CAUCASUS ACADEMY OF SECURITY EXPERTS

კიბერ უსაფრთხოების სერია

კიბერ კრიმინალი

ლეგალური და სადაზვერვო ასპექტები

ლაშა პატარაია

ინფორმაციული უსაფრთხოება
კიბერ კრიმინალი
ჰაკერები და მეკობრეები
ინსაიდერები
დაზვერვა და კიბერ შპიონაჟი
იურიდიული ასპექტები
ინფორმაციული ომები
კიბერ შეტევები

სარჩევი

საავტორო უფლებები

კიბერ კრიმინალი – ლეგალური და სადაზვერვო ასპექტები

ISBN: 978-9941-0-4397-0
UDC: 343.98:004.42 პ-211

გამოცემულია უსაფრთხოების ექსპერტთა კავკასიის აკადემიის მიერ, ინფორმაციული უსაფრთხოების კვლევების და ანალიზის ცენტრის მხარდაჭერით.

წიგნთან დაკავშირებით სხვადასხვა უფლებების მისაღებად ან უბრალოდ ინფორმაციისათვის შეგიძლიათ მიმართოთ უსაფრთხოების ექსპერტთა კავკასიის აკადემიას ელექტრონული ფოსტით: contact@globalcase.org ან გაეცნოთ ოფიციალურ ვებ-გვერდს: www.globalcase.org

რეცენზიები

რედაქტორები:

დავით კუხალაშვილი
ისტორიის მეცნიერებათა დოქტორი
პოლიციის პოლკოვნიკი

თენგიზ ენდელაძე
ისტორიის მეცნიერებათა დოქტორი
რეზერვის გენერალ-მაიორი

რეცენზენტები:

გიორგი ჯაბაური
ფიზიკა-მათემატიკურ მეცნიერებათა დოქტორი
თადარიგის პოლკოვნიკი

ლია ლუხავა
სამართლისა და ეკონომიკური კიბერნეტიკის მაგისტრი
რეზერვის კაპიტანი

დავით ჭოჭუა
ვენის უნივერსიტეტის დოქტორანტი
ექსპერტი ანტიტერორიზმის საკითხებში
საქართველოს საგარეო საქმეთა სამინისტროს აშშ-ს დეპარტამენტის დირექტორი

დავით კუხალაშვილი

ლაშა პატარაიას ნაშრომის „კიბერ კრიმინალი – ლეგალური და სადაზვერვო ასპექტები“ საკვლევი პრობლემა თანამედროვე მსოფლიოსათვის და საქართველოსათვის აქტუალურია. კვლევის დიდ მნიშვნელობას განაპირობებს საქართველოს უახლესს ისტორიაში, რუსეთის ფედერაციასთან 2008 წლის აგვისტოს საომარ მოქმედებების უარყოფითი შედეგები, რამაც საქართველოს სადაზვერვო და კონტრსადაზვერვო სივრცის კრახთან ერთად, ფაქტობრივ კონტროლს დაუქვემდებარებელი ტერიტორიების საზღვრების გაფართოებასთან ერთად, კიბერ ომში კოლოსალური დამარცხება განაპირობა.

ნაშრომი მოიცავს მდიდარ ისტორიულ ფაქტებსა და მოვლენებს, კიბერ კრიმინალისა და ამ კუთხით სადაზვერვო ქმედებების აღკვეთის მიზნით პრევენციულ რეკომენდაციებს, თანამედროვე ეტაპზე საქართველოში არსებულ საკანონმდებლო ბაზის განხილვას და მისი პრაქტიკული რეალიზების საშუალებებს.

წინამდებარე კვლევაში კიბერ კრიმინალსა და სადაზვერვო ორგანიზაციას შორის კავშირების ანალიზის გათვალისწინება კონტრსადაზვერვო ორგანიზაციის წინაპირობად შეიძლება იქცეს, რაც ეროვნული უსაფრთხოების მაჩვენებლების გაუმჯობესების ერთ-ერთი მნიშვნელოვანი გარანტია.

ავტორის დასკვნები, მსოფლიოში კიბერ კრიმინალისა და სადაზვერვო ორგანიზაციის კუთხით განვითარებული მოვლენების მასშტაბურობის შესახებ, იძლევა საშუალებას დავასკვნათ, რომ საქართველომ უმოკლეს ვადაში უნდა შეიმუშაოს კიბერ კრიმინალთან ბრძოლის ეფექტური პრევენციული, მათ შორის სადაზვერვო და კონტრსადაზვერვო ზომები, რომელშიც მნიშვნელოვანი როლი სამეცნიერო-კვლევით საქმიანობას უნდა მიენიჭოს.

ლაშა პატარაიას ხედვა ამ მხრივ განსაკუთრებით ფასეულია და ვისურვებდი, რომ რეალურად მოხდეს მისი იდეების დანერგვა ჩვენი ქვეყნის ეროვნული უსაფრთხოების საქმეში. აღსანიშნავია, რომ ეს მისი პირველი წიგნია და ასევე პირველი წიგნია საქართველოსთვისაც ამ სფეროში. ჩემთვის დიდი პატივია ვიყო ამ პროექტის ნაწილი და გუნდის წევრი, რომელიც ღირებულ ნაბიჯებს დგამს ქვეყნის გაძლიერების საქმეში. როგორც ახალგაზრდა, პერსპექტიულ მეცნიერს და საკუთარი საქმის უბადლო სპეციალისტს წარმატებას ვუსურვებ მის ასპარეზში ეროვნული უსაფრთხოებისათვის.

დავით კუხალაშვილი
ისტორიის მეცნიერებათა დოქტორი
პოლიციის პოლკოვნიკი

გიორგი ჯაბაური

მსოფლიო, ახალ ეპოქაში, ახალი გამოწვევების წინაშე დგას! ციფრული ტექნოლოგიების უსწრაფესი ტემპით განვითარებამ სრულიად ახალი, დღემდე შეუსწავლელი ამოცანები დაუსვა, როგორც ზოგადად კაცობრიობას, აგრეთვე სახელმწიფოს უმნიშვნელოვანეს ინსტიტუციას — სპეცსამსახურებს.

წინამდებარე ნაშრომი - „ კიბერ კრიმინალი – ლეგალური და სადაზვერვო ასპექტები“ წარმოადგენს თანამედროვე მსოფლიოს ერთ-ერთ უმნიშვნელოვანესი პრობლემის ანალიზს. ჩვენი სახელმწიფოსთვის მან თავი იჩინა საქართველო-რუსეთის 2008 წლის აგვისტოს საომარ მოქმედებებში, რასაც საქართველოს სადაზვერვო და კონტრსადაზვერვო სისტემის მოშლასთან ერთად კიბერ ომში სრული დამარცხება მოჰყვა.

მდიდარ ისტორიულ ფაქტებსა და მოვლენებზე დაყრდნობილი ნაშრომი მოიცავს კიბერდაზვერვისა და კიბერკონტრდაზვერვის ორგანიზაციის მნიშვნელოვან რეკომენდაციებს. მასში ასევე განხილულია კიბერ კრიმინალის კუთხით საქართველოში არსებული საკანონმდებლო ბაზა და ბოლო დროის უახლესი ინიციატივები ლოკალური თუ საერთაშორისო მასშტაბით.

ლაშა პატარაიას სამეცნიერო ნაშრომი იმსახურებს დადებით შეფასებას. ვფიქრობ, როგორც იმედის მომცემ მეცნიერს, საკუთარი ქვეყნისათვის მნიშვნელოვანი წარმატებების მოტანა შეუძლია, როგორც თეორიულ, ასევე პრაქტიკული მოქმედებების ასპარეზზე.

ნაშრომი საინტერესო იქნება, როგორც სამართალდამცავი ისე საჯარო სექტორის მოხელეთათვის, კერძო სექტორში დასაქმებული პირთათვის და მოსახლეობის ფართო ფენებისათვის.

გიორგი ჯაბაური
ფიზიკა-მათემატიკურ მეცნიერებათა დოქტორი
თადარიგის პოლკოვნიკი

თენგიზ ენდელაძე

უახლესს ისტორიაში, მთელი მსოფლიოს მასშტაბით, გახშირებულია სხვადასხვა სახის კრიზისების მიზანმიმართული ინსპირირება, რომლის ეფექტური ორგანიზების ერთ-ერთ ხელშემწყობად სადაზვერვო აქციების სწორად დაგეგმვა და განხორციელება უნდა მივიჩნიოთ.

ტექნოლოგიური განვითარების მიუხედავად სადაზვერვო საქმიანობაში ადამიანის როლი განსაკუთრებულია და კიბერ კრიმინალის თემა, სწორედ ადამიანის მიერ არის ორგანიზებული, რომელიც კონკრეტული პირის, სამრეწველო, სასიცოცხლო დანიშნულების ობიექტების და საერთოდ, კონკრეტული სახელმწიფოს დაზიანებისაკენ არის მიმართული.

ნაშრომის ერთ-ერთ ღირებულებას წარმოადგენს ის გარემოება, რომ მასში გაანალიზებულია 2008 წლის აგვისტოში საქართველოს წინააღმდეგ წარმოებული კიბერ ომი, რომელიც რუსეთის ფედერაციასთან საბრძოლო მოქმედებების პარალელურად მიმდინარეობდა და რომელშიც საქართველო დამარცხდა.

კვლევაში გამოკვეთილია კონკრეტული მიმართულებები, რომლის ირგვლივაც აუცილებელია საქართველოში დაჩქარებული ტემპებით დაიწყოს სამეცნიერო-კვლევითი და სასწავლო საქმიანობის ორგანიზაცია. მოსაზრების ჭეშმარიტებას ადასტურებს თანამედროვე ეტაპზე უცხო სახელმწიფოთა სტრატეგიული ინტერესების გადაკვეთის არსებობის მუდმივობა საქართველოში, რაც საბრძოლო ქმედებების ინსპირირებასთან ერთად, კიბერ ომის წარმოებასაც არ გამორიცხავს.

ვფიქრობ, წინამდებარე ნაშრომი საინტერესო იქნება დაინტერესებული მკითხველისათვის და ავტორი, როგორც ინოვატორი მეცნიერი, კიდევ მრავალ ღირებულ ნაშრომს წარმოუდგენს ქართულ საზოგადოებას.

თენგიზ ენდელაძე
ისტორიის მეცნიერებათა დოქტორი
რეზერვის გენერალ-მაიორი

დავით ჯოჯუა

წინამდებარე ნაშრომი წარმოადგენს საინტერესო და მნიშვნელოვან შენაძენს საქართველოში კიბერ-დანაშაულისა და კიბერ-უსაფრთხოების შესწავლის დარგისათვის. გამომდინარე იქიდან, რომ აღნიშნული პრობლემატიკის აკადემიური შესწავლა ჩვენს ქვეყანაში ახალი ფენომენია, ნაშრომის ფასეულობა კიდევ უფრო იზრდება.

ნაშრომი კარგად არის სტრუქტურირებული და საკითხთა ფართო სპექტრს მოიცავს. მიმოიხილავს რა როგორც კიბერსივრცის ტექნიკურ განზომილებას, ისე მასთან დაკავშირებულ საკანონმდებლო ბაზას, ნაშრომი ინტერდისციპლინა-რული ხასიათისაა. აღნიშნული მიდგომა აბსოლუტურად გამართლებულია, რადგან ციფრული უსაფრთხოების მისაღწევად ტექნიკური საშუალებების გარდა შესაბამისი საკანონმდებლო ბაზაც უნდა არსებობდეს.

საგულისხმოა, რომ ნაშრომი საკმაოდ იოლი საკითხავია, რაც მას ხელმი-საწვდომს და გასაგებს ხდის ფართო საზოგადოებისთვის. ვინაიდან ციფრული ტექნოლოგიები დიდი ხანია ჩვენი ყოველდღიური ცხოვრების განუყოფელი ნაწილი გახდა, არც ერთი ჩვენგანისათვის ურიგო არ იქნებოდა ელემენტარული უსაფრთხოების ნორმებისა და წესების ცოდნა.

ნაშრომს დამატებით ღირებულებას სძენს ის ფაქტი, რომ მის ავტორს სიღრმისეულ თეორიულ ცოდნასთან ერთად აღნიშნულ თემაზე პრაქტიკული მუშაობის დიდი გამოცდილება გააჩნია. ყოველივე ზემოაღნიშნულის გათვალის-წინებით, დარწმუნებული ვარ, რომ ლაშა პატარაიას ნაშრომი "კიბერ კრიმინალი – ლეგალური და სადაზვერვო ასპექტები" დაინტერესე-ბული მკითხველისათვის სასიამოვნო და საჭირო საკითხავი იქნება.

დავით ჯოჯუა
ვენის უნივერსიტეტის დოქტორანტი
ექსპერტი ანტიტერორიზმის საკითხებში
საქართველოს საგარეო საქმეთა სამინისტროს აშშ-ს დეპარტამენტის დირექტორი

ავტორისაგან

ძვირფასო მკითხველო! როდესაც ინფორმაციული უსაფრთხოებით დავინტერესდი საქართველოში ცოტამ თუ იცოდა ამ თემის შესახებ. შესაბამისად არ არსებობდა საგანმანათლებლო დაწესებულებები, სასწავლო პროგრამები, ადგილობრივი ლიტერატურა, რომლის საშუალებითაც შეიძლებოდა უფრო მეტის გაგება. თუმცა მეორემხრივ ჩემი პროფესიული ჩამოყალიბება საქართველოსთვის ძალიან რთულ და მეტად საინტერესო დროს დაემთხვა. რევოლუცია, შიდა პოლიტიკური დესტაბილიზაციის მცდელობები, ომი რუსეთთან, უცხო ქვეყნების სადაზვერვო აგენტურული ქსელის განსაკუთრებული აქტიურობა რეგიონში და რაღათქმა უნდა გლობალური მოვლენები, რომლებმაც უსაფრთხოების სფეროში ინდუსტრიული რევოლუციასავით იმოქმედეს. მქონდა პრივილეგია ამ ყოველივე ამისათვის თვალი მინიმალური დისტანციიდან მედევნებინა და სწორედ ერთ-ერთი ასეთი მოვლენა გახდა ჩემი მთავარი შთაგონების წყარო, გადამედგა მნიშვნელოვანი ნაბიჯი საქართველოში ინფორმაციული უსაფრთხოების, როგორც სფეროსა და პროფესიის ჩამოყალიბებისთვის.

2008 წლის რუსეთ-საქართველოს ომმა, კერძოდ სამთავრობო დონის უმსხვილესმა კიბერ აქტივობებმა, ინფორმაციულმა ომმა, კიბერ შეტევებმა და შპიონაჟის ახალმა სახეობებმა, რომლებიც სპეციალურად საქართველოს მსგავსი ქვეყნებისთვის შეიქმნა, გადამაწყვეტინა ჩამომეყალიბებინა პირველი ორგანიზაცია ინფორმაციული უსაფრთხოების სფეროში – ინფორმაციული უსაფრთხოების კვლევებისა და ანალიზის ცენტრი.

აღნიშნული ორგანიზაცია კავკასიის რეგიონში თავისი პროფილით ერთადერთია. იგი ასევე პირველი ადგილობრივი კვლევითი ცენტრია, რომელმაც 2008 წლის აგვისტოს მოვლენები კიბერ ომად შეაფასა. ეს თემა არასოდეს ყოფილა ასეთი მასშტაბით შესწავლილი ლოკალური ორგანიზაციების მიერ. ცენტრის ფარგლებში შეიქმნა პირველი სასწავლო პროგრამა ინფორმაციული უსაფრთხოების, დაზვერვის, ანტიტერორიზმისა და გლობალური უსაფრთხოების შესახებ.

ცენტრის გარშემო მრავალი პროფესიონალი შემოიკრიბა და სულ ცოტა ხნის შემდეგ გადაწყდა სპეციალურად, საგანმანათლებლო მიზნებისთვის ჩამოყალიბებულიყო აკადემია, რომელიც ცენტრის მიერ დაწყებულ საქმიანობას ახალ საფეხურზე აიყვანდა. ასე ჩამოყალიბდა უსაფრთხოების ექსპერტთა კავკასიის აკადემია, რომლის მიზანია უსაფრთხოების, როგორც პროფესიის განვითარება.

უსაფრთხოების სხვადასხვა კომპეტენციით აღჭურვილმა გამოცდილ პროფესიონალთა ადგილობრივმა გუნდმა საგანმანათლებლო პროექტებთან ერთად ძლიერი სამეცნიერო-კვლევითი პარტნიორული ქსელიც ჩამოაყალიბა.

ორგანიზაცია სამეცნიერო-კვლევითი აქტივობებსა და საგანმანათლებლო პროექტებში კიბერ კრიმინალის საკითხებს დიდ მნიშვნელობას ანიჭებს. ეს საქართველოსა და მსოფლიოში არსებულმა რეალობამაც განაპირობა, რომელიც გაჯერებულია ახალი საფრთხეებით, ბოლომდე შეუსწავლელი საკითხებით,

კონფლიქტებითა და სამართლებრივი კაზუსებით. წიგნის მიზანია მკითხველს სრული ინფორმაცია მიაწოდოს კიბერ უსაფრთხოების და კიბერ კრიმინალის ლეგალურ ასპექტებზე, მათ პარალელებზე სადაზვერვო საქმიანობასთან და თანამედროვე საფრთხეებზე. აღჭურვოს ცოდნით ამ საფრთხეების ანალიზისთვის და სწორი სამართლებრივი ინტერპრეტაციისთვის.

დარწმუნებული ვარ, ეს წიგნი ღირებული იქნება იურისტებისთვის, ჟურნალისტებისთვის და უსაფრთხოების სფეროში მოღვაწე პროფესიონალებისთვის, რამეთუ ეს მათთვის სრულიად ახალი პერსპექტივაა, რომელიც დაეხმარება მათ უკეთ გამოიყენონ თანამედროვე ტექნოლოგიები ქვეყნისათვის უმნიშვნელოვანეს სფეროებში.

განსაკუთრებული მადლობა მინდა გადავუხადო უსაფრთხოების ექსპერტთა აკადემიის გუნდს, რედაქტორებსა და რეცენზენტებს, რომლებმაც უდიდესი მხარდაჭერა გამიწიეს, რათა ეს წიგნი ამგვარი სახით ეხილა ქართულ საზოგადოებას.

მაშ ასე, წარმოგიდგენთ კავკასიის რეგიონში პირველ წიგნს კიბერ უსაფრთხოების შესახებ – "კიბერ კრიმინალი – ლეგალური და სადაზვერვო ასპექტები". ვიმედოვნებ, რომ ეს წიგნი თითოეული მკითხველისათვის დაუვიწყარი გამოცდილება იქნება.

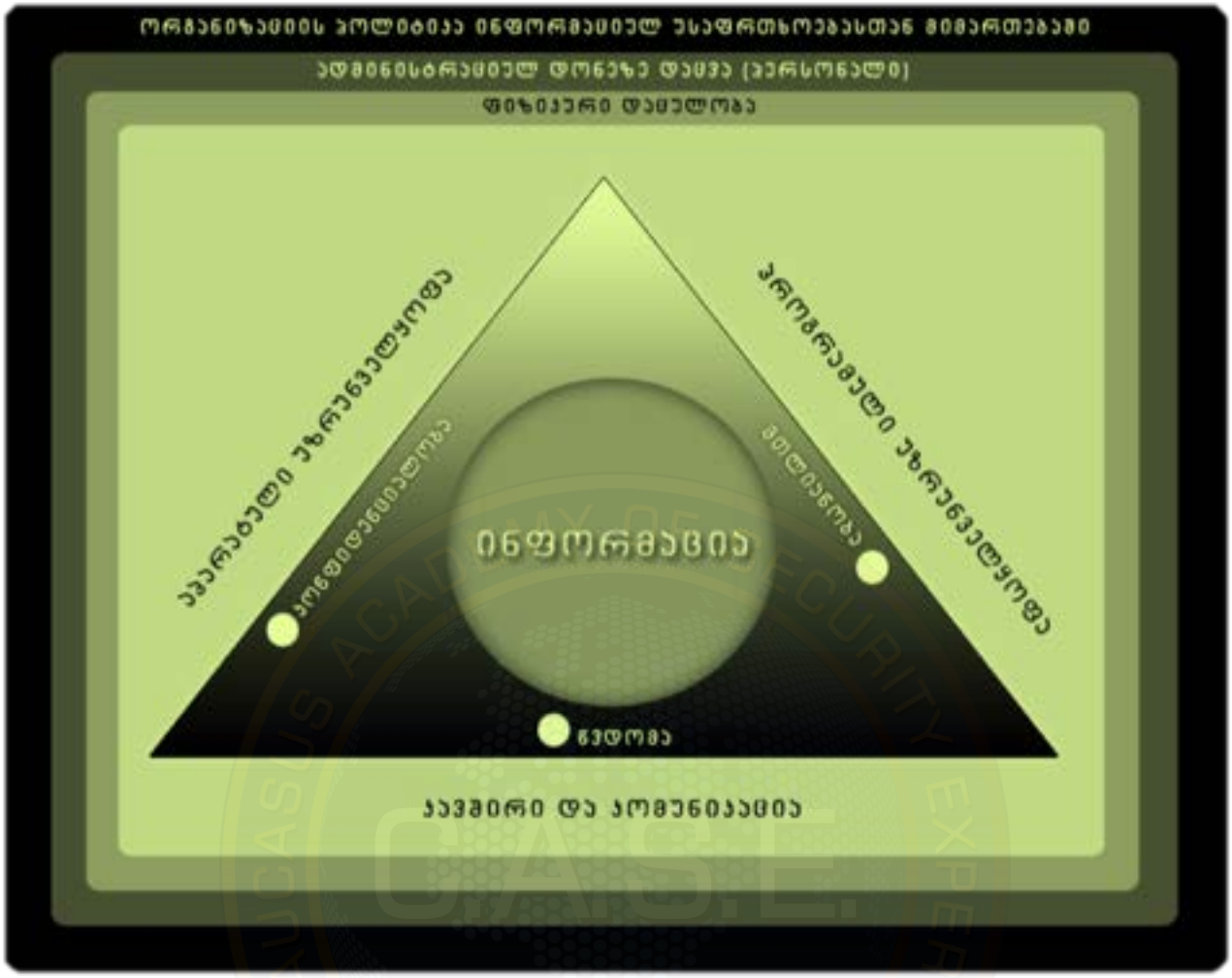
ლაშა პატარაია
უსაფრთხოების ექსპერტთა კავკასიის აკადემიის დირექტორი

ინფორმაციული უსაფრთხოება

თანამედროვე მსოფლიო სადაზვერვო ისტორიაში ინფორმაციული უზრუნველყოფის როლი ყველაზე მნიშვნელოვანია! ინფორმაციის მოპოვების, დამუშავებისა და გამოყენების პროცესის ეფექტურობა პირდაპირ კავშირშია ეროვნული უსაფრთხოების უზრუნველყოფასთან. თუმცა, ინფორმაციული უსაფრთხოება უკვე დიდი ხანია გასცდა მხოლოდ სახელმწიფოს წინააღმდეგ მიმართულ საშიშროებათა რიგს, იგი ასევე წარმოადგენს პრობლემას კორპორაციული სეგმენტისათვის. გავრცელებული დეფინიციებისა და ჩამოყალიბებული საზოგადოებრივი აზრის მიხედვით, სახელმწიფო და კერძო სექტორი ერთმანეთისაგან გამიჯნულია! თუმცა, ეროვნული უსაფრთხოების უზრუნველყოფისა და სადაზვერვო საქმიანობის პრინციპებიდან გამომდინარე დაუშვებელია მათი გამიჯვნა, რამეთუ კერძო სექტორი წარმოადგენს სახელმწიფოს უმნიშვნელოვან სტრატეგიულ ნაწილს და მისი ობიექტების დამაზიანებელმა ქმედებებმა შეიძლება ეროვნული უსაფრთხოების რღვევას ჩაუყაროს საფუძველი.

საქართველოში ინფორმაციული უსაფრთხოება აქტუალური, მაგრამ ჯერ-ჯერობით აუთვისებელი მეცნიერებაა, მაშინ როდესაც მსოფლიოს განვითარებული ქვეყნები სრულად იაზრებენ ამ სფეროსთან დაკავშირებულ საფრთხეებს და კოლოსალური აქტივობებით იბრძვიან მათ წინააღმდეგ.

კლასიკური დეფინიციის მიხედვით ინფორმაციული უსაფრთხოება გულისხმობს ინფორმაციისა და ამ ინფორმაციაზე დამოკიდებული ინფრასტრუქტურის დაცულობას. ინფორმაციული უსაფრთხოების მიზანი არის მასთან დაკავშირებული საფრთხის თავიდან არიდება და წინასწარი პროგნოზირება შემდგომი პრევენციული მექანიზმების შესამუშავებლად. ამ განმარტების უკეთ გასააზრებლად დიაგრამაზე წარმოდგენილია, ინფორმაციული უსაფრთხოების ის ასპექტები, რომლებიც უსაფრთხოების უზრუნველყოფისას საერთოა, როგორც კომერციული ისე სახელმწიფო სექტორისათვის.



დიაგრამის მიხედვით ინფორმაციული უსაფრთხოება კონცეპტუალურ დონეზე დაყოფილია სამ ძირითად ასპექტად:

- ორგანიზაციის პოლიტიკა ინფორმაციულ უსაფრთხოებაში;
- ინფორმაციის დაცულობა ადმინისტრაციულ დონეზე;
- ფიზიკური დაცულობა.

პირველ შემთხვევაში იგულისხმება ორგანიზაციის სწორი პრიორიტეტები და სამოქმედო გეგმა (პროტოკოლი), რომლის მიხედვითაც განსაზღვრულია: ინფორმაციის მოპარვა/განადგურება ან სხვა ინციდენტების შემთხვევებზე რეაგირება. ეს უკანასკნელი მოიცავს ყველა იმ საკითხს, რომელიც ინფორმაციულ უსაფრთხოებაში განიხილება და სწორედ ეს ფაქტორი განაპირობებს მის დიაგრამის სათავეში ყოფნას.

ინფორმაციული უსაფრთხოების ამგვარ კონცეფციას CIA სამკუთხედსაც უწოდებენ. იგი შემდეგნაირად იშიფრება: Confidentiality (კონფიდენციალობა), Integrity (მთლიანობა), Availiability (ხელმისაწვდომობა).

კონფიდენციალობა უზრუნველყოფს ინფორმაციის გამიჯვნას და წვდომას კონკრეტული სუბიექტებისათვის, რათა მხოლოდ შესაბამისი უფლებამოსილების მქონე პირებს ქონდეთ დაშვება მათთვის განკუთვნილ კონკრეტულ ინფორმაციასთან.

მთლიანობა გულისხმობს ინფორმაციის კორექტულობას, სისრულესა და მისი სტრუქტურის დაცვას არასანქცირებული მოდიფიკაციისგან ან განადგურებისაგან.

ხელმისაწვდომობა, ანუ წვდომის პროცესი უზრუნველყოფს კრიტიკული ოპერაციების უწყვეტობას და დაშვებული მომხმარებლების მუდმივი მუშაობის შესაძლებლობას. სხვაგვარად ამ უკანასკნელს ბიზნეს უწყვეტობასაც უწოდებენ. ეს კრიტიკულად მნიშვნელოვანი პროცესია განსაკუთრებით სამთავრობო და ძალოვანი უწყებების ოპერაციებში, ასევე საბანკო სექტორში, სადაც ერთიანი სისტემის თუნდაც მცირე დროით შეფერხება, დაკავშირებულია კოლოსალურ ზარალთან.

ჩვენი საზოგადოებისათვის განსაკუთრებით რთული აღმოჩნდა ახალი ტექნოლოგიების ათვისება და ამიტომ ტექნოლოგიების სფეროს პროფესიონალებს მუდმივად უწევთ იმის მტკიცება თუ რა როლი აქვს ინფორმაციულ ტექნოლოგიებს ნებისმიერ ინდუსტრიაში. ახლა როცა ტექნოლოგიებთან დაკავშირებული სარგებელი ყველამ გაიაზრა, როდესაც ტექნოლოგიები მაქსიმალურად არის ათვისებული, გაჩნდა კიდევ ერთი საკითხი – ადამიანური ფაქტორის მნიშვნელობა. როგორიც არ უნდა იყოს ტექნოლოგიების ათვისების მასშტაბები უნდა გვახსოვდეს, რომ ნებისმიერ პროცესში ადამიანს მაინც წამყვანი როლი უკავია, რაც მისი სახით მთავარი საფრთხის არსებობაზე უნდა მიანიშნებდეს. სხვაგვარად ამას ინსაიდერული საფრთხე ეწოდება.

ტექნოლოგიებზე საუბრისას, გასათვალისწინებელია, რომ ყველა საფრთხე კომფორტიდან გამომდინარეობს. ასეთ დროს ადამიანები უსაფრთხოებაზე მეტად კომფორტზე ფიქრობენ. დილემა კომფორტსა და უსაფრთხოებას შორის მუდმივი აქტუალობის მქონე საკითხია. როგორც ზემოთ აღინიშნა ერთ-ერთი მთავარი საფრთხე ინსაიდერულ ხასიათს ატარებს და ამიტომ კიბერ კრიმინალის განხილვას პირველ რიგში სწორედ ამ საკითხით ვიწყებთ.

ინსაიდერული საფრთხე

ინფორმაციული უსაფრთხოების ყველაზე დელიკატური ასპექტი მისი ადმინისტრაციულ დონეზე დაცულობაა. თავისმხრივ სისტემის ფიზიკური დაცულობაც მასზეა დამოკიდებული. უსაფრთხოების უზრუნველყოფა ადმინისტრაციულ დონეზე პირველ რიგში პერსონალის სათანადო მომზადებას მოითხოვს. საჭიროა იმ პირთა პერიოდული ტრენიგები, რომელთაც წვდომა აქვთ სენსიტიურ ინფორმაციასთან. ამგვარი წვდომა უნდა იყოს მკაცრი კონტროლის ქვეშ და ხორციელდებოდეს წვდომის უფლებების გამიჯვნით. სწორედ პერსონალი გახლავთ ინფორმაციის გაჟონვის ყველაზე პოპულარული წყარო, რაც უკავშირდება არამხოლოდ კორპორაციულ შპიონაჟს, არამედ უცხო ქვეყნების სადაზვერვო შეღწევადობასაც. ეს პრობლემა საკმაოდ აქტუალურია საქართველოში, რადგან საზოგადოებაში პრაქტიკულად არ არსებობს სათანადო კულტურა კონფიდენციალური ინფორმაციის მოფრთხილებისა. ალბათ ბევრი თქვენგანიც შესწრებია ფაქტებს, როდესაც სრულიად უადგილო ადგილას ზედმეტი "ქართული გულახდილობითა" და სრულიად გაუცნობიერებლად გაუციათ მნიშვნელოვანი კონფიდენციალური ინფორმაცია, მათ შორის მედია საშუალებებიდანაც. აქვე უნდა აღინიშნოს, რომ მედიის როლი ინფორმაციულ უსაფრთხოებაში არანაკლებ მნიშვნელოვანია.

არსებობს ინფორმციის გავრცელების უამრავი სცენარი. მათ შორის:

- ინფორმაციის გავრცელება გაუფრთხილებლობით
  იერარქიულად ეს სცენარი სიის სათავეში მისი პოპულარობის გამო მოექცა.
- ინფორმაციის გავრცელება დაცვითი მექანიზმების შესახებ
  ამგვარი ინფორმაცია თავისთავად იწვევს დაცული ინფორმაციის არამართლზომიერ მოპოვებას, ამგვარად ეს იგივეა რაც ინფორმაციის გამიზნულად გაცემა.
- ინფორმაციის გავრცელება შურისძიების მიზნით
  თუ ინფორმაცია წარმოადგენს მაკომპრომატირებელ მასალას ან კორპორაციულ საიდუმლოს, იგი შეიძლება გამიზნულად გაავრცელოს ბოროტმოქმედმა რათა მისი გავრცელებით დაზარალდეს მისი ობიექტი.
- ინფორმაციის მოპოვება პერსონალის გადაბირების ან მოსყიდვის საშუალებით
  ხშირად ამგვარად კონკურენტი კომპანიები იქცევიან, რათა ხელში ჩაიგდონ სენსიტიური ინფორმაცია. რა თქმა უნდა საუკუნეებია იგივე სქემა გამოიყენება ეორვნული უსაფრთხოების სფეროშიც.
- სამსახურიდან წამოსული პერსონალის მიერ გავრცელებული ინფორმაცია
  ამ ტიპის შემთხვევები ხშირად სამსახურიდან უსამართლო დათხოვნით ან არასათანადო მოპყრობით არის გამოწვეული. ზემოთ მოცემული სცენარები პოპულარულ შემთხვევებზეა აგებული, რაც სულაც არ ნიშნავს იმას რომ თანამედროვე კრიმინალებს უკეთესი მეთოდები არ აქვთ დამუშავებული. ეს

ყოველივე კი კიდევ ერთხელ გვაძლევს მიზეზს ვიყოთ უფრო ყურადღებით და არ გვიტოვებს მოდუნების უფლებას.

ინფორმაციის ფიზიკური დაცულობა უმეტეს შემთხვევაში დამოკიდებულია ზემოთ მოცემულ ფაქტორებზე, თუმცა იგი ადმინისტრაციული ასპექტების გარდა ასევე ტექნიკურ ნაწილსაც მოიცავს. რაც ნიშნავს იმას, რომ ნებისმიერ საფრთხეს, ინფორმაციული მთლიანობის დარღვევისა ან მისი არასანქცირებული გზით მოპოვებისა, უნდა ეწინააღმდეგებოდეს პროგრამულ-ტექნიკურ დონეზე შემუშავებული სპეციალური საშუალებები, რომლებმაც თავისმხრივ ასევე უნდა აკონტროლონ ინფორმაციის მიმოცვლა. ინფორმაციული უსაფრთხოების ტექნიკური ნაწილი სამ ნაწილად იყოფა:

- აპარატული უზრუნველყოფა
- პროგრამული უზრუნველყოფა
- კავშირი და კომუნიკაცია

თითოეულ ამ კომპონენტს მჭიდრო კავშირი აქვს ერთმანეთთან და წარმოადგენენ ურთიერთმოქმედი ელემენტებისაგან შემდეგარ თავდაცვით ჯაჭვს. ტექნიკური დონეზე მნიშვნელოვანია: მართვის ავტომატიზებული სისტემები, ანალიტიკური მოდულები, საფრთხის მუდმივი ანალიზი, ქსელური გასაღებები, კრიპტოგრაფიული საშუალებები, პროტოკოლირება და იდენტიფიკაცია/ავტორიზაციის მექანიზმები. ყოველივე ამის მოდელირება და იმპლემენტაცია უნდა ხდებოდეს შესაბამისი სტანდარტების გათვალისწინებით, სადაც სტანდარტიზაცია ერთ-ერთი უმთავრესი პრინციპია. ამ მოსაზრებას ამყარებს ის გარემოებაც, რომ ტექნოლოგიური პროგრესის შესაბამისად გამუდმებით იცვლება სტანდარტები და ყოველი მათგანი ინდივიდუალურია სხვადასხვა სპეციფიკის ორგანიზაციისათვის. აქვე უნდა აღინიშნოს, ის სასიკეთო ტენდენციაც, რომელიც ჩვენს ქვეყანაში სულ ახლახან დაიწყო. კერძოდ, მიღებულია კანონი ინფორმაციული უსაფრთხოების შესახებ, რომელიც ამ სფეროში სრულიად ახალ გარემოს ქმნის. აღნიშნული ინიციატივა და კანონი ვრცლად არის განხილული წიგნის შემდგომ თავებში.

რაც შეეხება დიაგრამის უმთავრეს ნაწილს – პირამიდას, რომლის უმთავრესი ნაწილი თავად ინფორმაციაა. მისი დაცვის მექანიზმები მუშავდება კონკრეტული გამოწვევების ადეკვატურად. ამ პროცესში სასიცოცხლოდ მნიშვნელოვანია რისკების სწორი შეფასება და საფრთხეების წინასწარ პროგნოზირება. საფრთხეები, რომლებიც მიმართულია ინფორმაციის წინააღმდეგ, CIA სამკუთხედის მიხედვით იყოფა სამ კატეგორიად: კონფიდენციალობა; მთლიანობა; წვდომა

კონფიდენციალობის დარღვევა, მეტწილად პერსონალთან არის დაკავშირებული და იგი ინფორმაციის არასანქცირებული გზით მოპოვებას უკავშირდება. ეს უკანასკნელი ასევე გულისხმობს ტექნიკური ბარიერების გადალახვას და სპეციალური საშუალებების გამოყენებით ინფორმაციის მოპოვება/განადგურებას ან მოდიფიკაციას. ამდენად ამავე მეთოდით ხდება მისი მთლიანობის დარღვევა. ხოლო რაც შეეხება წვდომას, იგი დამოკიდებულია როგორც ადმინისტრაციულ, ისე ფიზიკურ დაცულობაზე. წვდომაში იგულისხმება ინფორმაციის დაყოფა და მის გარკვეულ ნაწილებთან იერარქიული პრინციპით დაშვება. ანუ პერსონალს უნდა

კიბერ დანაშაული

ჰაკერები და კანონები ქართულ რეალობაში

შეეძლოს გარკვეულ ინფორმაციაზე წვდომა, მხოლოდ იმ შემთხვევაში თუ მას ამის უფლებას მისი თანამდებობრივი სტატუსი ან სამსახურეობრივი საჭიროება აძლევს. პერსონალში მკაცრად უნდა იმიჯნებოდეს ინფორმაცია. სწორედ ამ პრინციპების დარღვევა ქმნის საფრთხეს, რომელიც უკავშირდება ინფორმაციის გადინებას. ამგვარ საფრთხეებს მოიცავს ნებისმიერი კომპიუტერული პროგრამა თუ ქსელი, რომელსაც კავშირი აქვს:
სამეცნიერო დანიშნულების ქსელთან; ძალოვან სტრუქტურებთან; მმართველობის ნაციონალური მნიშვნელობის სისტემასთან და სხვა. ისინი წარმოადგენენ პოტენციურად საშიშ ინფრასტრუქტურას, რომლებიც შეიძლება გახდნენ როგორც კიბერ დამნაშავეების, ისე ტერორისტული დაჯგუფებების სამიზნეები.

ინფორმაციული უსაფრთხოების პრობლემები მოდებულია მთელს მსოფლიოში და შესაბამისად ინტერნეტი, როგორც გლობალიზაციის მოდელი მას სარკესავით ირეკლავს. ათეულობით პროპაგანდისტული კამპანია ტარდება გლობალურ ქსელში და იგი, იქცა სხვადასხვა კრიმინალური დაჯგუფებების თავშეყრის ადგილად. ინტერნეტის მომხმარებელთა რაოდენობა დღითიდღე მატულობს. მისი კონტროლი კი სულ უფრო და უფრო რთულდება. ინტერნეტის გლობალური სტატისტიკის მიხედვით ინტერნეტით მსოფლიოში დღეს უკვე ორ მილიარდზე მეტი ადამიანი სარგებლობს. აქედან, მხოლოდ საქართველოში 1,300,000 აბონენტია დათვლილი. სწორედ ამგვარი პოპულარობის გამო ინტერნეტი გაუტოლდა ტელევიზიას, გაუსწრო პრესას და იქცა მედია ბიზნესის საუკეთესო ნაწილად. ინტერნეტი საუკეთესო ინსტრუმენტია მასაზე მანიპულაციისთვის, რომელსაც პოლიტიკოსები უფრო ხშირად იყენებენ ვიდრე ბიზნესმენები მარკეტინგული მიზნებისთვის. ინტერნეტი იდეალური მოდელია დემოკრატიისა და შესაბამისად მას ხშირად ისევე ეძცევიან, როგორც დემოკრატიას.

Gartner

დასკვნა (2009 წ.) - "მაღალ ზარალიანი ინციდენტების 80 პროცენტი დაკავშირებულია შიდა-კორპორაციული ინფორმაციის გაჟონვასთან."

Cyber-Ark

გამოკითხულ თანამშრომელთა 85%-ის თქმით, ისინი არ გამორიცხავენ მათი დათხოვნის შემთხვევაში კონფიდენციალური ინფორმაციის გამოყენებას პირადი მიზნებისათვის. (2009 წ.)

Merrill Lynch

«დღესდღეობით ინფორმაციული უსაფრთხოების მენეჯერისთვის მონაცემების დაცვა პირველი პრიორიტეტია" (2008 წ.)

IDC
Analyze the Future

სერიოზული დარღვევების 70 პროცენტი ხორციელდება "ინსაიდერების" მონაწილეობით (2008 წ.)

კიბერ კრიმინალი

მსოფლიოს მასშტაბით კომპიუტერები დღეს უკვე თითქმის სრულად მოიცავს ყველა მნიშვნელოვან ლეგალურ ოპერაციას. მათ შორის საქართველოში იგი უკვე გამოიყენება არამხოლოდ სოციალური კომუნიკაციებისათვის, არამედ კონტრაქტების გასაფორმებლად, შესყიდვების საწარმოებლად და სხვადასხვა ინდუსტრიაში სრულფასოვანი ლეგალური ძალა გაჩნია.

იზრდება რა კომპიუტერის როლი და მისი გამოყენების არეალი სახელმწიფოში, პირდაპირპროპორციულად მატულობს კიბერდანაშაულებების საფრთხეც. შესაბამისად, ჩნდება ახალი, სპეციფიკური და გაჭიანურებული სასამართლო პროცესები, რადგან იურისტებსაც და მოსამართლეებსაც უჭირთ საქმის არსში სრულფასოვანი გარკვევა.

ამგვარ გარემოში სულ უფრო რთულდება როგორც კიბერ დანაშაულებების საწინააღმდეგო საკანონდმებლო ბერკეტების შემუშავება, ისე ზოგადად თანამედროვე ტექნოლოგიებთან დაკავშირებული საკითხების საკანონდმებლო დონეზე რეგულირება. სწორედ ამიტომ, მნიშვნელოვანია, რომ ამ საკითხის ირგვლივ სრულფასოვნად და მაქსიმალურად ინფორმირებულნი იყვნენ, როგორც კონკრეტული კომპეტენციის წრეები, ისე სამოქალაქო საზოგადოება.

ბოლო პერიოდში საქართველოში არაერთი საკანონმდებლო რეფორმა ჩატარდა, მიღებულ იქნა ახალი კანონმდებლობა კიბერ კრიმინალთან მიმართებაში, სხვადასხვა სამართალდამცავ უწყებებში შეიქმნა ახალი ორგანიზაციული სამტატო ერთეულები, მოხდა პროკურორთა გადამზადება და დავდექით შემდეგი რეალობის წინაშე – ჩვენ გვაქვს კიბერ კრიმინალის შემთხვევები, განახლებული კანონმდებლობა, რომელიც უშუალოდ მიმართულია მასზე და კარგად მომზადებული პროკურორები. ხოლო მეორე მხრივ კი, სრული დისბალანსი.

ადამიანი, რომელიც მოყვება კიბერ კრიმინალთან დაკავშირებულ ინციდენტში სამართლებრივი დავის პროცესში სრულიად უძლურია, რადგან საქართველოში ცოტა ადვოკატი თუ მოიძებნება, რომელიც ერკვევა კიბერ დანაშაულებებსა და თანამედროვე ტექნოლოგიებთან დაკავშირებულ საკითხებში. ეს კი ერთ-ერთ მთავარი პრინციპის, მხარეთა თანასწორობის დარღვევას იწვევს, რაც უფრო ფუნდამენტურ საკითხს, სამართლიან სამართალს ეხება.

ნებისმიერ სასამართლო პროცესში დაცული უნდა იქნეს მხარეთა თანასწორობის პრინციპი. როგორც კანტი აღნიშნავს, სამართლიანობა უზრუნველყოფილია არა სამართლის პრინციპებით, არამედ კანონების განხორციელების დემოკრატიული პროცედურით. ანუ, სხვა სიტყვებით რომ ვთქვათ – თუ სახელმწიფომ მიიღო კანონმდებლობა, მოამზადა პროკურორები და მეორე მხარეს არ არსებობს ძალა, რომელიც დაიცავს ბრალდებულს სასამართლო პროცესში, თავად სახელმწიფოა ვალდებული საგანმანათლებლო პროგრამებითა თუ ნებისმიერი სხვა საშუალებებით მოამზადოს კვალიფიური ადვოკატები, კიბერ კრიმინალის კუთხით. თუმცა ჩვენ ყოველთვის გვაქვს არჩევანი, მხოლოდ ვისაუბროთ

იმაზე თუ რა არის სწორი, ან თავად გადავდგათ კონკრეტული ნაბიჯები სიტუაციის გამოსასწორებლად.

აღნიშნულ საკითხს კიდევ უფრო მეტ აქტუალობას სძენს ის გარემოება, რომ საკადრო და საკვალიფიკაციო პრობლემები, რომლებიც უკავშირდება სასამართლო პროცესებს შეიძლება ეროვნული უსაფრთხოების რღვევის საფუძველიც გახდეს. კერძოდ, უძველესი პერიოდიდან დღემდე მასშტაბური უკანონო სასამართლო გადაწყვეტილებები, უარყოფითი საზოგადოებრივი აზრის, მასობრივი უკმაყოფილებისა და არეულობების საფუძველი ხშირად ყოფილა, რაც შემდგომ სახელმწიფო ხელისუფლების ძალადობრივი გზით შეცვლის აქსელერატორი გამხდარა კიდეც. ფაქტობრივად სახეზე გვაქვს სადაზვერვო საქმიანობის ერთ-ერთი აქტუალური სქემა, რომელსაც სახელმწიფოები ამა თუ იმ რეგიონში თავისი სასიცოცხლო და სტრატეგიული ინტერესების გასატარებლად დღესაც აქტიურად იყენებენ.

ამრიგად, თვალსაჩინოა კიბერ უსაფრთხოების ლეგალური ასპექტების მნიშვნელობა, როგორც სწორი სამართლებრივი ინტერპრეტაციის კუთხით, ისე საკანონმდებლო შემოქმედების მიმართულებით.

დანაშაულის სპეციფიკა

ჩვენი კანონმდებლობა კიბერ დანაშაულთან მიმართებაში დახვეწის პროცესშია და ამ ეტაპისთვის არც ისე მდიდარია, რათა სრულფასოვნად აღკვეთოს კომპიუტერული დანაშაულებების დიდი ნაწილი. თუმცა ისინი მაინც არსებობენ და მუშაობენ ჰაკერების წინააღმდეგ.

მხოლოდ კანონმდებლობის არსებობა რა თქმა უნდა არ წყვეტს პრობლემას. საჭიროა სწორი სამართლებრივი ინტერპრეტაცია მიეცეს ყოველ ფაქტს. ამისათვის კი მხოლოდ სამართლის ნორმების ცოდნა არ არის საკმარისი. მთავარია იურისტის კვალიფიკაცია და შესაბამისად იურიდიული განათლების კომბინირება ამ სფეროს სპეციფიკასთან. ჩვენს კანონმდებლობაში არსებობს კომპიუტერული დანაშაულებების აღმკვეთი სპეციფიკური ხასიათის ნორმები, მაგრამ არ უნდა დაგვავიწყდეს, რომ ხშირად ეს იგივე თაღლითობაა და სულაც არ არის აუცილებელი, რომ ჰაკერის მიერ ჩადენილი დანაშაული მაინც და მაინც კიბერ დანაშაულზე არსებული ნორმებით მოწესრიგდეს. როდესაც კონკრეტული დანაშაულის ფაქტს არ აწესრიგებს კანონი, იგი შესაძლებელია მოწესრიგდეს მსგავსი სამართლებრივი ნორმით. იურისპუდენციაში ასეთ შემთხვევას, კანონის ანალოგია ეწოდება. ჰაკერის მიერ ჩადენილი დანაშაული შეიძლება განიხილოს როგორც თაღლითობა, შპიონაჟი ან შანტაჟი, რაც საკმაოდ ხშირი შემთხვევაა. რაც შეეხება უშუალოდ კომპიუტერული დანაშაულის აღმკვეთ ნორმებს, ძირითადად ისინი ინფორმაციასთან არამართლზომიერი გზით შეღწევას, მის უნებართვო მოპოვება-განადგურებასა და ვირუსების შექმნა/გამოყენებას კრძალავენ.

როგორც უკვე აღინიშნა, აუცილებელი არ არის, კომპიუტერული დანაშაულების კონკრეტული გამოვლინებები აღიკვეთოს უშუალოდ ამ სფეროზე მორგებული

ნორმებით. კანონმდებლობა ფართო ცნებაა და არ შემოიფარგლება მხოლოდ კონკრეტული ფაქტების აღკვეთით. მისი თითოეული კომპონენტი ურთიერთ კავშირშია სხვა დანარჩენთან და ასე ფორმირდება დანაშაულთან ბრძოლის მძლავრი იარაღი. ყოველივეს უკეთ გასააზრებლად საკმარისია განვიხილოთ ყველაზე გავრცელებული კომპიუტერული დანაშაულები და შემდეგ უკვე იოლად ვიპოვით კავშირს სხვა კანონდარღვევებთანაც.

1. ვებ-რესურსების (ვებ-გვერდები, ინტერნეტ-პორტალები, ფორუმები და ა.შ.) გატეხვა, შემდგომი "დიფეისით" (რესურსის ვიზუალური მხარის ან განთავსებული მასალის მოდიფიკაცია, იერსახის შეცვლა).

ცხადია თითოეული შემთხვევა, ისევე როგორც ეს კონკრეტული ძალზედ სპეციფიკურია და შეიძლება განპირობებული იყოს სხვადასხვა მიზნების მისაღწევად. თუმცა ვიხელმძღვანელოთ პოპულარული შემთხვევების მაგალითებზე.

ეს დანაშაული შეიძლება ჩადენილ იქნას როგორც ვებ-რესურსიდან კონფიდენციალური ინფორმაციის მოსაპოვებლად, ისე მისი იერსახის შესაცვლელად მესამე პირის დაკვეთით ან ტიპური მავნებლობის გამოვლინებით. დანაშაული ასეთი შედეგებით, შეიძლება კლასიფიცირებულ იქნეს როგორც:

ა. პირადი ცხოვრების ხელშეუხებლობის დარღვევა - თუ რესურსი წარმოადგენდა სოციალურ ქსელს და მასზედ რეგისტრირდებოდა მისი მომხმარებლების პირადი ხასიათის მიმოწერა;

ბ. თაღლითობა – თუ ეს ოპერაცია ნაწილი იყო მთლიანი სცენარისა და თუ იგი ემსახურებოდა თაღლითურ მიზნებს;

გ. კომერციული ან პირადი საიდუმლოს მოპოვება და გავრცელება – თუ ობიექტიდან მოპარული, მოდიფიცირებული ან წაშლილი იქნა, ან თუ იგი გავრცელდა მფლობელის უნებართვოდ და მსგავსი არამართლზომიერი გზით;

2. "კრეკინგი" - ფასიანი პროგრამული უზრუნველყოფის გაუფასურება, დაცვის მოხსნა, მისი შემდგომი გავრცელების მიზნით (მათ შორის უკანონო რეალიზაციის), რასაც "მეკობრეობის" პრობლემისაკენ მივყავართ. იგი შეიძლება განვიხილოთ შემდეგნაირად:

ა. საავტორო უფლებების დარღვევა. ძალიან ხშირად, მეკობრეები და ჰაკერები ითვისებენ სხვის მიერ წარმოებულ პროგრამულ უზრუნველყოფას. ქმნიან ფიქტიურ ბრენდებს, რათა მომხმარებელს შეუქმნან ილუზია, რომ იგი არის პირველადი მწარმოებელი და არა მეკობრე/გადამყიდველი;
ბ. კომპილირებული პროგრამის უკანონო დეკომპილაცია. უმეტეს შემთხვევაში, როდესაც პროგრამული უზრუნველყოფა დაცულია არალიცენზირებული

კოპირებისაგან, კომპიუტერული თაღლითები ხსნიას მას დაცვას. ეს კი უმეტეს შემთხვევაში სწორედ მისი უკანონო დეკომპილაციით ხდება;

გ. კომერციული ზიანის მიყენება პროგრამის მწარმოებლისადმი. ცხადია, თუ მსგავსი სცენარები წარმატებით შეასრულეს მეკობრეებმა, მწარმოებელი მნიშვნელოვან ზარალს მიიღებს, რადგან ფაქტობრივად იგი ვეღარ გაუწევს კონკურენციას თავისივე პროდუქტს, რომელიც მეორე მხარემ "შავ ბაზარზე" მეათედ ან ზოგჯერ მეასედ ფასად შეიძლება გამოიტანოს. შემცირდება მისი გაყიდვების რაოდენობა, რაც შეიძლება სავალალო შედეგით შეიძლება დასრულდეს კომპანიისთვის, რადგან ამ პროდუქტის შექმნაზე მას შეიძლება ჰყავდეს დაქირავებული პროგრამისტების ჯგუფი, რაც საკმაოდ სოლიდურ ხარჯებს უკავშირდება;

დ. მომხმარებელთა უფლებების დარღვევა. ხშირად მომხმარებელი, რომელიც ვერ ერკვევა სპეციფიკურ ტექნიკურ საკითხებში, მოტყუებული რჩება. უფრო მეტიც, ის არამხოლოდ არალიცენზირებულ პროდუქტს ღებულობს, რომელსაც მრავალი შეზღუდვა აქვს ამავე მიზეზით, არამედ შეიძლება მავნებლური პროგრამებისა და ვირუსების მთელი კომპლექტი მოყვეს ფარულად, რაც რა თქმა უნდა მას არანაკლებ დააზარალებს.

აღსანიშნავია ის ფაქტიც, რომ ვებ-გვერდების დიფეისი ხშირად გამოიყენება კიბერ ომებისა და კიბერ ტერორიზმის დროსაც. ამ დროს დიფეისები ემსახურება ინფორმაციულ პროპაგანდას, ხალხის დაშინებასა და დეზინფორმაციას. ამდენად, გარკვეულ შემთხვევებში შესაძლებელია ამ მოვლენის დაკავშირება ეროვნულ უსაფრთხოებაზე მიმართულ გამიზნულ მოქმედებადაც. ამასთან დაკავშირებით ვრცელ ინფორმაციას მიიღებთ წიგნის შემდეგ გვერდებზე, რომლებიც კიბერ ტერორიზმსა და კიბერ ომებს ეხება. ახლა კი დავუბრუნდეთ პოპულარული კიბერ კრიმინალურ აქტივობებს.

3. "კარდინგი" - საბანკო ბარათების მფლობელების საიდენტიფიკაციო რეკვიზიტების მოპარვა მისი უკანონო ფინანსური ოპერაციებში შემდგომი გამოყენების მიზნით.
დანაშაულის არსი მდგომარეობს ბარათის მფლობელზე ინფორმაციის მოპოვებაში. კერძოდ, მის საიდენთიფიკაციო მონაცემების გამოყენებაში, რომლებსაც ჰაკერი ყიდის ან თავად სარგებლობს უკანონო ფინანსური ოპერაციებისათვის. ხშირად დამნაშავეები ე.წ. სოციალურ ინჟინერიას უფრო იყენებენ, ვიდრე სპეციფიკურ ტექნოლოგიურ მეთოდებს. ეს უკანასკნელი კი დიდ როლს თამაშობს სამართლებრივი კუთხით განხილვისას და ამგვარი განფენით დანაშაული შეიძლება კლასიფიცირებული იყოს როგორც ნდობის ბოროტად გამოყენება. ეს არის ზარალის მიყენება ტყულის ან ნდობის ბოროტად გამოყენების გზით. შესაბამისად, შეგვძილია ჩამოვაყალიბოთ კონკრეტული დამოკიდებულება აღნიშნულ დანაშაულთან მიმართებაში.

ა. ზარალის მიყენება ტყულის ან ნდობის ბოროტად გამოყენების გზით – თაღლითობა;

ბ. გაყალბება, როგორც პიროვნების ისე საბანკო ოპერაციების;

გ. ინფორმაციის არამართლზომიერი გზით მოპოვება.

4. "სპამინგი" - ელექტრონული შეტყობინებების მასიური არასანქცირებული დაგზავნა სარეკლამო ან რაიმე სხვა ხასიათის ინფორმაციის გასავრცელებლად. იგი შეიძლება განხილულ იქნას მრავალი კუთხით, მაგრამ არა კონკრეტული ფაქტით, როგორც სპამინგი, რადგან ეს უკანასკნელი პრაქტიკულ დონეზე არ ითვლება დანაშაულად. ამიტომ, ბრალდების ფორმირება დამოკიდებულია კონკრეტულ ფაქტზე, თუ რა მიზნით იქნა გავრცელებული ინფორმაცია. მაგალითად, თუ საზოგადოების დაშინების მიზნით ან კონფიდენციალური ინფორმაციის გასავრცელებლად, მაშინ დანაშაული სხვა პროფილს ღებულობს და სპამინგს, როგორც ცალკეულ ფაქტს, არსებითი მნიშვნელობა შეიძლება აღარ ქონდეს.

5. ელქტრონული საფოსტო ყუთების გატეხვა და მასში არსებული ინფორმაციის გამოყენება, გავრცელება, წაშლა მოდიფიკაცია, შემდგომი შანტაჟის, ფულის გამოძალვის ან რაიმე სხვა უკანონო მიზნებისათვის. თუ დააჯამებთ ზემოთ განხილულ ქმედებებს და ქვემოთ მოცემული კანონის ნორმებს, ცხადია, რომ ეს ქმედებები ისევე შეიძლება დაისაჯოს, როგორც ნებისმიერი სხვა დანაშაული. ამ მოვლენას ასევე შეიძლება კავშორი ქონდეს არალეგალურ ოპერატიულ-ტექნიკურ ოპერაციებთან და აქ მთავარი სწორედ დანაშაულის მოტივია.

ამონარიდი საქართველოს სისხლის სამართლის კოდექსიდან

თავი XXXV – კომპიუტერული დანაშაული

მუხლი 284. კომპიუტერულ სისტემაში უნებართვო შეღწევა

1. კომპიუტერულ სისტემაში უნებართვო შეღწევა,–

ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.

2. იგივე ქმედება:

ა) წინასწარი შეთანხმებით ჯგუფის მიერ;

ბ) სამსახურებრივი მდგომარეობის გამოყენებით;

გ) არაერთგზის;

დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია,–

ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით ორიდან ხუთ წლამდე.

შენიშვნა:

1. კომპიუტერული სისტემა არის ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით, ავტომატურად ამუშავებს მონაცემებს (მათ შორის, პერსონალური კომპიუტერი, ნებისმიერი მოწყობილობა მიკროპროცესორით, აგრეთვე მობილური ტელეფონი).

2. კომპიუტერული მონაცემი არის კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ნებისმიერი ფორმით გამოსახული ინფორმაცია, მათ შორის, პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას.

3. უნებართვო, გულისხმობს უკანონოს, აგრეთვე იმ შემთხვევას, როდესაც უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაუცია უფლება ქმედების ჩამდენი პირისათვის.

4. ამ თავში მნიშვნელოვნად ითვლება 2000 ლარზე მეტი ოდენობის ზიანი.

5. ამ მუხლით გათვალისწინებული ქმედებისათვის იურიდიული პირი ისჯება ჯარიმით, საქმიანობის უფლების ჩამორთმევით ან ლიკვიდაციით და ჯარიმით.

მუხლი 285. კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება

1. კომპიუტერული პროგრამის ან/და სხვა მოწყობილობის, აგრეთვე კომპიუტერულ სისტემაში შეღწევისათვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა ამ თავითა და ამ კოდექსის 158-ე მუხლით გათვალისწინებული დანაშაულის ჩადენის მიზნით,–

ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით ვადით სამ წლამდე.

2. ამ მუხლის პირველი ნაწილით გათვალისწინებული ქმედება:

ა) წინასწარი შეთანხმებით ჯგუფის მიერ;
ბ) სამსახურებრივი მდგომარეობის გამოყენებით;
გ) არაერთგზის;
დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია,–

ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით ვადით სამიდან ექვს წლამდე.

შენიშვნა: ამ მუხლით გათვალისწინებული ქმედებისათვის იურიდიული პირი ისჯება ჯარიმით, საქმიანობის უფლების ჩამორთმევით ან ლიკვიდაციით და ჯარიმით.

მუხლი 286. კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა

1. კომპიუტერული მონაცემის უნებართვო დაზიანება, წაშლა, შეცვლა ან დაფარვა,–

ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით იმავე ვადით.

2. ამ მუხლის პირველი ნაწილით გათვალისწინებული ქმედება, აგრეთვე კომპიუტერული მონაცემის უნებართვო ჩასმა ან გადაცემა, რამაც კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხება გამოიწვია,–

ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით ვადით სამ წლამდე.

3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება:

ა) წინასწარი შეთანხმებით ჯგუფის მიერ;
ბ) სამსახურებრივი მდგომარეობის გამოყენებით;
გ) არაერთგზის;
დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია,–
ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით სამიდან ხუთ წლამდე.

ამ მუხლით გათვალისწინებული ქმედებისათვის იურიდიული პირი ისჯება ჯარიმით, საქმიანობის უფლების ჩამორთმევით ან ლიკვიდაციით და ჯარიმით.

ზემოთ აღნიშნული სისხლის სამართლებრივი ნორმები აწესრიგებს უშუალოდ კომპიუტერულ დანაშაულებებთან დაკავშირებულ საკითხებს. თუმცა, ზღვარი პირობითია და ხშირად კომპიუტერით ჩადენილი დანაშაული სხვა პროფილს იძენს, რადგან კიბერ დანაშაულებათა უმრავლესობა ინფორმაციის უკანონო მოპოვება/გამოყენებას ეხება, ხოლო დამდგარი შედეგი უმეტეს წილად მხოლოდ გარემოებებია.

პირადი ცხოვრების ხელშეუხებლობა

ჰაკერების მიერ ჩადენილი დანაშაულების სახით ეს პრობლემა საკმაოდ აქტუალურია. ეს ყოველივე ქმნის ერთ-ერთ ყველაზე მნიშვნელოვან პრობლემას საზოგადოებისათვის. პრობლემას პირადი ცხოვრების ხელშეუხებლობისა, რომელიც ამ ბოლო დროს საზოგადოების მტკივნეულ თემად იქცა. ამაზე მინდა ცალკე ვისაუბრო, რადგან ასე თუ ისე ეს კრიმინალური პრეცედენტი განსხვავდება ჰაკერების მიერ ხშირად ჩადენილი სხვა დანაშაულებისაგან. განსხვავდება, მაგრამ ისეთივე დასჯადია, როგორც სხვა დანაშაულები. ეს დანაშაული იგივე კვალიფიკაციას იძენს, როგორც ელექტრონული ფოსტის გატეხვა და ზოგადად პირადი ხასიათის ინფორმაციის არამართლზომიერი გზით მოპოვება, ეს ყოველივე კი განხილულია საქართველოს კონსტიტუციაში, როგორც ადამიანის ფუნდამენტური უფლება-თავისუფლება.

ამონარიდი საქართველოს კონსტიტუციიდან - თავი მეორე, მუხლი 20
ადამიანის ძირითადი უფლებანი და თავისუფლებანი

1. ყოველი ადამიანის პირადი ცხოვრება, პირადი საქმიანობის ადგილი, პირადი ჩანაწერი, მიმოწერა, საუბარი სატელეფონო და სხვა სახის ტექნიკური საშუალებით, აგრეთვე ტექნიკური საშუალებებით მიღებული შეტყობინებანი ხელშეუხებელია. აღნიშნული უფლებების შეზღუდვა დაიშვება სასამართლოს გადაწყვეტილებით ან მის გარეშეც, კანონით გათვალისწინებული გადაუდებელი აუცილებლობისას.

რასაკვირველია, კონსტიტუციური განსაზღვრების გარდა, ადამიანის პირადი ცხოვრების ხელყოფასთან დაკავშირებული დანაშაულები წარმოადგენს საქართველოს სისხლის სამართლის კოდექსის რეგულირების საგანსაც. კერძოდ, სსსკ XXII თავი სრულად ეძღვნება ამ საკითხს.

ამონარიდი საქართველოს სისხლის სამართლის კოდექსიდან - თავი XXIII
დანაშაული ადამიანის უფლებებისა და თავისუფლებების წინააღმდეგ

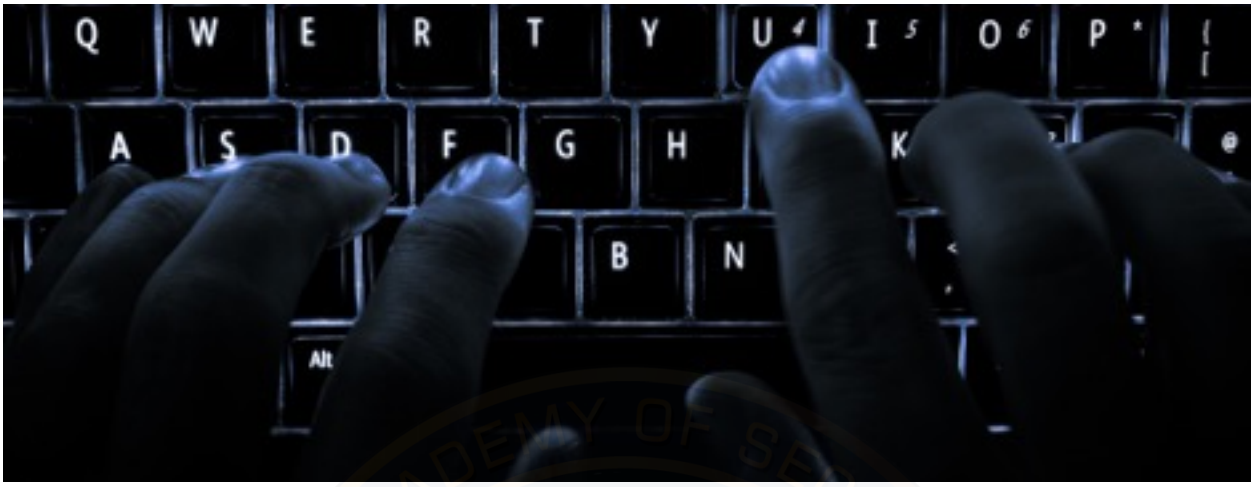
მუხლი 157. პირადი ან ოჯახური საიდუმლოს ხელყოფა
1. პირადი ან ოჯახური საიდუმლოს უკანონოდ მოპოვება, შენახვა ან გავრცელება,
-ისჯება ჯარიმით ანდა გამასწორებელი სამუშაოთი ვადით ერთ წლამდე ან/და თავისუფლების აღკვეთით იმავე ვადით.
2. პირადი ან ოჯახური საიდუმლოს უკანონოდ გამოყენება ან/და გავრცელება ამა თუ იმ ხერხით გავრცელებულ ნაწარმოებში, მასობრივი მაუწყებლობით ან სხვა საჯარო გამოსვლისას,
-ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.
3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება:
ა) ანგარებით;
ბ) არაერთგზის;

გ) იმის მიერ, ვისაც სამსახურებრივი მდგომარეობის, პროფესიული საქმიანობის ან სხვა გარემოების გამო ევალებოდა ამ საიდუმლოს დაცვა;
დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია,-
ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით სამ წლამდე ანდა თავისუფლების აღკვეთით ვადით სამ წლამდე, თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევით ვადით სამ წლამდე ან უამისოდ.

მუხლი 158. კერძო საუბრის საიდუმლოების დარღვევა
1. კერძო საუბრის უკანონოდ ჩაწერა ან მიყურადება ტექნიკური საშუალების გამოყენებით,
-ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.
2. კერძო საუბრის ტექნიკური საშუალებით მიღებული ჩანაწერის ანდა ტექნიკური საშუალებით მოპოვებული ინფორმაციის უკანონოდ გამოყენება ან გავრცელება,-
ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით სამ წლამდე ანდა თავისუფლების აღკვეთით ვადით ერთიდან სამ წლამდე.
3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება:
ა) ანგარებით;
ბ) არაერთგზის;
გ) რამაც მნიშვნელოვანი ზიანი გამოიწვია;
დ) სამსახურებრივი მდგომარეობის გამოყენებით,
-ისჯება თავისუფლების აღკვეთით ვადით ორიდან ხუთ წლამდე, თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევით ვადით სამ წლამდე.

მუხლი 159. პირადი მიმოწერის, ტელეფონით საუბრის ან სხვაბვარი ხერხით შეტყობინების საიდუმლოების დარღვევა
1. პირადი მიმოწერის ან საფოსტო გზავნილის, ტელეფონით ან სხვა ტექნიკური საშუალებით საუბრის ანდა ტელეგრაფით, ფაქსით ან სხვა ტექნიკური საშუალებით მიღებული ან გადაცემული შეტყობინების საიდუმლოების უკანონოდ დარღვევა,
-ისჯება ჯარიმით ან საზოგადოებისათვის სასარგებლო შრომით ვადით სამოციდან ას ოც საათამდე ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.
2. იგივე ქმედება:
ა) ანგარებით;
ბ) არაერთგზის;
გ) სამსახურებრივი მდგომარეობის გამოყენებით;
დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია,
გ) სამსახურებრივი მდგომარეობის გამოყენებით;
დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია,
-ისჯება ჯარიმით ან თავისუფლების აღკვეთით ვადით სამ წლამდე, თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევით ვადით სამ წლამდე.

ჰაკერები და სპეცსამსახურები კიბერ სივრცეში



ტერმინი ჰაკერი ნობელის პრემიის მფლობელ ცნობილ მათემატიკოსს ჯონ ნეშს (John Nash) ეკუთვნის. თავდაპირველი მნიშვნელობით ეს სიტყვა ნიშნავდა ადამიანს, რომელიც მოკლე გზას პოულობდა პრობლემის გადასაწყვეტად.

პირველი ჰაკერული ინცინდენტი 1972 წელს მოხდა, როდესაც ჯონ დრეიპერმა სასტვენის საშუალებით სატელეფონო სადგურის მოტყუება მოახერხა (იხ. ჰაკერების შესახებ ჯონ დრეიპერი)

ადამიანის მთავარი ღირსება ინდივიდუალიზმია. ის გამოარჩევს მას სხვებისაგან. ინდივიდუალიზმისთვის საჭიროა არ გავდე სხვებს, იყო დამოუკიდებელი აზროვნებასა და მოქმედებაში, დაარღვიო სტერეოტიპები, გაცდე ზღვარს, რასაც პარადოქსია, მაგრამ ჩვენ თვითონვე ვქმნით – დაახლოებით ასე ჟღერს ჰაკერის მოტივაცია. მართლაც, მათ საქმიანობას საკმაოდ დიდი ფილოსოფიური ბაზაც გააჩნია.

ადამიანი გამუდმებით ცდილობს თავი შეიზღუდოს და ამასთან იყოს თავისუფალი. ჩვენ ვქმნით კანონებს, რომლებსაც თავადვე ვარღვევთ. ვქმნით ვირტუალურ სივრცეს, ბარიერებს ინტერნეტში, რომლებსაც ჩვენვე ვლახავთ. ბარიერების გადალახვა კი განთავისუფლების გრძნობას, გაქცევის ილუზიას გავს. ეს ადამიანური ბუნებაა და მას ვერავინ შეცვლის.

ჰაკერებიც ამ ცხოვრებისეული კანონზომიერების ერთგვარი მიმდევრები არიან. ქმნიან სივრცეს საზღვრებით და თვითონვე არღვევენ მას. თუმცა მათი მოქმედება მხოლოდ ამ კანონზომიერებით არ არის განპირობებული. მთავარ მოტივატორად მეტწილად მაინც მატერიალური ასპექტები გვევლინება. ძნელია იმის გარკვევა თუ ვინ და რატომ აკეთებს ამას. მაგრამ ერთი რამ უდაოა, მათ ეს დღემდე კარგად გამოსდით და სწორედ ამიტომაც ისინი წარმოადგენენ მთავარ საფრთხეს ინფორმაციული უსაფრთხოების სფეროში.

თუ გავითვალისწინებთ, რომ ჰაკერული მოქმედებები ხშირად ატარებენ ისეთივე ხასიათს და ემსახურებიან ისეთივე მიზნებს, როგორც სხვადასხვა სპეცსამსახურების სადაზვერვო აქტივობები, მაშინ ნათლად დავინახავთ, რომ

ჰაკერები ერთ-ერთ ყველაზე ეფექტურ რგოლს შეიძლება წარმოადგენდნენ სადაზვერვო საქმიანობის ორგანიზაციაშიც.

როგორც დამნაშავეები, ჰაკერები საინტერესო, ამოუცნობი და რთულად პროგნოზირებადი სუბიექტები არიან. დამნაშავის ნებისმიერი ტიპი ისევე როგორც ეს კონკრეტული, ფორმირდება დანაშაულის პრეცედენტით. შემდეგ ეს პრეცედენტი ხშირ შემთხვევად იქცევა, დამნაშავეც იხვეწება და ვითარდება. დანაშაულებრივი მოქმედების პარალელურად იგი ცდილობს თავის ქცევას გამართლება უპოვოს და ამ ძიებაში ამყარებს საკუთარ მოტივაციას. სწორედ მოტივაცია არის ის ხედვა, რაც მათ აქვთ ცხოვრებაზე.

ჰაკერები ყოველთვის ვითარდებოდნენ ტექნოლოგიური პროგრესის პარალელურად და რაც მთავარია ისინი თანდათან იცვლებოდნენ. მათ უყალიბებოდათ და ეცვლებოდათ ფასეულობები. ბოლოს მოხდა ის, რომ შესაცვლელი აღარაფერი დარჩათ. მათ აღარ გააჩნიათ ფასეულობები. მათი იდეოლოგიური წინაპრები დიდი ინტელექტუალები იყვნენ, რომლებიც ინფორმაციული თავისუფლების იდეის გარშემო იბრძოდნენ. ანუ, იმ დროინდელი ჰაკერების მოტივი მატერიალურისგან შორს იყო. დღეს კი ყველაფერი შეიცვალა.

ვირტუალურმა გაუსწრო რეალურს და კომპიუტერი დანაშაულის იარაღად იქცა. ჰაკერები არსებობენ იმ სამყაროში რომელსაც თვითონვე ქმნიან და რომელიც ერთგვარი თავშესაფარია მათთვის. ისინი ცხოვრობენ კიბერსივრცეში, ციფრების გარემოცვაში, ნულებსა და ერთებს შორის ცხოვრობენ, შესაბამისად მათთვის ინფორმაციის მოძიება პრობლემას არ წარმოადგენს. ისინი არ გვანან ჩვეულებრივ ადამიანებს.

სად უნდა ვეძებოთ ასეთი საშიში იარაღის ფორმირების მიზეზი?.. მხოლოდ ინტერესი?!. ფული?!. როგორ იქცევა ადამიანი ვირტუალურ დამნაშავედ?.. – როდესაც ადამიანი ვერ ახერხებს თვითრეალიზაციას, საკუთარი ძალების სწორი მიმართულებით წარმართვას, იგი პოტენციური დამნაშავე ხდება, რადგან მისი შესაძლებლობები, როგორც წესი დანაშაულებრივ ქმედებებში იოლად რეალიზებადია. ასევე ყალიბდებიან ჰაკერების უმრავლესობაც. ისინი გრძნობენ, რომ ბევრად მეტი იციან და შეუძლიათ ვიდრე სხვებს, რომ ნელ-ნელა ყველაფერი რაც გარშემო ხდება მათთვის მომაბეზრებელი და უინტერესო ხდება. უფრო მეტს თხოვენ საკუთარ თავს და უფრო მეტი სურთ ვიდრე არსებულ გარემოში შეუძლიათ მიიღონ. ამ დროს კი მათ ცხოვრებაში ჩნდება კომპიუტერი. ინტერნეტი ერთგვარი თავშესაფარია ასეთი ადამიანებისთვის. ისინი ნელ-ნელა სწავლობენ მასთან ურთიერთობას და თანდათან ხვდებიან, რომ კომპიუტერიც უშვებს შეცდომებს, რაც უფრო აახლოებს მას ადამიანთან. ნელ-ნელა ყალიბდება კანონზომიერებები, კანონები, რომლებიც ბოლოს ერთად იყრიან თავს და დიდ ცოდნად, მძლავრ იარაღად იქცევიან. ზუსტად არავინ იცის ვინ სად და როგორ იწყებს... მათთვის ინტერნეტი მეორე სახლია, ახალი სამყარო, სადაც ყველას იცნობენ, მიუხედავად იმისა, რომ უმრავლესობა არც კი უნახავთ.

ჰაკერთა ტიპები

თეთრ ქუდიანი

ნაცრისფერ ქუდიანი

შავ ქუდიანი

ინტერნეტის გამოჩენის შემდეგ არც ისე დიდი ხნის წინ, გაჩნდნენ ჰაკერებიც. თუმცა მათი როლი ბევრად უფრო პოზიტიური იყო მაშინდელ საზოგადოებაში, ვიდრე ახლა. ისინი იყვნენ გენიოსები, რომლებსაც შეეძლოთ არაორდინალურად აზროვნება და ურთულესი პრობლემების გადაწყვეტა ან უბრალოდ მაღალკვალიფიცირებული სპეციალისტები. თუმცა გავიდა წლები და მათი საქმიანობა, ისევე როგორც იმიჯი, მკვეთრად შეიცვალა. ახლა ისინი ნადირობენ ინფორმაციაზე განურჩევლად მისი მნიშვნელობისა, იყენებენ მას შანტაჟისათვის, ტეხავენ და ავრცელებენ ფასიან პროგრამებს, რითაც აუფასურებენ პროგრამისტების საქმიანობას. წერენ ვირუსებს, ინფრასტრუქტურას და ა.შ. ახლანდელი ჰაკერები ძალიან განსხვავდებიან ადრინდელთაგან. ისინი გენიოსები იყვნენ, მართალია მათშიც იყვნენ ადამიანები ბოროტი ზრახვებით, მაგრამ ისინი ტერორისტები არ ყოფილან.

ჰაკერებს, ისევე როგორც დანარჩენ კრიმინალებს თავისებური წარმოდგენა აქვთ საკუთარ საქმიანობაზე და ამყარებენ მას ერთგვარი თვითგამართლებით. მათ შემთხვევაში ეს თვითგამართლება მიზანია - ინფორმაციული თავისუფლება. ეს ხშირ შემთხვევაში იმას გავს, როცა აგრესორი ქვეყანა თავის სამხედრო მოქმედებებს განმანთავისუფლებელ ოპერაციას უწოდებს. რაც შეეხება ჩრდილს მიფარებულ ჰაკერებს, დღეს მათი უმრავლესობა უმსხვილეს კომპანიებს ფლობს ინფორმაციული უსაფრთხოების კონსალტინგის ბიზნესში, მაგრამ ისტორიამ მაინც შემოინახა მათი წარსული, რომელიც საკმაოდ განსხვავდება დღევანდელი რეალობისგან. ახალ რეალობაში, სადაც ახალი გამოწვევები და საფრთხეებია, მოხდა ერთგვარი მათი გადაჯგუფებები და ჰაკერთა კატეგორიზაცია შემდეგნაირია:

სკრიპტერები

თინეიჯერები, რომლებსაც გააჩნიათ საბაზო უნარები კომპიუტერულ პროგრამირებაში და ამას გასართობად ან პოპულარობისთვის აკეთებენ. სპეცსამსახურებისთვის ისინი პერსპექტიული აგენტურის ძალზედ მომხიბვლელ რესურსს წარმოადგენენ.

ჰაკერთა დაჯგუფებები

სკრიპტერების ჯგუფი, რომლებსააც გააჩნიათ მეტი გამოცდილება, ახალი უნარები და მძლავრი ნეთვორქინგი. ისინი კონკრეტული მიზნების გარშემო ერთიანდებიან.

ჰაქტივისტები

საერთო სოციალური ან პოლიტიკური მოტივის მქონე ჰაკერთა ჯგუფი. ხშირად მათი საქმიანობა დაკავშირებულია სადაზვერვო ორგანიზაციის ისეთ მიმართულებაზე, რომელიც დაკავშირებულია კონსტიტუციური წესწყობილების რღვევასთან. ამდენად, ეს ჯგუფი განსაკუთრებით საყურადღებო და სარისკო რესურსს ჯგუფს მიეკუთვნებიან.

თეთრ ქუდიანი ჰაკერები

პირები, რომლებიც მინიმალურად იყენებენ ტექნიკურ საშუალებებს და ისე აღწევენ იგივე მიზნებს, რასაც სხვა ტიპის ჰაკერები. მათი მთავარი ინსტრუმენტი სოციალური ინჟინერიის მეთოდია. სადაზვერვო კუთხით ისინი გამოიყენებიან ისეთ მიმართულებებზე, რომლებიც მოიცავენ ოპერატიულ-ტექნიკურ ღონისძიებებს.

შავ ქუდიანი ჰაკერები

სხვადასხვა კომპეტენციის მაღალკვალიფიციური სპეციალისტები: პროგრამისტები, ქსელისა და მონაცემთა ბაზების ადმინისტრატორები, რომლებიც თავიანთ უნარებსა და ცოდნას იყენებენ ისეთ მოწყვლად ადგილებზე, როგორიც არის სახელმწიფო და კერძო სექტორის მსხვილი ინფრასტრუქტურა. ყოველივე კი სახელმწიფოსთვის სადაზვერვო და კონტრსადაზვერვო დისბალანსის ინდიკატორიც შეიძლება იყოს.

ნაცრისფერ ქუდიანი ჰაკერები

აღნიშნული კატეგორია აერთიანებს შავ და თეთრ ქუდიანი ჰაკერების კომპეტენციებს და ემსახურება სხვადასხვა სისტემებში მოწყვლადი ადგილების აღმოჩენას. ისინი ამას უსაფრთხოების ამაღლებისთვის აკეთებენ და ხშირად გვევლინებიან როგორც დამოუკიდებელ კონსულტანტებად, ისე სხადასხვა ორგანიზაციის წარმომადგენლებად, რომლებიც ე.წ. ეთიკური ჰაკინგის სერვისს წარმოადგენენ.

ორგანიზებული კრიმინალური დაჯგუფებები

ჰაკერთა ჯგუფი, რომლებიც ხშირად იმართებიან ჩვეულებრივი კრიმინალების მიერ, ისინი გამოირჩევიან კომპიუტერული თაღლითობის დახვეწილი მეთოდებით და მაქსიმალურად არიდებენ თავს კანონსა და სამართალდამცავებს. თუ გავითვალისწინებთ იმ გარემოებას, რომ კრიმინალები თავად წარმაოდგენენ სადაზვერვო სამსახურების შესწავლისა და ზემოქმედების აქტიურ ჯგუფს, მათი გამოყენებაც სადაზვერვო კუთხით განსაკუთრებით ნაკლებად დემოკრატიულ ქვეყნებშია გაიოლებული.

სამთავრობო დაფინანსების ჯგუფები

იგივე State Sponsored Cyber Crime, გამოირჩევა მძლავრი კომპიუტერული ინფრასტრუქტურით, მდიდარი რესურსებით და სახელმწიფოს დაკვეთით. მათი სამიზნე მოწინააღმდეგე ქვეყნის კრიტიკული ინფრასტრუქტურა, სამხედრო და საფინანსო ინსტიტუტებია.

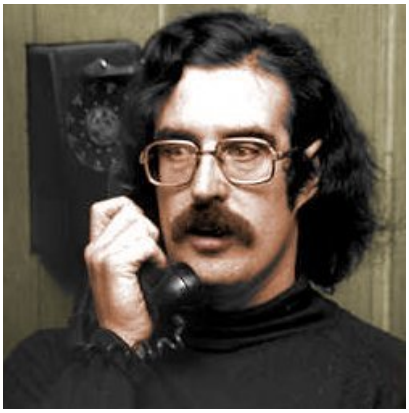
ავტომატიზებული ინსტრუმენტები

პროგრამული უზრუნველყოფა ასევე შეიძლება იყოს გააზრებული ერთგვარ ჰაკერად თუ იგი ასრულებს იმავე ფუნქციას, რასაც ნებისმიერი ზემოთ მოცემული ტიპის ჰაკერი. ამგვარი შემთხვევა კი საკმაოდ ხშირია ახალი ტიპის ვირუსებისა და მავნებლური პროგრამების სახით, რომელიც კოლოსალური სისწრაფით ვრცელდება გლობალურ ქსელში ყოველდღიურად.

ამრიგად, ჰაკერების როლი სპეცსამსახურების, განსაკუთრებით სადაზვერვო და კონტრსადაზვერვო მიმართულებით შეუცვლელია, რადგან ტექნოლოგიური მიდგომა ყოველთვის უფრო ნაკლებ რისკიანია, სადაც შესაძლებელია დისტანციური ზემოქმედება, მოითხოვება ნაკლები დროითა და ფინანსური რესურსების გამოყენება და რაც ყველაზე მთავარია მაქსიმალურად უზრუნველყოფილია ქმედებათა შენიღბვა ე.წ. სტელსის რეჟიმი.

როგორც რეალურ დროში, ისე შემდგომი მოკვლევის ეტაპზე შეუძლებელია დეტალების სრულფასოვნად გარკვევა. ყოველივე კი სრულად თავსებადია სადაზვერვო და კონტრსადაზვერვო მოქმედებების მთავარ პრინციპებთან. ორივე მოქმედება ყოველთვის ემსახურება ამა თუ იმ სახელმწიფოს ინტერესებს, შესაბამისად ვიტალური მნიშვნელობა გააჩნია თავად ამ სახელმწიფოს სრული ანონიმურობის შენარჩუნებას.

ცნობილი ჰაკერები



ჯონ დრეიპერი (**John Draper**)

ჯონ დრეიპერმა სახელი გაითქვა, როგორც პირველმა ფრიკერმა (ჰაკერი, რომელიც ტეხავს ფასიან სატელეფონო სერვისებს). მან შეიმუშავა საკუთარი მეთოდები, რითაც შეეძლო უფასოდ ესარგებლა ნებისმიერი სატელეფონო სერვისით. მისი ერთ-ერთი ყველაზე პოპულარული თაღლითობა ხორციელდებოდა სასტვენის საშუალებით, რის გამოც მას Cap'n Crunch-ი (კაპიტანი სასტვენი) შეარქვეს. 1972 წელს, აშშ-ს გამოძიების ფედერალური ბიუროს აგენტებმა მიაგნეს

დრეიპერს და დააკავეს. თუმცა მას ციხეში ყოფნის დროსაც არ შეუწყვეტია თავისი საქმიანობა. იმ პერიოდში დაწერა პროგრამა EasyWriter, რომელიც პირველი ტექსტური რედაქტორი იყო მსოფლიოში. ეს პროდუქტი მან კომპანია IBM-ს მიყიდა. იგი ერთ დროს მილიონერიც გახლდათ, მაგრამ მალევე გაკოტრდა.

ციხიდან გამოსვლის შემდეგ, იგი მსოფლიოს მრავალ ადგილას მოგზაურობდა და დაეძებდა სამსახურს, სადაც ბოლომდე შეძლებდა თვითრეალიზაციას. საბოლოოდ მან გადაწყვიტა, რომ დრო იყო თაღლითობისათვის თავი დაენებებინა და ჰაკერებს აქტიური ბრძოლა გამოუცხადა.

ჯონმა შექმნა საკუთარი კომპანია, რომელიც დღემდე აწარმოებს პროგრამულ უზრუნველყოფას. ასეთი მკვეთრი გადახვევა გზიდან, მრავალწლიანი ჰაკერობის შემდეგ, ომის გამოცხადება მათთვის, რომელთა რიგებს სულ ცოტა ხნის წინ თავადვე ეკუთვნოდა, ბევრისთვის შეიძლება გაუგებარი იყოს, მაგრამ ჯონმა ეს გააკეთა იმის შემდეგ, რაც გაიგო თავისუფლების ფასი, იმის შემდეგ რაც მიხვდა, რომ თავისი შესაძლებლობების კარგი საქმისთვის გამოყენებით არანაკლებ ფულს იშოვნიდა, მაგრამ რაც მთავარია, ფულთან ერთად იგი საზოგადოებაში დაიმკვიდრებდა თავს და ექნებოდა კარგი იმიჯი. არა იმ საზოგადოებაში, რომელშიც ამდენი ხნის მანძილზე იყო, არა ვირტუალურ სივრცეში, არამედ ნამდვილ, რეალურ სამყაროში. ეს მისთვის ძალიან მნიშვნელოვანი იყო, ამდენი წლის პატიმრობის, უიმედობის და მძიმე პერიოდის შემდეგ.

რობერტ მორისი **(Robert Morris)**

რობერტ მორისი ლეგენდად შემორჩა ჰაკერებს შორის. 1988 წელს, როცა რობერტი ჯერ კიდევ კორნელის უნივერსიტეტის სტუდენტი იყო, მსოფლიოში პირველი "ჭიაყელა" პროგრამა შექმნა. ამ პროგრამის ამოქმედების შედეგი კოლოსალური იყო, მან ერთდროულად ექვსი ათასი კომპიუტერის პარალიზება აშშ-ს ტერიტორიაზე მოახდინა. ამჟამად რობერტ მორისი მასაჩუსეტსის ტექნოლოგიური ინსტიტუტის პროფესორი გახლავთ. გარდა იმისა, რომ იგი პირველი ასეთი პროგრამის ავტორია, იგი ასევე პირველი პრეცედენტია იურისპუდენციაში და პირველი ადამიანი მსოფლიოში ვისაც კომპიუტერულ თაღლითობაში წაეყენა ბრალდება. თავდაპირველად მას თავისუფლების სამი წლით აღკვეთა მიესაჯა, ხოლო შემდგომ სასამართლო 10 400 ამერიკული დოლარის ოდენობის ჯარიმითა და 400 საათი საზოგადოებისათვის სასარგებლო საქმის მისჯით დაკმაყოფილდა.

კევინ მიტნიკი **(Kevin Mitnick)**

მისი სახელი დღემდე ყველამ იცის. კევინი მსოფლიოში ერთ-ერთი ყველაზე ცნობილი ჰაკერია. მან პირველად, ჯერ კიდევ ბავშობაში მისივე სკოლის კომპიუტერული ქსელი გატეხა. იგი ამაზე არ შეჩერებულა, მალევე გადავიდა სატელეფონო თაღლითობებზე, გატეხა ასობით სხვადასხვა კომპიუტერული ქსელი, პროგრამა და სახელი გაითქვა, როგორც საუკეთესო ჰაკერმა. კევინ მიტნიკი ლოს ანჯელესში იზრდებოდა, მაშინ როცა პერსონალური კომპიუტერების ინდუსტრია ფეხს იკიდებდა. უნდერგრაუნდის კულტურა სატელეფონო თაღლითობებით იყო გაჯერებული. სატელეფონო სერვისები კი ანალოგურიდან დიჯიტალურში გადასვლის პროცესში იყო. მან კომპიუტერისა და მოდემის გამოყენებით შესაძლებელი გახადა სატელეფონო სადგურის გამანაწილებლის მართვა, რასაც ერთ-ერთმა პირველმა ჯონ დრეიპერმა შეუწყო ხელი. კევინმა კი ამგვარი მანიპულაციები ახალ საფეხურზე აიყვანა და მეცნიერულ დონეზე შეისწავლა.

სწორედ ეს იყო მისი პირველი ნაბიჯები დიდ გზაზე, რომელმაც ამერიკის ყველაზე ცნობილ და მოთხოვნად ჰაკერობამდე მიიყვანა. განსხვავებით სხვა ჰაკერებისგან, კევინმა სატელეფონო სერვისებს გაცილებით დიდი გამოყენება უპოვა, ვიდრე მხოლოდ უფასო საერთაშორისო ზარები იყო. მან ამ სერვისების საშუალებით გაიხსნა ფანჯარა სხვა ადამიანების პირად ცხოვრებაში. იგი ძირითადად სამართალდამცავი და ძალოვანი უწყებების მიერ სპეციალურად შექმნილ ტექნიკურ საშუალებებზე გადიოდა, რომლითაც შემდეგ სატელეფონო მოსმენებს, პელინგაციასა და სხვა ოპერაციებს ატარებდა. ეს მას ეხმარებოდა მინიმალურ დისტანციაზე მიახლოვებოდა ფედერალურ ბიუროს და შემდეგ ვირტუოზულად დასხლტომოდა ხელიდან. აზარტი და ამბიციები კევინის მთავარი დრაივი და ამავდროულად სუსტი წერტილი იყო. მიტნიკის დევნა ფედერალური ბიუროს მიერ და მისი გაქცევები პოპულარობაზე მხოლოდ საუკეთესოდ მოქმედებდა. მისი ერთ-ერთი დაკავება 1983 წელს სამხეთ კალიფორნიის უნივერსიტეტში განხორციელდა, საიდანაც მან ინტერნეტის მაშინდელ ჩანასახში, ARPAnet-ში შეაღწია. იმ დროისათვის ის მხოლოდ საუნივერსიტეტო სამეცნიერო კვლევითი ქსელი იყო მაღალტექნოლოგიური პროექტებისათვის, რომელიც ამერიკის თავდაცვის დეპარტამენტის მიერ შეიქმნა.

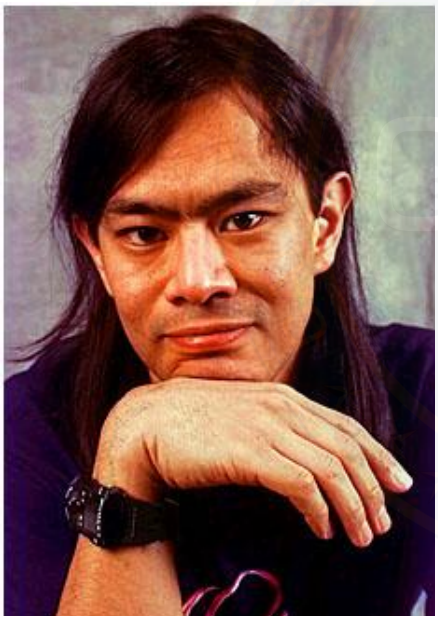
სამართალთალდამცავების მიერ მისი აყვანის მომენტში იგი პენტაგონის კომპიუტერულ სისტემაში ცდილობდა შეღწევას. მას 6 თვით არასრულწლოვანთა კოლონიაში თავისუფლების აღკვეთა მიუსაჯეს. განთავისუფლების შემდეგ კი მას "X HACKER" –ს უწოდებდნენ.

რათქმაუნდა არც ერთი მისი დაკავება არ გამხდარა ბარიერი კევინისთვის შეეწყვიტა თავისი დაწყებული საქმე. უფრო მეტიც, ეს ყოველივე უფრო მეტ მოტივს

აძლევდა. იგი კვალს თითქმის არ ტოვებდა და მისი გაშიფვრა წარმოუდგენელი იყო. თუმცა საბოლოოდ იგი კომპიუტერული უსაფრთხოების ერთ-ერთმა ექსპერტმა, ცუტომუ შიმამურამ გაშიფრა, რომელიც კევინის ყველაზე დასამახსოვრებელი კომპიუტერული თაღლითობის მსხვერპლი იყო.

როგორც ყველა დიდი ჰაკერი, ახლა კევინიც მეორე მხარეს იბრძვის. მას კარგად იცნობენ ა.შ.შ-ს კონგრესშიც კი და იგი ხშირად დამოუკიდებელი ექსპერტის რანგში გვევლინება.

კევინ მიტნიკი იმ ადამიანების ნაწილს განეკუთვნება ვინც ისტორიას ქმნის და აძლევს სხვა ადამიანებს ინსპირაციას. სწორედ ამგვარმა ადამიანებმა წამოიწყეს ტექნოლოგიური პროგრესი და მცირე ნაბიჯები ნახტომებად გადააქციეს. რასაკვირველია მისი ბიოგრაფია სავსეა დანაშაულებებით, მაგრამ იგი აქაც მნიშვნელოვნად გვეხმარება, მოგვცა რა საუკეთესო ქეისები და მაგალითები, რომლებიც შეუცვლელია კიბერ კრიმინალის შესწავლაში. მანვე გამოსცა წიგნი: ”სიცრუის ხელოვნება”, რომელმაც ფარდა ახადა სოციალური ინჟინერიისა და თაღლითობის უამრავ მეთოდს.



ცუტომუ შიმამურა **(Tsutomu Shimomura)**

ერთ-ერთი ყველაზე ცნობილი კომპიუტერული ექსპერტი.

ცუტომუ დაიბადა იაპონიის ერთ-ერთ ყველაზე გამორჩეულ ოჯახში. მისი მამა ოსამუ შიმამურა 2008 წლის ნობელის პრემიის მფლობელია. ცუტომუ მალევე მოხვდა აშშ-ში. კერძოდ, პრინსტონში, ნიუ ჯერსის შტატში, სადაც დაამთავრა პრინსტონის საშუალო სკოლა. კარიერული ზრდის გზაზე მან თავიდანვე მნიშვნელოვანი ნაბიჯები გადადგა. სწავლის დასრულებისთანავე იგი მოხვდა ლოს ალამოსის ეროვნულ ლაბორატორიაში, სადაც ფიზიკის მიმართულებით განაგრძო მოღვაწეობა. 1989 წელს იგი კალიფორნიის უნივერსიტეტის მკვლევარი მეცნიერი გახდა კომპიუტერული ფიზიკის დარგში. მალევე იგი სან დიეგოს სუპერ კომპიუტერების გამოთვლით ცენტრში დაწინაურდა. იგი ავტორიტეტული ექსპერტი გახდა კომპიუტერული უსაფრთხოების საკითხებში და აშშ-ს ეროვნული უშიშროების სააგენტოზე მუშაობდა.

ცუტომოუ მოღვაწეობდა სან-დიეგოს კომპიუტერულ ცენტრში, როდესაც 1994 წელს კევინ მიტნიკმა გატეხა მათი კომპიუტერული ქსელი და მოიპარა ინფორმაცია ფიჭურ კავშირსა და ცენტრის საიდუმლო ტექნოლოგიების შესახებ. კევინმა ეს არ იკმარა და ცუტომუს კომპიუტერშიც შეძლო შეღწევა. ცუტომუსთვის ეს მოთმინების

ბოლო წერტილი იყო, მან კევინზე ნადირობა დაიწყო, რასაც ბოლოს კევინის დაკავება მოჰყვა.

ამასთან დაკავშირებით 1996 წელს მან ჯონ მარკოფთან ერთად წიგნიც დაწერა Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw – By The Man Who Did It (დაკავება: ამერიკის ყველაზე მოთხოვნადი კომპიუტერული დამნაშავის დევნა და დაკავება – ადამიანისგან, რომელმაც ეს გააკეთა) რომლის მიხედვითაც ჰოლივუდში საკმაოდ წარმატებული ფილმის გადაიღეს. ცუტომუ არამხოლოდ წარმატებული ექსპერტია უსაფრთხოების სფეროში, არამედ კარგი პრომოუტერიც, რადგან სწორედ მან გახადა ეს ისტორია ასეთი პოპულარული.

ვლადიმერ ლევინი **(Владимир Левин)**

ვლადიმერ ლევინი ეროვნებით რუსი კომპიუტერული ექსპერტია, რომელმაც Citibank-ის კომპიუტერული ქსელი გატეხა და მილიონობით აშშ დოლარი მოიპარა. თავდაპირველად ვლადიმერი ცნობილი იყო როგორც მათემატიკოსი, რომელსაც ხარისხი გააჩნდა ბიოქიმიაში და მოღვაწეობდა სანკ პეტერბურგის სახელმწიფო ინსტიტუტში.

1994 წელს მან ჰაკერული გზით შეაღწია სითიბანკის უმსხვილეს საბანკო ანგარიშებში და მათგან გადარიცხა თანხები თავის თანამზრახველების ანგარიშებზე ფინეთში, ნიდერლანდებში, გერმანიაში, აშშ-სა და ისრაელში. მათგან სამი თანამზრახველი დაკავებულ იქნა თელავივში, როტერდამსა და სან ფრანცისკოში. დაკითხვისას მიცემული ჩვენების მიხედვით ვლადიმერი მუშაობდა კომპიუტერულ პროგრამისტად სანკ პეტერბურგის ერთ-ერთ კომპიუტერულ კომპანიაში – AO Saturn. 1995 წლის მარტში იგი შემჩნეულ იქნა ლონდონის აერპორტში, სადაც დიდი ბრიტანეთის ინტერპოლმა დააკავა კიდეც, რის შემდეგაც ადვოკატები ეწინააღმდეგებოდნენ აშშ-ში მის ექსტრადიციას. მიუხედავად ამისა ლორდთა პალატის მიერ უარყოფილი იქნა მათი აპელაცია.

საბოლოოდ იგი მაინც აშშ-ში მოხვდა, სადაც კიდევ დიდ ხანს იძიებდნენ საქმის დანარჩენ დეტალებს. მან ციხეში 3 წელი დაყო. თავისუფლების აღკვეთის გარდა, მას 240 015 აშშ დოლარის ოდენობის ჯარიმის გადახდაც დაეკისრა. სითიბანკს კი ამ ინცინდენტის შემდეგ მთელი რიგი რეორგანიზაციების გატარება დაჭირდა.

ამით კიდევ ერთხელ დასტურდება სტერეოტიპი, რომ გაცილებით ადვილია ადამიანები გააკვირვო და თავი დაამახსოვრო დანაშაულით, ვიდრე საპირისპიროთი. სწორედ ეს ხდება გადამწყვეტი ფაქტორი კომპიუტერული სპეციალისტისთვისაც გახდეს ჰაკერი.

ჯონათან ჯეიმსი

ჯონათან ჯეიმსი არის პირველი არასრულწლოვანი, რომელიც კომპიუტერული თაღლითობის გამო აღმოჩნდა ციხეში. თავდაპირველად მისთვის ეს ჩვეულებრივი გართობა იყო. მისი ყველაზე მასშტაბური ოპერაცია აშშ-ს თავდაცვის სამინისტროს ერთ-ერთ დანაყოფს (Defense Threat Reduction Agency) უკავშირდება. მან ხელში ჩაიგდო მაღალი რანგის თანამშრომლების სახელები და პაროლები, რასაც ხელი შეუწყო მისი მხრიდან საიდუმლო დოკუმენტებთან დაშვებამ. ამასთან ერთად, მან საერთაშორისო კოსმოსური სადგურის – ნასას კომპიუტერული ცენტრის გატეხვა მოახერხა. ამ ოპერაციით "ნასა" 41 მლნ. დოლარით დაზარალდა. თუმცა უსაფრთხოების ფასი არაფერია და ჯონათანის მსგავსმა ადამიანებმა შეძლეს ეჩვენებინათ, რომ უსაფრთხოების სისტემებს მუდმივი დახვეწა ჭირედება.

სადაზვერვო პარალელები ჰაკერთა საქმიანობაში

მოცემული ისტორიები ჰაკერების შესახებ რათქმაუნდა არის ძალიან კარგი ქეისები სამართლებრივი კუთხით, თუმცა ასევე მნიშვნელოვანია მათთან სადაზვერვო პარალელების გავლება. კერძოდ, სახეზეა:

1. სადაზვერვო და კონტრსადაზვერვო სამსახურების მხრიდან ჰაკერის კონტროლი;
2. დანაშაულის გამოვლენის შემთხვევაში ჰაკერის დაკავება და შემდგომი თანამშრომლობის უზრუნველყოფა;
3. თავისუფლების აღკვეთის ადგილებში ჰაკერისთვის ხელშეწყობა სამუშაოდ;
4. კერძო კომპანიებისა და ჰაკერების ჩართვა ეროვნული უსაფრთხოების სფეროში;
5. ჰაკერის მიერ უკანონო სატელეფონო მოსმენების ორგანიზაცია და სახელმწიფო მოხელეებზე მაკომპრომატირებელი მასალების მოპოვება და ბაზის წარმოება;
6. სახელმწიფო კონტროლს დაქვემდებარებული ჰაკერის დამოუკიდებელი ექსპერტის რანგში გამოყენება საზოგადოებრივი აზრის მომზადებისათვის;
7. კონტროლს დაქვემდებარებული ჰაკერების სანდოობის გადამოწმების მიზნით სხვადასხვა მოქმედებების, მათ შორის კონფლიქტების ინსპირირება;
8. კონტროლს დაქვემდებარებული ჰაკერების რეპუტაციის ამაღლება, მისი შემდგომი გამოყენება ქვეყნისათვის სასარგებლო სამეცნიერო საქმიანობაში;
9. ჰაკერული შეღწევის ობიექტზე უსაფრთხოების უზრუნველყოფის მიზნით რეორგანიზაციული პროცესების ინსპირაცია;
10. არასწორი საკადრო უზრუნველყოფის პირობებში არასასურველი პირის სახელმწიფო სამსახურში მოხვედრისა და საიდუმლო ინფორმაციასთან დაშვების ორგანიზაციით, სახელმწიფო სტრატეგიულ ობიექტზე ახალი მოწყვლადი ადგილების შექმნა.

კიბერ კრიმინალი საკომუნიკაციო სერვისების სფეროში

ადამიანის ფუნდამენტური უფლება – პირადი ცხოვრების ხელშეუხებლობა, ზოგჯერ, ჰაკერებზე ხშირად, კომუნიკაციების სფეროში დასაქმებული პირების მხრიდან ილახება. ადამიანების მხრიდან, რომლებიც მუშაობენ სხვადასხვა ინტერნეტ სერვის პროვაიდერ კომპანიებში, მობილური და სატელეფონო ქსელების ოპერატორებში. საქართველოს არსებული კანონმდებლობა ითვალისწინებს მსგავსი დანაშაულების აღკვეთასაც. რომ აღარაფერი ვთქვათ სამსახურეობრივი უფლებამოსილების ბოროტად გამოყენებაზე, ამგვარ პირთა პასუხისმგებლობა ასევე განსაზღვრულია საქართველოს კანონში ელექტრონული კომუნიკაციების შესახებ. აღნიშნული კანონის მერვე მუხლი სრულად ეთმობა ამ საკითხს.

ამონარიდი ელექტრონული კომუნიკაციების შესახებ საქართველოს კანონიდან
მუხლი 8
ინფორმაციის საიდუმლოების დაცვა ელექტრონული კომუნიკაციების სფეროში

1. ელექტრონული საკომუნიკაციო ქსელებით გადაცემული ინფორმაცია ამ მომხმარებლის საიდუმლოა და მისი დაცვა გარანტირებულია საქართველოს კანონმდებლობით. აღნიშნული უფლების შეზღუდვა შეიძლება სასამართლოს გადაწყვეტილებით ან მის გარეშე, საქართველოს კანონმდებლობით პირდაპირ განსაზღვრულ შემთხვევებში.

2. ელექტრონული კომუნიკაციების სფეროში დასაქმებული ყველა სუბიექტი ვალდებულია დაიცვას გადაცემული ინფორმაციის საიდუმლოება. ელექტრონული კომუნიკაციების სფეროს მუშაკები და სხვა პირები, რომლებიც დაარღვევენ ინფორმაციის საიდუმლოებას, პასუხს აგებენ საქართველოს კანონმდებლობის შესაბამისად.

კიბერ დანაშაულის შემდეგ, რიგით მეორე საკითხი აქტუალობის მიხედვით სწორედ სატელეკომუნიკაციო სერვისების მომხმარებელთა უფლებების დაცვაა. თუ კომპიუტერული თაღლითობის შემთხვევაში დამნაშავეებად ჰაკერები გვევლინებიან, ამ შემთხვევაში დამნაშავეები სერვისის მომწოდებელი კომპანიები და მათი თანამშრომლები არიან. საქართველოში განსაკუთრებით ხშირია შემთხვევები, როდესაც მომხმარებელი აწყდება უსამართლობას ინტერნეტ-პროვაიდერების მხრიდან, ფიჭური კავშირის ოპერატორებისა და სხვა ტიპის კომპანიებისაგან, რომლებსაც ბაზრის სიმცირისა და კონკურენტების ნაკლებობის გამო მომგებიანი პოზიცია უკავიათ ქართულ საკომუნიკაციო ბაზარზე. არც თუ ისე მომხიბვლელი ინტერნეტ ტარიფები, დაბალი სიჩქარე, მომხმარებლის კონფიდენციალური ინფორმაციის დაუცველობა და კიდევ მრავალი სხვა პრობლემა არის რეალობა ჩვენი ყოველდღიურობისა. წიგნის ეს ნაწილი გამიზნულია როგორც იურისტებისათვის, ისე რიგითი მომხმარებლებისთვისაც, რომელთაც სურთ იცოდნენ

საკუთარი უფლებების შესახებ და იმ ბერკეტებსა და მექანიზმებზე, რომლებსაც ქართული სამართლებრივი სივრცე აძლევს ან არ აძლევს მას. მთავარი ნორმატიული დოკუმენტი, რომელიც აწესრიგებს ინტერნეტისა და ზოგადად საკომუნიკაციო ბაზარზე მოქმედების სამართლებრივ ჩარჩოებს, გახლავთ კომუნიკაციების ეროვნული კომისიის მიერ მიღებული რეგლამენტი. საქართველოს კომუნიკაციების ეროვნული კომისია გახლავთ დამოუკიდებელი სახელმწიფო ორგანო, რომელიც 1999 წელს შეიქმნა ქვეყნის მასშტაბით საკომუნკაციო სფეროს რეგულირების მიზნით. ამ საკითხის ირგვლივ კომისიის სამართლებრივი რეგულაცია განსაზღვრულია რეგლამენტით ელექტრონული კომუნიკაციების სფეროში მომსახურების მიწოდების წესებისა და მომხმარებელთა უფლებების დაცვის შესახებ.

მეკობრეობა

ცალფეხა, ცალთვალა და სახეზე შავი ლენტით - ადამიანების უმრავლესობას დაახლოებით ასე წარმოუდგენია მეკობრეები. სიმართლე გითხრათ ისინი არ ცდებიან, მაგრამ ეს ის მეკობრეები არ არიან, რომელზედაც ახლა გიამბობთ. ისინი დიდი ხნის წინათ ჩაბარდნენ წარსულს და მხოლოდ ჰოლივუდურ ფილმებში შემორჩნენ პირვანდელი სახით. სხვათა შორის, ის მეკობრეები, რომლებზეც საუბარს ვაპირებ, ერთ-ერთი ყველაზე დიდი მტრები არიან ჰოლივუდისა და ზოგადად კინო თუ მუსიკალური ინდუსტრიისა. მეკობრეობა - XXI საუკუნის ახალი კრიმინალური სენია, რომელმაც განვითარება ჯერ კიდევ XX საუკუნეში მუსიკალური ფირფიტების კუსტარულად დამზადებითა და უკანონოდ გავრცელებით დაიწყო. მართალია ეს არალეგალური ბიზნესი არც ისე შემოსავლიანი იყო, თუმცა იგი მაინც არსებობდა და ფეხი მოიკიდა მთელი ყოფილი საბჭოთა კავშირის მასშტაბით. უნდა აღინიშნოს, რომ ფირფიტები არ კოპირდებოდა. მაშინდელი ტექნოლოგიები ამის საშუალებას არ იძლეოდა. მეკობრულ ფირფიტებზე იწერებოდა უცნობი მომღერლების მიერ შესრულებული სიმღერები, რომლებიც აყალბებდნენ საკუთარ პიროვნებას და შესაბამისად მსმენელის გემოვნებასაც.

მეკობრეობა საქართველოსთვის მეტად აქტუალური პრობლემაა და განიხილება ბარიერად ეკონომიკის სხვადასხვა სფეროში, განსაკუთრებით კი მუსიკალური, კინო და სამომხმარებლო პროგრამული უზრუნველყოფის ბაზრისათვის.

მეკობრეობა არ შეიძლება მხოლოდ ეკონომიკურ საფრთხედ იქნეს განხილული. თუ გავითვალისწინებთ, დაინტერესებული ქვეყნების სადაზვერვო ინტერესებს, მეკობრეობის ექსპორტი დაზვერვას დაქვემდებარებულ სახელმწიფოში, ამავე სახელმწიფოს ეკონომიკური ინტერესების მნიშვნელოვანი დაზიანების

უზრუნველსაყოფად არის ორგანიზებული. ეს ძალზედ წააგავს, უკვე კარგად აპრობირებულ მეთოდს კორუფციის ექსპორტის მხრივ.

იმ დროისთვის არანაკლებ აქტუალური იყო ეს საკითხი პრესაშიც, რამაც რუსეთი, როგორც მეკობრული ბიზნესის სამშობლო, აიძულა მიეღო მთელი რიგი კანონებისა ამ ფაქტების ასაკრძალად. რუსეთი ამ კანონებზე დღემდე აქტიურად მუშაობს, თუმცა შედეგი არაადეკვატურია <u>შექმნილი რეალობისა.</u> კონტრაფაქტული მუსიკალური ფირფიტებიდან არალიცენზირებულ კომპაქტ დისკებამდე ამ ბიზნესმა დიდი გზა გაიარა. საბჭოური აზროვნება, პოლიტიკური კულტურა და კორუფციის სიყვარული, საქართველოში დიდ ხანს იყო შემორჩენილი ტრადიციად და წლების მანძილზე იგი უდიდეს პრობლემას წარმოადგენდა. თუმცა საბედნიეროდ დღეს საქართველომ მოახერხა თავი დაეღწია ამ ყველფრისგან. დღეს იგი უფრო ძლიერი, დამოუკიდებელი და <u>ევროპულია.</u> ამდენად, ასეთ გარემოში დიდი მნიშვნელობა აქვს კარგი საინვესტიციო ბაზრის შექმნას ყველა სფეროში. შესაბამისად დგება საკითხი უამრავი ტექნოლოგიური პრობლემის, მათ შორის "მეკობრული ბიზნესის" საკითხის გადასაწყვეტად.

ბოლო მონაცემებით, საქართველო კვლავ ლიდერობს კომპიუტერული უზრუნველყოფის მეკობრულად გზით გავრცელებაში. რუსეთი კი ამავე მონაცემების მიხედვით მე-15-ე ადგილზეა.

2011 BSA GLOBAL SOFTWARE PIRACY STUDY-ის მიხედვით საქართველოში, მეკობრული გზით გავრცელებული პროგრამული უზრუნველყოფის კომერციული ღირებულება ბოლო 7 წლის განმავლობაში 211,000,000 $-ს აღემატება.

საზოგადოებაში მეკობრეობის პრობლემის მიმართ საკმაოდ ზედაპირული მიდგომა იგრძნობა, რადგან მომხმარებლებს არ აქვთ სრულფასოვანი ინფორმაცია მის შესახებ, რაც თავის მხრივ იმის შედეგია, რომ ამ საკითხებით საკმარისი რაოდენობისა და კომპეტენციის ადამიანები არ ინტერესდებიან. პრობლემას ყველა ხედავს, მხოლოდ გადაჭრის გზას ეძებენ სხვაგან. კომპიუტერის რიგითი მომხმარებლისთვის ერთი შეხედვით უმჯობესია, რომ იაფფასიანი მეკობრული პროდუქცია შეიძინოს ვიდრე ორიგინალი მწარმოებლის ლიცენზირებული პროდუქცია. ამისაკენ მას მხოლოდ ფასთასხვაობა უბიძგებს. შესაბამისად მიზეზი მხოლოდ ერთია - დაბალი ფასი. მაგრამ არსებობს უამრავი მიზეზი, თუ რატომ უნდა შეიძინოს მომხმარებელმა ლიცენზირებული პროდუქცია. მათგან შეგვიძლია გამოვყოთ ძირითადი უპირატესობები:

უსაფრთხოება

ორიგინალი პროგრამული უზურნველყოფა უსაფრთხოა, მაშინ როდესაც მეკობრული პროდუქციის უმრავლესობა მოდიფიცირებულია და ატარებს საზიანო ხასიათს. გარდა იმისა, რომ უფასო სარგებობისა და საკუთარი კომერციული მიზნებისათვის მეკობრეები მას ტეხენ და აზიანებენ, ისინი ასევე ატარებენ მზაკვრულ პოლიტიკას. კერძოდ, ამ პროგრამულ უზრუნველყოფას თან ურთავენ საკუთარ ჯაშუშურ და მავნებლურ პროგრამებს, რომლებიც ან აზიანებენ კომპიუტერს ან იპარავენ პირადი ხასიათის შემცველ ინფორმაციას. არსებობს ამგვარი ინფორმაცია თავს იყრის ჰაკერთა სხვადასხვა დაჯგუფებებში, რომლებიც შემდგომში სხვადასხვა მიზნებისათვის გამოიყენება.

ხარისხი

ლიცენზირებული და ორიგინალი პროგრამული უზრუნველყოფა ყოველთვის უფრო გამართულად მუშაობს და ხარისხიანია ვიდრე მეკობრული. უფასო ალტერნატივა კი დამახინჯებულ ვერსიას წარმოადგენს, რადგან ორიგინალის გატეხვისა და გაუფასურების პროცესში უამრავი რამ ფუჭდება პროგრამაში და ბუნებრივია ის ისე გამართულად ვეღარ იმუშავებს, როგორც პირვანდელი სახით მუშაობდა.

გარანტია და ტექნიკური მხარდაჭერა

ბუნებრივია, როდესაც მეკობრული გზით შეიძენთ პროგრამულ უზრუნველყოფას და რაიმე პრობლემა ან გაუგებრობა წარმოიშობა, მეკობრეს, რომლისგანაც მეასედ ფასად შეძენილია კონკრეტული პროგრამა მომხმარებელი ვერ მოთხოვს დახმარებას. წარმოიდგინეთ, რომ ასეთი გზით შეიძინეთ ტექსტური რედაქტირების პროგრამა, რომელშიც რამოდენიმე თვის, კვირის განმავლობაში წერდით მნიშვნელოვან სტატიას ან სულაც წიგნს. უცებ მოხდა ისე, რომ პროგრამა ”გაიჭედა” და თქვენი ნაშრომი უკვალოდ გაქრა, რაც სავსებით ბუნებრივია მეკობრული პროგრამების შემთხვევაში. წარმოიდგინეთ თქვენი თავი ასეთ სიტუაციაში. თქვენ ვერავის ვერაფერს მოსთხოვთ და ეს სრულიად სამართლიანი იქნება. ამ დროს, ლიცენზირებული პროგრამის მომხმარებელს შეუძლია ტექნიკური დახმარების ჯგუფს მიმართოს და აღადგენინოს

ნამუშევარი. უკიდურეს შემთხვევაში თუ პრობლემა ვერ მოგვარდება მომხმარებელს ასევე შეუძლია ზარალის ანაზღაურებაც მოითხოვოს. მთავარი კი მაინც ისაა, რომ ლიცენზირებული გზით შეძენილ პროდუქტს ასეთი რამ თითქმის არ ემართება.

რეპუტაცია

საქართველოში ჯერ კიდევ არსებობს არაერთი მსხვილი კომპანია და საჯარო დაწესებულება, რომლის შიგნითაც ჯერ კიდევ არალიცენზირებული პროგრამული უზრუნველყოფით სარგებლობენ. წარმოიდგინეთ პროგრამული უზრუნველყოფის დეველოპერი კომპანია, რომელიც საკუთარ მომხმარებლებს ეკონომიის მიზნით არალიცენზირებული პროგრამებით უმზადებს შეკვეთას. ეს ცუდად მოქმედებს არამარტო კომპანიის რეპუტაციასა და საერთო იმიჯზე, არამედ პირდაპირ გავლენას ახდენს მის ფინანსურ მდგომარეობაზე. ბუნებრივია ამგვარ ორგანიზაციას სოლიდურ შეკვეთას ნაკლებად ანდობენ. შესაბამისად, ეს კიდევ ერთი ფაქტორია ბიზნეს გარემოზე ნეგატიური ზემოქმედებისა.

კომფორტი

როდესაც ლიცენზირებული გზით იძენთ პროგრამას, როგორც წესი რეგისტრირდებით მისი მწარმოებელი კომპანიის ვებ-გვერდზე, სადაც უამარვი რამ შეგიძლიათ მიიღოთ: ტექნიკური დოკუმენტაცია, განახლებები (უფასოდ), დამატებითი პროგრამები, ტრენინგები და სხვა მრავალი ისეთი რამ, რაც მეკობრულ პროდუქციასთან შედარებით აშკარა უპირატესობას დაგანახებთ.

აუდიო და ვიდეო პროდუქციის მეკობრულ ვერსიებზეც იგივე პარამეტრები ვრცელდება. ორიგინალთან შედარებით მეკობრულ ალტერნატივას ბევრად დაბალი ხარისხი აქვს, დაახლოებით იმდენჯერ რამდენჯერაც ფასია ნაკლები. ამ ფასად კი ღებულობთ მხოლოდ უხარისხო ყდასა და კოლოფში, მოთავსებულ დისკს, რომელიც ძალიან მოკლე დროში გამოუსადეგარი ხდება. ამ ყოველივეს, თან ახლავს შემცირებული და ამოჭრილი ტიტრები. ორიგინალს კი, როგორც წესი, მრავალი ბონუსი გააჩნია. მაგალითად, ფილმის შეძენისას, გარდა იმისა, რომ ვღებულობთ საუკეთესო ხარისხის ვიდეო გამუსახულებას და რეალისტური ხმის ეფექტებს, ასევე შეგვიძლია ვიხილოთ საინტერესო ვიდეო დანართებიც. მაგალითად, ფილმის მსახიობების ინტერვიუები, გამოტოვებული კადრები, საინტერესო ისტორიები და სხვა. ერთი სიტყვით, მეკობრული პროდუქცია ახლოსაც კი ვერ მივა იმ სიამოვნებასთან, რასაც მომხმარებელი ლიცენზირებული პროდუქციით ღებულობს.

მეკობრეობის აღკვეთა ძალზედ მტკივნეულ რეფორმებს უკავშირდება და ამგვარ პროექტებთან დაკავშირებით უამრავი მოსაზრება არსებობს. პირველ რიგში, თავად მეკობრეობის აღკვეთა წარმოადგენს დილემას. ერთი მხრივ, არსებობს სახელმწიფოებრივი და გლობალური მიდგომა, ხოლო მეორე მხრივ მომხმარებლები, რომლებსაც არ სურთ დაელოდონ გლობალურ ტენდენციებს და არ არიან მზად ფინანსურად, შეიძინონ ორიგინალი პროდუქცია. ამგვარ

სიტუაციაში საუკეთესო გამოსავალი სახელმწიფო და კერძო სექტორს შორის კოოპერაციაა, რათა დაბალანსებული, ოპტიმალური ფორმით მოხდეს მეკობრეობის აღმოფხვრა. თუმცა არ უნდა დაგვავიწყდეს მომხმარებელთა ჩართულობაც, რა მხრივაც საზოგადოებრივი ცნობიერების ამაღლება გადამწყვეტ მნიშვნელობას ატარებს.

სპამი

არასასურველი წერილები თქვენს საფოსტო ყუთში

კომპანია მაიკროსოფტის მიერ ჩატარებული კვლევის მიხედვით გლობალურ ქსელში ბრუნვადი ელექტორნული ფოსტის 97% სწორედ სპამია. სხვადასხვა ვირუსებით დაინფიცირებულ კომპიუტერთა უმრავლესობაში სწორედ სპამით ხდება ინექცია. მისივე საშუალებით ვრცელდება არალეგალური ინტერნეტ კონტენტი. ინტერნეტ მარკეტინგი, სარეკლამო მომსახურება და PR სერვისი, ეს ყველაფერი ხშირად შელამაზებული სიტყვებია, რომლის უკან რეკლამისა და კიბერ კრიმინალის ეფექტური საშუალება, სპამი იმალება. ამ უკანასკნელმა ქართულ ინტერნეტ სივრცეში იოლად დაიმკვიდრა თავი. მას ძირითადად პატარა ან საშუალო მოცულობის კომპანიები იყენებენ. საკმაოდ ეფექტური და ამასთანავე იაფფასიანი რეკლამა ვრცელდება მასიურად დაგზავნილი ელექტრონული საფოსტო წერილების სახით და დიდ დისკომფორტს უქმნის ინტერნეტის მომხარებლებს. სწორად ამიტომ, რიგ ქვეყნებში იგი უკანონოდ ითვლება. მიუხედავად მისი ეფექტურობისა, როგორც პროდუქტის რეკლამირებისა და ზოგადად სასურველი სეგმენტის ინფორმირების საშუალება, იგი ცუდ გავლენას ახდენს ავტორის რეპუტაციაზე.

როდესაც სპამის მსხვერპლი ხდებით, ყოველ დღე ღებულობთ ათეულობით სარეკლამო წერილს და საფოსტო სერვისიც ვერ გიცავთ მისგან, როდესაც იაფფასიანი რეკლამით გაბეზრებენ თავს, თქვენ იწყებთ ფიქრს, რომ როგორმე დააღწიოთ თავი ამ საშინელებას, მაგრამ ყველაზე ცუდი ის არის, რომ სპამისგან დაცვაზე პრეტენზიას ვერსად განაცხადებთ, რადგან უფასო ელექტრონული სერვისით სარგებლობთ. რა თქმა უნდა საუკეთესო გამოსავალი ფასიან

ელექტრონულ ფოსტაზე გადასვლაა. თუმცა შეიძლება თქვენ ის უკვე გაქვთ, მაგრამ როგორც წესი ისინი გვხვდება კორპორაციულ ქსელში - ორგანიზაციის თანამშრომლებისთვის სპეციალურად გამოყოფილი სამსახურეობრივი ფოსტის სახით. ასეთ შემთხვევაში, სხვდასხვა კომპანიაში მომუშავე ადამიანებს, აქვთ პირადი ელექტრონული ფოსტა. ეს საქმიანი და პირადი ცხოვრების ერთგვარი დეფერენციაა. დაახლოებით ისე, როგორც სატელეფონო ნომრების შემთხვევაში: დღეს საქმიანი ადამიანების უმრავლესობა ორ ან მეტ ტელეფონს ატარებს სხვადასხვა ნომრით, ან უკეთეს შემთხვევაში დუალ ბარათიანი მობილური ტელეფონით სარგებლობს. მათგან ერთი სამსახურისთვის, ხოლო მეორე ახლობლებისა და მეგობრებისათვის. დეფერნეცია ელექტრონული ფოსტის მისამართების შემთხვევაში სავსებით ლოგიკურია. როდესაც თქვენ გაქვთ სამსახურებრივი ფოსტა, სადაც რეგისტრირებული ხართ, როგორც კონკრეტული ორგანიზაციის ერთ-ერთი თანამშრომლი, ცოტა უხერხულიც კი არის იმავე მისამართით დარეგისტრირდეთ რომელიმე გასართობ ვებ-რესურსზე ან სოციალურ ქსელში, რომელოც შეიძლება არ პასუხობდეს თქვენს საქმიან რეპუტაციას. წარმოიდგინეთ, თქვენი კომპანია მოყვა გაუგებრობაში, სადაც საჭირო გახდა თანამშრომლების მიმოწერის გადამოწმება. რათქმაუნდა თავს უხერხულად იგძრნობთ თუ თქვენს წერილებს შეისწავლიან. სწორედ ასეთ დროს, საუკეთესო გამოსავლად ისევ პირადი ელექტრონული ფოსტა რჩება უფასო საფოსტო სერვისებზე. გამოდის რომ ასე თუ ისე თქვენ მაინც გაქვთ პირადი საფოსტო მისამართი და გსურთ, რომ მასში კომფორტულად იგრძნოთ თავი ან ასე თუ არა, სპამმა მაინც რომ არ შეგაწუხოთ. სწორედ ამიტომ, აუცილებელია რაც შეიძლება ნაკლებ ვებ-რესურსზე დატოვოთ თქვენი ფოსტის მისამართი. ან იქონიოთ კიდევ ერთი ელექტრონული ფოსტა ისეთი ვებ-გვერდებისათვის, რომლებზედაც აუცილებელია მისი მითითება რეგისტრაციის დროს. სპამერების უმრავლესობა სწორედ ვებ-გვერდებიდან აგროვებენ საფოსტო მისამართების სიას.

აღნიშნული მიმართულება საინტერესოა სადაზვერვო შეღწევადობის თვალსაზრისითაც. გარდა ოპერატიულ ტექნიკური სამუშაოებისა, სპამი ასევე გამოიყენება ინფორმაციული პროპაგანდისთვის, საზოგადოებრივი აზრის ფორმირებისა და მასში სხვადასხვა ნეგატიური განწყობის ინექციისთვის. ამასთან ერთად, იგი ასევე გამოიყენება სადაზვერვო შესწავლის ორგანიზაციის პროცესშიც.

კიბერ ტერორიზმი და კიბერ ომები

ტერორიზმი, ექსტრემიზმის უკიდურესი ფორმაა, რომელიც შეიძლება პოლიტიკური, ეკონომიკური, სოციალური, რელიგიური თუ კრიმინალური მიზეზებით იყოს მოტივირებული. გამომდინარე სამოტივაციო ნაწილიდან, იგი უშუალო კავშირშია სადაზვერვო ოპერაციებთან.

თანამედროვე ტექნოლოგიების განვითარების პარალელურად, იზრდება მათი გამოყენება ტერორისტულ თუ სადაზვერვო საქმიანობაში. განვითარებულ ქვეყნებში გამუდმებით მიმდინარეობს ტერორიზმის პოტენციური საფრთხის ანალიზი და მათი

საწინააღმდეგო საშუალებების შემუშავება. საქართველო ამ სფეროში ნამდვილად არ იყო მოწოდების სიმაღლეზე, თუმცა ბოლო დროის განმავლობაში საკმაო ინტერესი და აქტუალობა შეიძინა ინფორმაციულმა უსაფრთხოებამ, რაც უდაოდ კარგი დასაწყისია. კერძოდ, ჩამოყალიბდა კონკრეტული სისხლისსამართლებრივი მიდგომა აღნიშნული საკხის ირგვლივ.

საქართველოს კანონმდებლობით კიბერ ტერორიზმი შემდეგნაირად არის განსაზღვრული:

მუხლი 3241. კიბერტერორიზმი

1. კიბერტერორიზმი, ესე იგი კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის საშიშროებას და ხელყოფს საზოგადოებრივ უსაფრთხოებას, სახელმწიფოს სტრატეგიულ, პოლიტიკურ ან ეკონომიკურ ინტერესს, ჩადენილი მოსახლეობის დაშინების ან/და ხელისუფლების ორგანოზე ზემოქმედების მიზნით, –

ისჯება თავისუფლების აღკვეთით ვადით ათიდან თხუთმეტ წლამდე.

2. იგივე ქმედება, რამაც ადამიანის სიცოცხლის მოსპობა ან სხვა მძიმე შედეგი გამოიწვია, –

ისჯება თავისუფლების აღკვეთით ვადით თორმეტიდან ოც წლამდე ან უვადო თავისუფლების აღკვეთით.

შენიშვნა: ამ მუხლით გათვალისწინებული ქმედებისათვის იურიდიული პირი ისჯება ლიკვიდაციით ან საქმიანობის უფლების ჩამორთმევით და ჯარიმით.

ბუნებრივია დღევანდელ რეალობაში, ახალი საფრთხეებისა და გამოწვევების პირობებში, ეს საკმარისი ვერ იქნება.

რასაკვირველია, არსებობს სხვადასხვა საერთაშორისო რეგულაციაც ამ საკითხთან მიმართებაში, თუმცა უნდა გავითვალისწინოთ, რომ თავად ტერმინი ომი – Act of War ხშირ შემთხვევაში პოლიტიკური ტერმინი უფრო არის, ვიდრე სამართლებრივი. პროცესის ტექნოლოგიურ ნაწილზე რომ აღარაფერი ვთქვათ, სწორედ ეს ართულებს კიბერ ომებსა და კიბერ ტერორიზმის საკითხებზე მუშაობას.

კლასიკური დეფინიციის მიხედვით, კიბერ ტერორიზმი არის კრიმინალური ქმედება, რომლის დროსაც გამოყენებულია კომპიუტერული და ტელესაკომუნიკაციო საშუალებები და რომლის მიზანიც კრიტიკული ინფრასტრუქტურის მწყობრიდან გამოყვანა წარმოადგენს.

საქართველოს კანონის მიხედვით ინფორმაციული უსაფრთხოების შესახებ, ასევე განისაზღვრა ერთგვარი კრიტიკული ინფრასტრუქტურა შემდეგი ტერმინით:

კრიტიკული ინფორმაციული სისტემის სუბიექტი. ამ კანონის შესახებ ვრცელ ინფორმაციას წიგნის მომდევნო თავებში გაეცნობით.

კიბერ ტერორიზმის სცენარებით განვითარებულ მოვლენებს შედეგად შეიძლება მოყვეს ადამიანთა მსხვერპლი, მატერიალური დანაკარგი და უამრავი სხვა პრობლემა.

კიბერ ტერორიზმმა უკვე მძლავრად მოიკიდა ფეხი თანამედროვე მსოფლიოში, რამაც ინფორმაციული უსაფრთხოების პრობლემას გლობალური სახე მისცა. შეიქმნა არაერთი მნიშვნელოვანი დოკუმენტი და სტანდარტი, რომელიც ამ სფეროს აწესრიგებს. ლეგალურ ასპექტებს თავი რომ დავანებოთ, ამ პრობლემატიკაზე მუშაობს მრავალი მსხვილი კომპანია მსოფლიოს სხვადასხვა წერტილში.

უნდა აღინიშნოს, რომ კიბერ ტერორიზმი არ წარმოადგენდა განსაკუთრებით აქტუალურ თემას. თუმცა 2001 წლის 11 სექტემბერს ნიუ-იორკსა და ვაშინგტონში მომხდარი ტერორისტული აქტის შემდეგ, მსოფლიო საზოგადოების დამოკიდებულება ტერორიზმის მიმართ მკვეთრად გამძაფრდა და უფრო მეტი ყურადღება დაეთმო ზოგადად ექსტრემიზმის პრობლემას. განხილული საკითხების რაოდენობა ერთი-ორად გაიზარდა და მათ შორის მაღალტექნოლოგიური ტერორიზმის სახელით მნიშვნელოვანი ადგილი დაიკავა კიბერ ტერორიზმმა. შეიქმნა ბევრი გაერთიანება ანტიტერორისტული საქმიანობისთვის და დაიწყო აქტიური მოქმედებები ექსტრემიზმის წინააღმდეგ.

ვიდრე კიბერ ტერორიზმის საფუძვლებზე გადავიდოდეთ, მნიშვნელოვანია პირველ რიგში თავად ტერორიზმი განვიხილოთ.

ტერორიზმის გარშემო ერთგვარი აზრთა სხვადასხვაობა არის, რის გამოც რთულია იგი კონკრეტული დეფინიციით განვსაზღვროთ. თავად ტერორისტებზე ამგვარი გამონათქვამიც კი არსებობს: "ერთისთვის ტერორისტი, სხვისთვის თავისუფლებისათვის მებრძოლია." ეს სიტყვები ჟერარდ სეიმურმა 1975 წელს, თავის წიგნში "ჰარის თამაშში" მოიხსენია.

აშშ-ს გამოძიების ფედერალური ბიუროს (Federal Bureau of Investigation - FBI) მიხედვით კი ტერორიზმი არის: "ძალისა და სისასტიკის უკანონო გამოყენება ადამიანების ან მათი საკუთრების წინააღმდეგ, მთავრობის იძულებისათვის, საზოგადოების ან და მისი რომელიმე სეგმენტის დასაშინებლად და გამყარებულია პოლიტიკური ან სოციალური მიზნებით."

ამერიკის შეერთებული შტატების მთავრობის დეპარტამენტის პოზიცია ტერორიზმის შესახებ შემდეგნაირად არის ჩამოყალიბებული: "წინასწარ დაგეგმილი, პოლიტიკურად მოტივირებული სისასტიკე, ჩადენილი სამოქალაქო სამიზნეებზე, ქვე-ნაციონალური ჯგუფის ან საიდუმლო აგენტების მიერ, რომელიც საზოგადოების დაშინებას ემსახურება."

საქართველოს სისხლის სამართლის კოდექსის XXXVIII თავის 323 მუხლის მიხედვით კი ტეროსისტული აქტი შემდეგნაირად არის განსაზღვრული: "ტერორისტული აქტი, ესე იგი აფეთქება, ცეცხლის წაკიდება, იარაღის გამოყენება ან სხვა ქმედება, რაც ქმნის ადამიანის სიცოცხლის მოსპობის, მნიშვნელოვანი

ქონებრივი ზიანის ან სხვა მძიმე შედეგის განხორციელების საშიშროებას, ჩადენილი მოსახლეობის დაშინების ან ხელისუფლების ორგანოზე, უცხო ქვეყნის ხელისუფლების ორგანოზე ან საერთაშორისო ორგანიზაციაზე ზემოქმედების მიზნით."

როგორც თავდაცვითი, ისე ტერორისტული საქმიანობისას არსებობს ძირითადი მოდელები და სქემები, რომლითაც ხდება მუშაობა. როგორც წესი, თავდაცვითი საშუალებების მოდელირებისას პირველ რიგში ხორციელდება მომხდარი ფაქტების ანალიზი, შემდგომ შესაძლო მოქმედებათა სურათის კონსტრუირება, ხოლო ამის შემდეგ შესაძლებელი ხდება პრევენციული ზომების შემუშავება. ძალზედ მნიშვნელოვანია ადეკვატური უსაფრთხოების სისტემის შექმნა, რადგან საფრთხეები ამ პოლიგონზე კოლოსალურია.

ტერორისტები თანამედროვე მსოფლიოში ხშირად იყენებენ კომპიუტერულ საშუალებებს, რათა კონკრეტული ქვეყნის (ების) ეკონომიკისთვის მნიშვნელოვანი ზიანის მიყენების მიზნით ნაციონალური თუ ტრანსნაციონალური მასშტაბით გაანადგურონ ელექტრონული ინფრასტრუქტურა. ტერორისტების მიერ ხშირად ხდება ქსელური ინფორმაციის არასანქცირებული მოპოვება, გავრცელება და ბოროტად გამოყენება, რომელიც დაცულია სახელმწიფო საიდუმლოს დონეზე, კონსტრუქციული მართვისა თუ თავდაცვისათვის.

ექსტრემისტები ხშირად ავრცელებენ და პროპაგანდას უწევენ თავიანთ შეხედულებებს. ისინი იყენებენ მსოფლიო ქსელს დეზინფორმაციის გასავრცელებლად, მოსახლეობის დაშინებისა და დაძაბული ფონის შესაქმნელად. ამდენად, ქსელური ინფრასტრუქტურის გამოყენება ერთ-ერთი საუკეთესო იარაღია პროპაგანდისთვის.

მაშ ასე, სად გადის ზღვარი ჰაკერის მიერ ჩადენილ მარტივ ხულიგნობასა, სამთავრობო დაფინანსების კიბერ ოპერაციებსა და კიბერ ომებს შორის?

ეს დღესდღეობით კიბერ სივრცის ერთ-ერთი ყველაზე აქტუალური კითხვაა, რადგან კიბერ შეტევა შეიძლება გახდეს საპასუხო სამხედრო აგრესიის მიზეზი. დღეს ამერიკის შეერთებული შტატების თავდაცვის დეპარტამენტმა უკვე მიიღო ინიციატივა, რომლის მიხედვითაც იგი სახელმწიფოს წინააღმდეგ განხორციელებულ სამთავრობო კიბერ შეტევას, კონვენციური სამხედრო მოქმედებებით უპასუხებს. ასევე გასათვალისწინებელია ჩრდილოატლანტიკური ალიანსის პოტენციალიც, რომელიც მსგავსი სცენარებით ყოველწლიურ სამხედრო სწავლებებსაც მართავს – Nato Cyber Coalition. ამ რეალობაში კიბერ აქტივობები განსაკუთრებულ საფრთხეს ატარებს, რომელმაც შეიძლება კოლოსალური მასშტაბების სამხედრო მოქმედებები გამოიწვიოს. მაგალითად, თუ შეტევა განხორციელდა ალიანსის წევრი სახელმწიფოს მიმართ, მოსალოდნელია რომ გამოყენებულ იქნება ვაშინგტონის შეთანხმების მეხუთე პუნქტი, რომლის მიხედვითაც წევრი სახელმწიფოს მიმართ განხორციელებული შეტევა ითვლება შეტევად ალიანსის წევრ-სახელმწიფოებზე.

ამ პირობებში, როდესაც კიბერ სივრციდან წარმოქმნილ საფრთხეს კიბერ სივრცის გარეთ რეალური ფიზიკური ზიანის შექმნა შეუძლია და ეროვნული უსაფრთხოების საკითხები სწორ სამართლებრივ ინტერპრეტაციაზე ხდება

დამოკიდებული, ჩვენ უბრალოდ არ გვაქვს უფლება ამ საკითხს სათანადო ყურადღება არ დავუთმოთ. უფრო მეტიც, დღეს საქართველოში მნიშვნელოვანი საკადრო დეფიციტია სწორედ იმის გამო, რომ ქვეყნის საგანმანათლებლო სივრცის უდიდესი ნაწილი საკმარისი ტემპით ვერ უწყობს ფეხს ტექნოლოგიურ პროგრესს. უფრო მეტიც, ეს ნაწილი მთლიანად ჩამორჩენილია და მოკლებულია ყოველგვარ ინოვაციებს. შესაბამისად, მსოფლიოს ახალი საფრთხეების წინააღმდეგ უკვე დროა აღვიჭურვოთ სათანადო ცოდნითა და კომპეტენციებით.

იმ რეალობიდან გამომდინარე, რომელშიც ბოლო ათწლეულებია ვიმყოფებოდით უსაფრთხოების სფეროში ერთ-ერთი მთავარი მიმართულება საკადრო რესურსებთან დაკავშირებული მანიპულაციების შესწავლა უნდა იყოს. თამამად შეიძლება ითქვას, რომ ყველა პრობლემის მთავარი წყარო ხშირად სწორედ საკადრო პოლიტიკა გახლდათ. დისბალანსი კვალიფიკაციასა და თანამდებობრივ სტატუსს შორის, არამიზნობრივი მივლინებები და სამსახურეობრივი სარგო, ე.წ. გავლენის აგენტურის გავრცელება და ა.შ. გახლავთ ის მწვავე პრობლემური საკითხები, რომლებიც ამრუდებნენ ქვეყნის ხერხემალს. ამდენად, უსაფრთხოების სფეროს ერთ-ერთ პრიორიტეტული მიმართულება სწორედ საკადრო პოლიტიკა და ადამიანური რესურსები უნდა გახდეს. ამ კუთხით კი მრავალი რამ არის გადასახედი.

ახლა, როცა კიბერ უსაფრთხოების ლეგალური ასპექტების მნიშნელობაზე ვისაუბრეთ, უკვე დროა კონკრეტულ ინციდენტებს ჩავუდრმავდეთ. წინა გვერდებზე უკვე იქნა განხილული ჰაკერების კატეგორიზაცია მათი აქტივობების მიხედვით, ახლა კი დროა თავად ეს აქტივობები გავმიჯნოთ.

კიბერ კონფლიქტებში, რომლებსაც რეალურ ომში გადაზრდის ხასიათი გააჩნიათ, გასათვალისწინებელია, რომ სამართლებრივი ნაწილი ბოლომდე ვერ დაფარავს ყველა დეტალს. თავად ტერმინიც "ომი", უფრო მეტად პოლიტიკური ტერმინია, ვიდრე ლეგალური დეფინიცია. ამდენად, ასეთი შემთხვევების გარჩევისას უნდა ვიხელმძღვანელოთ ტექნოლოგიური ასპექტებით. დავახასიათოთ თითოეული აქტივობა, მიზნები, სუბიექტები და შემდეგ უკვე მოვახდინოთ კატეგორიზაცია.
მაშ ასე, დავიწყოთ კიბერ კრიმინალით:

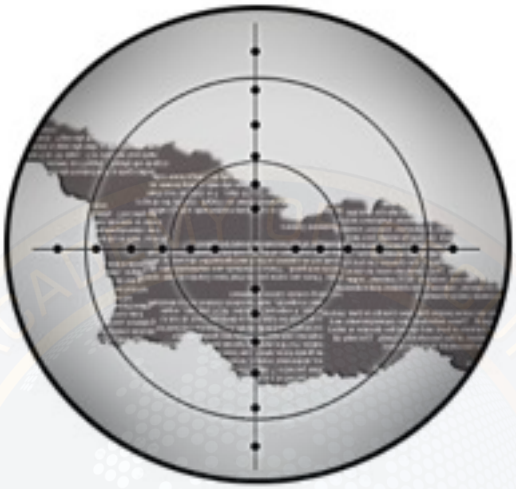
კიბერ კრიმინალის სუბიექტები ძირითადად ინდივიდები და ტრადიციული კრიმინალური დაჯგუფებები არიან, რომელთა მთავარი მოტივი ანგარებაა. ისინი ცდილობენ შეინარჩუნონ სრული ანონიმურობა, რაც შემთხვევების აღმოჩენასა და გამოძიებას მნიშვნელოვნად ართულებს. თუმცა სწორედ ის წარმოადგენს ერთ-ერთ იდენტიფიკატორსაც, რომლითაც ხდება სავარაუდო მონაწილეების დადგენა. სხვა კიბერ აქტივობების დროს, პოპულარობა ინფორმაციული პროპაგანდის ნაწილია და ამაზე შემსრულებლები ძალისხმევას არ იშურებენ.

კიბერ კონფლიქტი არის პოლიტიკური ან სოციალური მოტივის მქონე კონფლიქტი, რომელიც ტექნოლოგიურ ხასიათს ატარებს. მისი მთავარ შემსრულებლები ჰაქტივისტები არიან.

კიბერ ომი კიბერ უსაფრთხოების ერთ-ერთი ყველაზე კომპლექსური ასპექტია. მისი ზუსტი სამართლებრივი განსაზღვრა ძალზედ რთულია თავად ამ პრეცედენტის ტექნოლოგიური სპეციფიკიდან გამომდინარე. ეს არის სამხედრო კონფლიქტი

ინფორმაციული ტექნოლოგიების გამოყენებით, რომელიც მიმართულია სამიზნე ქვეყნის სასიცოცხლო და სტრატეგიული დანიშნულების ობიექტების წინააღმდეგ.

2008 წლის რუსეთ-საქართველოს კიბერ დაპირისპირება



2008 წლის აგვისტოს, როდესაც მსოფლიო შოკირებული იყო რუსეთის აგრესიით საქართველოს წინააღმდეგ, ბრძოლის ასპარეზზე XXI საუკუნის ახალი ტიპის მეომრები გამოჩნდნენ, ახალი იარაღითა და კოლოსალური შესაძლებლობებით. მთელი ამ ომის პარალელურად, გაიმართა კიდევ ერთი უმნიშვნელოვანესი ბრძოლა კიბერსივრცესა და მედიაში – კიბერ ომი. სოციალურ ქსელებსა და მედიაში ჰაკერთა ჯგუფები და სპეცსამსახურები ყველა რესურსს იყენებდნენ საკუთარი ინტერესების დასაცავად, თუმცა ეს ყველაფერი ომამდე გაცილებით ადრე დაიწყო. რუსეთის ხელისუფლება ცდილობდა შესაბამისი ფონი შეექმნა მომდევნო აქტივობებისთვის და ამისათვის ყველაზე ეფექტური საშუალებაც გამოინახა – სოციალური ქსელები, მედია და ზოგადად ინტერნეტი.

ომის პირველი სიმპტომები. მასიური კიბერ შეტევები ერთდროულად რამოდენიმე მნიშვნელოვან ობიექტზე განხორციელებით დაიწყო.

კიბერ შეტევები საქართველოს წინააღმდეგ იმგვარად იყო ორგანიზებული, რომ სამიზნეები პრიორიტეტების მიხედვით გადანაწილდა და ქრონოლოგიაც პარალელურ მოვლენებს ემთხვეოდა.

შეტევის ძირითად ობიექტებს წარმოადგენდნენ ვებ-რესურსები, რომლებიც კავშირში იყო ქვეყნის კრიტიკულ ინფრასტრუქტურასთან. ასევე მნიშვნელოვანი ზიანი მიადგა საინფორმაციო რესურსებს. შეიძლება ითქვას, რომ ამ სამიზნეებს უმაღლესი პრიორიტეტი ქონდა მინიჭებული.

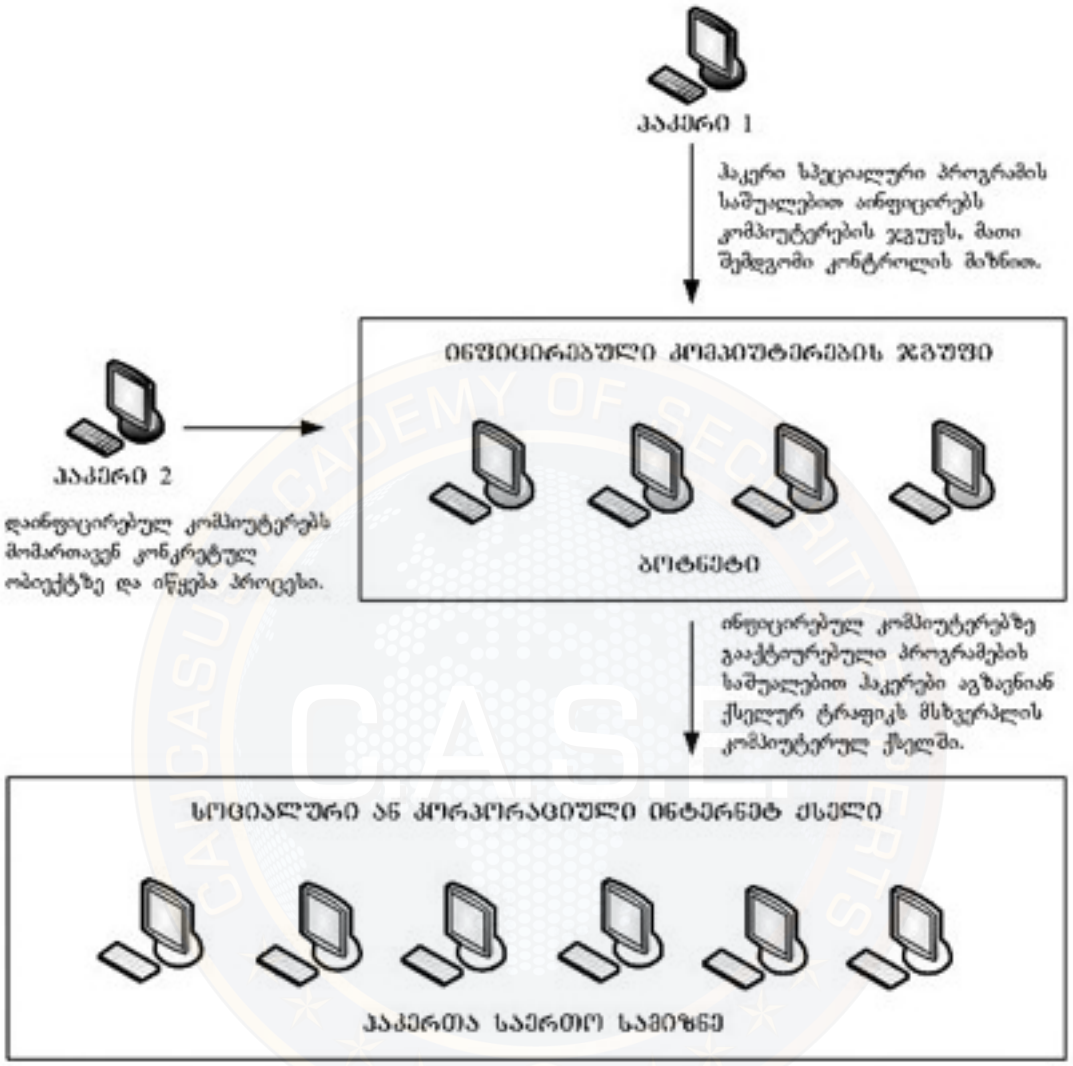
თანამედროვე ეტაპზე საომარ კონფლიქტში ჩართული ქვეყნისთვის სასიცოცხლოდ მნიშვნელოვანია კრიტიკულ სიტუაციებში ინფორმაციის გავრცელების საშუალება, როგორც ქვეყნის შიგნით, ისე მის საზღვრებს გარეთ. სწორედ ამიტომ, საქართველოში 2008 წლის საომარი მოქმედებების პირობებში, კიბერ აქტივობების ერთ-ერთ უმთავრეს მიზანს წარმოადგენდა:

- საჯარო ინსტიტუტების (სამთავრობო, საპარლამენტო, ძალოვანი და სხვა) ინფრასტრუქტურის მოშლა;
- მედია და კერძო სექტორის ინფრასტრუქტურის მწყობრიდან გამოყვანა, რათა შექმნილიყო მაქსიმალურად ქაოტური მდგომარეობა.

მოწინააღმდეგემ ასევე განახორციელა შეტევა ქსელურ ინფრასტრუქტურაზე და სხვადასხვა ელექტრონული სერვისების მომწოდებლებზე (ინტერნეტ პროვაიდერები, მობილური და საკომუნიკაციო ოპერატორები). კიბერ დაპირისპირებისას, რუსეთი კიდევ უფრო არაპროპორციული ძალით დაუპირისპირდა საქართველოს, ვიდრე ეს მან სამხედრო ფრონტზე განახორციელა. უნდა აღინიშნოს, რომ მიუხედავად მისი მასშტაბისა განსაკუთრებულ ტექნოლოგიურ ინოვაციურობას ადგილი არ ქონია. მასშტაბურობის ინსპირირება, ერთდროულად დიდი რაოდენობის ადამიანური რესურსის-ჩვეულებრივი მომხმარებლების კიბერ სივრცეში მობილიზებამ უზრუნველყო. რათქმაუნდა პროცესში აქტიურად იყვნენ ჩართულნი ჰაკერებიც და ექსპერტებიც, მაგრამ ისინი ხშირ შემთხვევაში საორგანიზაციო საკითხებს უფრო ითავსებდნენ. ამ რესურსს მართვა ჭირდებოდა. ჩნდება კითხვა – თუ როგორ შეეძლოთ ჩვეულებრივ ადამიანებს ასეთი ოპერაციების ჩატარება – სწორედ ამას მოიცავდა ზემოთ ნახსენები საორგანიზაციო საკითხები. – მთელი საიდუმლო სწორი ტექნოლოგიის შერჩევაშია, რომელიც არსებული სიტუაციის ოპტიმალურ გამოყენებას გულისხმობს.

ამ პროცესში განვიხილოთ ქართული რეალობა. ასეა თუ ისე, რუსეთთან შედარებით საქართველოში ბევრად მცირეა ტექნიკური სპეციალისტების რაოდენობა. ეს ბუნებრივიცაა რადგან, რუსეთის მოსახლეობა რაოდენობრივად ბევრად აღემატება ჩვენსას. თანაც სახეზეა უამრავი მიზანმიმართული, მათ შორის სადაზვერვო ორგანიზაციის ნიშნების შემცველი პროცესი ქვეყნის შიგნით, რომლებმაც კონკრეტული სფეროების ჩავარდნა გამოიწვია. თუმცა ეს კიდევ ერთი მასშტაბური თემა გახლავთ. დავუბრუნდეთ კიბერ აქტივობებს - როგორც ზემოთ აღინიშნა ომის დროს უახლესი ტექნოლოგიური მიღწევები მაინც და მაინც არ გამოყენებულა. ეს იმიტომ, რომ როდესაც საქმე დიდი რაოდენობის ადამიანურ რესურსთან გვაქვს, არსებობს მხოლოდ რამოდენიმე ტექნოლოგიური სტრატეგია, რომელიც ამ რესურსის ოპტიმალურად გამოყენების საშუალებას იძლევა.

კიბერ შეტევის ყველაზე გავცელებული მოდელის მიხედვით ჰაკერების მცირე ჯგუფი ორგანიზებას უწევს მთელს დანარჩენ რესურსს და თითოეულ კომპიუტერს მასში ცალკეული იარაღის ფუნქციას ანიჭებს. ამ სტრატეგიას "ბოტნეტის" შეკვრა ეწოდება. ქვემოთ მოცემულია "ბოტნეტის" მოქმედების პრინციპი.



როგრც წესი კომპიუტერების უმრავლესობა ეკუთვნით ჩვეულებრივ მომხმარებლებს, რომლებსაც ხშირად წარმოდგენაც კი არ აქვთ რა ხდება მათ კომპიუტერებში. ჰაკერები ახერხებენ ამგვარ კომპიუტერებში შეღწევას და მათში საკუთარი პროგრამის გააქტიურებას. მას შემდეგ რაც პროგრამა გააქტიურდება კომპიუტერზე ის უკვე დამოუკიდებლად იღებს მართვას და ავტონომიური ხდება. ამგვარი პროგრამები შენიღბულად მოქმედებენ. ყველა ეს ცალკეული ინსტრუმენტი მოქცეული ერთ მთლიანობაში დიდი ძალის მქონე იარაღად იქცევა.

ტექნოლოგიურად პროცესი ასე გამოიყურება: რომელიმე ქსელში ხდება კიბერ გაერთიანების შეკვრა, რომელშიც თითოეული კომპიუტერი ახორციელებს არჩეული საერთო ობიექტის მაქსიმალურ დატვირთვას. ანუ ე.წ. გადაჭარბებული "ტრაფიკის" (ქსელური ინფორმაციის) მიწოდებას. მსხვერპლის კომპიუტერს უწყვეტად ეგზავნება დიდი მოცულობის ინფორმაცია, რომელსაც იგი ავტომატურად ამუშავებს და ასე გრძელდება ვიდრე კომპიუტერის ან სერვერული ინფრასტრუქტურის მწყობრიდან გამოსვლამდე. ამ სქემის ყველაზე გავრცელებული ოპერაცია Ping-ის გამოყენებაა. ამ დროს, რაც უფრო მეტი კომპიუტერი ახორციელებს ობიექტის ერთდროულ "დაპინგვას", მით მეტად იტვირთება იგი და როდესაც დატვირთვის მაქსიმალურ დონეს აღწევს, სისტემა მწყობრიდან გამოდის. ტექნიკურად "დაპინგვა" არის ძალზედ მარტივი ქსელური ოპერაცია. მისი მეშვეობით როგორც წესი, მოწმდება კავშირი გარკვეულ ქსელურ ობიექტებს შორის. ამ დროს იგზავნება ბიტების გარკვეული რაოდენობა და პასუხის მიხედვით დგინდება კავშირის მდგომარეობა. დაპინგვის პროცედურა ძალიან მარტივია. ცალკეული დაპინგვისას საჭიროა მომხმარებელმა გამოიძახოს სპეციალური პროგრამა "Command Promt", რომელშიც მან შესაბამისი ბრძანება უნდა აკრიფოს. დაახლოებით ასე: ping www.dezinformaciulisaiti.ru (მაგალითი) და დაპინგვის ყოველი ოპერაციის დასრულების შემდეგ, კვლავ გაიმეოროს იგივე ბრძანება მინიმალური დროითი ინტერვალით.

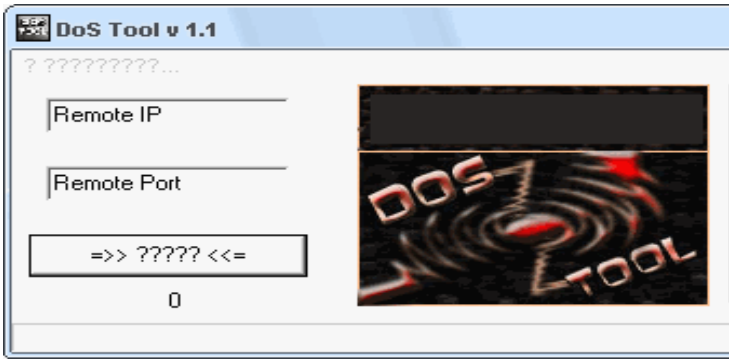
კომპიუტერის მომხმარებლების უმრავლესობისთვის ეს შეიძლება სირთულეს წარმოადგენდეს. თანაც მისი ერთჯერადი განხორციელება საკმარისი არ არის და მხოლოდ უმნიშვნელო ეფექტს იძლევა. ასეთ დროს საჭიროა პროცესის სრული ავტომატიზება, რისთვისაც იდეალური გადაწყვეტა მსუბუქი და მარტივი პროგრამების დაწერაა, რომლებსაც კიბერ დაჯგუფების წევრებს უგზავნიან და ისინი ააქტიურებენ მას. ერთ-ერთი ასეთი მცირე პროგრამის ფრაგმენტი, რომელიც გამოიყენებოდა კიბერ დაჯგუფებების მიერ აგვისტოს ინფორმაციული ომის დროს ასე გამოიყურება :

```
@echo offSET PING_COUNT=50SET PING_TOMEOUT=1000:PINGecho vpingavt rusul serverebsping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT%
```

რაც შეეხება რუსულ მხარეს, მათ ამას უფრო ორგანიზებული სახე მისცეს და კომპილირებული პროგრამები დაუგზავნეს კიბერ ხულიგნებს. ეს პროგრამაც იგივე ფუნქციას ასრულებდა და ასე გამოიყურებოდა

ცხადია გამოყენებულ იქნა გაცილებით კომპლექსური სქემებიც. ამ და სხვა ოპერაციების უფრო მეტი დეტალიზაცია არ იქნებოდა სწორი თუ გავითვალისწინებთ რა შეიძლება მოყვეს მის ბოროტად გამოყენებას.
დღეის მდგომარეობით ჰაკერული ტექნოლოგიები გარკვეულ დონეზე კომპიუტერის დამწყები მომხმარებლებისთვისაც კი გახდა ხელმისაწვდომი. მათაც შეუძლიათ გარკვეული ოპერაციების განხორციელება. საშიში თითქოს არაფერია, მაგრამ როდესაც ასეთი მომხმარებლების დიდ რაოდენობასთან გვაქვს საქმე, იგი უკვე სერიოზულ საფრთხედ განიხილება. თუმცა დავივიწყოთ დროებით ტექნიკური მხარე და მივუბრუნდეთ კონფლიქტს. მთელი მსოფლიო ჩაება ინფორმაციულ ომში, რომელმაც ინტერნეტის თითქმის ყველა კომპონენტი მოიცვა. მულტიმედია ვიდეო პორტალებით

დაწყებული სადისკუსიო ფორუმებით დამთავრებული მიდიოდა გააფთრებული ომი პროპაგანდისტებსა და იმ ადამიანებს შორის, ვისაც სურდა ჯანსაღი, ობიექტური ინფორმაციის მიწოდება საერთაშორისო საზოგადოებისათვის. დეზინფორმატორების ორგანიზებულობამ განაპირობა ის, რომ საქართველომ წააგო ინფორმაციული ბრძოლა. უნდა აღინიშნოს, რომ ამ პროცესში კოლოსალური რაოდენობის ინტერნეტ მომხმარებლები. ყველა თავისებურად ცდილობდა დაეცვა საკუთარი ქვეყნის ინტერესები. ცდილობდნენ ეჩვენებინათ დანარჩენი მსოფლიოსათვის თუ რა ხდებოდა სინამდვილეში - არაპროპორციული დაპირისპირება, უსამართლო აგრესია და ა.შ. ფაქტობრივად წაგებული იყო ბრძოლა და არა ომი, რადგან ინფორმაციულ ეპოქაში შეუძლებელია დიდ ხანს შენიღბო ტყუილი და ბუნებრივია მოგვიანებით დალექილი ინფორმაცია მალევე გავრცელდა. ყველა საუბრობდა ამ ომზე, თუმცა ძირითადად პოლიტიკურ და დიპლომატიურ ჭრილში, რადგან მრავალი ფაქტი მოგვიანებით გახდა ცნობილი და მრავალსაც ანალიზისათვის დრო ჭირდებოდა. სამწუხაროა რომ ჩვენი ქვეყნის დიპლომატიურმა წრეებმა იმ მომენტში ვერ მოახერხეს გამოეყენებინათ ძალიან კარგი შესაძლებლობა მიენიჭებინათ ამ მოვლენებისთვის კიბერ ომის სტატუსიც. ამ მიმართულებით აქტიური ქმედებების გამოუყენებლობის მნიშვნელობაზე მეტყველებს ის გარემოება, რომ მსოფლიო პრაქტიკაში ეს იყო დღემდე ცნობილი ერთადერთი საომარი ქმედება, რომელსაც შეიძლებოდა მინიჭებოდა კიბერ ომის სტატუსი.



რათქმაუნდა არსებობს კიბერ კონფლიქტების სხვა მასშტაბური პრეცედენტებიც, როგორც მაგალითად დანიაში 2006 წელს, ესტონეთში 2007-ში, ლიტვაში 2008 წელს და ირანშიც კი 2009 წელს, მაგრამ მათ არ ქონდათ შესაბამისი სამართლებრივი ბაზა, რათა კიბერ ომის სტატუსი მიენიჭებინათ ამ მოვლენებისთვის, რადგან ცნობილია ორი ძირითადი არგუმენტი მოვლენის კიბერ ომად შესაფასებლად: პირველი არის შესაბამისი სამართლებრივი ბაზის ქონა, ხოლო მეორე მყარი არგუმენტაცია. ეს უკანასკნელი კი საქართველოს შემთხვევაში საკმარისად არსებობდა. ამის სამართლებრივ არგუმენტს წარმოადგენდა ის გარემოება, რომ რუსეთი საქართველოსთან აწარმოებდა რეალურ, კონვენციურ ომს, ხოლო კიბერ აქტივობები, იყო ერთ-ერთი პარალელური პროცესი. ეს არის ერთ-ერთი გამოუყენებელი მომენტი თუ შეიძლება ამას ასე ეწოდოს. პრობლემაც ალბათ ტექნიკური ხასიათის უფრო იყო, რადგან ისევ და ისევ ამ სფეროს სპეციალისტების დეფიციტმა, არასაკმარისმა ინტერესმა ამ საკითხის მიმართ თუ კვალიფიკაციის არ არსებობამ გამოიწვია ის, რომ ვერავინ ურჩია დიპლომატიურ უწყებას სათანადო რეაგირება მოეხდინა ამ კუთხით. ახლა ეს სამწუხაროდ უკვე დაგვიანებულია.

დრო გადის, მაგრამ აღნიშნული კიბერ ომის აქტუალობა არ იკარგება. აგვისტოს მოვლენების პასიურ ფაზაში გადასვლიდან ერთგვარი ღია ანალიტიკური ციკლი დაწყებულია.

რაოდენ პარადოქსულიც არ უნდა იყოს, 2008 წლის რუსეთ-საქართველოს კიბერ დაპირისპირებაზე უცხოური პრესის წარმომადგენლები და ექსპერტები გაცილებით მეტს საუბრობენ და ყურადღებას უთმობენ მას ვიდრე ჩვენთან, საქართველოში.

სულ მალე გამოჩნდა პუბლიკაციები აღნიშნული მოვლენების შესახებაც. ერთ-ერთი ასეთი საინტერესო სტატია მოამზადა "Computerworld"-ის ცნობილმა მიმომხილველმა გრეგ კაიზერმა (Greg Kaiser), სადაც მან საინტერესო პარალელები გაავლო ესტონეთში მომხდარ ანალოგიურ მოვლენებთან და სხვადასხვა სააგენტოს მონიტორინგის შედეგები მოიყვანა. ესტონეთის შემთხვევა მართლაც ძალზედ ახლოს არის ჩვენს სიტუაციასთან. ჩვენ ბევრი შეგვიძლია ვისწავლოთ მათგან, რადგან თავად ისინი დღემდე სწავლობენ ჩვენს მაგალითზე.

საქართველო-რუსეთს შორის გამართული კიბერ ომი და შემდგომი მოვლენები კიბერ უსაფრთხოების საერთაშორისო საექსპერტო წრეებსა და ინსტიტუტებში ერთ-ერთ ყველაზე აქტუალურ თემად იქცა. სპეციალურად ამ მოვლენებზე დაყრდნობით დაიწერა უამრავი სტატია, გამოქვეყნდა სხვადასხვა ნაშრომი და სახელმძღვანელო. ეს აქტუალობა აბსოლიტურად ბუნებრივია, რადგან ამგვარი ფაქტები შესანიშნავ

მასალას წარმოადგენენ კვლევებისთვის, ანალიზისა და შემდგომი პრევენციული მექანიზმების შესამუშავებლად. დროა თვალი გავუსწოროთ ახალ რეალობას და ეს პრეცედენტი საქართველოშიც "ქეისად" იყოს გამოყენებული. ესტონეთი მსგავსი ინციდენტების შემდეგ იმდენად დაიხვეწა ამ მიმართულებით, რომ ერთ-ერთ წამყვან ქვეყანად იქცა ინფორმაციული უსაფრთხოების სფეროში. მათ სწორად გაანალიზეს მომხდარი ფაქტები და საპასუხოდ შექმნეს მთელი ინფრასტრუქტურა, ახალი ინსტიტუციური მექანიზმები, დახვეწეს და გადაახალისეს საკანონმდებლო ბაზა, ჩამოაყალიბეს სასწავლო პროგრამები. ერთი სიტყვით მათ ეს გაკვეთილი, მართლაც გაკვეთილად მიიღეს და საშინაო დავალებაც უმაღლეს ქულაზე მოამზადეს.

კიდევ ერთი საინტერესო გამოხმაურება მოყვა ინფორმაციულ ომს გაზეთ "New York Times"-ში, რომელიც კიდევ უფრო მნიშვნელოვანია თუ გავითვალისწინებთ მისი ავტორის ვინაობას - ჯონ მარკოფი. იგი დაკავშირებულია სკანდალური ჰაკერის, კევინ მიტნიკის ისტორიასთან და ერთ-ერთი ყველაზე პოპულარული მიმომხილველია ტექნოლოგიურ საკითხებში.

ახლა როცა ომს წარსულ ფორმატში ვაანალიზებთ ცხადი ხდება მრავალი რამ. როგორც ძლიერი, ისე სუსტი მხარეები, რომლებზედაც საჭიროა მეტი მუშაობა. ის არაორგანიზებულობა ინფორმაციულ ომში, ის დაბნეულობა კრიტიკულ სიტუაციაში, რომელიც ქვეყანაში იყო ისედაც მძიმე დროს, არის შედეგი იმისა, რომ არ არსებობდა ინფორმაციული უსაფრთხოების ერთიანი ჩამოყალიბებული პოლიტიკა და შესაბამისი დონის ინფრასტრუქტურა, რაც თავისმხრივ განაპირობა საფრთხეების არასწორმა შეფასებამ. ჩვენ შეგვიძლია ვისაუბროთ სადაზვერვო შეღწევადობაზე, რომელიც განაპირობებს საქართველოში კონკრეტული სფეროების ჩავარდნას და არასწორ პოლიტიკას, თუმცა არ უნდა დაგვავიწყდეს, რომ საზოგადოებრივი ცნობიერების ამაღლება და სამოქალაქო სექტორის რეალური აქტივობები ასევე შეიძლება იყოს ეფექტური მსგავს პროცესებში. მართალია არ იყო სათანადო დონეზე განვითარებული ინსტიტუტები რომლებიც ამ პრობლემებს გადაჭრიდნენ, თუმცა გარდა უსაფრთხოების პოლიტიკისა, მნიშვნელოვანია სათანადო საზოგადოებრივი აზრის მობილიზაციის უზრუნველყოფა. სწორედ ამიტომ პრობლემებზე ღია საუბარი მათი გადაჭრის საუკეთესო დასაწყისია, ხოლო წარსული შეცდომების დანახვა უკეთესი მომავლის პერსპექტივას განაპირობებს.

კანონი ინფორმაციული უსაფრთხოების შესახებ

სახელმწიფოსთვის ინფორმაციული უსაფრთხოების მძლავრი ინსტიტუტები ისეთივე მნიშვნელოვანია, როგორც ფიზიკური დაცულობა. საჭიროა სწორი ხედვა და პრიორიტეტები, უსაფრთხოება კი მათგან უმთავრესია, რომელსაც ინფორმაციულ ეპოქაში განვითარებული ქვეყნები ახალი მეთოდებით იცავენ.

ინფორმაციული უსაფრთხოება, როგორც ეროვნული უსაფრთხოების ერთ-ერთი უმთავრესი კომპონენტი, ტექნიკური და ადმინისტრაციული პროცედურების გარდა

ასევე მოითხოვს სათანადო ლეგალურ უზრუნველყოფასაც. ამ მხრივ კი საქართველოში 2012 წლამდე არ არსებობდა შესაბამისი საკანონმდებლო ბაზა. ინფორმაციული ტექნოლოგიების სამთავრობო და კერძო სექტორში აქტიურ დანერგვასთან ერთად და 2008 წლის მოვლენების გათვალისწინებით მოთხოვნა ამ სფეროს რეგულაციაზე მუდმივად იზრდებოდა. აღსანიშნავია, რომ თითქმის 4 წელი დასჭირდა ხელისუფლების მიერ იმ რეალობის გათვალისწინებას, რაც რუსეთთან კიბერ ომს მოყვა და შესაბამისი საკანონმდებლო ინიციატივის მისაღებად. ამ რეალობაში კი მხოლოდ ლეგალური უზრუნველყოფა ვერ იქნება საკმარისი. მითუმეტეს ამგვარი ტემპით მუშაობის პირობებში. ეს ყოველივე მეტყველებს სამთავრობო დონეზე ინფორმაციულ უსაფრთხოებასთან დაკავშირებული საკითხების დაბალ პრიორიტეტულობაზე. მაშინ როცა, თითქმის მთელი მსოფლიოს მასშტაბით, ტექნოლოგიური პროგრესის პარალელურად ინტენსიურად მიმდინარეობს კიბერ შეიარაღებისა და პრევენციის საშუალებების ათვისება, ჩვენს ქვეყანაში ჯერ კიდევ საჭიროა ახალი საფრთხეებისა და გამოწვევების შესახებ აქტუალობის პრობლემაზე მუშაობა. უნდა აღინიშნოს, რომ ადგილობრივ კორპორაციულ სექტორშიც არანაკლებ პრობლემურია აღნიშნული საკითხები. ამ მხრივ კი კანონი ინფორმაციული უსაფრთხოების შესახებ ერთგვარი აქსელერატორიც კი გახდა. კომპანიების დიდი ნაწილისთვის ინფორმაციული უსაფრთხოების საშუალებებით აღჭურვა, მონაცემთა დაცვა და კადრების მომზადება ნებაყოფლობითი საკითხი იყო და მხოლოდ კორპორაციულ იმიჯს ემსახურებოდა. აღნიშნულმა კანონმა კი კომპანიების ნაწილისთვის ინფორმაციული უსაფრთხოების უზრუნველყოფა სავალდებულო გახადა. კერძოდ, აღნიშნულმა კანონმა ქართულ სამართლებრივ სივრცეში შემოიტანა ერთგვარი დეფინიცია კრიტიკული ინფრასტრუქტურისთვის, რომელიც მასში შემდეგნაირად არის განსაზღვრული.

“კრიტიკული ინფორმაციული სისტემის სუბიექტი – სახელმწიფო ორგანო ან იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის.”

შეიძლება ითქვას, რომ ზემოთ მოცემული დეფინიცია ერთგვარი ჩანასახია კრიტიკული ინფრასტრუქტურის პრინციპისთვის. ეს უკანასკნელი კი არსებითად მნიშვნელოვანია ეროვნული უსაფრთხოების სფეროში საფრთხეების სწორი შეფასებისა და ადეკვატური რეაგირებისათვის. აღნიშნული მიდგომის მიხედვით, ამგვარ სუბიექტად შეიძლება ჩაითვალოს არამხოლოდ სახელმწიფო ორგანოები, არამედ კერძო სამართლის იურიდიული პირები, რომლებიც კავშირშია ენერგო სისტემასთან; საბანკო და საფინანსო სექტორთან; ტრანსპორტთან; ტელეკომუნიკაციასთან; ჯანდაცვასა და სამოქალაქო უსაფრთხოებასთან.

კანონი ინფორმაციული უსაფრთხოების შესახებ ავალდებულებს ზემოთ აღნიშნულ ობიექტებს ინფორმაციული უსაფრთხოების უზრუნველყოფის კონკრეტულ პროცედურებს, როგორებიცაა: შეღწევადობის (ინფორმაციული

სისტემების დაცულობის) ტესტების განხორციელება; ქსელური სენსორების (IDS-ების) გამოყენება; სტანდარტების დანერგვა და რისკების შეფასება;

ზემოთ მოცემული პროცედურების ადგილზე განხორციელება კი ამგვარი სუბიექტის სპეციალურ თანამშრომლებს ევალებათ, რომელთა შესახებაც კანონი ასევე აწესებს მოთხოვნებს კრიტიკული ინფორმაციული სისტემის სუბიექტებისათვის. კერძოდ, ამგვარი ორგანიზაციებისათვის იკვეთება ორი პირი საშტატო ნომენკლატურაში: ინფორმაციული უსაფრთხოების ოფიცერი და კომპიუტერული უსაფრთხოების სპეციალისტი. ორგანიზაციებში ამგვარი კადრების არსებობის შესახებ მოთხოვნამ, მალევე გამოაცოცხლა ვაკანსიების ვებ-გვერდები და უკვე გაჩნდა მოთხოვნა შესაბამის საკადრო უზრუნველყოფაზე, როგორც კერძო, ისე საჯარო სექტორში. ამ ეტაპისთვის საქართველოში რთულად მოიძებნება საკმარისი რაოდენობისა და კვალიფიკაციის კადრები ინფორმაციული უსაფრთხოების სფეროში. ისევე როგორც კომპანიები, რომლებიც გაწევენ მომსახურებას სტანდარტების დანერგვისა და შეღწევადობის ტესტების უზრუნველყოფის კუთხით. ამ მხრივ კი სავარაუდოა, რომ ქვეყანაში გარედან მოხდება ამგვარი რესურსების ინექცია. ეს ყოველივე კიდევ უფრო გაზრდის საშიშროებას კიბერდაზვერვის მიმართულებით, რადგან ამგვარ კომპანიებს შესაძლოა მაქსიმალური წვდომა მიენიჭოთ ქვეყნის კრიტიკული ინფრასტრუქტურის ობიექტებზე. როდესაც საუბარია ინფორმაციული უსაფრთხოების სტანდარტების დანერგვაზე, რისკების მართვაზე, შეღწევადობის ტესტებსა და სხვადასხვა სახის აუდიტზე, მნიშვნელოვანია გავაცნობიეროთ, რომ ეს ყოველივე ორგანიზაციის ინფრასტრუქტურაზე სრულ წვდომას მოითხოვს. ამდენად, სახეზეა დისბალანსი არსებულ სიტუაციასა და მიღებულ ინიციატივებს შორის, რომლებიც სფეროს რეგულაციასთან ერთად ახალ საფრთხეებს წარმოშობს.

როგორც ინფორმაციული უსაფრთხოების მთავარი ბირთვი – თავად ინფორმაცია, კანონში ასევე არის განსაზღვრული და კრიტიკულობის კლასიფიცირებულია მიხედვით სხვადასხვა ტიპად. ინფორმაციული აქტივების დაცვა კი კრიტიკული ინფორმაციული სისტემის სუბიექტთან ერთად იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტოს დაევალა, რომელსაც ამ მხრივ განსაკუთრებული პრივილეგიები ენიჭება. კანონპროექტის გამოქვეყნებისთანავე, რომელიც ამავე სააგენტოს მიერ არის შემუშავებული, სამოქალაქო საზოგადოებაში არაერთი ეჭვი და მოსაზრება გაჩნდა იმის თაობაზე, რომ ეს შეიძლებოდა აღქმულიყო, როგორც სახლმწიფოს მიერ კერძო ბიზნესში უხეში ჩარევა. თუმცა, აღნიშნული კანონი ვრცელდება მხოლოდ კრიტიკული ინფორმაციული სისტემის სუბიექტებზე და არ ეხება დანარჩენ კერძო თუ საჯარო იურიდიულ პირებს.

კანონთან ერთად, ასევე ჩამოყალიბდა კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი (CERT), რომელმაც უნდა უპასუხოს კრიტიკული ინფორმაციული სისტემის სუბიექტების წინაშე არსებულ ყველა კიბერ საფრთხეს. ამ მხრივ კი აღსანიშნავია, რომ CERT-ის პასუხისმგებლობაში არ შედის ქვეყნის დანარჩენი ინფრასტრუქტურა. კერძო კომპანია, რომელიც კიბერ შეტევით ისევე შეიძლება დაზარალდეს, როგორც

კრიტიკული ინფორმაციული სისტემის სუბიექტი, მარტო რჩება ამგვარი საფრთხეების წინაშე და სახელმწიფოს მხრივ არ არის უზრუნველყოფილი სათანადო დაცულობა. მაშინ როცა, ამგვარი შეტევების რაოდენობა ყოველდღიურად მატულობს და დაზარალებულთა რიცხვი, ისევე როგორც ზიანის ოდენობა კოლოსალურ ნიშნულებს აღწევს.

საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ

თავი I
ზოგადი დებულებები
მუხლი 1. კანონის მიზანი

ამ კანონის მიზანია, ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, დააწესოს საჯარო და კერძო სექტორების უფლება-მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში, აგრეთვე განსაზღვროს ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები.

მუხლი 2. ტერმინთა განმარტება

ამ კანონში გამოყენებულ ტერმინებს აქვს შემდეგი მნიშვნელობა:

ა) ინფორმაციული უსაფრთხოება – საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას;

ბ) ინფორმაციული უსაფრთხოების პოლიტიკა – ამ კანონით, საქართველოს სხვა ნორმატიული აქტებითა და საერთაშორისო შეთანხმებებით გათვალისწინებული ნორმებისა და პრინციპების, აგრეთვე პრაქტიკის ერთობლიობა, რომელიც ემსახურება ინფორმაციული უსაფრთხოების უზრუნველყოფას და შეესაბამება მისი დაცვის სფეროში დადგენილ საერთაშორისო სტანდარტებს;

გ) კიბერსივრცე – სივრცე, რომლის განმასხვავებელი ნიშანია ელექტრონული მოწყობილობებისა და ელექტრომაგნიტური სპექტრის გამოყენება ქსელით დაკავშირებული სისტემებისა და დამხმარე ფიზიკური ინფრასტრუქტურის მეშვეობით მონაცემთა შენახვისათვის, შეცვლისათვის ან გაცვლისათვის;

დ) კიბერშეტევა – ქმედება, როდესაც ელექტრონული მოწყობილობა ან/და მასთან დაკავშირებული ქსელი ან სისტემა გამოიყენება კრიტიკულ ინფორმაციულ სისტემაში შემავალი სისტემების, ქონების ან ფუნქციების მთლიანობის დარღვევის, შეფერხების ან განადგურების ან ინფორმაციის უკანონოდ მოპოვების გზით;

ე) კომპიუტერული ინციდენტი – ინფორმაციული უსაფრთხოების პოლიტიკის რეალური ან პოტენციური დარღვევა, რომელიც ხორციელდება ინფორმაციული

ტექნოლოგიის გამოყენებით და იწვევს ინფორმაციის უნებართვო წვდომას, გამჟღავნებას, დაზიანებას ან შეფერხებას ან ინფორმაციული რესურსის მიტაცებას;
ვ) კრიტიკული ინფორმაციული სისტემა ინფორმაციული სისტემა, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის;
ზ) კრიტიკული ინფორმაციული სისტემის სუბიექტი – სახელმწიფო ორგანო ან იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის;
თ) კონფიდენციალური ინფორმაცია – ინფორმაცია, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფას, სავარაუდოდ, მოჰყვება კრიტიკული ინფორმაციული სისტემის სუბიექტის ფუნქციებისათვის მნიშვნელოვანი ზიანი და რომლის კონფიდენციალურ ინფორმაციად კლასიფიცირების მიზანია ინფორმაციული აქტივების მართვის წესების უზრუნველყოფა, გარდა იმ წესებისა, რომლებითაც საქართველოს ზოგადი ადმინისტრაციული კოდექსი განსაზღვრავს საჯარო ინფორმაციის ხელმისაწვდომობას;
ი) შინასამსახურებრივი გამოყენების ინფორმაცია – ინფორმაცია, რომელიც განკუთვნილია მხოლოდ კრიტიკული ინფორმაციული სისტემის სუბიექტის თანამშრომლისათვის ან/და მასთან სახელშეკრულებო ურთიერთობის მქონე პირისათვის, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფა, სავარაუდოდ, გამოიწვევს კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ თავისი ფუნქციების შესრულების მნიშვნელოვან შეფერხებას ან ზიანს მიაყენებს სახელმწიფო ხელისუფლების ორგანოს უსაფრთხოებას, სახელმწიფო ინტერესს ან კერძო პირის საქმიან რეპუტაციას და რომლის შინასამსახურებრივი გამოყენების ინფორმაციად კლასიფიცირების მიზანია ინფორმაციული აქტივების მართვის წესების უზრუნველყოფა, გარდა იმ წესებისა, რომლებითაც საქართველოს ზოგადი ადმინისტრაციული კოდექსი განსაზღვრავს საჯარო ინფორმაციის ხელმისაწვდომობას;
კ) ინფორმაციული აქტივი ყველა ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის;
ლ) ინფორმაციული სისტემა ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების ნებისმიერი კომბინაცია, რომელიც ხელს უწყობს მართვას ან/და გადაწყვეტილების მიღებას;
მ) ქსელური სენსორი – მოწყობილობა, რომელიც სპეციალურად გამიზნულია ქსელის სეგმენტის მონიტორინგისთვის, ისეთი ქმედებების გამოსავლენად, რომლებიც მიუთითებს ინფორმაციული სისტემის წინააღმდეგ წარმოებულ შეტევაზე ან მასში შეღწევაზე.

მუხლი 3. კანონის მოქმედების სფერო
1. ამ კანონის მოქმედება ვრცელდება ყველა იურიდიულ პირსა და სახელმწიფო ორგანოზე, რომლებიც კრიტიკული ინფორმაციული სისტემის სუბიექტები არიან. ამ კანონის მოქმედება ასევე ვრცელდება ისეთ ორგანიზაციასა და უწყებაზე, რომლებიც კრიტიკული ინფორმაციული სისტემის სუბიექტს ექვემდებარებიან ან ამ სუბიექტთან დაკავშირებული არიან დასაქმების, სტაჟირების, სახელშეკრულებო ან სხვა ურთიერთობით და რომლებიც უზრუნველყოფენ ინფორმაციული აქტივის წვდომას ასეთი ურთიერთობის ფარგლებში.
2. კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხა მტკიცდება და შესაბამისი სუბიექტის კრიტიკულობის კლასიფიცირება დგინდება საქართველოს პრეზიდენტის ბრძანებულებით, რომლის პროექტს საქართველოს პრეზიდენტს დასამტკიცებლად წარუდგენს საქართველოს ეროვნული უშიშროების საბჭო. ამ ნუსხის შედგენის დროს მხედველობაში მიიღება შემდეგი კრიტერიუმები: ინფორმაციული სისტემის შეფერხების ან მწყობრიდან გამოსვლის სავარაუდო შედეგების სიმძიმე და მასშტაბი; სავარაუდო ეკონომიკური ზარალის სიმძიმე სუბიექტისათვის ან/და სახელმწიფოსათვის; ინფორმაციული სისტემის მიერ გაწეული მომსახურების აუცილებლობა საზოგადოების ნორმალური ფუნქციონირებისათვის; ინფორმაციული სისტემის მომხმარებელთა რაოდენობა; სუბიექტის მატერიალური მდგომარეობა და სავარაუდო ხარჯების ოდენობა, რომლებიც მისთვის ამ კანონიდან გამომდინარე ვალდებულებების დაკისრებას მოჰყვება.
3. ამ კანონის მოქმედება არ ვრცელდება მასმედიაზე, გამომცემლობათა რედაქციებზე, სამეცნიერო, საგანმანათლებლო, რელიგიურ და საზოგადოებრივ ორგანიზაციებსა და პოლიტიკურ პარტიებზე, მიუხედავად იმისა, თუ რამდენად მნიშვნელოვანია მათი საქმიანობა ქვეყნის თავდაცვისთვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის.
4. ნებისმიერ იურიდიულ პირსა და სახელმწიფო ხელისუფლების ორგანოს, რომელიც არ არის კრიტიკული ინფორმაციული სისტემის სუბიექტი, უფლება აქვს, ნებაყოფლობით აიღოს ამ კანონიდან გამომდინარე ვალდებულებები.
5. ამ კანონის მოქმედება არ ვრცელდება კრიტიკული ინფორმაციული სისტემის სუბიექტის წინასწარი თანხმობით ნებადართულ ქმედებაზე, რომლის მიზანია ინფორმაციული უსაფრთხოების ტესტირება.
6. ამ კანონის დებულებები გავლენას არ ახდენს საქართველოს კანონმდებლობით გათვალისწინებული იმ ნორმების მოქმედებაზე, რომლებიც არეგულირებს ინფორმაციის თავისუფლებას, პერსონალური მონაცემის დამუშავებას, სახელმწიფო, კომერციული და პირადი საიდუმლოებების დაცვას.

თავი II
ინფორმაციული უსაფრთხოების ორგანიზება და უზრუნველყოფა

მუხლი 4. ინფორმაციული უსაფრთხოების წესები

1. კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია მიიღოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები, რომლებიც ემსახურება ამ კანონის დებულებათა აღსრულებას და განსაზღვრავს ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკას.

2. ინფორმაციული უსაფრთხოების პოლიტიკა უნდა აკმაყოფილებდეს ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს (კრიტიკული ინფორმაციული სისტემის სუბიექტის კრიტიკულობის კლასიფიცირების გათვალისწინებით), რომლებსაც განსაზღვრავს საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი – მონაცემთა გაცვლის სააგენტო (შემდგომ მონაცემთა გაცვლის სააგენტო) სტანდარტიზაციის საერთაშორისო ორგანიზაციისა (ISO) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილი სტანდარტებისა და მოთხოვნების შესაბამისად.

3. კრიტიკული ინფორმაციული სისტემის სუბიექტი ამ მუხლის პირველი პუნქტის თანახმად მიღებულ ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებს განსახილველად წარუდგენს მონაცემთა გაცვლის სააგენტოს. მონაცემთა გაცვლის სააგენტოს ასევე ეცნობება ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებში შეტანილი ნებისმიერი ცვლილება. მონაცემთა გაცვლის სააგენტო ახორციელებს ამგვარად მოწოდებული დოკუმენტების ზოგად ანალიზს და წარადგენს რეკომენდაციებს მათში აღმოჩენილი ხარვეზების გამოსასწორებლად.

4. ამ მუხლის მე-3 პუნქტით გათვალისწინებული დოკუმენტების გარდა, მონაცემთა გაცვლის სააგენტოს ხელი არ მიუწვდება კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციასა და ინფორმაციულ აქტივზე, გარდა იმ შემთხვევისა, როდესაც კრიტიკული ინფორმაციული სისტემის სუბიექტი ნებაყოფლობით უზრუნველყოფს მონაცემთა გაცვლის სააგენტოსთვის ინფორმაციისა და ინფორმაციული აქტივის ხელმისაწვდომობას.

მუხლი 5. ინფორმაციული აქტივების მართვა

1. კრიტიკული ინფორმაციული სისტემის სუბიექტი, ამ კანონის მე-4 მუხლის პირველი პუნქტით გათვალისწინებული შინასამსახურებრივი გამოყენების წესების შესაბამისად, ატარებს ინფორმაციული სისტემების ინვენტარიზაციას ყველა ინფორმაციული აქტივის აღრიცხვის მიზნით, რის შედეგადაც ყოველ ინფორმაციულ აქტივს მიენიჭება კრიტიკულობის შესაბამისი კლასი – კონფიდენციალური ან შინასამსახურებრივი გამოყენების. ყველა სხვა ინფორმაციული აქტივი, რომელთა კლასიფიცირება საჭირო არ არის, ღია ინფორმაციად ითვლება.

2. ინფორმაციული აქტივების აღრიცხვის შედეგად აღიწერება ყოველი ინფორმაციული აქტივის მნიშვნელობა, ფასეულობა, უსაფრთხოებისა და დაცვის არსებული დონე.

3. ინფორმაციული აქტივის შექმნის დროს კრიტიკულობის შესაბამის კლასს ადგენს აქტივის ავტორი ან/და აქტივზე პასუხისმგებელი პირი.
4. ინფორმაციული აქტივების მართვის წესებს, კერძოდ, მათი აღწერის, კლასიფიცირების, წვდომის, გაცემის (გამოქვეყნების), შეცვლისა და განადგურების წესებს, ნორმატიული აქტით ადგენს მონაცემთა გაცვლის სააგენტო, გარდა იმ წესებისა, რომლებითაც საქართველოს ზოგადი ადმინისტრაციული კოდექსი განსაზღვრავს საჯარო ინფორმაციის ხელმისაწვდომობას.

მუხლი 6. ინფორმაციული უსაფრთხოების აუდიტი და ინფორმაციული სისტემების ტესტირება
1. კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობით, მონაცემთა გაცვლის სააგენტო ან მონაცემთა გაცვლის სააგენტოს მიერ ავტორიზებულ პირთაგან კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ შერჩეული პირი ან ორგანიზაცია ატარებს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების (ინფორმაციული უსაფრთხოების პოლიტიკის) მონაცემთა გაცვლის სააგენტოს მიერ დადგენილ უსაფრთხოების მინიმალურ სტანდარტებთან თავსებადობის შეფასებას (ინფორმაციული უსაფრთხოების აუდიტი). აუდიტის ჩატარების შემდეგ დგება დასკვნა, რომლის მოთხოვნების შესრულება სავალდებულოა.
2. ამ მუხლის პირველი პუნქტით გათვალისწინებული ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესს ნორმატიული აქტით ადგენს მონაცემთა გაცვლის სააგენტო.
3. მონაცემთა გაცვლის სააგენტოს მიერ ჩატარებული ინფორმაციული უსაფრთხოების აუდიტის საფასური განისაზღვრება კრიტიკული ინფორმაციული სისტემის სუბიექტთან გაფორმებული ხელშეკრულებით.
4. მონაცემთა გაცვლის სააგენტო ნორმატიული აქტით ადგენს ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირთა და ორგანიზაციათა მიერ ავტორიზაციის გავლის წესს, ავტორიზაციის პროცედურებს და ავტორიზაციის საფასურს.
5. კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობით, მონაცემთა გაცვლის სააგენტო ან მონაცემთა გაცვლის სააგენტოს წინასწარი ნებართვით – კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ შერჩეული დამოუკიდებელი, შესაბამისი კომპეტენციის მქონე პირი ან ორგანიზაცია ატარებს ინფორმაციული სისტემის შეღწევადობის (პენეტრაციის) ტესტს და ამ სისტემის მოწყვლადობის შეფასებას წინასწარ დაგეგმილი და დოკუმენტირებული ამოცანის მიხედვით.
6. თუ ამ მუხლით გათვალისწინებული აუდიტის ან ტესტირების შედეგად გამოვლინდა ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნებთან შეუსაბამობა, კრიტიკული ინფორმაციული სისტემის სუბიექტი ატარებს შეუსაბამობის მიზეზის ანალიზს და, საჭიროების შემთხვევაში, განსაზღვრავს და ახორციელებს სათანადო გამოსასწორებელ ღონისძიებებს, რომელთა გრაფიკსაც წარუდგენს მონაცემთა გაცვლის სააგენტოს.

მუხლი 7. ინფორმაციული უსაფრთხოების მენეჯერი
1. კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია განსაზღვროს კონკრეტული პირი (პირები) ან თანამშრომელი (თანამშრომლები), რომელიც (რომლებიც) პასუხისმგებელია (პასუხისმგებელი არიან) კრიტიკული ინფორმაციის სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მოთხოვნების შესრულებისათვის (ინფორმაციული უსაფრთხოების მენეჯერი).
2. ინფორმაციული უსაფრთხოების მენეჯერის ძირითადი მოვალეობებია:
ა) ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნების შესრულების ყოველდღიური მონიტორინგი;
ბ) ინფორმაციული აქტივებისა და მათი წვდომის აღწერა;
გ) ინფორმაციული უსაფრთხოების პოლიტიკის შინაუწყებრივი დოკუმენტაციის მომზადება;
დ) ინფორმაციული უსაფრთხოების ინციდენტების შესახებ ინფორმაციის შეგროვება და მათზე რეაგირების მონიტორინგი;
ე) ინფორმაციული უსაფრთხოების საკითხებზე ანგარიშგება და სხვა სახის ადმინისტრაციული/საორგანიზაციო საქმიანობა;
ვ) ინფორმაციული უსაფრთხოების ზოგადი და დარგობრივი ტრენინგების ორგანიზება და ჩატარება;
ზ) სხვა მოვალეობები, რომლებსაც განსაზღვრავს კრიტიკული ინფორმაციული სისტემის სუბიექტი.
3. ინფორმაციული უსაფრთხოების მენეჯერი ანგარიშვალდებულია კრიტიკული ინფორმაციული სისტემის სუბიექტის ხელმძღვანელის ან მის მიერ შესაბამისად უფლებამოსილი თანამშრომლის ან ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების უფლებამოსილების მქონე პირთა ჯგუფის (კოლეგიური ორგანოს) წინაშე. ყველა მნიშვნელოვანი გადაწყვეტილება, რომლებიც შეეხება ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელებას, მიიღება ამ პუნქტით განსაზღვრული პირის (პირების) მიერ ან მასთან (მათთან) წინასწარი შეთანხმებით.
4. ინფორმაციული უსაფრთხოების მენეჯერი ადგენს ინფორმაციული უსაფრთხოების სამოქმედო გეგმას და ამ გეგმის შესრულების შესახებ ყოველწლიურ ანგარიშს წარუდგენს ამ მუხლის მე-3 პუნქტით განსაზღვრულ პირს (პირებს) და მონაცემთა გაცვლის სააგენტოს.

თავი III
კიბერუსაფრთხოების უზრუნველყოფა
მუხლი 8. მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი
1. ამ კანონის დებულებათა აღსრულებას, კერძოდ, საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, ასევე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ სხვა, მასთან დაკავშირებულ საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული

საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი – ჩ ღთ. V. (შემდგომ – დახმარების ჯგუფი).

2. კიბერუსაფრთხოების პრიორიტეტულ საფრთხეებს მიეკუთვნება:

ა) კიბერშეტევა, რომელიც საფრთხეს უქმნის ადამიანთა სიცოცხლესა და ჯანმრთელობას, სახელმწიფო ინტერესებს ან ქვეყნის თავდაცვისუნარიანობას;

ბ) კიბერშეტევა კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული სისტემების წინააღმდეგ;

გ) კიბერშეტევა, რომელიც საფრთხეს უქმნის სახელმწიფოს, ორგანიზაციის ან კერძო პირის ფინანსურ რესურსებს ან/და საკუთრების უფლებას;

დ) სხვა ნებისმიერი ქმედება, რომელიც, მისი ხასიათიდან, მიზნიდან, წყაროდან, მოცულობიდან ან რაოდენობიდან ან მისი აღკვეთისათვის საჭირო რესურსების ოდენობიდან გამომდინარე, კრიტიკული ინფორმაციული სისტემის ნორმალური ფუნქციონირებისათვის საკმარისი საფრთხის შემცველია.

3. დახმარების ჯგუფის მოვალეობებია:

ა) კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა;

ბ) კომპიუტერული ინციდენტების დროული გამოვლენა;

გ) კომპიუტერულ ინციდენტებზე რეაგირება და მათზე რეაგირების კოორდინაცია;

დ) კომპიუტერული ინციდენტების აღრიცხვა და მათზე რეაგირების პრიორიტეტების დადგენა და კატეგორიზაცია;

ე) კომპიუტერული ინციდენტების ანალიზი;

ვ) კომპიუტერული ინციდენტების შედეგების გამოსწორებისა და ზიანის მინიმიზაციის პროცესში დახმარების გაწევა;

ზ) კომპიუტერული ინციდენტების პრევენციისკენ მიმართული ზომების კოორდინაცია და ამგვარი ზომების დანერგვაში დახმარების გაწევა;

თ) ინფორმაციული უსაფრთხოების საკითხებზე ცნობიერების ამაღლება, მათ შორის, კრიტიკულ ინფორმაციულ სისტემაში არსებული საფრთხეებისა და სუსტი წერტილების შესახებ ინფორმაციის მიწოდება, თუ ინფორმაციის ამგვარი ხელმისაწვდომობა ზიანს არ აყენებს ინფორმაციულ უსაფრთხოებას;

ი) შესაძლო საფრთხეების შესახებ მომხმარებელთა ფართო წრის გაფრთხილება და მისთვის სათანადო ინფორმაციის მიწოდება;

კ) ინფორმაციული უსაფრთხოების საკითხებზე საგანმანათლებლო და ინფორმაციული უზრუნველყოფა;

ლ) საერთაშორისო დონეზე ინფორმაციული უსაფრთხოების საკითხებში წარმომადგენლობა და კოორდინაცია;

მ) სხვა მოვალეობები, რომლებიც დაკავშირებულია ინფორმაციული უსაფრთხოების მიზნებთან და განისაზღვრება კანონით ან სხვა ნორმატიული აქტით.

4. დახმარების ჯგუფს უფლება აქვს, მოითხოვოს კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივის, ინფორმაციული სისტემის ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალი საგნის წვდომა, თუ ამგვარი წვდომა

აუცილებელია მიმდინარე ან მომხდარ კომპიუტერულ ინციდენტზე სათანადო რეაგირებისათვის. ინფორმაციული უსაფრთხოების მენეჯერი მოთხოვნის გონივრულ ვადაში განხილვის შედეგად დახმარების ჯგუფს დაუყოვნებლივ აცნობებს შესაბამისი წვდომის შესაძლებლობის ან შეუძლებლობის შესახებ.

5. დახმარების ჯგუფის კომპეტენცია, მუშაობის პროცედურები, კომპიუტერულ ინციდენტებზე რეაგირების მექანიზმები და საქმიანობის სხვა წესები დგინდება მონაცემთა გაცვლის სააგენტოს ნორმატიული აქტით.

მუხლი 9. კომპიუტერული უსაფრთხოების სპეციალისტი

1. კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია განსაზღვროს კონკრეტული პირი (პირები) ან თანამშრომელი (თანამშრომლები), რომელიც (რომლებიც) პასუხისმგებელია (პასუხისმგებელი არიან) კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული სისტემების უსაფრთხოების პრაქტიკული უზრუნველყოფისათვის (კომპიუტერული უსაფრთხოების სპეციალისტი).

2. კომპიუტერული უსაფრთხოების სპეციალისტის ძირითადი მოვალეობებია:

ა) კომპიუტერული სისტემების ყოველდღიური მონიტორინგი და შეფასება;

ბ) კომპიუტერული ინციდენტების იდენტიფიცირება და მათზე რეაგირება;

გ) კომპიუტერული ინციდენტებისა და უსაფრთხოების ზომების ანალიზი და ანგარიშგება;

დ) დახმარების ჯგუფთან კოორდინაცია;

ე) სხვა მოვალეობები, რომლებსაც განსაზღვრავს კრიტიკული ინფორმაციული სისტემის სუბიექტი.

3. კომპიუტერული უსაფრთხოების სპეციალისტი ანგარიშვალდებულია კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული ტექნოლოგიების სამსახურის ხელმძღვანელის ან მის მიერ შესაბამისად უფლებამოსილი თანამშრომლის წინაშე.

4. კომპიუტერული უსაფრთხოების სპეციალისტი ხელმისაწვდომი უნდა იყოს ნებისმიერ დროს, მათ შორის, სამუშაო საათების შემდეგ. იგი ვალდებულია უზრუნველყოს მონაცემთა გაცვლის სააგენტოსთან მუდმივი კოორდინაცია კრიტიკული ინფორმაციული სისტემის სუბიექტზე მიმდინარე ან სავარაუდო კიბერშეტევის პირობებში, ასევე ამ კიბერშეტევის შედეგების აღმოფხვრის პროცესში.

5. თუ მიმდინარე ან სავარაუდო კიბერშეტევა განსაკუთრებულ საფრთხეს უქმნის ქვეყნის თავდაცვისუნარიანობას, ეკონომიკურ უსაფრთხოებას, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალურ ფუნქციონირებას, მონაცემთა გაცვლის სააგენტო უფლებამოსილია განახორციელოს კომპიუტერული უსაფრთხოების სპეციალისტების დროებითი კოორდინაცია კიბერშეტევის თავიდან აცილების, მოგერიების ან/და მისი შედეგების აღმოფხვრის მიზნით.

მუხლი 10. კომპიუტერული ინციდენტის იდენტიფიცირება

1. კრიტიკული ინფორმაციული სისტემის სუბიექტი ახორციელებს კომპიუტერული ინციდენტების იდენტიფიცირებას, რაც მოიცავს თითოეული ინციდენტის შესწავლასა და აღწერას და მასზე რეაგირებას.
2. კრიტიკული ინფორმაციული სისტემის სუბიექტთან შეთანხმებით, მონაცემთა გაცვლის სააგენტო და კომპიუტერული უსაფრთხოების სპეციალისტი კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელში ახორციელებენ კომპიუტერული ინციდენტების იდენტიფიცირებისა და კვლევისათვის აუცილებელი ქსელური სენსორის (სენსორების სისტემის) კონფიგურირებასა და მართვას. ქსელური სენსორის კონფიგურაციის წესები დგინდება მონაცემთა გაცვლის სააგენტოს ნორმატიული აქტით.
3. კომპიუტერული ინციდენტის იდენტიფიცირების შესახებ დაუყოვნებლივ ეცნობება დახმარების ჯგუფს და, აუცილებლობის შემთხვევაში, ხორციელდება გადაუდებელი ღონისძიებები ამ ინციდენტის შესახებ ინფორმაციის შენახვისა და დაცვის მიზნით.
4. დახმარების ჯგუფი შეისწავლის და აღწერს კომპიუტერულ ინციდენტებს და ახორციელებს მათზე ადეკვატურ რეაგირებას ამ კანონით გათვალისწინებული ფუნქციების შესრულებისას.

თავი IV
გარდამავალი და დასკვნითი დებულებები
მუხლი 11. გარდამავალი დებულებები
1. ამ კანონის ამოქმედებიდან 6 თვის ვადაში საქართველოს პრეზიდენტმა გამოსცეს ბრძანებულება „კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ“.
2. ამ კანონის ამოქმედებიდან 6 თვის ვადაში მონაცემთა გაცვლის სააგენტომ გამოსცეს შემდეგი ნორმატიული აქტები:
ა) ბრძანება „მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ“;
ბ) ბრძანება „კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისათვის მინიმალური სტანდარტების დამტკიცების შესახებ“;
გ) ბრძანება „ქსელური სენსორის კონფიგურაციის წესების შესახებ“;
დ) ბრძანება „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შესახებ“;
ე) ბრძანება „ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირთა და ორგანიზაციათა მიერ ავტორიზაციის გავლის წესის, ავტორიზაციის პროცედურებისა და ავტორიზაციის საფასურის შესახებ“;
ვ) ბრძანება „ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის შესახებ“;
ზ) ბრძანება „ინფორმაციული აქტივების მართვის წესების შესახებ“.

მუხლი 12. დასკვნითი დებულება
ეს კანონი ამოქმედდეს 2012 წლის 1 ივლისიდან.
საქართველოს პრეზიდენტი მ. სააკაშვილი

თბილისი,
2012 წლის 5 ივნისი.
№6391-Iს

კიბერ ლექსიკონი

Access
დაშვება, წვდომა, კავშირი ქსელთან.

Access level
წვდომის დონე

Access Privileges
წვდომა კონკრეტულ ფაილებთან. ამასთან, განსაზღვრული ოპერაციების ჩატარების უფლებებით.

Application
პროგრამული უზრუნველყოფა. პროგრამა.

Archie
FTP სერვერებზე განთავსებული ფაილების ძიების საშუალება.

ARJ
MS DOS პლატფორმის პოპულარული პროგრამა, ფაილების არქივირებისთვის.

ASCII
სტანდარტული კოდირების აბრევიატურა, რომელიც ასე იშიფრება: American Standard Code for Information Interchange

AT - ბრძანებები
მოდემთან სამუშაო ბრძანებები.

Backbone
ინტერნეტის მთავარი, მაღალსიჩქარიანი მაგისტრალი.

Bandwidth
სიხშირეთა დიაპაზონი. ქსელში ინფორმაციის გადაცემის სიჩქარის საზომი.

Baud
ქსელში გადაცემული ინფორმაციის რაოდენობა წამში.

BBS
Bulletin Board System - ინტერნეტ სერვისი ტიპი, რომლის საშუალებითაც მომხარებლებს შეუძლიათ: წაიკითხონ, გამოაქვეყნონ სხვადასხვა შეტყობინება ან

სტატია, გაცვალონ და ჩამოტვირთონ ფაილები. ასე მაგალითად: ფორუმები, ჩატები და სოციალური ქსელის სხვა კომპონენტები.

BPS
ერთი ბიტი წამში. ინფორმაციის საზომი ერთეული.

Broadband
მაღალსიჩქარიანი კავშირის ხაზი.

Busy
მოდემის შეტყობინება, დაკავებული ხაზის შესახებ.

Capacity
მოცულობა. ასევე ინფორმაციის გადაცემის მაქსიმალური სიჩქარე.

Carrier
კავშირი. თითქმის იგივე რაც Connect.

CATV
საკაბელო ტელევიზია.

Client Application
კლიენტ-სერვერული არიტექტურით აგებული პროგრამული უზრუნველყოფის სამომხმარებლო ნაწილი.

CMC
Computer Mediated Commonwealth - კავშირი კომპიუტერების გამოყენებით.

Command line
პროგრამული ბრძანების ხაზი.

Communication Link
კომუნიკაცია-კავშირისათვის საჭირო პროგრამული და ტექნიკური უზრუნველყოფა.

Connect
კომუნიკაციის ლოგიკური გზა, განსაზღვრული ორი “სოკეტის” საშუალებით.

Connection
კავშირი.

Cracker
ჰაკერების ქვე ტიპი. ადამიანი, რომელიც დაკავებულია ფასიანი პროგრამული უზრუნველყოფის გაუფასურებით. ბევრი საერთო აქვთ მეკობრეებთან.

CTCP
Client To Client Protocol. IRC-ის მახასიათებელი პროტოკოლი.

Data compression
მონაცემების შეკუმშვა, კომპრესაცია, მოცულობის შემცირება.

Data link
კავშირის ხაზი.

Database
მონაცემთა ბაზა.

DCE
ქსელური უზრუნველყოფისთვის საჭირო ტექნიკური საშუალებები.

Dedicated Line
გამოყოფილი ხაზი.

Dialtone
ტელეფონის ზუმერი, როდესაც ხაზი არ არის დაკავებული.

Distribution
მომხმარებლის მიერ განსაზღვრული სივრცე ელექტრონული ფოსტის გასაგზავნად.

DNS
Domain Name System. მისამართების დომენური სისტემა. რომელიც ახდენს ციფრების კონვერტაციას ასოებში და პირიქით, რითაც უნიკალურ მისამართს ანიჭებს კონკრეტულ ობიექტს ლოკალურ და გლობალურ ქსელში.

Domain
ინტერნეტის ქვედანაყოფი. ყოველ მისამართს აქვს თავისი “კუდი”. მაგალითად: .com, .net, .mil, .org და ა.შ. ისინი განისაზღვრება დანიშნულების ან ქვეყნის მიხედვით.

Editor
პროგრამული უზრუნველყოფა, რომელიც განკუთვნილია რაიმეს რედაქტირებისათვის.

ELM
Electronic Mail. UNIX-ის ელექტრონული ფოსტა.

EMACS
UNIX-ის ტექსტური რედაქტორი.

FAQ

Frequently asked questions. დოკუმენტაცია, რომელიც შედგება პასუხებით ყველაზე ხშირად დასმულ შეკითხვებზე კონკრეტული თემის გარშემო.

Firewall
ვირტუალური კედელი, ჰაკერებსა და კომპიუტერის მომხმარებელს შორის, რომელიც იცავს ამ უკანასკნელს მის სისტემაში არამართლზომიერი შეღწევებისა და მავნე პროგრამების თავდასხმისაგან.

Freenet
ინტერნეტით უფასო სარგებლობა.

Freeware
უფასო პროგრამული უზრუნველყოფა.

Fricker
ჰაკერების ქვე ტიპი. ადამიანი, რომელიც დაკავებულია სატელეფონო ხულიგნობით. მაგალითად მოსმენებით და ფასიანი სერვისების გატეხვით მათი შემდგომი უფასო მოხმარების მიზნით.

FSF
Free Software Foundation - უფასო პროგრამული უზრუნველყოფის ფონდი..

FTP
File Transfer Protocol – გლობალურ ქსელში ფაილების ბრუნვის, მიმოცვლის მეთოდი.

FSP
FTP-ს მსგავსი, ფაილების გადაცემის სისტემა.

FTP - Client
FTP-სთან დაკავშირებისთვისათვის საჭირო პროგრამული უზრუნველყოფის ტიპი.

GNU
UNIX-ის პლატფორმაზე არსებული უფასო პროგრამული უზრუნველყოფის გავრცელება.

GUI
Graphical User Interface - მომხმარებლის გრაფიკული ინტერფეისი.

Handshake
თანხმობა მოდემებს შორის.

Hyperlink
ბმული. კავშირი ინფორმაციის სხვადასხვა წყაროსთან.

Host
მთავარი კომპიუტერი.

HTTP
HyperText Transport Protocol - ინფორმაციის მიმოცვლის სისტემა ინტერნეტში.

IMHO
In My Humble Opinion - "ჩემი მოკრძალებული აზრით". განსაკუთრებით პოპულარულია სოციალურ ქსელში ურთიერთობისას.

IP Address
32 ბიტიანი მისამართი ინტერნეტ პროტოკოლისა, რომელიც შეიცავს კომპიუტერის უნიკალურ მისამართს.

ISDN
Integrated Switched Digital Network - მაღალსიჩქარიანი ციფრული სატელეფონო სისტემა.

ITR
Internet Talk Radio - ერთგვარი ვირტუალური რადიოსადგური, რომელიც განთავსებულია ქსელში.

LAN
Local Area Network - ლოკალური ქსელი.

Login
მომხარებლის საიდენტიფიკაციო სახელი. ასევე, ავტორიზაციის პროცესი.

MIME
Multipurpose Internet Mail Extensions - ელქტრონული ფოსტით, მულტიმედია ფაილების გადაცემის პროტოკოლი (გრაფიკული და მუსიკალური ფაილები).

Net
კომპიუტერული ქსელი.

Network
კომპიუტერული ქსელი - კომუნიკაციის საშუალება (კაბელები, სატელეფონო ხაზები, თანამგზავრული კავშირი და ა.შ.).

PDN
Public Data Network - ღია ქსელი ყველა მომხარებლისთვის.

POP
Post Office Protocol - ელექტრონული ფოსტის პროტოკოლი.

Protocol
მეთოდი, რომლის საშუალებითაც ხდება ინფორმაციის მიმოცვლა სერვერსა და მომხარებელს შორის.

Remote
დაშორებული, მოწყვეტილი კავშირი. როდესაც ინფორმაცია იმყოფება სერვერზე და თქვენ მუშაობთ მასზე სხვა კომპიუტერის ან მობილური ტელეფონის გამოყენებით, დაშორებულ მანძილზე.

Remote computer
სერვერი, რომელზედაც დაშორებული კავშირის დროს იმყოფება ინფორმაცია.

Remote control
დისტანციური მართვა.

Root Folder
მთავარი საქაღალდე სერვერზე, ფალების კატალოგი.

Rout
მარშრუტი.

Router
მარშრუტიზატორი.

Script
პროგრამული სცენარი. პროგრამული კოდი, რომლის მოქმედებაც წინასწარ არის გაწერილი.

Server
სისტემა, რომელსაც შეუძლია ქსელის ორგანიზება. მთავარი კომპიუტერი.

Shareware
ფასიანი პროგრამული უზრუნველყოფა, რომელიც დაცულია ან გავრცელებულია სადემონსტრაციო ვერსიის სახით.

Sharing
რაიმე რესურსის ერთდროული გამოყენება – გაზიარება.

SMTP
Simple Mail Transport Protocol - საფოსტო გზავნილების მიმოცვლის პროტოკოლი.

Spam

ელექტრონული ფოსტის მასიური დაგზავნა. ხშირად გამოიყენება პატარა კომპანიების სარეკლამო მიზნებისთვის, მაგრამ რაკი სპამი ცუდ ტონად ითვლება, იგი სულ უფრო და უფრო ნაკლებად პოპულარული ხდება.

TCP
Transmission Control Protocol - მთავარი სატრანსპორტო პროტოკოლი. ინფორმაციის მიმოცვლის ერთ-ერთი ყველაზე პოპულარული პროტოკოლი, დახურული და ღია კავშირისთვის.

TCP/IP
Control Protocol/Internet Protocol - ინტერნეტთან მაკავშირებელი სტანდარტული პროტოკოლი.

Telnet
კომუნიკაციისათვის საჭირო პროტოკოლი. პროგრამა, რომელსაც აქვს საკუთარი სპეციალური ბრძანებები, სერვერებთან და ინტერნეტთან სამუშაოდ.

Traffic
ინფორმაციის ნაკადი.

UDP
ერთ-ერთი ყველაზე მნიშვნელოვანი ქსელური პროტოკოლი.

URL
Uniform Resource Locator - სტანდარტული მისამართი WWW ან FTP ტიპის რესურსებისა.

Whois
ინტერნეტში ძებნის საშუალება, რომლითაც დგინდება ვებ-რესურსების მისამართის ავტორის ვინაობა და მისი სარეგისტრაციო ინფორმაცია.

ბიბლიოგრაფია

წიგნში გამოყენებული მასალების ჩამონათვალი:

დაზვერვისა და კონტრდაზვერვის ისტორიული საფუძვლები - დავით კუხალაშვილი

სამართლის ზოგადი თეორია (2007) ბიძინა სავანელი

ინტერნეტის გლობალური სტატისტიკა: http://www.internetworldstats.com

საქართველოს იუსტიციის სამინისტროს საკანონმდებლო მაცნეს ვებ-გვერდი: https://matsne.gov.ge/

Homeland Security: Principles and Practice of Terrorism Response By Paul M. Maniscalco and Dr. Hank T. Christen

Shadow Market - 2011 bsa global software piracy study

CYBER CRIME AND INFORMATION WARFARE - Dr Peter Grabosky
Australian Institute of Criminology, ACT

NY Times - Before the gunfire - By John Markoff

აშშ-ს გამოძიების ფედერალური ბიუროს სპეციალური ანგარიშები ტერორიზმზე 2002-2005 წლებისთვის

ჰაკერების შესახებ ბიოგრაფიული მონაცემები მოძიებულია ინტერნეტ ენციკლოპედია Wikipedia–ზე და შემდეგი წიგნიდან: Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw – By The Man Who Did It – Tsutomo Shimamura with John Markoff

Защита от компьютерного терроризма - А. Соколов, О. Степанюк

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - Т. Л. Партыка, И. И. Попов

INFORMATION SECURITY - Principles and Practice Second Edition by Mark Stamp
San Jose State University - San Jose, CA

Cyber Attacks Knock Out Georgia's Internet Presence – Gregg Keizer

INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS - Eneken Tikk, Kadri Kaska, Liis Vihul

Cyber Attacks Against Georgia: Legal Lessons Identified NATO Unclassified Version 1.0 by Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul

უსაფრთხოების ექსპერტთა კავკასიის აკადემია

ADVANCING SECURITY AS A PROFESSION!
უსაფრთხოების როგორც პროფესიის განვითარებისთვის!

სამხედროების, სამართალდამცავების, დიპლომატების, მსხვილი კორპორაციებისა და სტუდენტების მომზადების მრავალწლიანი გამოცდილების უსაფრთხოების ექსპერტთა კავკასიის აკადემია (CASE) თავისი სპეციფიკით ერთადერთი კვლევითი და საგანმანათლებლო ორგანიზაციაა სრულიად კავკასიის მასშტაბით. CASE-ის სტუდენტები არიან IT სპეციალისტები, სამხედროები, იურისტები, დიპლომატები, ჟურნალისტები. სხვადასხვა პროფესიის, ასაკისა და ინტერესის ადამიანები.
ახალი საფრთხეებისა და გამოწვევების წინააღმდეგ, რომლებიც ჩვენი საზოგადოების, ბიზნესისა და ეროვნული უსაფრთხოების წინაშე დგას, აკადემიის გარშემო შეიკრიბა გამოცდილ პროფესიონალთა ძლიერი გუნდი, უსაფრთხოების სხვადასხვა სპეციალური სამსახურების თანამშრომლები, ანალიტიკოსები, ინსტრუქტორები, სამხედრო ექსპერტები და სხვა სფეროს წარმომადგენლები კერძო და სახელმწიფო სექტორიდან. ჩვენი მიზანია ხელი შევუწყოთ უფრო უსაფრთხო და სტაბილური გარემოს ჩამოყალიბებას. ამ მეტად ამბიციური მიზნების განსახორციელებლად ჩვენ გვაქვს მოვლენების განსაკუთრებული ხედვა, გაგვაჩნია ძლიერი გუნდი, ექსპერტიზა, გამოცდილება და მოტივაცია. აკადემიის საქმიანობა ითვალისწინებს მჭიდრო თანამშრომლობას როგორც სახელმწიფო და კერძო სექტორთან, ისე საერთაშორისო ორგანიზაციებთან. იმისათვის, რომ დავნერგოთ სფეროს ახალი სტანდარტები, მოვამზადოთ კვალიფიციური ადამიანური რესურსი და ხელი შევუწყოთ უსაფრთხო გარემოს ფორმირებას, უსაფრთხოების ექსპერტთა კავკასიის აკადემია ახორციელებს სპეციალურ ტრენინგებს, რომლებიც კავკასიის მასშტაბით სხვაგან არსად არის ხელმისაწვდომი, ატარებს რეგიონალურ და საერთაშორისო კონფერენციებს, ნერგავს ინოვაციურ საგანმანათლებლო პროგრამებს, ეწევა ყოველდღიურ ანალიტიკურ საქმიანობას და ეხმარება სფეროს სპეციალისტებს გამოცდილების გაცვლასა და ერთმანეთთან დაკავშირებაში. აკადემია აერთიანებს სადაზვერვო, ანტი-ტერორისტულ, ტექნოლოგიურ, პოლიტიკურ და დიპლომატიურ საკითხებს, რათა შეავსოს გამოტოვებული ადგილები გლობალური და ეროვნული უსაფრთხოების გარემოში და ხელი შეუწყოს უსაფრთხოების, როგორც პროფესიის განვითარებას.
უსაფრთხოების ექსპერტთა კავკასიის აკადემია (CASE) ძირითად საგანმანათლებლო და კვლევით საქმიანობასთან ერთად ახორციელებს სხვადასხვა ღონისძიებებს საზოგადოებრივი ცნობადობის ასამაღლებლად და უსაფრთხოების, როგორც პროფესიის განვითარებისთვის. ჩვენ გვჯერა, რომ გლობალური უსაფრთხოების გარემოს აქტუალური პრობლემების საუკეთესო გადაწყვეტა სწორედ კვალიფიციურ საკადრო რესურსში და ინფორმირებულ საზოგადოებაშია.

სრული ინფორმაციისთვის ეწვიეთ აკადემიის ოფიციალურ ვებ-გვერდს: www.globalcase.org

კიბერ უსაფრთხოების ტრენინგები IT განათლების საუკეთესო პროვაიდერისაგან!

IT განათლების საუკეთესო პროვაიდერი

როდესაც საუბარი კორპორაციული უსაფრთხოების ერთ-ერთ ყველაზე დელიკატურ ასპექტზეა, მნიშვნელოვანია შეარჩიოთ სწორი პარტნიორი, რომელიც მაღალი პროფესიული სტანდარტით, მდიდარი გამოცდილებითა და პროფესიონალების გუნდით შეძლებს რეალურად დაიცვას თქვენი ორგანიზაცია დღეს არსებული გამოწვევებისაგან. უსაფრთხოების ექსპერტთა კავკასიის აკადემია იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტოსა და ICT ბიზნეს საბჭოს მიერ აღიარებულია IT განათლების საუკეთესო პროვაიდერად. ორგანიზაციის რეპუტაციაზე ინსტრუქტორების გუნდის გარდა ასევე მეტყველებენ ის სახელები, ჩვენს პორტფოლიოში, რომლებიც საკუთარ უსაფრთხოებას CASE-ს ანდობენ.

უსაფრთხოების ექსპერტთა კავკასიის აკადემია

სამხედროების, სამართალდამცავების, დიპლომატების, მსხვილი კორპორაციებისა და სტუდენტების მომზადების მრავალწლიანი გამოცდილების უსაფრთხოების ექსპერტთა კავკასიის აკადემია (CASE) თავისი სპეციფიკით ერთადერთი კვლევითი და საგანმანათლებლო ორგანიზაციაა სრულიად კავკასიის მასშტაბით. CASE-ის სტუდენტები არიან IT სპეციალისტები, სამხედროები, იურისტები, დიპლომატები, ჟურნალისტები. სხვადასხვა პროფესიის, ასაკისა და ინტერესის ადამიანები.

ახალი საფრთხეებისა და გამოწვევების წინააღმდეგ, რომლებიც ჩვენი საზოგადოების, ბიზნესისა და ეროვნული უსაფრთხოების წინაშე დგას, აკადემიის გარშემო შეიკრიბა გამოცდილ პროფესიონალთა ძლიერი გუნდი, უსაფრთხოების სხვადასხვა სპეციალური სამსახურების თანამშრომლები, ანალიტიკოსები, ინსტრუქტორები, სამხედრო ექსპერტები და სხვა სფეროს წარმომადგენლები კერძო და სახელმწიფო სექტორიდან. ჩვენი მიზანია ხელი შევუწყოთ უფრო უსაფრთხო და სტაბილური გარემოს ჩამოყალიბებას. ამ მეტად ამბიციური მიზნების განსახორციელებლად ჩვენ გვაქვს მოვლენების განსაკუთრებული ხედვა, გაგვაჩნია ძლიერი გუნდი, ექსპერტიზა, გამოცდილება და მოტივაცია. აკადემიის საქმიანობა ითვალისწინებს მჭიდრო თანამშრომლობას როგორც სახელმწიფო და კერძო სექტორთან, ისე საერთაშორისო ორგანიზაციებთან. იმისათვის, რომ დავნერგოთ სფეროს ახალი სტანდარტები, მოვამზადოთ კვალიფიციური ადამიანური რესურსი და ხელი შევუწყოთ უსაფრთხო გარემოს ფორმირებას, უსაფრთხოების ექსპერტთა კავკასიის აკადემია ახორციელებს სპეციალურ ტრენინგებს, რომლებიც კავკასიის მასშტაბით სხვაგან არსად არის ხელმისაწვდომი, ატარებს რეგიონალურ და საერთაშორისო კონფერენციებს, ნერგავს ინოვაციურ საგანმანათლებლო პროგრამებს, ეწევა ყოველდღიურ ანალიტიკურ საქმიანობას და ეხმარება სფეროს სპეციალისტებს გამოცდილების გაცვლასა და ერთმანეთთან დაკავშირებაში. აკადემია აერთიანებს სადაზვერვო, ანტი-ტერორისტულ, ტექნოლოგიურ, პოლიტიკურ და დიპლომატიურ საკითხებს, რათა შეავსოს გამოტოვებული ადგილები გლობალური და ეროვნული უსაფრთხოების გარემოში და ხელი შეუწყოს უსაფრთხოების, როგორც პროფესიის განვითარებას.

უსაფრთხოების ექსპერტთა კავკასიის აკადემია (CASE) ძირითად საგანმანათლებლო და კვლევით საქმიანობასთან ერთად ახორციელებს სხვადასხვა ღონისძიებებს საზოგადოებრივი ცნობადობის ასამაღლებლად და უსაფრთხოების, როგორც პროფესიის განვითარებისთვის. ჩვენ გვჯერა, რომ გლობალური უსაფრთხოების გარემოს აქტუალური პრობლემების საუკეთესო გადაწყვეტა სწორედ კვალიფიციურ საკადრო რესურსში და ინფორმირებულ საზოგადოებაშია.

SD5L1
GOLDEN SEAL CERTIFICATION

გაამყარეთ თქვენი ცოდნა აღიარებული სერთიფიკაციით და დაიმკვიდრეთ თავი პროფესიაში, რომელიც ერთ-ერთი ყველაზე მოთხოვნადი და მაღალანაზღაურებადია მთელს მსოფლიოში. ეს საჭიროა ყველგან სადაც ინფორმაციაა და ამ ინფორმაციას აქვს ფასი.

დღევანდელ რეალობაში უსაფრთხოება მნიშნელოვანი ფაქტორი გახდა არამხოლოდ ბიზნესის უწყვეტობისა და რისკების მართვის კონტექსტში, არამედ მთელს ბაზარზე. სერთიფიკაციის დროს გადამწყვეტი მნიშნელობა აქვს ორგანიზაციის რეპუტაციას. CASE-მა პირველად დაიწყო საქართველოში კიბერ უსაფრთხოების ტრენინგები. სხვა მრავალ პუბლიკაციასთან ერთად აკადემიამ გამოსცა საქართველოში პირველი კიბერ უსაფრთხოების სახელმძღვანელო. CASE-ი არის აშშ-ს კიბერ საინიციატივო ფორუმის, უსაფრთხოების პროფესიონალთა ტრანსატლანტიკური საბჭოსა და სხვა ავტორიტეტული ორგანიზაციების წევრი. CASE-ის სერთიფიკაცია გააჩნია ასეულობით სერთიფიცირებულ პროფესიონალს, რომელიც წარმატებით აგრძელებს კარიერას ქვეყნის სახელმწიფო, სამართალდამცავ, სამხედრო, საგანმანათლებლო და ბიზნეს სექტორში. აკადემია დაჯილდოვებულია საქართველოს სახელმწიფო ავტორიტეტული ორგანიზაციების მიერ როგორც IT განათლების საუკეთესო პროვაიდერია. ჩვენს რეპუტაციაზე ასევე მეტყველებენ ცნობილი სახელები პორტფოლიოდან, რომლებიც საკუთარ უსაფრთხოებას CASE-ს ანდობენ. ეს სწორედ ის ბეგრაუნდია, რომელთანაც ასოცირებული სერთიფიკაცია რეალურ ღირებულებას ატარებს.

შეიტყვეთ მეტი ჩვენს შესახებ და გაიგეთ რას ამბობენ ისინი, ვინც უკვე გაიარა ჩვენი კურსები. დაკლიკეთ მოცემულ ბმულს: youtube.com/watch?v=5GX7g-HI7CE

ასეულობით სერთიფიცირებული პროფესიონალი!

გიორგი გაბიძაშვილი
თავდაცვითი სექტორი

CASE-მა მომცა სიღრმისეული ცოდნა უსაფრთხოების საკითხებში და აღმჭურვა უნარებით, რომლებსაც წარმატებით ვიყენებ ჩემს სამსახურში ყოველდღურად.

ეკა ჯანჯღავა
საბანკო სექტორი

CASE-ი აძლევს ადამიანებს იმ ცოდნას, რომელიც საქართველოს მასშტაბით არც ერთ ორგანიზაციას არ შეუძლია მისცეს!

მიხეილ დავიდოვი
საჯარო სექტორი

აკადემიამ მომცა უნიკალური გამოცდილება და ცოდნა, რაც ყველაზე მნიშვნელოვანია. მე CASE-ელი ვარ!

ნინო გაბრიჩიძე
სტუდენტი

CASE-მა მომცა ცოდნა და კარგი სამეგობრო წრე, რომელიც აქ შევიძინე. ეს ჩემთვის დაუვიწყარი გამოცდილებაა!

ასეულობით სერთიფიცირებული სტუდენტი, მსხვილი კორპორაციები და სახელმწიფო ორგანიზაციები

აკადემია აღიარებულია კიბერ უსაფრთხოების სფეროში მოღვაწე წამყვანი საერთაშორისო ორგანიზაციების მიერ და ასევე მიღებული აქვს ჯილდო საქართველოს ავტორიტეტული სახელმწიფო ორგანოების მიერ როგორც IT განათლების საუკეთესო პროვაიდერი. ჩვენს პორტფოლიოში შედის არაერთი პუბლიკაცია უსაფრთხოების სხვადასხვა საკითხებზე. მათ შორის საქართველოში პირველი სახელმძღვანელო კიბერ უსაფრთხოების შესახებ.

CASE-ის სერვისებით სარგებლობენ უმსხვილესი ადგილობრივი და საერთაშორისო ორგანიზაციები. მათ შორის არიან: მეკობრეობასთან ბრძოლის საკითხებში Microsoft; კორპორაციულ ტრენინგებში British Petroleum-ის კონტრაქტორი კომპანიები; კვლევით პროექტებში Publicis Dialog; სახანძრო უსაფრთხოებაში მსხვილი ინფრასტრუქტურული ობიექტები, როგორიცაა მთაწმინდის პარკი და ა.შ

ქვემოთ მოცემულია კლიენტებისა და პარტნიორების მხოლოდ მცირე ჩამონათვალი. სრული ინფორმაციისთვის ეწვიეთ: globalcase.org

საკონტაქტო ინფორმაცია

ოფისი.: +995 322476006
ელ.ფოსტა.: contact@globalcase.org

ვებ-გვერდი: www.globalcase.org
www.case.ge