კიბერდანაშაული და კიბერტერორიზმი XXI საუკუნის მთავარი საფრთხე

შოთა ბერუაშვილი

,,წარმოდგენილია მაგისტრის აკადემიური ხარისხის მოსაპოვებლად",

თბილისი, 0177
ივლისი, 2019

შოთა ბერუაშვილი _____

საიდენტიფიკაციო ნომერი _____

თბილისის ღია სასწავლო უნივერსიტეტი

სკოლა: ჰუმანიტარულ და სოციალურ მეცნიერებათა

საგანმაათლებლო პროგრამა: საერთაშორისო ურთიერთობები

,,ჩვენ, ქვემორე ხელისმომწერნი ვადასტურებთ, რომ გავეცანით შოთა ბერუაშვილის მიერ შესრულებულ ნაშრომს დასახელებით: ,,კიბერდანაშაული და კიბერტერორიზმი XXI საუკუნის მთავარი საფრთხე" და ვაძლევთ რეკომენდაციას განხილულ იქნას თბილისის ღია სასწავლო უნივერსიტეტის ჰუმანიტარულ და სოციალურ მეცნიერებათა სკოლისსაგამოცდო კომისიის მიერ მაგისტრის აკადემიური ხარისხის მოსაპოვებლად"

თარიღი _____

ხელმძღვანელი : სოფო ჩქოფოია, ასოცირებული პროფესორი

_____

რეცენზენტი:

_____

ხარისხის მართვისა და სტრატეგიული განვითარების სამსახურის უფროსი:

ნათია ვაჭარაძე

_____

რეზიუმე

წარმოდგენილი სამაგისტრო ნაშრომი იკვლევს კიბერდანაშაულის გამოვლენის ფორმებს და კიბერტერორიზმის წარმოშობას, როგორც საერთაშორისო ტერორიზმის ერთ-ერთ გამოვლინებას.

თანამედროვე მსოფლიოში ტერორიზმის პრობლემა საერთაშორისო უსაფრთხოებისათვის ერთ-ერთ მთავარ გამოწვევას წარმოადგენს. დღეს აღნიშნულ პრობლემას უდიდესი ყურადღება ეთმობა, რაც გამოწვეულია იმით, რომ თვითონ ტერორი, როგორც ბრძოლის ერთერთი ხერხი ფართოდ გამოიყენება მთელმსოფლიოში და უდიდეს მასშტაბებს აღწევს. ტერორიზმის მრავალ გამოვლინებათაგან, ყველაზე მნიშვნელოვანი, ყურადსაღები და უმთავრესი გამოწვევა თანამედროვე მსოფლიოსთვის გახლავთ კიბერტერორიზმი.

„კიბერსივრცე“-არის ინფორმაციული და ტექნოლოგიური ინფრასტრუქტურის ურთიერთკავშირში არსებული კომპლექსი, სადაც შედის გლობალური ინტერნეტისა და ტელეკომუნიკაციის ქსელები, კომპიუტერული სისტემები, ასევე, ჩართული პროცესორები, სერვერები და მაკონტროლირებელი მოწყობილობები, რომლებიც გამოიყენება მრეწველობის სხვადასხვა დარგში. ახალი ტექნოლოგიების განვითარებასთან ერთად იზრდება საფრთხეები, რომლებიც დიდ ზიანს აყენებს კიბერსივრცეს და მის მომხმარებელს. სახელმწიფოს და სახელისუფლებო ორგანოებს პირველ რიგში აინტერესებთ ეროვნული უსაფრთხოების უზრუნველყოფა, კრიტიკული ინფორმაციისა და ინფორმაციული ინფრასტრუქტურის დაცვა როგორც უცხო სახელმწიფოს, ისე არასამთავრობო სუბიექტებისა და დაჯგუფებების მხრიდან ხელყოფისგან, რათა თავიდან იქნას აცილებული ინფორმაციის მოპარვა ან/და გადაცემა, ქსელის დაზიანება ან/და საერთოდ განადგურება.

ყოველდღიურად მსოფლიოში იგზავნება მილიარდობით ელექტრონული წერილი, რომელთაგანაც 80%-ზე მეტი არის სპამი. სპამ-ბოტი არის სპეციალური პროგრამა, რომელიც აგროვებს ელ-ფოსტის მისამართებს ინტერნეტში,

ავტომატურად ათვალიერებს სხვადასხვა ვებგვერდებს, ფორუმებს დააგროვებსელ-ფოსტის მისამართებს, ხოლო შემდეგ მიღებულ იინფორმაცია ხვდება სპამერების წერილების მასობრივი დაგზავნის სიაში, რისი საშუალებითაც შემდეგ იგზავნება სპამი. ნაშრომში ასევე მიმოხილულია ის ძირიტადი ვირუსები რომელბსაც იყენებენ კიბერშეტევების დროს, როგორც ტერორისტები ასევე სხვა სახის დამნაშავეები.

ტექნოლოგიის განვითარებას თანერთად ტერორისტების მიერ ინტერნეტის გამოყენებაც უფრო მეტად გავრცელდა. ტერორისტების საინტერნეტო კომუნიკაცია ხშირად შეიცავს მათ ოპერატიულ გეგმებს და მეთოდებს, რომელთა გაშიფვრის შემთხვევაშიც შესაძლოა ანტიტერორისტული ბრძოლის მეთოდების შემუშავება, მათი ვიანაობის დადგენა და ფონდების გადარიცხვების შესახებ ინფორმაციის მოპოვება.

ჩვენი მიზანი იყო წარმოგვეჩინა ტერორისტული საქმიანობის საფუძვლები და სახეები, მათ შორის ისეთის, როგორიც არის ინტერნეტტერორი და ინტერნეტში არსებული ტერორისტული რიტორიკა, ის წინაპირობები, რომლებიც იწვევს მათწარმოშობას და განაპირობებს მათ მომავალ საქმიანობას. შესწავლილ უნდა იქნეს ტერორიზმის წინააღმდეგ ბრძოლის გზები, რომელიც ხელისშემწყობი ფაქტორი გახდება აღნიშნულ დანაშაულთან ეფექტური ბრძოლის საქმეში. მიზანი უნდა იყოს იმ საფუძვლების კვლევაძიება, რაც იწვევს ტერორისტული აქტივობის ზრდას.

სპეციალიზაციის რომელი სფეროც არ უნდა იყოს, ანტიტერორიზმის ანალიტიკოსები საჭიროებენ მაღალი დონის მომზადებას. როგორც უკვე არაერთმა მკვლევარმ ააღნიშნა, არაბულის ცოდნა არ არის საკმარისი და არც მარტო არაბულად მოლაპარაკეები გვჭირდებაა. საჭიროა, კარგად ვერკვეოდეთ იქაურ კულტურასა და ტრადიციებში. პრიორიტეტული უნდა გახდეს ინფორმაციის მონიტორინგისა და მისი მოპოვებისათვის მომზადება.

ნაშრომში ცალკე თავად არის განხილული ასევე კიბერსაფრთხეები ბავშვებისთვის. და მოცემულია რეკომენდაციები, როგორ ავარიდოთ ბავშვები

მსგავს საფრთხეებს. ინტერნეტში ხშირია ბავშვებზე გავრცელებული კიბერ ჩაგვრაც, ეს არის ძალადობის ფორმა, რომელიც ხორციელდება სოციალური ქსელების საშუალებით. ძირითდად „მესიჯებით“, რომლებიც ხშირად მუქარის შემცველიაასეთია მაგალითად „ლურჯი ვეშაპი“

რადგან ნებისმიერი სახელმწიფო შეიძლება აღმოჩნდეს კიბერტერორიზმის მსხვერპლი, ამიტომ ამ პრობლემის მოგვარება სახელმწიფოთა შეთანხმებულ მოქმედებას მოითხოვს.კიბერუსაფრთხოება მოიცავს საქართველოს თავდაცვის სამინისტროს საქმიანობის ყველა იმ სფეროსაც, სადაც გამოიყენება ინფორმაციული ტექნოლოგიები, იქნება ეს სამხედრო/თავდაცვითი ოპერაციების დაგეგმვა, სამხედრო წვრთნების წარმოება, ლოგისტიკური მხარდაჭერა თუ სხვა, რათა უზრუნველყოფილი იქნას ინფორმაციის მთლიანობა, ხელმისაწვდომობა და დროული გაზიარება.

კვლევის შედეგად ნაჩვენებია, რომ კიბერდანაშაული და კიბერტერორიზმი უმთავრესი გამოწვევა და საფრთხეა, როგორც მსოფლიოსათვის, ასევე, ჩვენი ქვეყნისთვის.

Summery

The presented bachelor`s work examines the forms of revealing an international terrorism and emerge of cyber terrorism, as the demonstration of one of international terrorism types.

In modern world, the terrorism issue presents one of the main challenge for international security. Nowadays the mentioned problem has taken the biggest attention, which is caused by the fact, that the terror itself, as one of the methods of the fight is widely used throughout the world and it covers the huge scales.

One of the most significant among the demonstration of terrorism and one of the main challenge for the modern world is cyber terrorism.

As every state could be the victim of cyber terrorism, thus the settlement of the said issue needs the agreed action of different states.

Cyber security covers all those fields of activity of the Ministry of Defense of Georgia, where the IT is being used, regardless of projecting the military / defense operations, arranging the military trainings, logistical support, etc. in order to ensure the unity, availability and timely sharing of the information.

The cyber space is the complex existed in the interconnection of informational and technological infrastructure, where the global internet and telecommunication networks are covered, also the computer systems, turned processors, servers and controlling devices, which are used in different fields of the industry.

Alongside with developing technologies there are increasing the threats as well, which deal a big damage to cyber space and its users. The state and authoritative bodies first of all are interested to ensure the national security, to protect the critical information and informational infrastructure from foreign states, non-governmental subjects and groups, in order to prevent the stealing or / and transferring of necessary information, network damage or / and total demolition.

As a result of research, there are shown, that cyber terrorism, like one of the types of international terrorism is one of the main challenge and the threat for the world and for our country as well, which personally became the object of cyber-attack during the August, 2008 war. According to the existed opinions, those properties are analyzed, according to which the local and international experts assign to the mentioned war with the status of "cyber-war". There are reviewed and discussed those document of state policy and strategy, which ensure to prevent from such cyber-terrorist attacks and there are raised the relevant conclusions.

შინაარსი

შესავალი

თემის აქტუალობა:გლობალიზაციასთან ერთად საერთაშორისო ურთიერთობებში უსაფრთხოების ცნება საკმაოდ კომპლექსური გახდა და დაგვანახა, რომ მხოლოდ ტრადიციული გზებით ეროვნული საზღვრების დაცვა მოსალოდნელ საფრთხეებს ვეღარ უმკლავდება. ინფორმაციული ტექნოლოგებისა და სისტემების განვითარებამ მართალია წარმოშვაუამრავიკეთილდღეობამაგრამ ამასთან ერთად თავი იჩინა სხვადასხვატიპისჰიბრიდულმასაფრთხემ, როგორიცარის კიბერდანაშაული და კიბერტერორიზმი. დღესდღეობითამგვარი საფრთხეები სულუფროდაუფროთვალსაჩინოხდებასოციალურმედიაში. ინტერნეტზედამოკიდებულებასწრაფადიზრდებამსოფლიოსმასშტაბით, რაცქმნის, საერთაშორისოკიბერტერორისგანხორციელებისთვისეროვნულპლატფორმას და უსაფრთხოებებისთვისპირდაპირსაფრთხესწარმოადგენს. შესაბამისად, ტერორიზმი გვევლინება, როგორც გლობალიზაციის ერთ-ერთი მთავარი გამოწვევა, რომლის წინააღმდეგ ბრძოლაში ჩართულია ქვეყნებისა და საერთაშორისო ორგანიზაციების დიდი რაოდენობა.დღესდღეობით აღნიშნულ პრობლემას უდიდესი ყურადღება ეთმობა, რაც გამოწვეულია იმით, რომ თვითონ ტერორი, როგორც ბრძოლის ერთ-ერთი ხერხი ფართოდ გამოიყენება მთელ მსოფლიოში და უდიდეს მასშტაბებს აღწევს.

ტერორიზმის მრავალ გამოვლინებათაგან, ყველაზე მნიშვნელოვანი, საყურადღებო და ერთ-ერთი უმთავრესი გამოწვევა თანამედროვე მსოფლიოსთვის გახლავთ კიბერტერორიზმი. ტექნოლოგიური პროგრესის მიღწევად მიიჩნევა, რომ თანამედროვე მსოფლიოში ინფორმაციის უმთავრესი რესურსი სახელმწიფოებისათვის, სახელმწიფოს შიგნით არსებული ორგანიზაციებისთვის, კომპანიებისთვის თუ სხვა კერძო თუ სახელმწიფო სუბიექტებისთვის ციფრულ/ელექტრონულ სივრცეებში არის განთავსებული, შესაბამისად, ტერორიზმის უმთავრესი სამიზნე არის ამ სივრცეებში შეღწევა და ინფორმაციის მოპოვება, განადგურება, დამუშავება და.ა.შ. სახელმწიფოებისათვის

კი კიბერტერორიზმთან ბრძოლა ერთ-ერთი უმთავრესი პრიორიტეტია. ამდენად კიბერდანაშუალი და კიბერტერორიზმი შესწავლის თვალსაზრისით ერთ ერთ აქტუალურ საკითხს წარმადგენს.

მიგვაჩნია, რომ აღნიშნული საკითხის კვლევა აქტუალურია, რადგან ერთი მხრივ, კიბერსაფრთხეებთან ბრძოლა მსოფლიო უსაფრთხოების მთავარ გამოწვევას წარმოადგენს. ხოლო მეორე მხრივ, ჩვენი ქვეყნის რთული პოლიტიკური მდგომარეობიდან გამომდინარე, როცა ქვეყნის 20% ოკუპირებულია, მუდმივად გრძელდება მცოცავი ოკუპაცია. შესაბამისად, საქართველოს, როგორც გეოპლიტიკურად სასაზღვრო რეგიონის ქვეყანას განსაკუთრებული სტრატეგიისა და პოლიტიკის გატარება სჭირდება კიბერსაფრთხეების პრევენციისა და თავიდან არიდების კუთხით.

ნაშრომის მიზანი: ყოველივე აღნიშნულის გათვალისიწინებით, ჩვენი მიზანია, ნაშრომის ფარგლებში, მოვახდინოთ დეფინიციების გამიჯვნა კიბერტერიზმისა და კიბერდანაშუალს შორის შევისწავლოთ კიბერდანაშუალისა და კიბერტერორიზმის წარმოშობის წინაპირობები, მიმოვიხილოთ კიბერსაფრთხეების ფორმები და ბოლოს, განვიხილოთ ევროკავშირისა და ნატოს პოლიტიკა, ასევე საქართველოს როლი კიბერსაფრთხეებთან გამკლავების პროცესში.

კვლევს შედეგები: კვლევის შედეგად ნაშრომში, არსებულ მოსაზრებებზე დაყრდნობით, დაზუსტებულია კიბერდანაშუალისა და კიბერტერორიზმის დეფინიციები ასევე ნაჩვენებია, რომ მართალია, მსოფლიო მასშტაბით სახელმწიფოები აქტიურად ცდილობენ შეიმუშავონ სწორი სტრატეგია და სამართლებრივი მიდგომები კიბერტერორიზმის საფრთხეებთან გასამკლავებლად, თუმცა ამ მიმართულებით გაცილებით მეტი სამუშაოა შესასრულებელი, კერძოდ, საჭიროა შესაბამისი კანონმდებლობის დახვეწა, რაც დაარეგულირებს უკვე არსებული თითოეული სუბიექტის - ურთიერთკოორდინირებულ საქმიანობას, განსაზღვრავს თითოეული სუბიექტის მოქმედების ფარგლებსა და დამატებით ვალდებულებებს.

ლიტერატურის მიმოხილვა:კიბერტერორიზმის საკითხის შესასწავლად ჩვენი კვლევის პროცესში, დავეყრდენით ანა ჭიღიტაშვილის მონოგრაფიას ,,ტერორიზმი როგორც გლობალური პრობლემა: კრიმინოლოგიური ანალიზი და ბრძოლის მეთოდები საქართველოში„ ასევე, საქართველოს ტექნიკური უნივერსიტეტის მიერ გამოცემულ კრებულს ,,საეთაშორისო ტერორიზმი“ (2016).

აღნიშნული საკითხების კვლევისას გამოვიყენეთ, კიბერუსაფრთხოების საკითხევბში ექსპერტ ლაშა პატარაიას მონოგრაფია კიბერკრიმინალი ლეგალური და სადაზვერვო ასპექტები“ (2012), ასევე, აქტიურად ჩავრთეთ ამ დარგის ექსპერტთა მოსაზრებები, გამოთქმული საქართველოს კიბერუსაფრთხოებასთან დაკავშირებით, ინტერნეტ რესურსები და ამ მიმართულებით შემუშავებული ქართული საკანონმდებლო ბაზა. ასევე სოფო ჩქოფოიას საერთაშორისო ტერორტიზმის ისტორიულ-პოლიტიკური ასპექტები“ ვ. სვანაძე, ა. გოცირიძის მონოგრაფია - კიბერთავდაცვა (კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები), ასევე ხათუნამ შვილდაძე, გლობალური მნიშვნელობის კიბერდომეინი და ახალიგამოწვევები, ასევე სხვა არაერთი მნიშვნელოვანი ინტერნეტწყაროებში განთავსებული მასალა (იხ. ბიბლიოგრაფია)

თავი 1. ტექნოლოგიური განვითარება და კიბერტერორიზმი

1.1 კიბერუსაფრთხოებისადა კიბერტერორიზმის დეფინიცია, მსგავსება და განსხვავება

ტერმინის ,,კიბერტერორიზმი“ პირველად 1980 წელს კალიფორნიის უსაფრთხოებისა და დაზვერვის ინსტიტუტის უფროსმა მეცნიერ-თანამშრომელმა, ბარი კოლინმა, გამოიყენა კიბერსივრცისა და ტერორიზმის გასაერთიანებლად, ხოლო პირველი სამუშაო განსაზღვრება სპეციალურ აგენტს – მარკ პოლიტს ეკუთვნის, რომლის მიხედვითაც, კიბერტერორიზმი ეს არის სუბნაციონალური ან ფარული აგენტების მიერ წინასწარ განზრახული პოლიტიკურად მოტივირებული ძალადობა ,,მშვიდობიანი” (არამებრძოლი) სამიზნის წინააღმდეგ.

კიბერუსაფრთხოების საკითხი კი ეხება ტექნოლოგიებს, მიმდინარე პროცესებს და პრაქტიკას, რაც შექმნილია ქსელის, ტექნოლოგიური მოწყობილობების, პროგრამების და მონაცემების დასაცავად თავდასხმის დროს, რაც ზიანს მიაყენებს არაავტორიზებული წვდომისგან. კიბერ უსაფრთხოებას საინფორმაციო ტექნოლოგიების უსაფრთხოებასაც უწოდებენ.

აუცილებლად უნდა აღინიშნოს ის საზიანო შედეგი, რომელიც ჰაკერულ ქმედებას შეიძლება მოჰყვეს. იურიდიული თვალსაზრისით, კიბერსივრცეში ინფორმაციის განზრახ განადგურება აუცილებლად არის ტერორისტული ქმედების შემადგენელი ნაწილი, მისი მიზნისა და შედეგის გათვალისწინებით.[1]

რადგან ნებისმიერი სახელმწიფო შეიძლება აღმოჩნდეს კიბერტერორიზმის მსხვერპლი, ამიტომ ამ პრობლემის მოგვარება სახელმწიფოთა შეთანხმებულ მოქმედებას მოითხოვს. როგორც ზემოთ აღვნიშნეთ, აშშ-მ 2002 შემდეგ კი 2007 წელს შეიმუშავა ინფორმაციული უსაფრთხოების დოქტრინა; 2000 წელს რუსეთმაც მიიღო უსაფრთხოების დოქტრინა, აგრეთვე დიდი ბრიტანეთიც განსაკუთრებული ყურადღებით ეკიდება კიბერუსაფრთხოების საკითხებს.

[1]კიბერტერორიზმის პრობლემატიკა ანუ XXI საუკუნის საფრთხეhttp://freeview.ge/xxi/

აღნიშნულის გათვალისწინებით, გასაკვირი არაა, რომ კიბერუსაფრთხოება მოიცავს საქართველოს თავდაცვის სამინისტროს საქმიანობის ყველა იმ სფეროსაც, სადაც გამოიყენება ინფორმაციული ტექნოლოგიები, იქნება ეს სამხედრო/თავდაცვითი ოპერაციების დაგეგმვა, სამხედრო წვრთნების წარმოება, ლოჯისტიკური მხარდაჭერა თუ სხვა, რათა უზრუნველყოფილი იქნას ინფორმაციის მთლიანობა, ხელმისაწვდომობა და დროული გაზიარება.

საქართველოს კანონმდებლობით კიბერტერორიზმი განიმარტება, როგორც ,,კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის საშიშროებას და ხელყოფს საზოგადოების უსაფრთხოებას, სახელმწიფო სტრატეგიულ პოლიტიკურ ან ეკონომიკურ ინტერესს, ჩადენილი მოსახლეობის დაშინების ან/და ხელისუფლების ორგანოზე ზემოქმედების მიზნით, - ისჯება თავისუფლების აღკვეთით 10-დან 15 წლამდე.[2]

თანამედროვე ეტაპზეგლობალურიქსელებისმიმართარსებულმზარდინტერესსთანახლავსმისიუ საფრთხოებისუზრუნველსაყოფად მიმართული საკმაოდ მნიშვნელოვანი ნაბიჯებიც.

„კიბერსივრცე“ ეს არის ინფორმაციული და ტექნოლოგიური ინფრასტრუქტურის ურთიერთკავშირში არსებული კომპლექსი, სადაც შედის გლობალური ინტერნეტისა და ტელეკომუნიკაციის ქსელები, კომპიუტერული სისტემები, ასევე, ჩართული პროცესორები, სერვერები და მაკონტროლირებელი მოწყობილობები, რომლებიც გამოიყენება მრეწველობის სხვადასხვა დარგში.

ახალი ტექნოლოგიების განვითარებასთან ერთად იზრდება საფრთხეები, რომლებიც დიდ ზიანს აყენებს კიბერსივრცეს და მის მომხმარებელს. სახელმწიფოს და სახელისუფლებო ორგაონოებს პირველ რიგში აინტერესებთ ეროვნული უსაფრთხოების უზრუნველყოფა, კრიტიკული ინფორმაციისა და ინფორმაციული ინფრასტრუქტურის დაცვა, როგორც უცხო სახელმწიფოს, ისე

[2] კიბერტერორიზმისპრობლემატიკაანუ XXI საუკუნისსაფრთხეhttp://freeview.ge/xxi

არასამთავრობო სუბიექტებისა და დაჯგუფებების მხრიდან ხელყოფისგან, რათა თავიდან იქნას აცილებული ინფორმაციის მოპარვა ან/და გადაცემა, ქსელის დაზიანება ან/და საერთოდ განადგურება.

უდავოა, რომ სახელმწიფოს უსაფრთხოების რეალურ საფრთხეს წარმოადგენს კიბერშეტევები, რომლებიც მიმართულია ისეთი სასიცოცხლო მნიშვნელობის მქონე ინფრასტრუქტურის განადგურებისკენ, როგორებიცაა სატელეკომუნიკაციო ქსელების, ენერგოგენერირებისა და ნავთობგადამამუშავებელი სიმძლავრეების სისტემები, ასევე ელექტრომომარაგების, საფინანსო, ჯანდაცვისა და სატრანსპორტო სისტემები.

კიბერდანაშაულთან ბრძოლის ერთ-ერთ მთავარ პრობლემას წარმოადგენს ის ფაქტი, რომ ხშირად ძალზედ რთულია ზუსტად დაადგინო არამარტო უშუალო შემსრულებლები, არამედ მათი ადგილსამყოფელი ან ის ქვეყანა, საიდანაც განხორციელდა შეტევა. ამიტომ, დამნაშავეს ან დამნაშავეთა ჯგუფს შეუძლია ადვილად დამალოს არამარტო თავისი მონაწილეობა კიბერშეტევის ორგანიზებაში, არამედ თავისი თავი დააფიქსიროს როგორც ქსელის სხვა მომხმარებლად ან საერთოდ დარჩეს ანონიმურად.

ანა ჭიღიტაშვილის მიხედვით, კიბერსაფრთხეების წარმოშობის წყაროებს წარმოადგენენ როგორც სახელმწიფო და კერძო სექტორის წარმომადგენლები, ისე სხვადასხვა სახისა და ნიშნით შექმნილი ორგანიზაციები და ფიზიკური პირები. მკვლევარი ვლ. სვანიძე ეყრდნობა რა შეერთებული შტატების კონტროლის პალატის მასალებს, კიბერსაფრთხეების წარმოშობის წყაროებსაკვალიფიცირებს შემდეგგვარად:

- სახელმწიფო - უცხოეთის ქვეყნების სადაზვერვო სამსახურები კომპიუტერულ ტექნოლოგიებს იყენებენ ინფორმაციის შეგროვებისა და ჯაშუშობისთვის. მსგავსი ქმედებები სადაზვერვო სამსახურების მხრიდან შეიძლება მიმართული იყოს, როგორც მეგობარი, ისე მოწინააღმდეგე ქვეყნების მიმართ, ან არასახელმწიფო სუბიექტების წინააღმდეგ. სახელმწიფო თავისი სადაზვერვო სამსახურების გამოყენებით, ახორციელებს კიბერშეტევებს

პოტენციური მოწინააღმდეგე სახელმწიფოების მიმართ დეზინფორმაციის, დესტაბილიზაციის, დაშინების ან ფართომასშტაბიანი კიბერომის წარმოების მიზნით. ასევე საყურადღებოა ის გარემოება, რომ ხშირად ხდება პიროვნების უსაფრთხოებისა და უფლებების დარღვევა. კერძოდ, სახელმწიფოს სპეციალურმა სამსახურებმა შეიძლება მიმართონ ისეთ ქმედებებს, რომელთა გამოყენებითაც ხდება მოქალაქეთა პერსონალური მონაცემების გადაჭერა, მოპარვა და გამოყენება. მსგავსი ქმედებები ხშირ შემთხვევაში ხდება სასამართლოს შესაბამისი ორგანოების სანქციისა და სწორი დემოკრატიული კონტროლის გარეშე;

- კორპორაციები, კომპანიები-დაკავებულნი არიან სამრეწველო/კორპორაციული ჯაშუშობითა და/ან დივერსიული საქმიანობით, რაშიც ისინი ხშირად იყენებენ ჰაკერებსა და ორგანიზებულ დამნაშავეთა ჯგუფებს. კომპანიების, კორპორაციებისა და კერძო სექტორის სხვა წარმომადგენლებს შეუძლიათ დაარღვიონ ადამიანის უფლებები პიროვნების პერსონალური მონაცემების შეგროვებისა და ანალიზის გზით, ან ზოგ შემთხვევაში მოცემული მონაცემების სახელმწიფო ორგანოებთან ან სხვა დაინტერესებულ პირებთან გაცვლით;

- ჰაკერები - იყო დრო როცა ჰაკერების მხრიდან ქსელებში არასანქცირებული შეღწევა ან პროგრამების გატეხვა დაკავშირებული იყო ჰაკერთა საზოგადოებაში ავტორიტეტის მოპოვებასთან ან წვრილმან ხულიგნობასთან. დღესდღეისობით სურათი კარდინალურად არის შეცვლილი, კერძოდ ჰაკერთა უმრავლესობის ქმედება ატარებს კრიმინალურ ხასიათს. ადრე თუ ჰაკერებისთვის ქსელის გატეხვისათვის საჭირო იყო კომპიუტერული ტექნოლოგიების სფეროში სპეციალური უნარ - ჩვევების ცოდნა, როცა ამჟამად საკმარისია ინტერნეტიდან შესაბამისი ინსტრუქციებისა და პროტოკოლების გადმოქაჩვა და მათი გამოყენება შერჩეულ საიტზე კიბერშეტევის ორგანიზებისთვის. ამის გამო, კიბერშეტევის განხორციელება მომხმარებლისთვის გახდა უფრო ადვილად ხელმისაწვდომი. ჰაკერთა მომსახურეობით სარგებლობენ არამარტო კორპორაციები და კომპანიები, არამედ სადაზვერვო ან სხვა სახის სპეციალური სამსახურებიც;

• ჰაკტივისტები - ტერმინი „ჰაკტივიზმი“ (hacktivism) წარმოიშვა ორი სიტყვის „Hack“ და “Activism” შეერთებით და ის აღნიშნავს სოციალური პროტესტის გამოხატვის ახალ მოვლენას, რომელიც წარმოადგენს თავისებურ სინთეზს რაღაცის მიმართ გამოხატული პროტესტის სოციალური აქტიურობისა და ჰაკერობის, რომელიც მიმართულია გარკვეული ვებ - გვერდების ან საფოსტო სერვისების წინააღმდეგ. თავიანთი პოლიტიკური მიზნების მისაღწევად, ჰაკტივისტები მიისწრაფვიან დააზიანონ ან საერთოდ მწყობრიდან გამოიყვანონ ზოგიერთი ვებ - გვერდი;

• კიბერ დივერსანტები ქსელის უკმაყოფილო მომხმარებელთა რიცხვიდან - ზოგადად, უკმაყოფილო მომხმარებლები წარმოადგენენ სერიოზულ საფრთხეს, ვინაიდან ისინი კარგად იცნობენ სისტემის მუშაობის პრინციპებს და შეუძლიათ თავიანთი ეს ცოდნა გამოიყენონ დესტრუქციული მიზნებისთვის. მაგალითად, სისტემის დასაზიანებლად ან კონფიდენციალური ინფორმაციის მოსაპარად. შეერთებული შტატების ფედერალური საგამოძიებო ბიუროს (FBI) მონაცემებით, სისტემის მომხმარებლებისა და გარე წყაროების მხრიდან კიბერშეტევის ორგანიზების შესაძლებლობის ერთმანეთთან შეფარდება შეადგენს 2:1;

• ტერორისტები - ცდილობენ ინფრასტრუქტურის მნიშვნელოვანი ობიექტები გამოიყვანონ მწყობრიდან, საერთოდ გაანადგურონ ან გამოიყენონ თავიანთი მიზნებისთვის. მათი ქმედება სერიოზული საფრთხის ქვეშ აყენებს ქვეყნების ეროვნულ უსაფრთხოებას, იწვევს ადამიანთა მასიურ მსხვერპლს, ასუსტებს ეკონომიკას, ასევე ზიანს აყენებს საზოგადოების მორალურ მდგომარეობასა და ამცირებს მათ სანდოობას ხელისუფლების მიმართ. ყველა ტერორისტული ორგანიზაცია და დაჯგუფება არ ფლობს საკმარის ცოდნასა და ტექნიკურ საშუალებებს ეფექტური კიბერშეტევის განხორციელებისთვის, თუმცა არსებობს თეორიული დაშვება, რომ მათ მიიღონ მსგავსი ცოდნა და შესაძლებლობა, ან დახმარებისთვის მიმართონ ორგანიზებული დანაშაულის წარმომადგენლების მომსახურებას[3];

[3] ჭიღიტაშვილი ა 10. ჭიღიტაშვილი ანა, ტერორიზმი როგორც გლობალური პრობლემა: კრიმინოლოგიური ანალიზი და ბრძოლის მეთოდები საქართველოში თბილისი 2009 :25-32

- ბოტნეტი - ინტერნეტ - ბოტი ბოტნეტში წარმოადგენს პროგრამას, რომელიც ფარულად არის დაყენებული მსხვერპლის/ობიექტის კომპიუტერულ მოწყობილობაში, რაც დამნაშავეს/ბოროტმოქმედს საშუალებას აძლევს დავირუსებული კომპიუტერის რესურსების გამოყენებით, შეასრულოს გარკვეული ქმედებები. ჰაკერების ეს სახეობა თავისი პროგრამებით ავირუსებენ კომპიუტერების დიდ რაოდენობას, რომელთა რესურსებსაც შემდეგ იყენებენ კიბერშეტევის კოორდინირებისთვის, ასევე „სპამის“ გასაგზავნად, ფიშინგისთვის და სხვა მავნე ქმედებისთვის. მსგავსი სახის ქსელები წარმოადგენენ არალეგალური ვაჭრობის ობიექტს;
- ფიშერები - ეს არის ფიზიკური პირები ან პატარა დაჯგუფებები, რომლებიც იყენებენ ფიშინგის ტექნოლოგიებს პერსონალური რეკვიზიტების მოპარვისა და ფასიანი ინფორმაციების გადაყიდვის მიზნით. თავიანთი მიზნების მისაღწევად ფიშერები ხშირად იყენებენ „სპამებს“ და ჯაშუშურ პროგრამებს;
- სპამერები - ფიზიკური ან იურიდიული პირები, რომლებიც მასიურად აგზავნიან არამოთხოვნილ ელექტრონულ ფოსტას დაფარული ან მცდარი ინფორმაციით, რომლის მიზანია ფიშინგითა და ჯაშუშური პროგრამების გამოყენებით კონკრეტულ ორგანიზაციებზე კიბერშეტევის განხორციელება;
- ჯაშუშური და მავნე პროგრამების შემქმნელები - ფიზიკური ან იურიდიული პირები, რომლებსაც გააჩნიათ დანაშაულებრივი ზრახვები კომპიუტერების მომხმარებლებზე კიბერშეტევის განსახორციელებლად;

კიბერშეტევების დროს შეიძლება გამოყენებული იყოს ჰაკერული მეთოდები, რომლის მიზანია მონაცემთა მთლიანობის განადგურება ან მათი დამახინჯება და ცვლილებების შეტანა. მისი ქვესახეობებია:

- პროპაგანდა და დეზინფორმაცია-უცხოეთის სახელმწიფოების ტერიტორიებზე მმართველი რეჟიმების დესტაბილიზაციის მოწყობის, პოლიტიკური პროცესების ან კომერციული საქმიანობის შედეგებზე გავლენის მოხდენის მიზნით, არასწორი მონაცემების შეყვანა/გავრცელება ან არსებულ მონაცემებში ცვლილებების შეტანა;

- დაშინება - ვებ - გვერდებზე შეტევების განხორციელების მიზანია მომხმარებლის (როგორც სახელმწიფო მოხელის, ისე ფიზიკური ან იურიდიული პირის) იძულება წაშალოს ან შეცვალოს საიტის შინაარსი /პოლიტიკა;
- განადგურება - უცხო სახელმწიფოებისთვის ან კონკურენტებისთვის ზარალის ან მავნებლობის მიყენების მიზნით, მონაცემების მუდმივი და მიზანმიმართული განადგურება. კერძოდ, მსგავსი შეტევები შეიძლება განხორციელდეს უფრო მასშტაბური კონფლიქტის დროს არსებული სხვა მოქმედებების პარალელურად.
- დაშვება სისტემაზე განხორციელებული კიბერშეტევის შედეგად, სისტემის ლეგიტიმურ მომხმარებელს ექმნება ისეთი პირობები, რომ მას არ შეუძლია სისტემაში შესვლა და აღარ აქვს დაშვება სისტემის მიერ შემოთავაზებულ რესურსებზე, ან ასეთი დაშვება არის გართულებული. ქვესახეობები:
- საგარეო ინფორმაცია - განხორციელებული შეტევები, რომლის შედეგად შეუძლებელია სახელმწიფო და კერძო სექტორის სერვისებზე ღია დაშვება. კერძოდ, მასიური საინფორმაციო საშუალებებისა და სახელმწიფო თუ კერძო სტრუქტურების საინფორმაციო საიტები;
- ჯაშუშობა - კორპორაციების, კომპანიებისა და ფირმების მხრიდან ინფორმაციის მოპოვება თავისი კონკურენტების მიმდინარე და მომავალი საქმიანობის შესახებ. ჯაშუშურ საქმიანობაში სახელმწიფოს მონაწილეობა, რომელიც მიმართულია უცხო ქვეყნებისა და ფიზიკური თუ იურიდიული პირების წინააღმდეგ;
- პერსონალური მონაცემების მოპარვა - ფიშინგის ან მსგავსი ანალოგიური შეტევების განხორციელება, რომლის მიზანია მოტყუების გზით მომხმარებელი იძულებული გახადოს აცნობოს თავისი პერსონალური მონაცემები, მაგალითად საბანკო ანგარიშები. ვირუსების დაგზავნა, რომლებიც მომხმარებლის პერსონალური კომპიუტერიდან აკეთებს მონაცემთა კოპირებასა და ჩატვირთვას;
- „პიროვნების მოპარვა“ - იგულისხმება მომხმარებლის პერსონალური რეკვიზიტების მოპარვა. ტროიანი და მსგავსი პროგრამები გამოიყენება პირადი მონაცემების მოსაპარად;

- ინფორმაციის მოძიება საერთაშორისო ქსელში-სხვადასხვა სახის ინფორმაციის, კერძოდ, პერსონალური მონაცემების მოპოვების მიღების მიზნით, გამოიყენება ღია წყაროებიდან ინფორმაციის მოპოვების ტექნოლოგიები;
- მაქინაციები - ხშირად ხორციელდება სპამის გამოყენებით, რომელიც ვრცელდება ელექტრონული ფოსტის საშუალებით. აქვე შეიძლება განვიხილოთ მაქინაციების ის სქემები, რომლებიც მომხმარებლებს სთავაზობს არარსებულ სერვისებსა და საქონელზე წინასწარ გადახდას.

სამეცნიერო ლიტერატურაში გამოყოფილია ასევე კიბერომის ცნება, რომელიც განიმარტება, როგორც ,,სამხედრო კონფლიქტი ინფორმაციული ტექნოლოგიების გამოყენებით, რომელიც მიმართულია სამიზნე ქვეყნის სასიცოცხლო და სტრატეგიული დანიშნულების ობიექტების წინააღმდეგ“ [4]

[4]პატარაია ლაშა კიბერკრიმინალი ლეგალური და სადაზვერვო ასპექტები, თბილისი, 2012გვ 98

1.2. ინფორმაციის გაზიარებით გამოწვეული პრობლემები

ტექნოლოგიების ხანაში სოციალური მედია იმდენად წინ მიიწევს, რომ შეიძლება ვივარაუდოთ, მალე ის აბსოლუტურად ჩაანაცვლებს ტრადიციულ მედია საშუალებებს. ტექნოლოგიების განვითარებამ, ინფორმაციის სწრაფი გავრცელების ტენდენცია მოიტანა, შესაბამისად ინტერნეტ, იგივე ონლაინ მედიის გააქტიურება გამოიწვია, რამაც ტელევიზიით, რადიოთი და მითუმეტეს გაზეთებით ინფორმაციის გავრცელების მეთოდს მნიშვნელოვანი კონკურენცია გაუწია. შეიძლება ითქვას, რომ 21–ე საუკუნეში ახალი ამბების პირველადი წყარო საზოგადოებისთვის , ხელში დასაჭერი, „პატარა ყუთი“ გახდა, ტელევიზორს ადამიანები მხოლოდ მაშინ რთავენ, როდესაც სოციალური მედიით გავრცელებულ კონკრეტულ საკითხთან დაკავშირებით დეტალების დაზუსტება სურთ. აღსანიშნავია ისიც, რომ ონლაინ მედიის საშუალებით ინფორმაციას იგებენ არა მარტო ახალგაზრდები, რომლებიც შედარებით უკეთ ადაპტირდებიან ტექნოლოგიებთან, არამედ ხანშიშესული ადამიანებიც. სტატისტიკა მეტყველებს იმაზე, რომ ხანშიშესული ადამიანებიც საკმაოდ აქტიურად მოიხმარენ სოციალურ ქსელებს.

ადამიანი, რომელიც დილით სახლიდან მიდის სკოლაში, უნივერსიტეტში, სამსახურში ან თუნდაც ნებისმიერ სხვა ადგილას, მას არ შეუძლია თან წაიღოს ტელევიზორი, მაგრამ უმეტეს შემთხვევაში მას ექნება მობილური ტელეფონი და აქედან გამომდინარე, შეძლებს მიიღოს ყოველწამიერი ინფორმაცია ქვეყანაში მიმდინარე მნიშვნელოვანი მოვლენებისა და მსოფლიოში მომხდარი ახალი ამბების შესახებ.

მიუხედავად იმისა, რომ არსებობს ვრცელი შეთანხმება, რომ ინფორმაციის გაზიარება აუცილებელია უსაფრთხოების გაძლიერებისთვის, ინფორმაციის გაზიარების ბოლოდროინდელმა გაფართოებამ წამოჭრა რიგი პოტენციური

პრობლემები, რომლებიც მოითხოვს ყურადღებით მართვასა და ზედამხედველობას. მაგალითად, სამართალდამცავ ორგანოებს ამჯერად შესაძლოა დაეკისროთ აღსრულებითი ქმედებები დაფუძნებული საერთო ინფორმაციაზე, რომელიც არასარწმუნოა, და ამდენად არსებობს დიდი რისკი, რომ დაზვერვის სამსახურების მიერ გაზიარებული ინფორმაცია გამჟღავნდება შემდგომ სამართლებრივ პროცედურებში. დიდი რისკის ქვეშ დგება ინდივიდუალური პირების უფლებების, განსაკუთრებით მათი პირადი ცხოვრების ხელშეუხებლობის დაცვის საკითხი. პირებს ნაკლებად ექნებათ შესაძლებლობა გამოცადონ საერთო ინფორმაციის სიზუსტე, რადგანაც, ხშირ შემთხვევაში, მათ არ ეცოდინებათ, რომ ინფორმაცია მათ შესახებ საერთო გამოყენებისაა და არ არის ხელმისაწვდომი.

ბევრ ქვეყანაში, დაზვერვის სამსახურებს, ტრადიციულად, არ სურთ საიდუმლო ინფორმაციის გაზიარება პოლიციასთან და სხვა სამართალდამცავ ორგანოებთან. კანადის საკითხის შემსწავლელმა კომისიამ დაასკვნა, რომ ამგვარმა დამოკიდებულებამ წვლილი შეიტანა 1985 წელს ინდოეთის ავიახაზების დაბომბვისა და ასევე, დაბომბვის შემდგომ სხვადასხვა ნაკლოვანების გამოძიების წარმატებით განხორციელების საქმეში.6 დაზვერვის სამსახურებს აქვთ ინფორმაციის დაცვის ტენდენცია, რადგანაც ისინი შიშობენ, რომ ინფორმაციის გაზიარება გამოიწვევს მის საბოლოო გამხელას, რასაც თავის მხრივ მოყვება მნიშვნელოვანი წყაროებისა და მეთოდების შესაძლო გამოაშკარავება და საფრთხეს შუქმნის სამსახურის უნარიანობას მომავალში დაზვერვის მონაცემების შეკრებისათვის. გარდა ამისა, თუ ინფორმაციის მოპოვება განხორციელდა იმგვარად, რაც მიუღებელი იქნება სასამართლო პროცესისათვის, მისი გაზიარება სამართალდამცავ ორგანოებთან შესაძლებელია გახდეს უფრო მეტად პრობლემური. პოლიციის ორგანოები, რომლებიც დაზვერვის სამსახურებზე მეტ სურვილს იჩენენ ინფორმაციის გაზიარების საქმეში, ასევე გამოთქვამენ წუხილს, რომ ინფორმაციის გაზიარება ძირს გამოუთხრის მათ უნარს გამოიძიონ უშიშროების საფრთხეები და იმოქმედონონ შესასაბამისად.

ისინი, ვისაც დავალებული აქვთ დაზვერვის სამსახურის მეთვალყურეობა აწყდებიან ყველაზე დიდ სირთულეს. ისინი გამუდმებით უნდა იყვნენ დიდი რაოდენობით გაზიარებული ინფორმაციის საქმის კურსში, რომლის მოცულობა იმდენად დიდია, რომ იძულებული არიან სისტემატურად დაეყრდნონ აუდიტს, რომელიც ამოწმებს მხოლოდ შერჩეულ ინფორმაციას. დაზვერვის სამსახურები, ასევე, აწყდებიან სირთულეებს გაზიარებული საიდუმლო ინფორმაციის მისაწვდომობისა და მიკვლევადობის მოსაპოვებლად. მაგალითად, ზედამხედველობის ორგანოს, რომლის იურისდიქციაც ვრცელდება პოლიციაზე, შესაძლებელია არ ქონდეს უფლებამოსილება გამოიკვლიოს თუ, როგორ განხორციელდა დაზვერვის სამსახურისგან პოლიციის მიერ მოპოვებული ინფორმაციის შკრება. ეს განსაკუთრებით შეეფერება სიმართლეს, როდესაც ინფორმაციის მომწოდებელი არის უცხოური სააგენტო.

მრავალ იურისდიქციაში, დაზვერვისა და უშიშროების სამსახურების ქსელები (ზოგჯერ «გაერთიანებულ ცენტრად» წოდებული)შექმნილია იმისთვის, რომ თავი მოუყაროს ინფორმაციას უსაფრთოების საშიშროებების შესახებ, რომელიც უზრუნველყოფილია მრავალრიცხოვანი შიდა და უცხოური წყაროს მიერ. აღნიშნული ქსელებიდან ზოგიერთი მათგანი უცხოურ სააგენტოებს ნებასაც კი აძლევს ერთმანეთთან გაცვალონ ინფორმაცია. საჭიროა, რომ ქვეყნის შიგნით არსებულ სააგენტოებს ხელი მიუწვდებოდეთ მსგავსი ქსელების მიერ შეკრებილ და გავრცელებულ ინფორმაციაზე, რათა სრულყოფილად გაიგონ მათ მეთვალყურეობის ქვეშ მყოფი სააგენტოს ოპერაციები - მითუმეტეს, თუ სააგენტო აწვდის ან იღებს ინფორმაციას ამგვარი რეგიონული, ეროვნული და ზეეროვნული ინსტიტუტებისაგან.

ინფორმაციის გაზიარების გაზრდაზე ერთ-ერთ რეაგირებას წარმოადგენს, როგორც ეროვნულ, ასევე უცხოურ სააგენტოებს შორის საგანგებო საკითხების შესწავლის დაწესება სპეციალური იურისდიქციით შეამოწმოს ინფორმაციის გაზიარება მრავალრიცხოვან სააგენტოებს შორის. ჩანართები 1 და 2 განიხილავს

ანალოგიური საგანგებო შესწავლის მაგალითებს კანადასა და გაერთიანებულ სამეფოში.

დაზვერვის სამსახურებს ცხადად ესაჭიროებათ ინფორმაციის გაცვლა შიდა და უხოურ პარტნიორებთან. სამსახური, რომელიც უბრალოდ აგროვებს დაზვერვის მონაცემებს, გაზიარების გარეშე ვერ მოახერხებს გააფრთხილოს სხვები გამოვლენილი საფრთხეების შესახებ. მრავალი თანამედროვე საფრთხის ტრანსნაციონალური ბუნება მოითხოვს ინფორმაციის გაზიარების გაზრდის აუცილებლობას ეროვნულ და საერთაშორისო დონეებზეც.

თუმცაღა, ინფორმაციის გაზიარების ზრდას ახლავს ხარვეზებიც. მან შესაძლოა გამოიწვიოს პირადობის ხელშეუხებლობისა და სხვა უფლებების დარღვევები იმგვარად, რომელიც არც კანონით არის ნებადართული და არც ეთიკურადაა გამართლებული. იგი რისკის ქვეშ აყენებს მგრძნობიარე წყაროებიდან მოპოვებული საიდუმლო ინფორმაციის გამოაშკარავებასაც.

ინფორმაციის გაზიარებამ ეროვნული და ზეეროვნული ქსელების (გაერთიანებული ცენტრების) მეშვეობით შესაძლოა გამოიწვიოს ანგარიშვალდებულების გაბნევა და დამახინჯება.ზედამხედველობის საპარლამენტო და ექსპერტთა ორგანოებს, რომელთა მანდატიც მათ იურისდიქციას ერთ სააგენტოზე ავრცელებს, ხშირ შემთხვევაში, ხელი არ მიუწვდებათ ქსელების ჩანაწერებეზე, რომლებშიც მონაწილეობენ დაზვერვის სამსახურები - მისაწვდომობის არარსებობამ კი, შეიძლება სერიოზულად შეაფერხოს მათი სამეთვალყურეო საქმიანობა.

ეროვნული საზღვრების მიღმა ინფორმაციის გაზიარებამ შესაძლებელია, ასევე, გამოიწვიოს პოლიტიკის პრინციპების კონფლიქტი, მაგალითად, როდესაც ადამიანის უფლებებზე სარწმუნო ჩანაწერების მქონე ქვეყნები იძულებული არიან გაცვალონ ინფორმაცია იმ ქვეყნებთან, რომლებსაც ამ მხრივ მოეპოვებათ მწირი ჩანაწერები. ანალოგიური გზით ინფორმაციის გაცვლამ შესაძლოა ერთი სახელმწიფო გახადოს ადამიანის უფლებებზე ძალადობის თანამონაწილე,

როგორიცაა წამება, რომელიც განახორციელა ინფორმაციის გამზიარებელმა პარტნიორმა.

მოკლედ, დაზვერვის სამსახურები ვერ შეასრულებენ თავიანთ საქმეს, თუ ისინი ერთობლივად იტყვიან უარს ინფორმაციის გაცვლაზე; და მაინც, ინფორმაციის გაზიარების გაზრდა მრავალ რისკთანაა დაკავშირებული. ინდივიდუალურ პირებთან დაკავშირებით იგი მოიცავს ადამიანის უფლებების დარღვევას, განსაკუთრებით პირადი ცხოვრების ხელშეუხებლობის უფლებას. რაც შეეხება დაზვერვის სამსახურებს, რისკები ეხება არასარწმუნო და/ან არამართებული გზით მოპოვებული ინფორმაციის გავრცელებას, რომელმაც შესაძლებელია შელახოს სამსახურის რეპუტაცია და გამოიწვიოს მწირი რესურსების არაეფექტური გამოყენება.ზედამხედველობის ორგანოებს კი ემუქრებათ რისკები, რომლებიც ახლებურად ზღუდავს მათ შესაძლებლობას გაიგონ, თუ რა სახის ინფორმაცია არის საერთო და როგორ მოხდა მათი გაზიარება[5].

[5]დაზვერვის სამსახურებზე ზედამხედველობის განხორციელება : სახელმძღვანელო, ჰ. ბორნი ა.უილსი თბილისი, DCFI 183-188

1.3. საინფორმაციოლაშქრობა

msoflioSi aRiarebuli yvelaze saxifaTo virusebi

კომპიუტერული ვირუსი ეს არის საზიანო პროგრამა, რომელიც აღწევს კომპიუტერულ სისტემაში მალულად, ახდენს ინფორმაციის და პაროლების კოპირებას, კომპიუტერის პროგრამულ კოდში შეაქვთ ცვლილებები, რომელიც აყენებს ზიანს კომპიუტერს და მის მომხმარებელს.

თავდაპირველად ვირუსებს ქმნიდნენ ძირითადად გასართობად, თუმცა დღეს უკვე სხვა მიზნებისთვის იყენებენ. ვირუსები არის სხვა და სხვა სახის, გააჩნია იმას თუ რა მიზნისთვის არის შექმნილი. ვირუსის გავრცელება ხდება სხვა და სხვა საშუალებებით, თავდაპირველად ის ხვდება კომპიუტერში და შემდეგ ხდება ფაილების დავირუსება. ვირუსების გავრცელება ხდება ინფორმაციის მატარებელი მოწყობილობებით, რომელთაც მიეკუთვნება კომპაქტ-დისკები ჩDშ და USB.

ვირუსების გავრცელება ხდება ინტერნეტით, ელექტრონული ფოსტით და ინტერნეტიდან გადმოწერილი სხვადასხვა პროგრამებით და ფაილებით.

ვირუსების შემოგზავნა ხდება ძალიან ხშირად დაუცველ კომპიუტერულ სისტემაში, ვირუსის მიზანია ასევე დაცულ კომპიუტერულ სისტემაშიც იპოვოს ხარვეზი და ეს გამოიყენოს შესაღწევად. მოტყუებით როცა ვირუსის ფორმა დამაჯერებელია მომხმარებლისათვის, რომ ის მისთვის საჭიროა.

ინტერნეტის ისტორიაში ყველაზე სახიფათო ვირუსებს მიეკუთვნება:

ტვინი (Brain) - სხვა ვირუსებისაგან განსხვავებით ეს ვირუსი ნაკლებად სახიფათოა, რადგან ის გადაიცემა დისკეტების მეშვეობით, თუმცა აღსანიშნავია, რომ სწორეს ამ ვირუსმა პირველად ისტორიაში გამოიწვია ნამდვილი ვირუსული ეპიდემია. ვირუსი შექმნეს ძმებმა ამჯათ და ბაზით ფარუგ ალვიმ. ვირუსის გავრცელება დაიწყო 1986 წელს, აღმოჩენა კი მოხდა 1987 წლის ზაფხულში. არსებული ინფორმაციით ვირუსმა მარტო აშშ-ის ტერიტორიაზე 18 ათასზე მეტი კომპიუტერი დაავირუსა. ვირუსის შექმნა ემსახურებოდა მიზანს, ადგილობრივი

პირატების დასჯას, რომლებიც ძმებისაგან იპარავდნენ მათ მიერ შექმნილ პროგრამულ უზრუნველყოფას. ვირუსი გამოირჩევა იმითაც, რომ ის იყო პირველი სტელს-ვირუსი, ანუ დაზიანებული სექტორის წაკითხვის მცდელობისას ვირუსი აპარებდა მის დაუზიანებელ ორიგინალს.

იერუსალიმის (Jerusalem) - ვირუსი შეიქმნა 1988 წელს ისრაელში. სწორედ აქედან წარმოიშვა მისი სახელწოდებაც. მას ასევე უწოდებენ "პარასკევი 13 რიცხვი", რაც ნიშნავს იმას, რომ ვირუსის აქტივაცია იწყებოდა სწორედ პარასკევს 13 რიცხვში და სრულად შლიდა მონაცემებს მყარი დისკიდან, მისი გავრცელება ხდებოდა დისკების მეშვეობით.

მორისის მატლი(ჭია) Morris worm (Worm) - ვირუსი აღმოჩენილ იქნა 1988 წლის ნოემბერში და დაიკავა პირველი ადგილი საშიშ ინტერნეტ-ვირუსების რეიტინგში. მწყობრიდან გამოიყვანა კომპიუტერები, მის მიერ მიყენებულმა ზარალმა შეადგინა 96 მილიონი დოლარი.

მიქელანჯელო Michelangelo («March6») - შეიძლება ითქვას, რომ ამ ვირუსის სიძლიერე შეფასებულ იქნა გადამეტებულად, თუმცა შეიძლება ითქვას, რომ ის იყო ერთ-ერთი დაუნდობელი ვირუსი, ვრცელდებოდა დისკეტების მეშვეობით, ხოლო აქტიურობას იწყებდა 6 მარტს, სწორედ ამ დღეს კი ის შლიდა ყველა მონაცემებს მყარი დისკიდან.

ჩერნობილი (CIH) - შეიქმნა ტაივანელი სტუდენტის მიერ 1998 წელს, ვირუსი კომპიუტერში ხვდებოდა ინტერნეტის, ელექტრონული ფოსტისა და დისკების მეშვეობით, იმალებოდა და გარკვეულ მომენტში იწყებდა აქტივიზაციას და იწყებდა მყარი დისკიდან მონაცემების წაშლას. რამდენიმე წლის შემდეგ 26 აპრილს ვირუსი კვლავ იღვიძებდა და აგრძელებდა თავის საქმიანობას.

მელისა Melissa - შეიქმნა 1999 წელს, ის პირველი ცნობილი საფოსტო მატლია, აზიანებდა ფაილებს და აგზავნიდა საკუთარ ასლებს. ვირუსი სწრაფად ვრცელდებოდა და ამიტომ მის მიერ მიყენებული ზარალი 100 მილიონ დოლარზე მეტად შეფასდა.

(«ბედნიერების წერილი») ILOVEYOU - შეიქმნა 2000 წელს, იგზავნებოდა უსაშველო რაოდენობით ამ სახელწოდებით და ეშმაკურად ატყუებდა ინტერნეტ

მომხმარებელს, გახსნისთანავე შლიდა კომპიუტერის მნიშვნელოვან ფაილებს, დააზიანა მსოფლიოში არსებული კომპიუტერების 10 %, რამაც გამოიწვია ზარალი 5.5 მილიარდი დოლარის ოდენობით.

ნიმდა - Nimda. 2001 წელი - მისი სახელწოდება წარმოიშვა «ადმინ» - ის შებრუნების შედეგად. კომპიუტერში შეღწევისთანავე ვირუსი თვითნებურად ეუფლებოდა ადმინისტრატორის უფლებებს, რის შემდეგაც ცვლიდა და ანგრევდა საიტების კონსტრუქციას, ახდენდა IP- მისამართებზე შეღწევის ბლოკირებას, შექმნიდან 22 წუთში ვირუსი უკვე იქცა ყველაზე გავრცელებულ ვირუსად.

მატლის (ჭია)(Worm) 2008 წელი - ერთ-ერთია ბოლო ვირუსებისგან, რომელიც გავრცელდა მთელ მსოფლიოში და მოიპოვა ძალზე საშიში კომპიუტერული მატლის (ჭია) იმიჯი. შეტევას ახორციელებს Mიცროსოფტ ჭინდოწს – ის ოჯახის ოპერატიულ სისტემებზე. ვირუსმა დააზიანა მსოფლიოში 12 მილიონზე მეტი კომპიუტერი, ის პოულობს სუსტ ადგილს ჭინდოწს –ში, რომელიც უკავშირდება ბუფერის გადამეტებულ შევსებას და მოტყუებითი ღPჩ-მოთხოვნის დახმარებით ადგენს კოდს, რომლის მეშვეობითაც თიშავს ჭინდოწს – ის განახლებებს და სერვისის სამსახურებს, ასევე ახდენს ანტივირუსების მწარმოებელი მსხვილი კომპანიების საიტებში შესვლის ბლოკირებას.

ბოტნეტი – Botnet - ბოტნეტი არის ბევრი ინფიცირებული კომპიუტერებისაგან შემდგარი ქსელი, რომელიც დისტანციურად იმართება კიბერ დამნაშავის მიერ კომპიუტერის მომხმარებლის დაუკითხავად, დაინფიცირებულ კომპიუტერს ქვია ბოტი ან ზომბი.

ბოტნეტი არის მძლავრი და სახიფათო იარაღი კიბერ დამნაშავის ხელში, რომლის საშუალებითაც შოულობს ფულს, ბოტნეტის მფლობელს შეუძლია მისი მართვა ნებისმიერი ადგილიდან, ინტერნეტის სტრუქტურა იძლევა მისი ანონიმურობის გარანტიას.

ბოტ კომპიუტერების მართვა შესაძლებელია პირდაპირი ან არაპირდაპირი გზით, პირდაპირი მართვის დროს დამანაშავეს შეუძლია დაამყაროს კავშირი ინფიცირებულ კომპიუტერთან და მართოს ის სპეციალური მავნე პროგრამის საშუალებით, ხოლო არაპირდაპირი მართვის შემთხვევაში ბოტ კომპიუტერი

თვითონ უკავშირდება მართვის ცენტრს ან სხვა ინფიცირებულ კომპიუტერებს, უგზავნის მოთხოვნას და შემდგომ ასრულებს მიღებულ ბრძანებას.

ნებისმიერ შემთხვევაში მომხმარებლისათვის შეუმჩნეველი ხდება, რომ მისი კომპიუტერი გამოიყენება კიბერ დამნაშავის მიერ, ამიტომ ბოტ კომპიუტერებს ხშირად ეძახიან ხოლმე ზომბირებულ კომპიუტერებს.

კიბერ დამნაშავეები ბოტნეტს იყენებენ მრავალი კრიმინალური საქმიანობისათვის, დაწყებული სპამის გაგზავნით და დამთავრებული სახელმწიფო ქსელებზე კიბერ შეტევით.

სპამის გაგზავნა არის ყველაზე გავრცელებული ფორმა, მრავალათასიანი ბოტნეტის მეშვეობით სპამერებს შეუძლიათ გააგზავნონ მილიონობით ელექტრონული წერილი მცირე დროის მონაკვეთში და ასევე ამ გზით გაავრცელონ ვირუსი, რომელიც შემდგომ გაზრდის ინფიცირებული კომპიუტერების რაოდენობას.

ძალიან ხშირად გამოიყენება კიბერ შანტაჟი, ბევრი კომპანია მუშაობს ინტერნეტის მეშვეობით, მათი ვებ გვერდების ან ელექტრონული სერვერის გათიშვა მათ აყენებს უდიდეს ზიანს, ხოლო ფირმა იმისთვის რომ დაიბრუნოს სტაბილურობა ფულს უხდის შანტაჟისტებს, ამ ტიპის შეტევის დროს ზომბირებული კომპიუტერიდან ერთდროულად იგზავნება ათასობით მოთხოვნა სამიზნე სერვერზე, შედეგად სერვერი ვერ ასწრებს ამდენი მოთხოვნის დამუშავებას, იტვირთება და ხდება ხელმიუწვდომელი.

ზომბირებული კომპიუტერის მეშვეობით დამნაშავეს შეუძლია განახორციელოს კიბერ დანაშაული, გატეხოს სხვისი ვებ გვერდი ან გადარიცხოს მოპარული ფულადი სახსრები და ამ დროს დარჩეს ანონიმური, რადგან ამ დროს ზომბი კომპიუტერი გამოიყენება, როგორც ე.წ პროქსი სერვერი დამნაშავის რეალური მისამართის დასამალად.

ხდება ასევე ბოტნეტის გაყიდვა ან გაქირავება, დამნაშავეები ყიდიან ხოლმე უკვე მზა ქსელებს, რომელიც მიეკუთვნება კიდევ ერთი კიბერ დანაშაულს.

კონფიდენციალური და პირადი ინფორმაციის მოპარვა არის ერთ-ერთი ყველაზე გავრცელებული, ბოტი, რომლითაც ინფიცირებულია კომპიუტერი

შეუძლია გადმოიწეროს მავნე პროგრამა მაგ. ტროიანი რომელიც პაროლებს იპარავს და შედეგად ყველა ზომბირებულ კომპიუტერზე ავტომატურად გავრცელდება ეს პროგრამა რისი მეშვეობითაც დამნაშავეებს შეეძლებათ მიიღონ სხვა ინფიცირებული კომპიუტერების მომხმარებელთა პაროლები.

კიბერ დამნაშავეებმა კარგად იციან, რომ ადრე თუ გვიან ვირუსს მაინც აღმოაჩენს ანტივირუსი და წაშლის მავნე ბოტ პროგრამებს და ამით ისინი დაკარგავენ ზომბირებულ კომპიუტერებს ბოტნეტ ქსელიდან, ამიტომ ისინი ხშირად ცვლიან პროგრამულ კოდებს, რათა უფრო რთულად აღმოსაჩენი გახდეს ვირუსი.

ხშირად შეუძლებელია ხოლმე ბოტნეტის მფლობელის პოვნა, კომპანიები რომლებიც მუშაობენ უსაფრთხოების საკითხებზე სხვადასხვა მეთოდებით პოულობენ ხოლმე ბოტნეტის ცენტრებს, ხურავენ მათ და აკვირდებიან, თუ რამდენი კომიუტერი იყო მიერთებული მასზე, მაგრამ რადგანაც დაინფიცირებული კომპიუტერების რაოდენობა ძალზედ დიდია და განლაგებულია სხვადასხვა ქვეყნებში შეუძლებელია მათი დახმარება, საქმეს ართულებს ისიც, რომ კიბერ დამნაშავეს შეუძლია შექმნას ახალი მართვის ცენტრები და დაიბრუნოს კონტროლი.

სპამი – SPAM - რამდენიმე წლის წინ ძალიან ცოტა ადამიანმა თუ იცოდა რა იყო სპამი, თუმცა დღეს უკვე ალბათ არ არსებობს არცერთი ელექტრონული ფოსტის მომხმარებელი რომელმაც არ იცის მისი მნიშვნელობა.

სპამი ეს არის ელექტრონული წერილის ტიპი, რომელიც მასობრივად და ანონიმურად იგზავნება მიმღების ელექტრონული ფოსტის მისამართზე, მის დაუკითხავად და სურვილის გარეშე, წერილები ძირითადად სარეკლამო ხასიათისაა და განკუთვნილია რაიმე მომსახურების ან საქონლის რეკლამირებისათვის.

პიროვნება, რომელიც აგზავნის ამ წერილებს არის სპამერი, სპამს ასევე იყენებენ ფიშინგური შეტევების განსახორციელებლად, მრავალ ქვეყანაში სპამირება ისჯება კანონით.

ყოველდღიურად მსოფლიოში იგზავნება მილიარდობით ელექტრონული წერილი, რომელთაგანაც 80%-ზე მეტი არის სპამი. სპამ-ბოტი არის სპეციალური პროგრამა, რომელიც აგროვებს ელ-ფოსტის მისამართებს ინტერნეტში, ავტომატურად ათვალიერებს სხვადასხვა ვებ გვერდებს, ფორუმებს და აგროვებს ელ-ფოსტის მისამართებს, ხოლო შემდეგ მიღებული ინფორმაცია ხვდება სპამერების წერილების მასობრივი დაგზავნის სიაში, რისი საშუალებითაც შემდეგ იგზავნება სპამი. ასევე შესაძლებელია ნებისმიერი მომხმარებლის კომპიუტერიდან მოხდეს სპამის გაგზავნა ათასობით კომპიუტერზე, მომხმარებლისათვის სპამ ბოტის არსებობა არის ძალზედ სახიფათო, რადგან კომპიუტერის IP მისამართიდან გაგზავნილი სპამი ადრე თუ გვიან მოხვდება რომელიმე შავ სიაში, რის შემდგომ მას შეექმნება პრობლემები გააგზავნოს ჩვეულებრივი წერილები, რადგან ამ შემთხვევაში მიმღების სერვერი ავტომატურად ბლოკავს მისგან მოსულ ნებისმიერ წერილს.

არსებობს სპამთან საბრძოლველად მრავალი გზა, Yაჰოო, Gმაილ, Hოტმაილ, Mაილ.რუ უყენიათ ანტი-სპამ სისტემები, რომლებიც ბლოკავენ ან ამისამართებენ სპამს სხვა ყუთში. თუმცა სპამისგან 100% - ით დაცვა არ არსებობს რადგანაც სპამერები მუდმივად ცვლიან მეთოდებს.

სპამისგან დასაცავად არ უნდა ვუპასუხოთ სპამ წერილებს, არ უნდა გაიხსნას სპამ წერილში მითითებული არც ერთი ლინკი, რადგან მასზე დაჭერით შეიძლება გადავიდეთ სახიფათო ვებ-გვერდზე. ელექტრონული მისამართის გამოქვეყნება უნდა მოხდეს ”@”, ელექტრონული ნიშნის მითითების გარეშე და ასევე გამოყენებული უნდა იქნეს გამოტოვებები.

ფიშინგი (ინგლ. თევზაობა) – დანაშაულებრივი ფორმა, რომლის მიზანია მომხმარებელს გამოსძალოს პირადი ინფორმაცია, საიდენტიფიკაციო მონაცემები, პაროლი, საკრედიტო ბარათის ან საბანკო ანგარიშის ნომერი და სხვა კონფიდენციალური ინფორმაცია.

ფიშინგ წერილი არის ელ. მისამართზე გამოგზავნილი ყალბი წერილი, რომელიც თითქოსდა გამოგზავნილია ბანკიდან, ორგანიზაციიდან, რომელთანაც მომხმარებელს აქვს შეხება, წერილში ითხოვენ ხოლმე პირადი მონაცემების

განახლებას მოცემულ ვებ-გვერზე. ფიშინგ წერილები არის მაღალი ხარისხით გაყალბებული, წერილი არის ბანკის ან სერვის პროვაიდერის ლოგოთი, რომელიც არის ზუსტი ასლი, ინფორმაციის შეგროვების შემდეგ ხდება მომხმარებლის გადამისამართება რეალურ ვებ-გვერდზე. მომხმარებლის პირადი მონაცემები კი უკვე ხელმისაწვდომი ხდება თაღლითებისათვის, რომლებთაც აქვთ შემუშავებული გეგმა თუ როგორ მოიპარონ ფული სხვისი ანგარიშიდან.

ფიშინგთან საბრძოლველად რამდენიმე წლის წინ შეიქმნა ანტი-ფიშინგის სამუშაო ჯგუფი, (Anti-Phishing Working Group - APWG), სადაც გაერთიანებულები არიან ფიშინგის სამიზნე კომპანიები, ასევე უსაფრთხოების პროგრამული უზრუნველყოფის მწარმოებლები და კიბერ დანაშაულთან მებრძოლი კომპანიები, 2500 კომპანიაზე მეტი. რომლებიც ერთმანეთს ატყობინებენ ახალი ფიშერული შეტევების შესახებ და აწვდიან საზოგადოებას არსებულ ინფორმაციებს.

რამდენიმე თვის წინ გახდა ცნობილი, რომ მსოფლიოს ახალი კომპიუტერული ვირუსი ემუქრება, სახელწოდება - DUQU, დანიშნულება - ინფორმაციის შეგროვება, აღმოჩენილია რამდენიმე მსხვილი ევროპული კომპანიისა და ორგანიზაციის სისტემაში, წყარო - უცნობია.

XXI საუკუნეში, ომის კიდევ ერთი იარაღი, DUQU აღმოაჩინეს შყმანტეც ანტივურუსული სისტემების მწარმოებელმა კომპანიის სპეციალისტებმა.

დევიდ ჯონსი (ექსპერტი)– "ეს ძალიან საშიში ვირუსია, ეს რომელიმე მოყვარული ჰაკერის შექმნილი არ არის, შექმნისას გამოყენებულია ბოლო ტექნოლოგიური მიღწევები, რაც იმას ნიშნავს, რომ ავტორებმა ის სრულად კონკრეტული მიზნებისთვის დაამზადეს".

ახალი ვირუსი თითქმის იდენტურია ცნობილი სტაქსნეტ-ის, რომელმაც კინაღამ ირანის ბირთვული პროგრამა ჩაშალა, რაც სპეციალისტების აზრით მათ საერთო წყაროზე მიუთითებს, თუმცა ფუნქცია განსხვავებულია. დიუქიუს მთავარი დანიშნულება არა დივერსია, არამედ საჭირო ინფორმაციის შეგროვებაა.

ახალი ვირუსი უკვე აღმოჩენილ იქნა, ევროპის ქვეყნების რამოდენიმე ცნობილ კომპანიისა და ორგანიზაციის კომპიუტერულ სისტემაში. STUXNET,

უილიამ ლინი - “ეს არის ვირუსები, რომლებმაც საფრთხე ციფრული სამყაროდან რეალურში გადაიტანა, ერთმა უკვე შეაფერხა ატომური ელექტრო სადგურის მუშაობა, მეორე კი სავარაუდოდ იგივეს დიდ ინდუსტრიულ კომპანიაში გააკეთებს. ეს სრულიად ახალი საფეხურია თანამედროვე კიბერ ომში”

საფრთხეების ზრდის შესახებ უკვე ინფორმირებულია პენტაგონი, ცოტა ხნის წინ ამ დრომდე დაუდგენელმა კომპიუტერულმა ვირუსმა იმ სისტემას შეუტია, საიდანაც ამერიკული სამხედრო თვითმფრინავები იმართება. უწყებამ განაცხადა, რომ ამერიკა ახალ კიბერ 11 სექტემბრის მოლოდინშია.

XXI საუკუნეში ჰიტები და ბაიტები შესაძლოა უკვე უფრო საშიში აღმოჩნდეს ვიდრე ტყვიები და ბომბები, კიბერთავდასხმები მომავლის ნებისმიერი კონფლიქტის მნიშვნელოვანი კომპონენტი გახდება. იქნება ეს სახელმწიფოთაშორის კონფლიქტი თუ ტერორისტული თავდასხმა”

ტექნოლოგიის განვითარებასთან ერთად ტერორისტების მიერ ინტერნეტის გამოყენებაც უფრო მეტად გავრცელდა. ტერორისტების საინტერნეტო კომუნიკაცია ხშირად შეიცავს მათ ოპერატიულ გეგმებს და მეთოდებს, რომელთა გაშიფვრის შემთხვევაშიც შესაძლოა ანტიტერორისტული ბრძოლის მეთოდების შემუშავება, მათი ვიანაობის დადგენა და ფონდების გადარიცხვების შესახებ ინფორმაციის მოპოვება.

ჩვენი მიზანი იყო წარმოგვეჩინა ტერორისტული საქმიანობის საფუძვლები და სახეები, მათ შორის ისეთის, როგორიც არის ინტერნეტტერორი და ინტერნეტში არსებული ტერორისტული რიტორიკა, ის წინაპირობები, რომლებიც იწვევს მათ წარმოშობას და განაპირობებს მათ მომავალ საქმიანობას. შესწავლილ უნდა იქნეს ტერორიზმის წინააღმდეგ ბრძოლის გზები, რომელიც ხელის შემწყობი ფაქტორი გახდება აღნიშნულ დანაშაულთან ეფექტური ბრძოლის საქმეში. მიზანი უნდა იყოს იმ საფუძვლების კვლევა ძიება, რაც იწვევს ტერორისტული აქტივობის ზრდას.

სპეციალიზაციის რომელი სფეროც არ უნდა იყოს, ანტიტერორიზმის ანალიტიკოსები საჭიროებენ მაღალი დონის მომზადებას. როგორც უკვე არაერთმა მკვლევარმა აღნიშნა, არაბულის ცოდნა არ არის საკმარისი და არც მარტო

არაბულად მოლაპარაკეები გვჭირდებაა. საჭიროა, კარგად ვერკვეოდეთ იქაურ კულტურასა და ტრადიციებში. პრიორიტეტული უნდა გახდეს ინფორმაციის მონიტორინგისა და მისი მოპოვებისათვის მომზადება. თუ გავითვალისწინებთ იმას, რამდენად დამოკიდებულნი არიან ისლამისტი რადიკალები მსოფლიო ინტერნეტ ქსელებზე, დასავლეთის მთავრობებმა უნდა გამონახონ გზები ტექნიკური და ლინგვისტური ექსპერტიზის ასამაღლებლად, რათა უფრო ეფექტურად მოხდეს მათ რესურსებში შეღწევა. ექსპერტიზის საჭირო დონის მისაღწევად საჭიროა წლები, რათა მათ ეფექტურად გაშიფრონ კოდები, რომლებიც ხშირად გამოიყენება ჩეთებში. ამ ექსპერტებს ასევე ესაჭიროებათ ტექნოლოგიის ძალიან მაღალ დონეზე ფლობა, რათა მათ მოიპოვონ კოდირებულ ფაილებში არსებული ინფორმაცია. აქედან გამომდინარე, ეს პროგრამა უნდა იყოს შეფასებული, როგორც გრძელვადიანი ინვესტიცია. ამასთანავე, საჭიროა, აქტიური ძალისხმევა სათარგმნი ტექნოლოგიის უფრო სწრაფად განვითარებისთვის. ტერორიზმთან მებრძოლ ქვეყნებს შორის კი უნდა გაიზარდოს ინფორმაციის გაცვლა ამ სფეროში.

1.4 კიბერუსაფრთხოება და ბავშვები

ტექნოლოგიების განვითარებამ ხელი შეუწყო ცხოვრების ტემპის აჩქარებასა და გამარტივებას. ტექნოლოგიებს დღეს ნებისმიერ ადგილას შევხვდებით. მის გარეშე ცხოვრებაც კი წარმოუდგენლად გვეჩვენება. ერთერთი ყველაზე ფართოდ გამოყენებადი ტექნიკა კომპიუტერია, რომელშიც გლობალური ქსელი ინტერნეტი თავსდება. ინტერნეტი არის ყველაზე სწრაფი ინფორმაციის წყარო, ის აგრეთვე სოციალიზაციას უწყობს ხელს და კომუნიკაციისა და გართობის ერთერთი ფორმაცაა.

ინტერნეტი ყველასათვის ხელმისაწვდომია. ჩვეულებრივ ადამიანებს ინტერნეტის მხოლოდ 4%- თან მიუწვდებათ ხელი, ხოლო დანარჩენი 96% „ღრმა ქსელს“ და „ბნელ ქსელს“ წარმოადგენს. ინტერნეტს ხშირად აისბერგსაც ადარებენ. ინტერნეტის 100 %- ის ფლობა მხოლოდ გარკვეული ბრაუზერების საშუალებითაა შესაძლებელი, რომელსაც ნებისმიერი ადამიანი გადმოწერს. სწორედ ინტერნეტის საინტერესო და იდუმალი მხარეების გამოხშირია ბავშვებზე არასასურველი შინაარსის გავრცელება, როგორებიცაა: ძალადობა, პორნოგრაფია, სახიფათო თამაშები.

ინტერნეტში ხშირია ბავშვებზე გავრცელებული კიბერ ჩაგვრაც, ეს არის ძალადობის ფორმა, რომელიც ხორციელდება სოციალური ქსელების საშუალებით. ძირითდად „მესიჯებით“, რომლებიც ხშირად მუქარის შემცველია მაგალითად „ლურჯი ვეშაპი“ .

ბავშვებზე ხშირად ხორციელდება ჰაკერის თავდასხმა სუსტი IP მისამართის გამო. ჰაკერებს ინტერნეტ მომხმარებლებსაც უწოდებენ , ისინი იპარავენ სუსტი მისამართებიდან პირად ინფორმაციას და მას ძირითადად ფინანსების მოპოვების მიზნით იყენებენ.

ხშირია კითხვები იმასთან დაკავშირებით თუ როგორ უნდა მივხვდეთ ბავშვს რა ქსელებთან აქვს კავშირი? ამის გარკვევა მარტივია ბავშვი მშობლის შემოსვლისთანავე თუ ხურავს პროგრამებს, თიშავს კომპიტერს და ცდილობს მშობელს უბიძგოს ოთახის დატოვებისკენ, მშობელს მოეთხოვება შეუმოწმოს შვილს ბრაუზერის ისტორია ან ათქმევინოს რომელ ქსელში იყო შესული. მშობელმა არ უნდა აუკრძალოს ბავშვს ინტერნეტის მოხმარება. მთავარიაესაუბროს ინტერნეტის უსაფრთხოებაზე, აუხსნას უსაფრთხოების წესები (Net Nanny), და დაადგინონ ინტერნეტის მოხმარების დრო.

აუცილებელია მშობელსა და ბავშვებს ჰქონდეთ ყოველდღიური კომუნიკაცია რადგან საფრთხე მუდამარსებობს, ყოველწამს შეიძლება გამოსტყუონ პატარებს ინფორმაცია აუცილებლად უნდა ავუხსნათ ბავშვებს მოსალოდნელი საფრთხეები და არსებობის შემთხვევაში მოგმართონ მშობლებს.

უსაფრთხოების თემაზე საუბარი ბავშვებთან ისეთივე მარტივია, როგორც მოზრდილ ადამიანებთან, რადგანაც ბავშვებს, ისევე როგორც ზრდასრულებს არ სურთ აღმოჩნდნენ მოტყუებულ მდგომარეობაში. უბრალოდ უნდა ავუხსნათ მათ, რომ არსებობენ ადამიანები, რომლებიც ცდილობენ სარგებლის მიღებას სხვების მოტყუების, მათი კუთვნილი ინფორმაციის ან ფულის მითვისების გზით. საჭიროა განვუმარტოთ ბავშვებს, რომ ყველაფერი ისე არ არის, როგორც ერთი შეხედვით ჩანს - ამიტომ, მნიშვნელოვანია დაფიქრება ყოველი ონლაინ- ქმედების განხორციელებამდე. არ მივცეთ ზემოხსენებულ საუბარს ერთჯერადი სახე, არამედ დავუბრუნდეთ მას დროდადრო, ვკითხოთ ბავშვს რაიმე საეჭვო ხომ არ შეუნიშნავს ბოლო პერიოდში. თქვენმა შვილებმა შესაძლოა იმაზე გაცილებით მეტი იცოდნენ კიბერუსაფრთხოების შესახებ, ვიდრე თქვენ ფიქრობთ.

არსებობს უსაფრთხოებასთან დაკავშირებული საფრთხეები, რომლებიც კონკრეტულად ბავშვებსა და თინეიჯერებზეა გათვლილი, თუმცა საფრთხეების უმეტესი ნაწილი გათვლილია პოტენციურ მსხვერპლზე, ასაკის გათვალისწინების გარეშე. ხანდახან ჰაკერები იყენებენ

მიმზიდველ ვებ-გვერდებს ბავშვებში ინტერესის გამოწვევის მიზნით, მაგალითად „ფან- კლუბებს“, YouTube-ს, Instagram-ს და ა.შ; და გამომდინარე იქიდან, რომ მოზრდილი ადამიანებისთვისაც კი რთული განსასხვავებელია ოფიციალური და ყალბი ვებ-გვერდები, ბავშვები, რომელთაც ჯერ არ აქვთ ჩამოყალიბებული კრიტიკული აზროვნების უნარ-ჩვევები რათქმაუნდა გაცილებით ძნელი იქნება განსხვავების აღმოჩენა.

საფრთხის შემცველი ბმულები დიდი ალბათობით შესაძლოა განთავსებული იყოს ისეთ პოპულარულ ვიდეო-პორტალებზე, როგორიცაა მაგალითად YouTube. აუხსენით თქვენს შვილს, რომ თუ შენიშნავს ბმულს, რომელიც არასათანადო ან შეუსაბამო შინაარსის მასალას შეიცავს, გაცნობოთ ამის შესახებ. თუ ისინი წააწყდნენ ყალბ ვებ- გვერდს, სავარაუდოდ მოახდინეს მისი იგნორირება, რადგანაც მსგავსი ვებ-გვერდები საკმაოდ ჭკვიანურადაა შეფუთული კიბერკრიმინალების მიერ. მოზარდებმა კარგად უნდა გაითავისონ, რომ გაცნობის, ახალი მეგობრების შეძენისთვის განკუთვნილი და საჭორაო საიტები ხშირადარცთუ ისე უსაფრთხოა.

გამომდინარე იქიდან, რომ ბავშვებს არ გააჩნიათ საკუთარი საკრედიტო ბარათები, თქვენ შესაძლოა იფიქროთ, რომ ისინი დაცულნი არიან ფინანსური დანაშაულებების მსხვერპლის სტატუსისგან, მაგრამ თუკი ბავშვები და მშობლები საერთო კომპიუტერს იყენებენ, მათი ონლაინ-აქტივობები მათ შორის ონლაინ- შოპინგი, მშობლების მიერ სახლის კომპიუტერით განხორციელებული საბანკო თუ სამსახურთან დაკავშირებული საქმიანობა ცალსახად ახდენს გავლენას სხვებზე; და მშობლებმა აუცილებლად უნდა იცოდნენ, თუკი შვილებმა შეამოწმეს ბრაუზერის ისტორია, ისინი შეძლებენ იგივე ვებ-გვერდებზე შესვლას, რომლებიც მათი მშობლების მიერ იქნა გამოყენებული სახლის კომპიუტერის მეშვეობით.

მოზარდების მსგავსად და ხშირად უფრო მეტადაც კი, ბავშვებს და თინეიჯერებს შეუძლიათ გულშემატკივრობა -"გულშემატკივართა საიტები" და ჩატით საუბარი საყვარელ ცნობილ ადამიანებთან ან ადამიანებზე. არსებობს უამრავი ვარსკვლავის საიტი, რომლებსაც მართავს თვითონ ცნობილიადამიანი ან გასართობი ამბების

გამომცემელი ორგანიზაცია. თუმცა აუცილებელია ზედმეტი სიფრთხილის გამოჩენა ისეთ საიტებზე შესვლისას, რომლებიც შესაძლოა მოხვდნენ ძიების შედეგებში, თუმცა რეალურად არ მიეკუთვნებოდნენ ვარსკვლავებს. ასეთი ვებ-გვერდები როგორც წესი ძიების შედეგების ქვედა ზღვარზე ხვდებიან.

არსებობს სოციალური მიზეზი, რის გამოც ბავშვებზე ხდება ჰაკერული შეტევა. ერთ-ერთი ფორმაა ბავშვის პაროლის გამოყენებით მის სოციალურ ანგარიშზე შესვლა და უხერხული შინაარსის შეტყობინებებისა თუ გამოსახულებების გაზიარება, სპამის გავრცელება ან ისეთი ბმულების დაპოსტვა, რომლებიც შესაძლოა შეიცავდეს მავნე კოდს. ასწავლეთ შვილებს არ გაუზიარონ პაროლები თუნდაც უახლოეს მეგობრებს და ყოველთვის დახურონ ანგარიშები, როდესაც ისინი გამოიყენებენ საჯარო გამოყენების კომპიუტერს, როგორიცაა სკოლაში და საჯარო ბიბლიოთეკებში განთავსებული კომპიუტერები.

ბრაუზერი „იმახსოვრებს“ პაროლებს, თუ არ იყენებთ ბრაუზერის რეჟიმს „პირადი“ ან „ინკოგნიტო“, ან არ შლით ისტორიას მისი გამოყენების შემდეგ.

ზოგჯერ სამიზნე ხდება ბავშვის პირადობის მოწმობა - სადაც მითითებულია დეტალური ინფორმაცია მათ შესახებ (მაგალითად, სახელი, მისამართი და სოციალური დაცვის ნომერი), რათა მიიღონ კრედიტი ან ჩაიდინონ დანაშაული ბავშვის სახელით. ბავშვები არიან კარგი სამიზნე იმიტომ, რომ აქვთ ყველაზე სრულყოფილი საკრედიტო (მათ არასდროს ჰქონიათ ნასესხები ფული, შესაბამისად არასდროს დაუგვიანიათ გადახდა) ისტორია და ამ ფაქტის გამოვლენაც იქნება შეუძლებელი მანამ, სანამ მოზრდილ ასაკში თვითონ არ მიმართავენ ბანკს სტუდენტური სესხის ან საკრედიტო ბარათის ასაღებად.

ბავშვებსა და მოზარდებს უყვართ ყველა ფუნქცია, რასაც მათ სმარტფონი და ტაბლეტი სთავაზობთ, დაწყებული თამაშებით და დასრულებული ფოტოს გაზიარებით. არსებობს ასობით ათასი აპლიკაცია სმარტფონებისა და ტაბლეტებისთვის, თუმცა ყველა მათგანი არ მიეკუთვნება სანდო რეპუტაციის მქონე მომწოდებელს. სანამ ბავშვებს მისცემთ აპლიკაციის ჩამოტვირთვის უფლებას, დარწმუნდით, რომ მათ (და თქვენც) იციან, რისთვის არის განკუთვნილი აპლიკაცია, რა ინფორმაციას აგროვებს და რაში იყენებს ამ

მონაცემებს.აპლიკაციებისთვის იშვიათობას არ წარმოადგენს მომხმარებლის ადგილმდებარეობის იდენტიფიკაცია და ისეთი დეტალების დადგენაც კი, როგორიცაა ასაკი და სქესი.

თითქმის ყველა ტელეფონის დაბლოკვა შეიძლება მარტივი რიცხვითი კოდით, პაროლით ან ანაბეჭდით, რომელთა გარეშეც საგანგებო სამსახურების გარდა ვერავისთან დაკავშირებას ვერ შეძლებთ. ამ მეთოდით შეძლებთ თქვენს ტელეფონში შენახული ინფორმაციის დაცვას არასანქცირებული ზარებისგან და მოახდენთ ცუდი ზრახვების მქონე ადამიანების მიერ თქვენი ტელეფონის გამოყენებით უხერხული შეტყობინებების ან კომენტარების გაკეთების პრევენციას.

სმარტფონებს გააჩნიათ კონფიდენციალურობის და უსაფრთხოების პარამეტრები, რომელთა მეშვებითაც კონტროლდება კონკრეტულ ინფორმაციასთან ხელმისაწვდომობა, მაგალითად: რომელი აპლიკაციის მეშვეობით ხდება თქვენი კონტაქტების, კალენდარისა და ადგილმდებარეობის მართვა. ყურადღებით დააკვირდით პარამეტრებს და შეცვალეთ ისინი საჭიროების შემთხვევაში.

მიუხედავად იმისა, რომ არსებობს ბევრი უფასო ლეგიტიმური პროგრამა, რომელიც კანონიერად აკისრებს მომხმარებელს გადასახადს განახლებისთვის, თამაშების მომდევნო დონეზე გადასვლისთვის, თამაშების გმირებისთვის დამატებითი უნარების შეძენისთვის, ასევე არსებობს არალეგიტიმური აპლიკაციები, რომლებიც ცდილობენ მომხმარებლის შეცდომაში შეყვანას და მათთვის გარკვეული სერვისების მიყიდვას. ლეგიტიმური აპლიკაციის შემთხვევაშიც კი ბავშვმა უნდა იცოდეს, როდის შეიძლება ან როდის არ არის მიზანშეწონილი აპლიკაციის ან მის მიერ შემოთავაზებული სერვისების შესყიდვა. ნებისმიერი აპლიკაციის ჩამოტვირთვა შეთანხმებული უნდა იყოს მშობელთან.

ხშირია შემთხვევები, როდესაც კრიმინალები ავრცელებენ აპლიკაციებს მომხმარებლისგან პირადი ინფორმაციის არასანქცირებულად მითვისების მიზნით. არსებობს ასევე ლეგიტიმური აპლიკაციის ჰაკერების მიერ ხელში ჩაგდების რისკიც. გამოსავალი არის ჩამოტვირთოთ აპლიკაციები მხოლოდ ავტორიტეტული “app store”-დან - სასურველია გაეცნოთ რეიტინგებსა და

შეფასებებს. ყველაზე მეტ ინფორმაციას ბავშვები მეგობრებისგან იღებენ და აუცილებელია შევახსენოთ მათ, რომ გარდა მეგობრებისა, საჭიროა აპლიკაციის რეიტინგსა და ჩამოტვირთვის რაოდენობაზე ყურადღების გამახვილება. თუ შეგექმნათ ეჭვის საფუძველი და აპლიკაცია უკვე გადმოწერილი გაქვთ, წაშალეთ დაუყოვნებლივ.

ეს მნიშვნელოვანია მობილური მოწყობილობის ყველა მომხმარებლისათვის. "Pew Internet Research"-ის ბოლო კვლევაზე დაყრდნობით თინეიჯერების 46%-ს (გოგონების 59%-ს) გამორთული აქვს ადგილმდებარეობის განმსაზღვრელი ფუნქცია. ზოგიერთი სერვისი, მაგალითად სანავიგაციო სისტემები და პროგრამები ეხმარება მშობლებს შვილების ადგილმდებარეობის კონტროლში მათი

უსაფრთხოების მიზნით, თუმცა ყველა აპლიკაცია ამ ფუნქციის გააქტიურებას არ საჭიროებს (ზოგიერთი მას საკუთარი მარკეტინგული მიზნებისათვის იყენებს). შეგიძლიათ გამორთოთ „geolocation" ფუნქცია ტელეფონში, მაგრამ ხშირად უფრო მართებულია მისი გათიშვა მხოლოდ კონკრეტული აპლიკაციებისათვის. ასე რომ გადახედეთ ბავშვის მიერ ხშირად გამოყენებადი აპლიკაციების პარამეტრებს და თუ რომელიმე მათგანს ჩართული აქვს ადგილმდებარეობის დადგენის ფუნქცია, რაც თქვენთვის მიუღებელია, გამორთეთ ფუნქცია ან წაშალეთ აპლიკაცია.

ტექნოლოგია და მასთან დაკავშირებული რისკები მზარდი და განვითარებადია, როდესაც ახალი და მასშტაბური ტექნოლოგია შემოდის, მილიონობით ადამიანი აპირებს მის გამოყენებას, მათგან მცირე რაოდენობის ხალხი - ბოროტი მიზნებით. მსგავსი ინტერესების მქონე ადამიანები მაქსიმალურად შეეცდებიან მათ ხელთ არსებული როგორც სოციალური, ისე

ტექნიკური ბერკეტების გამოყენებას მიზნის მისაღწევად. როგორც უსაფრთხოების ექსპერტები ცდილობენ განავითარონ საკუთარი უნარ-ჩვევები და შესაძლებლობები, იგივე წარმატებით ვითარდებიან კიბერკრიმინალებიც. ეს ყოველთვის იქნება „კატა-თაგვობანა"-ს ტიპის თამაში და უსაფრთხოებასთან დაკავშირებულ საფრთხეებსაც სავარაუდოდ კიდევ დიდხანს ვერ გავექცევით.

გარდა თქვენს მიერ გამოყენებული ტექნოლოგიური საშუალებებისა, გაცილებით სანდო დაცვაა კრიტიკული აზროვნება- აღქმა მაგალითად იმისა, რომ რამდენიმე წამიანი შეჩერება ბმულზე დაკლიკების, აპლიკაციის ჩამოტვირთვის, პაროლის ან პირადი ინფორმაციის შეყვანის შედეგების შესაფასებლად მნიშვნელოვანია. თუ ვინმე თქვენი ოჯახის წევრებს შორის უშვებს შეცდომას, შეეცადეთ არ მოახდინოთ მწვავე რეაგირება. მშვიდად შეაფასეთ, თუ რა იყო არასწორი და შეეცადეთ დახმარებას, თავი აარიდეთ „ბრალის წაყენებას“. გაითვალისწინეთ, რომ არსებობს უამრავი დიდი კომპანია და სამთავრობო უწყება, რომლებიც გახდნენ ჰაკერული თავდასხმის მსხვერპლი.

რისკების არსებობა არ ნიშნავს იმას, რომ აღარ უნდა გამოიყენოთ ტექნოლოგიური საშუალებები ან აუკრძალოთ ბავშვს მათთან მიახლოება. თუმცა აუცილებლობას წარმოადგენს

რისკების შემცირებაზე ზრუნვა და დაშვებული შეცდომების საკუთარი ძალებითგამოსწორების უნარების გამომუშავება.როგორც სხვა დანარჩენ საკითხებთან მიმართებაში, ჩვენ ტექნოლოგიასთან დაკავშირებული შესაძლო რისკების მინიმუმამდე დაყვანაც შეგვიძლია საღი აზროვნების მეშვეობით და გაფრთხილებებისთვის ყურადღების მიქცევით. უსაფრთხოებასთან დაკავშირებული რისკები დიდი პრობლემაა, თუმცა თანამედროვე ტექნოლოგიებით მიღებულ სარგებელს ცხოვრების შეცვლა შეუძლია. (კიბერუსაფრთხოებასთან დაკავშირებული სახელმძღვანელო მშობლებისათვის)[6]

[6] კიბერუსაფრთხოებასთანდაკავშირებულისახელმძღვანელომშობლებისათვის
http://csbd.gov.ge/news.php?year=2016&news_number=14&news_type=tips&lang=ge

თავი 2. მსოფლიო კონვენცია კიბერტერორიზმის წინააღმდეგ

2.1 ევროკავშირიდა ნატო კიბერტერორიზმის წინააღმდეგ

2002 წელს პრაღის სამიტზე ნატოს წევრ სახელმწიფოთა ლიდერებმა კიბერტერორიზმი მნიშვნელოვან საფრთხედ აღიარეს,ლრ „ნატოს კიბერთავდაცვის პროგრამა“, რომელიც მოიცავდა მოქმედებათა პროგრამის სამ ფაზას. პირველი ფაზისას შეიქმნა „ნატოს კომპიუტერული ინციდენტის საპასუხოუნარიანობა“ (NCIRC), რომელიც მეორე ფაზისას სრულ სამუშაო რეჟიმში შევიდა. მესამე ფაზა მოიცავს პირველი ორი ფაზისგან მიღებული გამოცდილების პრაქტიკაში დანერგვას და კიბერტერორიზმთან ბრძოლაში თანამედროვე თავდაცვითი საშუალებების გამოყენებას.

აღსანიშნავია, რომ 2007 წლის 14 ივნისს, რაც ესტონეთზე მასიური კიბერშეტევა განხორციელდა, ნატოს წევრ სახელმწიფოთა თავდაცვის მინისტრები შეთანხმდნენ, რომ კიბერტერორიზმის წინააღმდეგ აქტიური ბრძოლა იყო საჭირო. სწორედ ამიტომ ნატომ კიბერთავდაცვის ცენტრი შექმნა ესტონეთში.

“კიბერთავდასხმებისგან დაცვის კუთხით ნატო და ევროკავშირი ერთად უფრო ძლიერი იქნებიან. თანამშრომლობის გააქტიურება ამ შეთანხმების ფარგლებში, საშუალებას მოგვცემს უკეთესად მოვახდინოთ კიბერთავდასხმების პრევენცია, ასევე გავაუმჯობესოთ ჩვენი შესაძლებლობა, მოვახდინოთ მათი პროგნოზირება, აღმოჩენა და რეაგირება”, – განაცხადა ნატო-ს გენერალური მდივნის თანაშემწემ სორინ დუკარუმ.

როგორც ნატო-ს ვებგვერდზეა აღნიშნული, ბრიუსელში გაფორმებული შეთანხმება საერთო უსაფრთხოების უზრუნველყოფის კუთხით, ნატო-ევროკავშირის ერთობლივი თანამშრომლობის "კონკრეტული მაგალითია".

პირველად ამერიკის შეერთებულმა შტატებმა შეიმუშავა სტრატეგია 2000 წელს კიბერუსაფრთხოების კუთხით.კიბერუსაფრთხოების საფრთხის ზიანის თავიდან ასაცილებლად,ევროპაც მალე დარწმუნდა თუ რამხელა მასშტაბის ზიანის მოტანა შეეძლო კიბერტერორიზმს მსოფლიოსთვის და დაიწყეს კოლექტიური მუშაობა,მოსალოდნელი საფრთხის წინააღმდეგ,2007 წლიდან ევროპამ უფრო აქტიურად დაიწყო ზრუნვა კიბერსივრცის გაძლიერებაზე,რადგან მიხვდნენ თუ რამდენად უსუსურები იყვნენ მის წინააღმდეგ, როდესაც რუსეთი თავსდაესხა ესტონეთს,კიბერსივრცის დაცვაზე ესტონეთმა სამართლებრივი რეგულაციების გატარება დაიწყო,ევროკავშირი თუ ნატოს წევრი სახელმწიფოები თანხმდებიან იმაზე, რომ ერთად უფრო ნაყოფიერად იბრძოლებენ კიბერტერორიზმის წინააღმდეგ ვიდრე ცალცალკე საერთო ხედვა ყველა ქვეყნისა განსხვავდება, მაგრამ რიგ საკითხებში მათი პრინციპები ერთმანეთს ემთხვევა.ევროკავშირის წევრებმა წარმოადგინეს სახელმწიფო სტრატეგია კიბერტერორიზმის წინააღმდეგ.

ესტონეთიარის ქვეყანა, რომელმაც მძიმე დარტყმა მიიღო რუსეთისაგან, დაიწყო ინფორმაციული სისტემების უსაფრთხოებაზე ზრუნვა, ესტონეთი კიბერუსაფრთხოების დაცვაზე დიდ დროს და რესურსს ხარჯავს და რეგიონში ერთ ერთი მოწინავე პოზიცია უკავია.

ფინეთი არის ქვეყანა რომელმაც 2008 წელს მიიღო კიბერუსაფრთხოების სტრატეგია მისი ძირითადი აზრი არის ეკონომიკის პრობლემა,რაც გულისხმობს შემდეგს საზოგადოების ცნობიერების ამაღლებას ინფორმაციული თვალსაზრისით.

სლოვაკეთი დიდ მნიშვნელობას ანიჭებს საკუთარი უსაფრთხოების დაცვას, მან სტრატეგია შეიმუშავა 2008 წელს, მთავარ საკითხს წარმოადგენს ინფორმაციის

დაცვა,სლოვაკეთი ყოველთვის ცდილობს რომ საფრთხე გააუვნებელყოს,მუდმივად ავითარებს მას.

გერმანია ქვეყანა, რომელმაც სტრატეგია 2011 წელს შეიმუშავა მას საფუძვლად დაუდეს კრიტიკული ინფორმაციის დაცვა,ორიენტირებული არიან კიბერშეტევის დროულ გამოვლენაზე,ასევე სტრატეგიაში მკაფიოდ არის განსაზღვრული ბიზნესის დაცვა.

საფრანგეთი კიბერუსაფრთხოების სტრატეგია, რომელიც საფრანგეთმა2011 წელს შეიმუშავა აგებულია სისტემის შესაძლებლობებზე ინფორმაციული თვალსაზრისით. ის წინუნდა აღუდგეს კიბერსივრცეში არსებულ დარღვევებს,ის ორიენტირებულია ინფორმაციულობის კონფიდენციალობაზე, საფრანგეთს შესწევს უნარი ყოველდღიურად დახვეწოს ის.

ლიეტუა ქვეყანამ გეზი აიღო ელექტრონული ინფორმაციის განვითარებაზე სტრატეგიამ უნდა უზრუნველყოს პერსონალური მონაცემების დაცვა, 2011 წელს განსაზღვრეს ქვეყნის ხედვა კიბერტერორიზმის წინააღმდეგ,

ლუქსემბურგი სტრატეგიაში ნათლად არის განსაზღვრული საკომუნიკაციო ტექნოლოგიების მნიშვნელობა, ქვეყანა სრულად აცნობიერებს საფრთხეს რომელიც შესაძლოა მას დაემუქროს სწორედ ამიტომ შეიმუშავეს 2011 წელს სტრატეგია.

ჩეხეთის რესპუბლიკა ძირითადად ზრუნავს მოსალოდნელი საფრთხეების თავიდანარიდებას,კონფედენციალობის დაცვაზე,ყველაფერს აკეტებს სახელმწიფო რომ მოსალოდნელ საფრთხეს მზათყოფნაში შეხვდეს სტრატეგია 2011წელს მიიღეს.

დიდი ბრიტანეთი გაერთიანებული სამეფო არის ქვეყანა რომელიც ცდილობს რომ ყველა საკითხში იყოს მოწინავე პოზიციაზე ამიტომაც დიდ ყურადღებას უთმობს კიბერუსაფრთხოების განვითარებას, ქვეყანა ორიენტირებულია ინოვაციებზე,ცდილობს ისარგებლოს კიბერუსაფრთხოების ყველა უპირატესობით.

ჰოლანდია მიისწრაფვისინოვაციებისაკენ ის ცდილობს სანდო სისტემის ფუნქციონირებას,ნიდერლანდების სამეფო დიდ რესურსს დეებს რომ კიბერსივრცე დაცული იყოს რაც ასახეს კიდეც ქვეყნის სტრატეგიაში, რომელიც 2011 წელს მიიღეს.

ევროკავშირი ახორციელებს ინფორმაციის გაცვლას თავის წევრ ქვეყნებთან, რათა ინოვაციები ერთმანეთს გაუზიარონ,ისინი მჭიდრო კავშირში არიან ნატოს წევრ ქვეყნებთან, რათა მოხდეს დროული პრევენცია რეალური საფრთხისა, ისინი გასცემენ რეკომენდაციებსა და რჩევებს,მათ შეიმუშავეს სახელმძღვანელო მთელი ევროპის მაშტაბით.

2.2. საქართველო კიბერდანაშუალის წინააღმდეგ

ინფორმაციული და კომუნიკაციების ტექნოლოგიების განვითარებამ მნიშვნელოვნად შეუწყო ხელი საქართველოს კიბერსივრცეში გამოწვევების, რისკების, საფრთხეებისა და მათი წყაროების წარმოქმნას. კიბერუსაფრთხოების მნიშვნელობა, მასთან დაკავშირებული საფრთხეები და გამოწვევები ასახულია საქართველოს სტრატეგიული და უწყებრივი დაგეგმვის შემდეგ დოკუმენტებში: „საქართველოს ეროვნული უსაფრთხოების კონცეფცია“, „საქართველოს საფრთხეების შეფასების დოკუმენტი“, „თავდაცვის სტრატეგიული მიმოხილვა.“, „საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების სამოქმედო გეგმა“, „საქართველოს ეროვნული სამხედრო სტრატეგია“.

საქართველოს თავდაცვისუნარიანობის სტრატეგიაში აღნიშნულია, რომ ,,კიბერსივრცექმნისერთიანკომპლექსურგარემოსმასშიშემავალიინფორმაციულიდ აკომუნიკაციებისტექნოლოგიებისმოწყობილობებითადაქსელებით, რაცსაშუალებასაძლევსსაქართველოსთავდაცვისსამინისტროსსამოქალაქოფისს, შეიარაღებულიძალებისგენერალურიშტაბისსტრუქტურულქვედანაყოფებსადასამ ინისტროშიშემავალსაჯაროსამართლისიურიდიულპირებსგანახორციელონსხვადა სხვატიპისკომუნიკაცია, ძალებისადასაშუალებებისმართვა”.

ასევე, გაწერილია სამომავლო გეგმებიც. უფრო კონკრეტულად აღნიშნულია, რომ მომავალშიკიბერსივრცეკიდევუფროკომპლექსურიდამასშტაბურიგახდება, გაიზრდებასახელმწიფოსტრუქტურებისდამოკიდებულებაინფორმაციულტექნოლ ოგიებზე, რაცგანაპირობებსახალირისკებისადასაფრთხეებისწარმოქმნას. სწორედაქედანგამომდინარე, აუცილებელიაკიბერუსაფრთხოებისისეთიმოქნილიმექანიზმებისშექმნა, რომლებიცეფექტურადუპასუხებენახლადწარმოქმნილგამოწვევებს.

,,კიბერუსაფრთხოებისუზრუნველყოფისმნიშვნელოვანნაწილს, აგრეთვეწარმოადგენსახალიკიბერშეტევებისადმიინფორმაციულისისტემებისმდგრადობისამაღლება, პრევენციულიღონისძიებებისშემუშავებადაგატარება“.

საქართველოს სახელმწიფოს პოლიტიკის მიხედვით, კიბერუსაფრთხების დაცვისთვს გადადგმული ნაბიჯები პასუხობს კიბერსივრცეში გლობალურ გამოწვევებს და თავსებადია ნატოსა და ევროკავშირის ქვეყნების პრინციპებთან კიბერუსაფრთხოების სფეროში.

ამასთანავე, 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.

აღსანიშნავია, რომ კიბერუსაფრთხოების უზრუნველსაყოფად მნიშვნელოვანია თავდაცვის სისტემაში შემავალი სტრუქტურული ერთეულების მჭიდრო თანამშრომლობა, ასევე, უწყებათაშორისი ძალისხმევა და კოორდინირებული მუშაობა არასამთავრობო სექტორთან. კიბერუსაფრთხოების სფეროში სახელმწიფოს ერთიანი ძალისხმევის ორგანიზება ხელს შეუწყობს კიბერსივრცეში არსებული საფრთხეების პრევენციასა და კიბერინციდენტების შედეგად მიღებული ზიანის შემცირებას.

კიბერუსაფრთხოების პოლიტიკა მოიცავს რამდენიმე მნიშვნელოვან პრიორიტეტს, კიბერუსაფრთხოების პოლიტიკის პირველი პრიორიტეტული ამოცანაა, განსაზღვროს კიბერსივრცის უსაფრთხოების უზრუნველყოფასთან დაკავშირებული სტრატეგია. პოლიტიკა აღწერს იმ პრინციპებს, რომლებიც

განაპირობებენ ინფრასტრუქტურის უსაფრთხოების უზრუნველყოფას და იმ სტანდარტების დანერგვას, რომელთა გამოყენება მყარ საფუძველს შეუქმნის ინფორმაციული სისტემებისა და ქსელების ეფექტურ დაცვას თავდაცვის სფეროში. პოლიტიკა ხაზს უსვამს კიბერუსაფრთხოების წარმატებული და ოპერატიული დაცვის მიზნით ადგილობრივი სტრუქტურების მჭიდრო და აქტიურ კოორდინაციასა და მათი ჩართულობის აუცილებლობას.

პოლიტიკის მეორე პრიორიტეტული ამოცანაა საქართველოს შეიარაღებული ძალების ინფორმაციული სისტემების დაცვა პოტენციური კიბერშეტევებისგან, დაზვერვის და რადიო-ელექტრონული ბრძოლის ხერხების და საშუალებების, ფსიქოლოგიური ოპერაციების აქტიური წინააღმდეგობის საშუალებებისა და მეთოდების განვითარება.

კიბერშეტევების მზარდი რაოდენობიდან გამომდინარე, საქართველოს სახელმწიფოს პრიორიტეტია უსაფრთხო და ადეკვატური ინფორმაციული გარემოს შექმნა, რაც სტაბილური ფუნქციონირებისა და მოქმედების საწინდარია. კიბერსივრცის დინამიკური და სპეციფიკური ხასიათიდან გამომდინარე, ქვეყანაში დადგა საჭიროება თავდაცვის სფეროში კიბერსივრცესთან დაკავშირებული ყველა საკითხი განხილულ იქნეს თავდაცვის სამინისტროს კიბერუსაფრთხოების პოლიტიკის ჭრილში, რაც ითვალისწინებს ინტეგრირებულ ხედვასა და სტრატეგიის კოორდინირებულ განხორციელებას.სახელმწიფო გვაფრთხილებს რომ არ შევიყვანოთ ჩვენი პირადი ინფორმაცია საეჭვო საიტებზე,არ ენდოთ ელ–ფოსტას რომელიც თქვენგან პირადი ინფორმაციასთან ,ან საბანკო დეტალების შეყვანას ითხოვს. პირად ინფორმაციის მაგალითად ბარათის მონაცემების ან ვებ–გვერდზე შეყვანას ყოველთვის დააკვირდით, იმყოფებით თუ არა დაცულ ვებ–გვერდზე, რადგან ვებგვერდი შეიძლება გაყალბებული იყოს. ნუ ენდობით ინფორმაციას რომელიც თქვენგან სწრაფ რეაგირებას ითხოვს. გახსოვდეთ რომ კიბერ დამნაშავე თქვენთვის კარგად ნაცნობი იმიჯით ცდილობს, რომ თქვენ გამოგტყუოთ ინფორმაცია.

ყურადღება მიაქციეთ თქვენს მობილურ ნომრებზე მოსულ ესემესს, რომელიც საუკეთესო შემოთავაზებებით გვირევს თავგზას. ასეთი აქციების

ბმული არის თაღლითური საიტი, რომლის მიზანია ჩვენი ბარათის მონაცემების მოპოვება, შემდეგ კი ბარათის მონაცემების საშუალებით მომხმარებლის კუთვნილი თანხების მითვისება. მსგავს შემოთავაზებებს ხალხი ადვილად თანხმდება, თუმცა შემდეგ არიან დაზარალებულები და ტყუილის მსხვერპლი

დასკვნა

XXI საუკუნეში კლავიატურა უფრო საფრთხის შემცველი შეიძლება აღმოჩნდეს, ვიდრე ტყვიები და ბომბები, კიბერთავდასხმა დღეს უკვე წარმოადგენს ყველა არსებული კონფლიქტის მნიშვნელოვან კომპონენტს. ტექნოლოგიის განვითარებამ ტერორისტებს მისცა საშუალება ინტერნეტის ეფექტურად გამოყენების, რაც კიდევ უფრო აახლოვებს მათ ერთმანეთთან.

ტერორისტების კომუნიკაცია ინტერნეტში ხშირად მოიცავს ინფორმაციას მათი ოპერატიული გეგმებისა და მეთოდების შესახებ, მათი გაშიფრვის შემთხვევაში შესაძლოა შემუშავებულ იქნას ანტიტერორისტული ბრძოლის მეთოდები, დადგინდეს მათი ვინაობა და მივიღოთ ინფორმაცია მათ ინანსებთან დაკავშირებით.

ჩვენი მიზანი იყო განგვეხილა ტერორისტული საქმიანობის გამომწვევი მიზეზები, საფუძვლები და სახეები, მათ შორის ისეთის, როგორიც არის კიბერტერორიზმი და ამ ამ სახის ტერორიზმის ის წინაპირობები, რომლებიც იწვევს მათ წარმოშობას და განაპირობებს მათ მომავალ საქმიანობას. აუცილებელია საერთო თანამშრომლობით შესწავლილ იქნას ტერორიზმის წინააღმდეგ ეფექტური ბრძოლის გზები, რომელიც ხელს შეუწყობს კიბერდანაშაულთან ეფექტური ბრძოლის საქმეში. მთავარია მოხდეს იმ საფუძვლების ძიება, რაც ხელს უწყოს ტერორისტული აქტივობის ზრდას.

სპეციალიზაციისდა მიუხედავად, ტერორიზმის ანალიტიკოსებს დღეს ესაჭიროებათ მაღალი დონის მომზადება. როგორც არაერთი მკვლევარი აღნიშნავს, მხოლოდ არაბულის ცოდნა არ არის საკმარისი არსებული პრობლემის მოსაგვარებლად. თითოეული ქვეყნის პრიორიტეტს უნდა წარმოადგენდეს ინფორმაციის მონიტორინგისა და მისი მოპოვებისათვის მომზადება. უნდა გამოინახოს გზები ტექნიკური ლინგვისტური ექსპერტიზის ასამაღლებლად, რათა მოხდეს ტერორისტების რესურსებში შეღწევა.

მართალია ესპერტიზის საჭირო დონის მისაღწევად წლები დაგვჭირდება, რათა ეფექტურად გაიშიფროს კოდები, რომლებიც ხშირად გამოიყენება

მიმოწერის დროს, თუმცა მთავარია, რომ ეს დადებითად აისახება კიბერტერორიზმის წინააღმდეგ ბრძოლის საქმეში. ექსპერტები ტექნოლოგიებს უნდა ფლობდნენ მაღალ დონეზე, რათა შეძლონ მოიპოვონ კოდირებულ ფაილებში არსებული ინფორმაცია. ასევე აუცილებელია მოხდეს სათარგმნი ტექნოლოგიების სწრაფად განვითარება. ქვეყნებს შორის კი უნდა გაიზარდოს ინფორმაციის გაცვლა ამ სფეროში.

გამოყენებული ლიტერატურა:

1. დაზვერვის სამსახურებზე ზედამხედველობის განხორციელება : სახელმძღვანელო, ჰ. ბორნი ა.უილსი თბილისი, DCFI 2012

2. ვირსალაძე თამთა კიბერტერორიზმი და საქართველო: რა რესურსები არსებობს ქვეყნაში მსგავს გამოწვევებთან საბრძლველად“. ჟ. ,,Politcommersant” 2016 წელი

3. პატარია, ლაშა კიბერკრიმინალი ლეგალური და სადაზვერვო ასპექტები, თბილისი, 2012

4. „საქართველოს ეროვნული უსაფრთხოების კონცეფცია“, კომპიუტერული პრგრამა ,,Codex”

5. საერთაშორისო ტერორიზმი :(იდეოლოგია და ტერორიზმი): [სახელმძღვანელო] /ე. გვენეტაძის საერთო რედაქციით ; საქ. ტექნ. უნ-ტი, 2016.

5. .„საქართველოს საფრთხეების შეფასების 2010-2013 წ.წ. დოკუმენტი“, კომპიუტერული პრგრამა ,,Codex”

6. „თავდაცვის სტრატეგიული მიმოხილვა 2013-2016 წწ.“, კომპიუტერული პრგრამა ,,Codex”

7.„საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგია“ კომპიუტერული პრგრამა ,,Codex”

8. .„საქართველოს ეროვნული სამხედრო სტრატეგია“,კომპიუტერული პრგრამა ,,Codex”

9. სვანაძე, ვლადიმერ, კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები, 2015

10. ჭიღიტაშვილი ანა, ტერორიზმი როგორც გლობალური პრობლემა: კრიმინოლოგიური ანალიზი და ბრძოლის მეთოდები საქართველოში თბილისი 2009

11. ჩქოფოია სოფო საერთაშორისო ტერორიზმის ისტორიულ-პოლირტიკური ასპექტები თბილისი, 2017

12. ვახანია თინათინ უსაფრთხოება და საერთაშორისო ტერორიზმი გლობალიზაციისკონტექსტში 2013

http://intermedia.ge/%E1%83%A1%E1%83%A2%E1%83%90%E1%83%A2%E1%83%98%E1%83%90/27164-%E1%83%A3%E1%83%A1%E1%83%90%E1%83%A4%E1%83%A0%E1%83%97%E1%83%AE%E1%83%9D%E1%83%94%E1%83%91%E1%83%90-%E1%83%93%E1%83%90-%E1%83%A1%E1%83%90%E1%83%94%E1%83%A0%E1%83%97%E1%83%90%E1%83%A8%E1%83%9D%E1%83%A0%E1%83%98%E1%83%A1%E1%83%9D-%E1%83%A2%E1%83%94%E1%83%A0%E1%83%9D%E1%83%A0%E1%83%98%E1%83%96%E1%83%9B%E1%83%98-%E1%83%92%E1%83%9A%E1%83%9D%E1%83%91%E1%83%90%E1%83%9A%E1%83%98%E1%83%96%E1%83%90%E1%83%AA%E1%83%98%E1%83%98%E1%83%A1-%E1%83%99%E1%83%9D%E1%83%9C%E1%83%A2%E1%83%94%E1%83%A5%E1%83%A1%E1%83%A2%E1%83%A8%E1%83%98/50/ (ამოღებულია 1.06.17)

13. ინტერვიუ ექსპერტ ლადო სვანაძესთან http://www.interpressnews.ge/ge/interviu/333106-kargi-iqneboda-thu-kiberusafrthkhoebis-sakithkhebze-sheiqmneboda-makoordinirebeli-organo-romelic-premiers-daeqvemdebareba.html?ar=A(ამოღებულია 1.06.17)

14. კიბერტერორიზმისპრობლემატიკაანუ XXI საუკუნისსაფრთხე http://freeview.ge/xxi/ (ამოღებულია 1.06.17)

15. ორგანიზაციაგრენა: http://elearning.grena.ge/mod/page/view.php?id=345

16. საერთაშორისო ტერორიზმი-გლობალური პილიტიკური პრობლემა https://pirveli4ever.wordpress.com/2010/06/23/%E1%83%A1%E1%83%90%E1%83%94%E1%83%A0%E1%83%97%E1%83%90%E1%83%A8%E1%83%9D%E1%83%A0%E1%83%98%E1%83%A1%E1%83%9D-%E1%83%A2%E1%83%94%E1%83%A0%E1%83%9D%E1%83%A0%E1%83%98%E1%83%96%E1%83%9B%E1%83%98-%E1%83%92/ (ამოღებულია 1.06.17)

17. სამოქალქოგანათლებისლექსიკონი http://www.nplg.gov.ge/gwdict/index.php?a=term&d=5&t=2683

18. ურუშაძე თამარ ,,სუიციდური ტერორიზმის ორგანიზაციული და ინდივიდუალური მოტივები“ http://ydcgblog.blogspot.com/2013/03/blog-post_6848.html (ამოღებულია 1.06.17)

19. EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT (TE-SAT):Report 2016 https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2016 (ამოღებულია 1.06.17)

20. კიბერუსაფრთხოებასთან დაკავშირებული სახელმძღვანელო მშობლებისათვის http://csbd.gov.ge/news.php?year=2016&news_number=14&news_type=tips&lang=ge