამეცნიერო ლიტერატურაში დათმობილი აქვს საკმაოდ ბევრი გამოკვლევა[2], თუმცა მეცნიერებს შორის დღემდე ვერ მოხერხდა საერთო აზრის ფორმირება ამ ფენომენთან მიმართებაში, თუ რა უნდა და რა შეიძლება ჩაითვალოს სახელმწიფო უშიშროების განმსაზღვრელ ფაქტორებად შიდა და საგარეო დონეზე [2,5].

წინამდებარე სტატიაში გვსურს, საუბარი წარვმართოთ საინფორმაციო უსაფრთხოების ერთ-ერთი მთავარი მიმართულების-კიბერუსაფრთხოების აქტუალურ საკითხებზე.

კიბერუსაფრთხოების სფეროს განვითარება ისრაელის სახელმწიფოსთვის განსაკუთრებით პრიორიტეტულია და მნიშვნელოვანი, გამომდინარე იქიდან, რომ იგი წარმოადგენს ყველაზე კომპიუტერიზებულ ქვეყანას ახლო აღმოსავლეთში. მაღალი ტექნოლოგიების წარმატებული ფლობა და მათი განვითარება თავისთავად პირდაპირპროპორციულია ამ სფეროში მოსალოდნელი საფრთხეებისა და რისკების.

ისრაელის სახელმწიფოში განსაკუთრებული ყურადღება ეთმობა საინფორმაციო უსაფრთხოებასა[3] და მის ერთ-ერთ მნიშვნელოვან მიმართულებას და კომპონენტს-

[2] კამათი „უსაფრთხოების“ ცნებასთან დაკავშირებით მომდინარეობის შუა საუკუნეების ხანიდან. მაგალითისთვის იტალიელი ფილოსოფოსი და პოლიტიკური მოღვაწე ნიკოლო მაკიაველი აღნიშნავდა, რომ სახელმწიფოს საფრთხე შესაძლოა შეექმნას ორი მხრიდან-ქვეშევრდომი და სხვა სახელმწიფოთა მხრიდან. მისი აზრით, საგარეო საფრთხეებთან გამკლავება შესაძლებელია ძლიერი არმიისა და თავდადებული ჯარისკაცების ხარჯზე, ამასთან შიდა საფრთხეები თავისთავად უვნებელყოფდება, ვინაიდან მშვიდობა შენარჩუნებულია ქვეყნის შიგნით. გერმანელი სოციოლოგი და პოლიტოლოგი კარლ დოიჩი უსაფრთხოებას განსაზღვრავდა, როგორც „დაცულობას, ძირითადი სასიცოცხლო ფასეულობების“. ფრანგი სამართალმცოდნე და საზოგადო მოღვაწე ჟორჟ ვედელი იხრებოდა იმ აზრისკენ, რომ უსაფრთხოება არის პრევენციული ღონისძიებების გატარება და საზოგადოების ან ცალკეული ჯგუფების მიმართ არსებული საფრთხეების აღმოფხვრა.

[3] საინფორმაციო უსაფრთხოება-ინფორმაციის, მომსახურებების, სისტემების და ტელეკომუნიკაციების დაცვა ნებისმიერი ფორმით. საინფორმაციო უსაფრთხოება მოიცავს ტექნიკურ უსაფრთხოებას, კერძო პირების ქმედებებს და ორგანიზაციულ პროცედურებს. საინფორმაციო უსაფრთხოების წინააღმდეგ მიმართული საფრთხეები მოიცავს პირადი საიდუმლოებების დარღვევას, ელექტრონულ ფოსტაზე უსარგებლო, რეკლამის მიზნით შეტყობინებების გამოგზავნას, სამრეწველო ჯაშუშობას, პირატულ კოპირებას, კომპიუტერულ ვირუსებს, ქსელურ ტერორიზმს და ელექტრონული ომის წარმოებას. ნებისმიერი ზემოთ ჩამოთვლილი საფრთხე შეიძლება ერთ წამში მთელს მსოფლიოში გავრცელდეს, საინფორმაციო ქსელების გავლით. ინფორმაციულ უსაფრთხოებაში იგულისხმება: ინფორმაციის კონფიდენციალურობის, მთლიანობის (ურღვევობის) და ხელმისაწვდომობის დაცვა.

კიბერუსაფრთხოებას[4] და კიბერთავდაცვას[5]. თვალნათელია, რომ კიბერნეტიკულ ეპოქაში, ტექნოლოგიების განვითარებასთან და ხელმისაწვდომობასთან ერთად იზრდება საფრთხეებისა და გამოწვევების რაოდენობა და მოცულობა. ტექნოლოგიებისა და ინფრასტუქტურის მოხერხებულ და კომფორტულ გამოყენებასთან ერთად იქმნება საკუთარი სისტემისა და კრიტიკული ინფორმაციული[6] მოწყობილობებისა და მატარებლების დაცულობის საშიშროება და პრობლემა, რაც ნებისმიერი ქვეყნისთვის უდავოდ პრიორიტეტულია და საკვანძო.

ისრაელი მსოფლიოში წარმოადგენს ერთ-ერთ წამყვან ქვეყანას, რომელსაც სოლიდური ინვესტირება უწევს კიბერ უსაფრთხოების სფეროში. სტარტაპ[7]-კომპანიების რეკორდული რაოდენობა, მოწინავე კიბერ არმია და განათლების სისტემის პროგრესირება, ამ ყველაფერმა ისრაელს, ხელი შეუწყო ინოვაციების ცენტრად ჩამოყალიბებაში და სახელმწიფო კიბერ სივრცის დაცულობის სფეროში წარმატების მიღწევაში.

ჯერ კიდევ 2002 წელს, კიბერ სივრცეში აქტიური დივერსიების დაწყებამდე, ისრაელის სახელმწიფომ მკაფიოდ განსაზღვრა ქვეყნისთვის პრიორიტეტული ინფორმაციული

---

[4] კიბერუსაფრთხოება (ინგლ. *Cybersecurity)* გაცილებით ფართო ცნებაა და მოიცავს კიბერთავდაცვასაც, იგი არა მარტო სახელმწიფო ქსელებისა და ინფრასტრუქტურის დაცულობასა და უსაფრთხოებას გულისხმობს, არამედ კერძო პირებისა და სექტორების მფლობელობასა და სარგებლობაში არსებული კიბერმოწყობილობების უსაფრთხოებას. ნებისმიერი არასანქცირებული მოქმედება კიბერსივრცეში შეიძლება მიჩნეულ იქნეს კიბერუსაფრთხოების საპირისპირო პროცედურად. კიბერუსაფრთხოება, როგორც ინფორმაციული უსაფრთხოების ერთ-ერთი მიმართულება, ძირითადად უკავშირდება ქსელებისა და პროგრამული უზრუნველყოფის თავდაცვითი და პრევენციული ღონისძიებების გატარებას, რათა თავიდან იქნეს აცილებული ან აღკვეთილი მიმდინარე კიბერაგრესია. ნებისმიერი თავდასხმა კიბერსივრცეში უკავშირდება კონფიდენციალურ ინფორმაციაზე ხელმისაწვდომობის მიღებას, მის დამახინჯებას, შეცვლას ან განადგურებას, ასევე მოპოვებული ინფორმაციის სანაცვლოდ ფულის გამოძალვას. კიბერუსაფრთხოება ასევე ითვალისწინებს კიბერჰიგიენას, სისტემაში შესასვლელი პაროლებისა და სხვა პირადი ინფორმაციების დაცულობას, პლასტიკური ბარათების და სხვა ფულად საკრედიტო ინფორმაციების დაცულობასა და გაუხმაურებლობას, უსაფრთხოების პოლიტიკის დაგეგმვასა და გატარებას.

[5] კიბერთავდაცვა-(ინგლ. *Cyberwarfare)* ჩრდილო-ატლანტიკური ხელშეკრულების ორგანიზაციამ ტერმინი „კიბერუსაფრთხოება“ შეცვალა ტერმინით „კიბერთავდაცვა“, რაც შესაძლოა, უკავშირდებოდეს ვაშინგტონის (ჩრდილო-ატლანტიკური ხელშეკრულება, ვაშინგტონი, კოლუმბიის ოლქი - 4 აპრილი, 1949 წ.) შეთანხმების მე-5 მუხლის ამოქმედებას, რომელიც ითვალისწინებს აგრესიის გამომვლენი სახელმწიფოს მიმართ ფიზიკური ძალის გამოყენების შესაძლებლობას [12]. ხშირად კიბერთავდაცვას-კიბერწინააღმდეგობასაც უწოდებენ, კიბერომს, წინააღმდეგობის გაწევას კიბერნეტიკულ სივრცეში, ინტერნეტ სივრცეში კომპიუტერული წინააღმდეგობის გაწევა. საინფორმაციო ომის ერთ-ერთი სახეობა. მიმართულია კომპიუტერული სისტემების დესტაბილიზაციისკენ და წვდომის მისაღებად სახელმწიფო დაწესებულებების, ფინანსური და საქმიანი ცენტრების ქსელებზე და დაცულ ინფრასტრუქტურაზე, უწესრიგობისა და ქაოსის გამოსაწვევად ქვეყანაში, რომელსაც ინტერნეტზე და კიბერსივრცეზე მინდობილი აქვთ ყოველდღიური ცხოვრება და საქმიანობა. კიბერწინააღმდეგობა შეიძლება გამოიხატებოდეს ვანდალიზმში, პროპაგანდაში, ჯაშუშობაში, უშუალო თავდასხმებში კომპიუტერულ სისტემებსა და სერვერებზე.

[6] კრიტიკული ინფრასტრუქტურა-იურიდიული პირების, სახელმწიფო ორგანოებისა და საქმიანობის სფეროების ერთობლიობა, რომლის ინფორმაციული სისტემების უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის.

[7] სტარტაპი-არის დროებითი ორგანიზაცია, რომელიც ეძებს მაღალი მოგების პოტენციალის მქონე ბიზნეს მოდელს და აქვს ექსპონენტური ზრდის პოტენციალი.

უსაფრთხოებისა და დაცულობის საკითხი და მისი უზრუნველყოფა ეროვნულ დონეზე დაავალა შიდა უშიშროების სამსახურს „შაბაქს[8]“ (შინ-ბეთს). გადაწყვეტილება გამოდგა შედეგიანი, მისი რეალიზების შემდეგ ისრაელის კრიტიკული ინფრასტრუქტურა ანგარიშგასაწევ თავდასხმას აღარ დაქვემდებარებია, მიუხედავად ყოველდღიური უმნიშვნელო კიბერ შეტევებისა, რომელთა ინტენსივობა უშედეგობის გამო იყო მზარდი [3, 22-34].

დღევანდელი მდგომარეობით ქვეყნის კიბერ უსაფრთხოებაზე პასუხისმგებლობა აღებული აქვს ისრაელის ეროვნულ კიბერ-დირექტორატს (INCD[9]), რომელიც აერთიანებს წარსულში კიბერ უსაფრთხოებისა და ტექნოლოგიური დაცვის სფეროებში ცალ-ცალკე მოქმედ ორ (INCB[10] და NCSA[11]) სამთავრობო დაწესებულებას. მიუხედავად კომპეტენციების გამიჯვნისა, ინფორმაციული უსაფრთხოების უზრუნველყოფის ვალდებულება შეინარჩუნა „შაბაქმაც“.

2010 წელს ისრაელის პრემიერ-მინისტრმა, ქვეყანის რეალური საფრთხეების წინაშე აღმოჩენის შემდეგ, შექმნა სპეციალური ჯგუფი, „კიბერ ინიციატივის“ სახელით ცნობილი, რომელსაც დაევალა ეროვნული კიბერ პროგრამის შემუშავება. ჯგუფის მიერ შემუშავებული რეკომენდაციების მიხედვით, სასურველი გახდა შექმნილიყო ეროვნული კიბერ ბიურო და სამოქალაქო სექტორის უსაფრთხოების აღმასრულებელი ორგანო [4, 47-53].

2011 წელს ისრაელის მთავრობის დადგენილების შესაბამისად, ეროვნულ დონეზე სამოქალაქო კიბერუსაფრთხეობის განმტკიცების მიზნით შეიქმნა ისრაელის ეროვნული კიბერ ბიურო (INCB). მის კომპეტენციაში შევიდა ქვეყნის პრემიერ-მინისტრისთვის და მთავრობის შემადგენლობაში შემავალი სხვა სამინისტროებისთვის კონსულტაციების გაწევა და დახმარების აღმოჩენა ხსენებულ სფეროში. აღნიშნულ ორგანოს დავალებული ჰქონდა ეროვნული კიბერუსაფრთხოების პოლიტიკის გატარება ქვეყნის მთელ ტერიტორიაზე. კიბერთავდასხმების აცილებისა და განეიტრალების მიზნით ბიუროს ასევე უნდა ეზრუნა ნაციონალური ინფრასტუქტურის გაუმჯობესებაზე და მათი დაცულობის ამაღლებაზე, რათა უზუნველყოფილიყო ნორმალური და უსაფრთხო ცხოვრება ისრაელის სახელმწიფოში. ამავდოულად ბიუროს ამოცანათა რიგს განეკუთვნებოდა თავდაცვითი ღონისძიებების განვითარება და ეროვნული

[8] შაბაქი-იგივე შინ-ბეთ (ივრთ. שב"כ - שירות הביטחון הכלל -შირუთ ხა ბითახონ ხა კლალი)-ქვეყნის პრემიერ-მინისტრის დაქვემდებარებაში არსებული უსაფრთხოების სპეციალური სამსახური, შიდა უსაფრთხოების უზრუნველმყოფი, სამსახურის ერთ-ერთი მიმართულებაა კონტრდაზვერვითი საქმიანობა.

[9] INCD-Israel National Cyber Directorate-ისრაელის ეროვნული კიბერდირექტორატი, ქვეყნის პრემიერ-მინისტრის კანცელარიის მმართველობაში შემავალი ორი ორგანოს გაერთიანების შედეგად 2018 წელს შექმნილი სამსახური, რომელიც უზრუნველყოფს სახელმწიფო და კერძო სტრუქტურებში კიბერუსაფრთხოების პოლიტიკის რეალიზაციას და დაცვას.

[10] INCB-Israel National Cyber Bureau-ისრაელის ეროვნული კიბერბიურო, 2018 წლამდე მოქმედი ორგანო, შეუერთდა NCSA-ს, შედეგად შეიქმნა INCD.

[11] NCSA- National Cyber Security Authority-ეროვნული კიბერუსაფრთხოების ორგანო, ისრაელის პრემიერ-მინისტრის კაბინეტს დაქვემდებარებული ორგანო 2016-2018 წლებში, რომელიც უზრუნველყოფდა ქვეყნის სამოქალაქო კიბერსივრცის დაცვას. 2017 წლის დასასრულს ორგანო გაუერთიანდა NCSA-ს, რომელიც ასევე მოქცეული იყო პრემიერ-მინისტრის კანცელარიის მმართველობის ქვეშ და შეიქმნა ერთიანი ეროვნული კიბერბიურო. ბიურომ აიღო ქვეყნის პრემიერ-მინისტრის საკონსულტაციო ვალდებულება კიბერპოლიტიკის საკითხებში.

ძალისხმევის გაძლიერება კიბერნეტიკული მიმართულებით, საბოლოო ჯამში კი ისრაელის კიბერუსაფრთხოების სფეროში ლიდერ სახელმწიფოდ გადაქცევის ხელშეწყობა.

2015 წლის თებერვალში INCB მოახდინა გარღვევა, კერძოდ, შეიმუშავა მთავრობის ორი დადგენილება (N2443 და N2444) კიბერუსაფრთხეობის სფეროში და შექმნა საფუძველი ეროვნული კიბერუსაფრთხეობის სტრატეგიის მნიშვნელოვანი ელემენტების რეალიზაციის. ასევე, ერთ-ერთი ამ დაგენილების საფუძველზე შეიქმნა კიბერუსაფრთხეობის სფეროში, ეროვნულ დონეზე მომუშავე მეორე ორგანიზაცია (NCSA) [4, 59-64].

NCSA-ს პასუხისმგებლობა აღებული ჰქონდა ქვეყნის კიბერსივრცის დაცვაზე, ყველა ოპერატიულ-დაცვითი ღონისძიებების რეალიზაციისა და ექსპლუატაციის საფუძველზე, რათა ეროვნულ დონეზე განხორციელებულიყო სრული და უწყვეტი რეაგირება კიბერშეტევებთან მიმართებაში. გარდა სხვა დაკისრებული ამოცანებისა, ორგანოს თავისი ქოლგის ქვეშ მოქცეული ჰქონდა ისრაელის სერტი (IL-SERT), ასევე მის კომპეტენციას განეკუთვნებოდა ქვეყნის კიბერთავდასხმებთან მედეგობისა და მათთან გამკლავების მზაობის გაზრდაზე ზრუნვა.

IL-CERT[12]-მა (ისრაელის კომპიუტერულ შემთხვევებზე რეაგირების ჯგუფი), სხვა ქვეყნების ანალოგიური დანაყოფების მსგავსად, პასუხისმგებლობა აიღო ეროვნული კიბერუსაფრთხეობის სფეროში ინციდენტების მართვასა და მოქმედებათა კოორდინაციაზე, პროაქტიულ და პრევენციულ ღონისძიებებზე მათ წარმოშობამდე, ინფორმაციის გაცვლასა და საზოგადოების ინფორმირებაზე ინფორმაციის უსაფრთხოებისა და კონფიდენციალურობის დაცვის სფეროში. ჯგუფი ახორციელებს მსგავსი ღონიძიებების გამოკვლევას, მათ შეფასებას, ასევე საზოგადოებისთვის პერიოდულად აქვეყნებს ინფორმაციას, თუ რა ხერხებითა და მეთოდებით, დაცვის რომელი საშუალებებით არის შესაძლებელი მოსალოდნელ საფრთხეებთან და ინციდენტებთან გამკლავება და თავიდან აცილება [13].

რაც შეეხება ეროვნული კიბერუსაფრთხოების დირექტორატს (INCD), იგი უშუალოდ ფუნქციონირებს და მოქმედებს პრემიერ-მინისტრის ხელმძღვანელობის ქვეშ და წარმოადგენს უსაფრთხოების ოპერატიულ, არასაიდუმლო ორგანოს, რომელსაც დავალებული აქვს ისრაელის სამოქალაქო კიბერსივრცის მონიტორიგი სხვადასხვა ინსტუმენტებისა და საშუალებების დახმარებით, რათა უზრუნველყოფილ იქნას სრულყოფილი და საიმედო დაცვა. ისრაელის სამხედრო ძალები, სპეციალური სამსახურებისა და დანაყოფების ფუნქციონირების საფუძველზე პასუხისმგებლობას იზიარებენ სამხედრო კიბერსექტორში ინფორმაციის და ინფრასტუქტურის დაცულობასთან დაკავშირებით. მათთან ერთად კოორდინირებულ საქმიანობას ეწევიან ისრაელის სხვადასხვა სახელმწიფო სამსახურები, მათ შორის უშიშროების სააგენტო, რომელიც ორიენტირებულია ტერორისტული და კიბერტერორისტული საფრთხეების განეიტრალებაზე, პოლიცია, რომელიც აწარმოებს ბრძოლა კიბერდანაშაულთან წინააღმდეგ [4, 70].

ხსენებული უწყებებისა და სამსახურების კოორდინირებული მუშაობა გარკვეულ ასპექტებში იძლევა ეროვნული ძალისხმევის წარმატებული სინქრონიზაციის საშუალებას კიბერ უსაფრთხეობისა და კიბერსივრცის დაცულობის სფეროში, რაც ქვეყნისთვის ძალიან მნიშვნელოვანია.

[12] **I**srael'S **C**omputer **E**mergency **R**esponse **T**EAM-ისრაელის კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი. https://il-cert.org.il/. დღეს უკვე დამოუკიდებელი პროფესიული ორგანიზაცია.

უნდა აღინიშნოს, რომ გარდა სახელმწიფო უწყებებისა, ისრაელის კიბერსივრცის დაცვაში მონაწილეობას იღებენ ისრაელში ოპერირებადი კომპანიებიც, მათ შორის ცნობილი კომპანია „რაფაელი“[13]. „რაფაელი“, როგორც კიბერუსაფრთხოების ერთ-ერთი წამყვანი და თანამედროვე ცენტრის მფლობელი, გარდა სამხედრო მრეწველობისა, წარმოადგენს ისრაელის კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფის მთავარ ქვეკონტრაქტორს [19]. ჯგუფის საქმიანობას ისრაელის სახელმწიფოში დიდი ხნის ისტორია არა აქვს, თუმცა, გამოცდილების სიმწირის მიუხედავად იგი უკვე წარმოადგენს გიგანტურ სამთავრობო ცენტრს კიბერუსაფრთხეობის სფეროში მძლავრი საფრთხეების აღმოჩენის, მონიტორინგისა და გაუვნებელყოფის კუთხით ეროვნულ დონეზე. აქვე უნდა აღინიშნოს, კონცერნი „რაფაელი“ ასევე წარმოადგენს კომპანია „მატრიქსის“[14] ქვეკონტრაქტორს, რომელმაც გაიმარჯვა სახელმწიფო ბანკის მიერ შემუშავებულ კონკურსში ქსელების კიბერუსაფრთხოების უზრუნველყოფის სფეროში. ქსელის დანიშნულებას წარმოადგენს ბანკების მიერ რისკების შეფასებისა და კონკურენციის გაზრდის მიზნით ორგანიზაციებს შორის სამომხმარებლო კრედიტების თაობაზე ერთმანეთის ინფორმირება [5, 50-60].

გარდა კომპანია „რაფაელისა“, კიბერუსაფრთხოების სფეროში საქმიანობით დაკავებულია ისრაელის სტრარტაპ კორპორაცია SCADAfence[15] სკადაფენსი, რომელიც უზრუნველყოფს საერთაშორისო გლობალური ქსელებით[16] მოსარგებლე მრეწველობითა და პროდუქციის წარმოებით დაკავებული კომპანიების კორპორატიული ქსელების პროგრამულ მხარდაჭერას და მათ უსაფრთხოებას. თვალნათელია, რომ თანამედროვე ეპოქაში ხსენებული ტიპის ორგანიზაციების ქსელები უფრო დაუცველები გახდნენ კიბერთავდასხმების მიმართ, რის გამოც SCADAfence-ის მომსახურებით დაინტერესებული კომპანიების რიცხვი დღითიდღე იზრდება. ასეთ კომპანიებს ძირითადად წარმოადგენენ სოლიდური საავტომობილო, ფარმაცევტული, ქიმიური და ენერგეტიკულ სფეროში მომუშავე საწარმოები.

აღნიშვნის ღირსია ასევე ის ფაქტი, რომ 2016 წლის დასაწყისში ისრაელის ეკონომიკისა და მრეწველობის სამინისტროს და კიბერბიუროს ერთობლივი ძალისხმევით ფუნქციონირება დაიწყო პროგრამა KIDMA (ივრთ. კიდმა-აბრევიატურა კიბერუსაფრთხოების სფეროში კვლევების

[13] რაფაელი-Rafael ისრაელის კომპანია, რომელიც აწარმოებს შეიარაღებას, საჰაერო თავდაცვით და რაკეტსაწინააღმდეგო ტექნიკას, ასევე წარმატებით ოპერირებს კიბერუსაფრთხოების სფეროში, არის შეიარაღების მსხვილი ექსპორტიორი. ორგანიზაცია დაარსდა 1948 წელს, თავდაპირველად ეწოდა Hemed. შემდგომში შეიცვალა სახელწოდება Emet. 1958 წელს კომპანიამ ისევ შეიცვალა სახელწოდება და ეწოდა Rafael. კომპანიის ერთ-ერთი წარმატებული პროექტია ჰაერსსაწინააღმდეგო, რაკეტთავდაცვითი კომპლექსი „რკინის გუმბათი“, (ივრთ. კიფათ ბარზელ).

[14] მატრიქსი-ისრაელის წამყვანი კომპანია 2000 წლიდან, რომელის საქმიანობს ტექნოლოგიების დანერგვისა და პროგრამული უზრუნველყოფის სფეროში, გააჩნია სახელმწიფო და კერძო სექტორებთან დიდხნიანი გამოცდილება კიბერუსაფროების პროგრამული პროდუქტების მიწოდებისა და პროგრამული უზრუნველყოფის მიმართულებით. ასევე ფინანსურ და საბანკო სექტორთან წარმატებული ურთიერთობის სოლიდური სტაჟი.

[15] SCADAfence-კიბერუსაფრთხოების ერთადერთი პლატფორმა, რომელიც შექმნილია რთული, მსხვილმასშტაბიანი ქსელების ოპერაციული ტექნოლოგიების უწყვეტი და შეუფერხებელი მუშაობისთვის.

[16] გლობალური ქსელი (WAN – Wide Area Network)- ქსელი, რომელიც აერთიანებს სხვადასხვა ქალაქების, რეგიონების და სახელმწიფოების კომპიუტერებს.

განვითარება) მეორე დონემ[17] [18]. პროგრამის იდეას წარმოადგენდა ის, რომ შენარჩუნებულიყო ისრაელის კიბერუსაფრთხოების სფეროში ლიდერის როლი და საერთაშორისო ბაზარზე აწეული ყოფილიყო კონკურენციის ნიშნული. სწორედ მსგავსი პროგრამების დანერგვისა და განვითარების ხარჯზე აღწევენ ებრაული კომპანიები წარმატებებს საერთაშორისო ინდუსტრიაში[18], რომელთაგან ორი (ForeScout Technologies-IT Security და Ability Inc- Mobile Security) შევიდა NASDAQ (ნასდაქში)[19], რამდენიმემ კი მიიღო ათეულობითი მილიონი დოლარი ინვესტიციის სახით [6, 89-90].

2017 წლის იანვარსა და თებერვალში, ისრაელის ქალაქ თელ-ავივში გაიმართა საერთაშორისო გამოფენა Cybertech 2017, რომელიც ეხებოდა კონკურსს უსაფრთოების სფეროში საუკეთესო სტარტაპის გამოვლენის მიზნით. კონკურსის შედეგად საუკეთესო სტარტაპად დასახელდა ისრაელის ინოვაციური ტექნოლოგია Aperio Systems, რომელსაც გააჩნია შესაძლებლობა მოახდინოს სისტემაში საეჭვო აქტივობის იდენტიფიცირება, ავტომატურად გააგზავნოს შეტყობინება და დამოუკიდებლად მოახდინოს ქმედების კორექტირება მნიშვნელოვან ობიექტებზე ინფრასტუქტურის დაზიანების მცდელობის დროს. (იქნება ეს წყალმომარაგების თუ ელექტროქსელების ობიექტი) [4, 66].

ამჟამად გვსურს, საუბარი განვაგრძოთ კიბერ უსაფრთხოების სფეროში მომსახურე სამართალდამცავ უწყებებზე.

2012 წელს ისრაელის პოლიციის სამმართველოში „ლახავი-433[20]“ შეიქმნა კიბერდანაშაულთან ბრძოლის დანაყოფი, რომელსაც ფუნქციურად განესაზღვრა კიბერნეტიკის სფეროში ჩადენილი დანაშაულების გამოძიება. გარდა იმისა, რომ ისრაელი არკეთილმოსურნე ქვეყნების მხრიდან ყოველდღიურად განიცდის კიბერ თუ სხვა სახის აგრესიას, ასევე თვალშისაცემი სიხშირით გამოირჩევა სოციალურ ქსელებსა თუ სხვა მომიჯნავე სფეროებში არაავტორიზებული და უკანონო შეღწევისა და თავდასხმის ფაქტები. ეს შეიძლება იყო პირადი დაცული სივრციდან ინფორმაციისა და ფულადი თანხის მოპარვა, სახელგამტეხი ინფორმაციის გავრცელება, დაშანტაჟება, მუქარა (ბულინგი), ბანკომატებიდან და საბანკო ანგარიშებიდან ფულადი სახსრებისა და პერსონალური ინფორმაციის მართლსაწინააღმდეგო დაუფლება, უკანონო ვაჭრობა ინტერნეტსივრცეში და სხვა. სწორედ მსგავსი დანაშაულების გამოძიება და მათი პრევენცია

[17] 2012 წლიდან ისრაელში ფუნქციონირებს სპეციალური პროგრამა KIDMA, რომელიც საბიუჯეტო დაფინანსებაზე მყოფ კომპანიებს კიბერპროდუქტის შექმნაში სთავაზობს მომსახურებას აღნიშნულ სფეროში. პროგრამა 3 წელიწადში ერთხელ იღებს ფინანსურ მხარდაჭერას 26 მლნ. აშშ დოლარის ოდენობით.

[18] ბრიუს ოსტის (NASDAQ-ის ხელმძღვანელის მოადგილე) განცხადებით, მაღალი ტექნოლოგიების ყოველი მე-5 კომპანია, რომელიც მონაწილეობს ფასთა კოტირებაში ნიუ-იორკის ბირჟაზე-NASDAQ, არის ისრაელის მოქმედი ან ყოფილი კომპანია. ბირჟაზე მონაწილე ებრაულ კომპანიათაგან-80 არის სახელმწიფო [17].

[19] ნასდაქი-(NASDAQ, მომდინარეობს აკრონიმიდან National Association of Securities Dealers Automated Quotations — ფასიან ქაღალდთა დილერების ავტომატური კოტირებების ეროვნული ასოციაცია) — აშშ-ის ელექტრონული სააქციო ბირჟა. დაფუძნდა ფასიან ქაღალდთა დილერების ეროვნული ასოციაციის (NASD) მიერ. კორპორაციის ამჟამინდელი აღმასრულებელი დირექტორია რობერტ გრიფილდი.

[20] ლახავი-443-(იგრთ. ბასრი, მახვილი) יחידת להב 433, (იეხუდათ ლაახავ არბა შალოშ შალოშ)- ისრაელის პოლიციაში 2008 წელს შეიქმნილი სპეციალური დანაყოფი, რომელშიც გაერთიანდა 5 სამართალდამცავი ორგანო. დანაყოფის კომპეტენციას განეკუთვნება ნაციონალური მასშტაბის დანაშაულებათა გამოძიება, კერძოდ, კორუფციისა და სხვა განსაკუთრებით მძიმე და მძიმე კატეგორიი დანაშაულებათა გამოძიება.

ევალება პოლიციის აღნიშნულ დანაყოფს, რომელიც სტუქტურულად ექვემდებარება ისრაელის პოლიციის ერთ-ერთ ყველაზე პრესტიჟულ და ავტორიტეტულ სამმართველოს ლახავი 433 [7, 83-87].

პოლიციური დანაყოფის პარალელურად ისრაელის სახელმწიფო პროკურატურაში 2015 წელს გენერალური პროკურორის გადაწყვეტილებით შეიქმნა კიბერდანაშაულთან ბრძოლის განყოფილება, სადაც კონცენტრირებულ იქნა კიბერდანაშაულთან და კიბერტერორიზმთან გამკლავებისთვის და ბრძოლისთვის აუცილებელი ყველა საშუალება და ძალისხმევა. დასახელებული დანაყოფის შექმნის გადაწყვეტილება მიღებულ იქნა კიბერდირექტორატთან კონსულტაციის საფუძველზე, რა დროსაც გამოიკვეთა მისი არსებობის აუცილებლობა. სამსახურის პროფილურ საქმიანობას განეკუთვნება: კიბერდანაშაულის და რადიოელექტრონული დაზვერვის (SIGINT) [21] სფერო, ციფრული მტკიცებულებების მოპოვება, მიყურადება და კავშირგაბმულობის არხებიდან მონაცემების მოპოვება. პროკურატურის ახლად შექმნილი დანაყოფი საპროცესო ზედამხედველობას უწევს პოლიციის კიბერდანაშაულთან ბრძოლის სამსახურის და იუსტიციის სამინისტროს ტექნოლოგიებისა და ინფორმაციების საქმეთა სამმართველოს წარმოებაში არსებულ საქმეებს [8-25].

გარდა დასახელებული უწყებებისა და კომპანიებისა, კიბერსაფრთხეებთან ბრძოლის სოლიდური გამოცდილება გააჩნიათ სამხედრო სექტორს დაქვემდებარებულ და სპეციალური დანიშნულების მქონე სამსახურებს.

ისრაელის თავდაცვის არმიის გენერალური შტაბის სტრუქტურულ ქვედანაყოფს წარმოადგენს სამხედრო დაზვერვის სამმართველო „ამანი“[22], რომელიც დაკავებულია საგარეო დაზვერვის წარმოებით, იგი „შაბაქთან“ და „მოსადთან[23]“ ერთად შედის ისრაელის ძირითად სპეცსამსახურთა სამეულში. სწორედ მის დაქვემდებარებაშია რადიოელექტრონული დაზვერვის დანაყოფი 8200 (ივრთ. იეხიდა შმონა მათაიმ, 8200 יחידה) [14], რომელიც დაკავებულია რადიოელქტრონული ინფორმაციის შეგროვებითა და დეშიფრაციით, ასევე სხვა ოპერაციებით. დასახელებულ დანაყოფს, გარდა დაზვერვის მნიშვნელოვანი ფუნქციისა, დავალებული აქვს კიბერუსაფრთხოების უზრუნველყოფა რადიოელექტრონულ სასიგნალო დონეზე [9, 63; 10, 50].

სამხედრო სექტორში, კიბერუსაფრთხოების უზრუნველყოფას, გარდა ხსენებული დანაყოფისა, ახორციელებს ისრაელის თავდაცვის არმიის სახმელეთო ჯარების (ზროა ხა იაბაშა) შემადგენლობაში 2017 წელს შექმნილი კიბერთავდაცვის მიმართულება (ანაფ საიბერ). ახალი მიმართულება ექვემდებარება სახმელეთო ჯარების კავშირგაბმულობის შტაბს (მახლექეთ ტიკშუვ).

---

[21] Sigint-signal intelligence-რადიოელექტრონული დაზვერვა-სადაზვერვო საქმიანობის ერთ-ერთი მიმართულება, შესაბამისი ტექნოლოგიების გამოყენებით მიწოდებული სიგნალების გადაჭერა და მოპოვებული ინფრომაციის ანალიზი. რადიოელექტრონული დაზვერვა მოიცავს რადიო (comint), რადიოტექნიკურ (elint), რადიოლოკაციურ (radint) დაზვერვას.

[22] ამანი-(ივრთ. אמ"ן ივრთ-დან המודיעין ענף אגאף ხა მოადინ — დაზვერვის სამმართველო), ისრაელის თავდაცვის არმიის გენერალური შტაბის სტრუქტურული ქვედანაყოფი.

[23] მოსადი-(ივრთ. ჰამოსად ლემოდიინ ულეთაფკიდიმ მეიუხადიმ, დაზვერვისა და სპეციალური დანიშნულების ორგანო). ისრაელის სადაზვერვო სამსახური, დაკავებულია საგარეო სადაზვერვო საქმიანობით, წარმოადგენს ერთ-ერთ წარმატებულ სპეცსამსახურს მსოფლიოში.

აღნიშნულ მიმართულებას აქვს სხვა დასახელებაც: „ანაფ სევერ“. სევერ-სვივათ რეშეთ საიბერ (ანუ ქსელური სივრცე, ინგლისურენოვანი სიტყვა „საიბერის“ ივრითიზაცია.) ახალი სამსახურის ამოცანას წარმოადგენს ყველა სახეობის შეირაღების და სახმელეთო ჯარების სამხედრო ტექნიკის დაცვის უზრუველყოფა თავდასხმისგან და მათზე კონტროლის მოპოვებისგან. დანაყოფს დაევალა არა მარტო სარგებლობაში არსებული სისტემების დაცვა, არამედ შემუშავებისა და საგამოცდო ეტაპზე არსებული სისტემებისა და ტექნიკის დაცვაც. მიმართულება შედგება რამდენიმე სექტორისგან: მათ შორის (მადორი), რომელიც პასუხისმგებელია დაცვითი საშუალებების შექმნაზე, მათ საბრძოლო ტექნიკაში დანერგვაზე, მიმართულება კომპლექტდება გენერალური შტაბის კავშირგაბმულობის მთავარი სამმართველოს (ანაფ ხა ტიკშუვ) შემადგენლობიდან. გარდა მოხსენიებული მიმართულებისა, ახლადშექმნილი სამსახურის შემადგენლობაში სამმართველოების სახით შედის სისტემების დაცვის (ხატივათ ხა-ხაგანა), კიბერუსაფრთხოების (ხატივათ ხა საიბერ) და კომპიუტერული ქვედანაყოფების (მაარახ ხა-მიხშუვ) მიმართულებები [4, 43].

ალბათ, სიახლეს არ წარმოადგენს, რომ ისრაელის სპეცსამსახურები ითვლებიან ერთ-ერთ ყველაზე ეფექტურ და ეფექტიან სამსახურებად მსოფლიოში. ინტერნეტის განვითარებასთან ერთად, მათი საქმიანობის სფეროს დაემატა კიბერუსაფრთხოების უზრუნველყოფა. როგორც უკვე აღვნიშნეთ, კიბერნეტიკული განყოფილება „შაბაქში“ შეიქმნა საუკუნის დასაწყისში, თავიდან მის ამოცანას წარმოადგენდა ისრაელის ქსელების გამოყენებით ინფორმაციის უსაფრთხო და საიმედო გადაცემა. თუმცა კომპიუტერიზაციის სწრაფმა განვითარებამ, ვირტუალური სივრცის ტოტალურმა გაფართოებამ გამოიწვია მასშტაბური, სტრუქტურული ცვლილებების საჭიროება.

კიბერინდუსტრიასა და კიბერუსაფრთხოებაში მოწინავე ქვეყნის ადგილის დაკავება უდავოდ დიდ ძალისხმევასთან და ინტელექტუალური და ეკონომიკური რესურსების მოხმარებასთან არის დაკავშირებული. ხშირად პროფესიონალიზმი და წარმატებულობა ხდება ნეგატიური ეჭვის საბაბი. ისრაელის შემთხვევაში სახელმწიფო, რომელიც წარმატებულად ფლობს თანამედროვე მაღალ ტექნოლოგიებს და თავად ეწევა მათ ინდუსტრიას, მიიჩნევა საფრთხის წარმომშობ ქვეყნად. ისრაელი არაერთხელ იქნა დადანაშაულებული კიბერთავდასხმების განხორციელებაში, მაშინ, როდესაც იგი თავად არის არაკეთილმოსურნე ქვეყნების მხრიდან სისტემატიური თავდასხმებისა და აგრესიის მსხვერპლი.

2011 წელს თეირანმა ისრაელი დაადანაშაულა ზღვის ფსკერის საბურღი დანადგარებისა და მოწყობილობების მწყობრიდან გამოყვანის მიზნით კიბერთავდასხმაში. ისრაელი, სხვა ქვეყნებთან ერთად მიეკუთვნება იმ სახელმწიფოთა რიცხვს, რომელიც ეჭვმიტანილია ირანის ბირთვული პროგრამის მიმართ კიბერაგრესიისა და თავდასხმების განხორციელებაში. დადანაშაულების საფუძვლად მიიჩნეულია ის ფაქტი, რომ ჩვეულებრივი სამხედრო შეტევების განხორციელება რთულია პოლიტიკური მიზეზების გამო, ამიტომ ისინი მიმართავენ კიბერშეტევებს [15].

აღნიშნულ ბრალდებას წინ უსწრებდა 2010 წელს კიბერსივრცეში ახალი ვირუსის „სტაქსნეტის“ (STAXNET) გამოჩენა, რომლის ავტორობაში ამერიკის შეერთებულ შტატებთან ერთად სახელდებოდა ისრაელი. ვირუსმა უზარმაზარი საფრთხე შეუქმნა ბირთვულ და ინდუსტრიულ ობიექტებს. გავრცელებული ცნობების თანახმად „სტაქსნეტი“[24] შეიჭრა ირანის

[24] სტაქსნეტ-კომპიუტერული ვირუსი, რომელიც აზიანებს ოპერაციული სისტემა „ვინდოუსის“ მართვის ქვეშ არსებულ კომპიუტერულ სისტემებს. აღმოჩენილია 2010 წელს, მისი შეღწევა განხორციელდა არამარტო კომპიუტერულ სისტემებში, არამედ სამრეწველო სისტემებში, რომელიც იმართებოდა ავტომატიზირებული პროცესების მეშვეობით.

ბუშერის[25] ბირთვული ელექტროსადგურის საკომპიუტერო სისტემაში და შეაფერხა მისი ნორმალური მუშაობის რეჟიმი.

ისრაელისა და ამერიკის შეერთებული შტატების კოალიცია დასახელდა ასევე 2012 წელს ჩატარებული იმ კვლევის შედეგად, რომელიც უკავშირდებოდა „სტაქსნეტისგან“განსხვავებული, თუმცა გაცილებით მოქნილი ვირუსის „ფლეიმის“ Flame შემუშავებას. იგი, მისი წინამორბედის მსგავსად, მიზნად ისახავდა ირანის ბირთვული პროგრამის ფუნქციონირების შეფერხებას და სისტემიდან ინფორმაციის ხელმისაწვდომობის უზრუნველყოფას [5, 13-25].

უნდა აღინიშნოს, რომ, გარდა ისრაელის მხრიდან აგრესიის მომდინარეობის თაობაზე ბრალდებებისა, თვით ისრაელიც ხშირად დაქვემდებარებია აქტიურ კიბერშეტევებს, მათ შორის პალესტინის მხრიდან, უშუალოდ ღაზას სექტორიდან. „ქსელის ჯიხადისტები“ ცდილობენ, კიბერთავდასხმებით შეაეფერხონ ებრაული მოსახლეობის ნორმალური და სტაბილური ცხოვრება და წარმოშვან შიში, თუმცა ამის საშუალებას არ იძლევიან ებრაული სპეცსამსახურები, რომლებიც მყისიერ და ეფექტიან რეაგირებას ახდენენ აგრესიასთან და აგრესორთან მიმართბაში. სარაკეტო ავიადარტყმებით ისრაელის მხარემ გაუსწორა ანგარიში მიმდინარე წლის მაისში „ხამასის“ დაჯგუფებას, დადგინდა თავდასხმის მომდინარეობის ლოკაცია, რომლის მიმართაც განხორციელდა თავდასხმა. ისრაელის რეაქცია, მიიჩნევა ისტორიაში პირველ ფაქტად, როდესაც ქვეყანამ აქტიური კონფლიქტის დროს ხაკერულ თავდასხმაზე რეაგირება მოახდინა სამხედრო მოქმედებებით [11, 64-67].

ისრაელისთვის, გარდა ღაზას სექტორიდან მომდინარე კიბერსაფრთხეებისა, მნიშვნელოვან გარემოებად მიიჩნევა კიბერაგრესია ირანისა და სხვა არაბული სახელმწიფოების მხრიდან. ამ უკანასკნელთა ხაკერპოტენციალი მიმართულია ისრაელის მიმართ ინტენსიურ კიბერთავდასხმებზე, რათა დაასუსტონ ობიექტი სახელმწიფოს კიბერმედეგობა, შეარყიონ ქვეყნის პოლიტიკური და ეკონომიკური მდგრადობა, ნეგატიური ცვლილებები შეიტანონ მოსახლეობის ყოველდღიურ ცხოვრებაში და გამოიწვიონ მათი დაშინება, რაც საბოლოო ჯამში შექმნის დაუცველობის სინდრომის საფრთხეებს საზოგადოებაში.

თანამედროვე ეპოქაში მარტივ ჭეშმარიტებას წარმოადგენს ის ფაქტი, რომ ქვეყნის სიძლიერე და განვითარება დამოკიდებულია მის უშიშროებასა და დაცულობაზე. ჩვენს შემთხვევაში, ისრაელი, წარმოადგენს სწორედ იმ სახელმწიფოს, რომელისთვისაც უშიშროება და დაცულობა პრირიტეული მიმართულებებია. მის წინაშე მდგარი საფრთხეები და გამოწვევები მართლაც რომ საგულისხმოა და საყურადღებო. არაბული სახელმწიფების არაკეთილგანწყობა და ყოველდღიური აგრესია ისრაელისთვის სოლიდურ თავსატეხს წარმოადგენს. დაპირისპირებულ მხარეებს შორის კონფლიქტი ათული წლებია, რაც გრძელდება, ამ ყველაფერს თანამედროვე ეპოქაში დაემატა კიბერაგრესია და მათი საშუალებებით შპიონაჟი, ინფორმაციის დატაცება, ინფრასტრუქტურის დაზიანება, მოსახლეობის დაშინება, სადაზვერვო ღონისძიებების და ტერორის მეთოდების გამოყენება კიბერსივრცეში. ვინაიდან ისრაელისთვის ეროვნული უშიშროება და თავდაცვა პრიორიტეტულია, ქვეყანა თანამედროვე გამოწვევებსა და საფრთხეებს უმკლავდება მაღალი ტექნოლოგიების გამოყენებით. ისრაელის მოქმედებებზე დაკვირვებით შეგვიძლია, გამოვიცნოთ ქვეყნის წარმატების ფორმულა.

[25] ბუშერი-ქალაქი ირანში, რომლის მახლობლად მდებარეობს ირანის ბირთვული რეაქტორი.

ისრაელის სკოლებში დაწყებით კლასებში სწავლობენ კითხვას, წერას და კოდირებას. ქვეყანაში არსებობს ბაღები, სადაც ასწავლიან კომპიუტერთან და რობოტოტექნიკასთან[26] მუშაობას. მე-4 კლასიდან მოსწავლეები აქტიურად სწავლობენ პროგრამირებას, განსაკუთრებული ნიჭით დაჯილდოებული უფროსკლასელები კი დაშიფრვის ტექნოლოგიას და „შავქუდიან ხაკერობასთან“[27] ბრძოლის მეთოდებს.

ისრაელი მიზანმიმართულად იყენებს არმიას, როგორც საკადრო რეზერვს, რათა უზრუნველყოს კიბერუსაფრთხოების სფერო კვალიფიციური სამუშაო რესურებით. ვინაიდან ქვეყანაში სამხედრო სავალდებულო სამსახური საყოველთაო სახისაა, სამხედრო დაზვერვის სამსახურს საშუალება ეძლევა შეარჩოს სამხედრო მოსამსახურეთაგან ყველაზე წარმატებული ახალგაზრდები. არის შემთხვევები, როდესაც ახალგაზრდები ითხოვენ სამხედრო სამსახურის გადავადებას სპეციალობის მისაღებად. მას შემდეგ, რაც მიიღებენ ტექნიკურ ხარისხს, ირიცხებიან სამხედრო სავალდებულო სამსახურში სპეციალობის მიხედვით, სადაც უწევთ მსახური დაახლოვებით 3-4 წლის განმავლობაში, რომლის პარალელურადაც იმაღლებენ კვალიფიკაციას და იძენენ გამოცდილებას.

რამდენადაც ისრაელის კიბერუსაფრთხეობის ინფრასტრუქტურა წარმოადგენს თვალსაჩინო ლიდერს მსოფლიო ინდუსტრიაში, საერთაშორისო კომპანიები ისწრაფვიან ებრაულ სახელმწიფოსთან თანამშრომლობისკენ. 2016 წელს ისრაელის პრემიერ-მინისტრმა ბენიამინ ნეთანიაჰუმ გაეროს გენერალურ ასამბლეაზე განაცხადა: „ისრაელის მოსახლეობა შეადგენს მსოფლიო მოსახლეობის[28] 1%-ის მეათედს[29] (ანუ საერთო რაოდენობის მეათასედი), მიუხედავად ამისა, ჩვენ შევძელით და წინა წელს მოვიზიდეთ მსოფლიო კერძო ინვესტიციების 20% კიბერუსაფრთხოების სფეროში. მე მსურს, გაიაზროთ ეს რიცხვი. ისრაელის წვლილი კიბერუსაფრთხოებაში სოლიდურია და ანგარიშგასაწევი. ისრაელი წარმოადგენს გლობალურ კიბერძალას. ისრაელს შეუძლია, შემოგთავაზოთ აუცილებელი დახმარება, თუ ხაკერები ორიენტირებულნი იქნებიან თქვენს ბანკებზე, თვითმფრინავებზე, ელექტრო ქსელებსა თუ ნებისმიერ სხვა კავშირში მყოფ ინფრასტუქტურაზე“ [21].

აღნიშნულის გათვალისწინებით, გასაკვირი არ უნდა იყოს, რომ უმსხვილესმა ტრანსნაციონალურმა კორპორაციებმა, მათ შორის Microsoft, Google, Apple, Cisco, IBM, Intel, HP, Siemens, General Electric, Philips Medical, PayPal დააფუძნეს საკუთარი კვლევითი და კიბერნეტიკული განვითარების ცენტრები ისრაელში.

ორგანიზაცია Start-Up Nation Central მონაცემების მიხედვით, 2018 წელს ისრაელის ექსპორტის საერთო მოცულობამ კიბერუსაფრთხოების ინდუსტრიაში შეადგინა 3,8 მლრდ. აშშ დოლარი, აღნიშნული დარგის კომპანიებმა კი მიიღეს ინვესტიცია 815 მლნ. აშშ დოლარის ოდენობით საწარმოო და პირადი კაპიტალის სახით.

---

[26] რობოტოტექნიკა-გამოყენებითი მეცნიერება, რომელიც დაკავებულია ავტომატიზირებული ტექნიკური სისტემების შემუშავებით და მიიჩნევა მნიშვნელოვან ტექნიკურ საფუძვლად წარმოების განსავითარებლად.

[27] შავქუდიანი ხაკინგი-არაეთიკური ხაკინგი-უნებართვო შეღწევა კომპიუტერულ ქსელში, პირადი სარგებლის მიღების, მუქარის ან შანტაჟის მიზნით. ტერმინის ავტორი-რიჩარდ სტოლმენი.

[28] მსოფლიო მოსახლეობის რიცხოვნობა შეადგენს თითქმის 8 მლრდ-ს. 7 763 035 301 ადამიანი. ისრაელის მოსახლეობა 8 670 110. https://countrymeters.info/ru/World#population_2019

[29] 1%-ანუ მე-100.

კვლევითი ცენტრის „Cyber Security Ventures“ მონაცემების მიხედვით, ისრაელის 9 კომპანია შედის ტოპ-100-ულში, მსოფლიოში ყველაზე წარმატებული და შემოსავლიანი კომპანიების რიგებში კიბერუსაფრთხოების სფეროში. მაგალითისთვის კომპანია „Check Point Software“ იკავებს სარეგიტინგო მეოთხე ადგილს საბაზრო ღირებულებით 15 მლრდ. აშშ დოლარით.

ისრაელს, სტარტაპ-ინდუსტრიის წარმატებული განვითარების გამო, უწოდებენ მეორე სილიკონის ველს[30]. სტრატაპების ინდუსტრიაში ერთ-ერთი გამოცდილი და მაღალრეიტინგული ბრენდია „Startup Nation“, უცნაური რეალობაა ის ფაქტი, რომ ისრაელის სამხედრო დაზვერვის დანაყოფს 8200-ს, ეწოდა „საიდუმლო სტარტაპ-მანქანა“. ეს კი გამომდინარე იქიდან, რომ მრავალი ვალმოხდილი სამხედრო, რომელიც მსახურობდა ზემოხსენებულ დანაყოფში, გახდა მაღალანაზღაურებადი სტრატაპების ავტორი.

აღნიშვნის ღირსია ასევე ის ფაქტი, რომ 2018 წლის 30 ნოემბერს, არგენტინაში პირველად გაიმართა G-20[31] ქვეყნების რიგით მე-13 საერთაშორისო სამიტი. არგენტინის თავდაცვის სამინისტროს წარმომადგენლებმა სამიტის გამართვამდე ერთ წლით ადრე ებრაელ კოლეგებთან ხელი მოაწერეს 5 მლნ. დოლარის ღირებულების კონტრაქტს, რომელიც ითვალისწინებდა მომსახურების გაწევას კიბერუსაფრთხეობისა და კიბერდაცვის სფეროში G-20-ის სამიტზე. მომსახურების ფარგლებში გათვალისწინებული იყო ინფორმაციული უსაფრთხოების სფეროში საგანგებო სიტუაციებსა და კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფების ჩანერგვა [16].

საბოლოო ჯამში შეგვიძლია, დადასტურებით ვიმსჯელოთ, რომ ისრაელის კიბერუსაფრთხოების სფეროში მიღწეული წარმატების საფუძველს წარმოადგენს მაღალკავალიფიციური სპეციალისტების მრავალრიცხოვანი შტატი, მრავალწლიანი სამუშაო გამოცდილება, ნოვატორული მიდგომები, თანამედროვე ტექნოლოგიების განვითარება და მოწინავე-ლიდერ და დაცულ სახელმწიფოდ ჩამოყალიბების დაუოკებელი ჟინი.

მუდმივი მისწრაფება თვითგადარჩენისკენ, აქტივიზაციას უწევს ისრაელიანთა ერთადერთ ბუნებრივ რესურსს-მათ ინტელექტს. მათ არ სცხვენიათ შეკითხვების და ექსპერიმენტების, არ ეშინიათ წარუმატებლობის, უბრალოდ ისინი სწრაფად იწყებენ მოქმედებას და არ კარგავენ დროს ფიქრსა და ეჭვებში.

[30] სილიკონის ველი-Silicon Valley (სილიკონის ველი კაჟისგან მიღებული ნაერთის, სილიციუმის გამო ეწოდა, რომელიც მიკროსქემებში ფუძეშრედ გამოიყენება)-მაღალტექნოლოგიური ზონაა, სადაც მაღალტექნოლოგიური ინდუსტრიის ობიექტებია განლაგებული. მის ძირითად ამოცანას მეცნიერული იდეების პრაქტიკაში დანერგვის დროის შემცირება წარმოადგენს. "სილიკონ ველის" მსგავს ზონებს გააჩნიათ სპეციალური ინფრასტრუქტურა: შენობა-ნაგებობები, ტელეკომუნიკაცია, სპეციალური საგადასახადო და საბაჟო შეღავათები და ა.შ."სილიკონის ველის" დედაქალაქად არაოფიციალურად ქალაქ სან-ხოსეს (კალიფორნიის ქალაქი) მოიხსენიებენ.

[31] დიდი ოცეული (ინგლ. Group of Twenty, G-20) საერთაშორისო ფორუმის ფორმატი, როდესაც ერთმანეთს ფინანსთა მინისტრები და ცენტრალური ბანკების ხელმძღვანელები ხვდებიან. 2009 წელს უმაღლეს დონეზე მიღებული გადაწყვეტილების მიხედვით, დიდი ოცეული მსოფლიო ეკონომიკის მთავარი სტრატეგიული ეკონომიკის ფორუმია. დიდი ოდეული აერთიანებს მსოფლიოში ეკონომიკურად წამყვან და სწრაფად განვითარებად ქვეყნებს [20]. https://www.g20.org/index.php/en/g20

გამოყენებული ლიტერატურის ჩამონათვალი

1. გვენეტაძე ეპიფანე. „საერთაშორისო უშიშროების ასპექტები“, თბილისი, 2017 წ.
2. Цитович Я.В., Понятие «национальная безопасность» и особенности ее обеспечения (на примере Государства Израиль) Россия, Москва; 2019 г
3. Казанин М.В., Военный и гражданский аспекты кибербезопасности Израиля. 2018 г.
4. Гельман З. Кибербезопасность по-израильски, Тель-Авив, 2019 г.
5. Диогенес Ю, Озкайя Э: Кибербезопасность. Стратегии атак и обороны. Перевод: Беликов Д. изд. ДМК-Пресс, 2020 г.
6. Демидов О. и Касенова М. Кибербезопасность и управление интернетом: Москва. изд Статут, 2013 г.
7. Север А. «Моссад» и другие спецслужбы Израиля. 2011 г.
8. Седов С. Сионизм: ставка на террор.–изд. Москва, 1984 г.
9. Дегтярев К. Энциклопедия спецслужб. – Москва., 2008 г.
10. Блехман Р. Мосад, Аман, Шабак, или Возмездие по-еврейски Уцененный товар (№1), 2008г.
11. Бирюк В. Секретные операции XX века: Из истории спецслужб. – СПб., 2003 г.

ინტერნეტ რესურსები

12. https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=ka
13. https://il-cert.org.il/
14. https://he.wikipedia.org/wiki/%D7%99%D7%97%D7%99%D7%93%D7%94_8200
15. https://www.gov.il/en/departments/news/119en
16. https://www.7kanal.co.il/News/News.aspx/205594
17. https://shofar7.com/2015/05/17/20-%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D0%B9-%D0%BA%D0%BE%D1%82%D0%B8%D1%80%D1%83%D1%8E%D1%89%D0%B8%D1%85%D1%81%D1%8F-%D0%B2-nasdaq-%D0%B8%D0%B7%D1%80%D0%B0%D0%B8%D0%BB%D1%8C%D1%81/
18. https://mfa.gov.il/mfa/innovativeisrael/sciencetech/pages/israel-launches-kidma-2-cyber-security-program-21-dec-2015.aspx
19. https://www.rafael.co.il/worlds/cyber-security/
20. https://www.g20.org/index.php/en/g20
21. https://mfa.gov.il/MFARUS/PressRoom/2016/Pages/PM-Netanyahu-speech-at-UNGA-22-9-16.aspx