**ლექცია № 1.** **ინფორმაციული უსაფრთხოება, როგ­ორც ინფორმაციული ომის შემადგენე­ლი ნაწილი.** ინფორმაციული უსაფრთ­ხოების მნიშვნელობა და ადგილი სა­ხელმწიფო უსაფრთხოების დოქტრი­ნაში. ინფორმაციული უსაფრთხოების უზრუნველყოფის ამოცანები. ინფორ­მაციული რესურსების კლასიფიკაცია. კონფიდენციალური ინფორმაცია და სახელმწიფო საიდუმლოება.

ინფორმაციული ომის თეორიას, რომლის ჩამოყალიბება, ფორმალიზაცია, მოხდა სულ რაღაც სამი-ოთხი ათწლეულის წინ, დღეს უკვე გააჩნია ფართო გამოყე­ნებითი მნიშვნელობა. მას აქტიურად ითვალისწინებენ მრავალი ქვეყნის ინფორმა­ციული უსაფრთხოების შემუშავებისას. პირველად აშშ-ში შეიქმნა საპრეზიდენტო კომისია ე.წ. კრიტიკული ინფრასტრუქტურის დასაცავად, შემდეგ ამ კომისიის დას­კვნებზე შემუშავდა პრეზიდენტის № 63 დირექტივა, რომელიც 1998 წელს გახდა ინფორ­მაციული უსაფრთხოების უზრუნველყოფის სამთავრობო პოლიტიკის საფუძ­ველი. აშშ-ის თავდაცვის სამინისტროს მიერ იქნა გამოყენებული ქსელცენტრუ­ლი ომის ახალი სამხედრო დოქტრინა. ინფორმაციული ომი, ინფორმაციული ოპერაცია ქსელ­ცენტრული ომის დოქტრინის შემადგენელი ნაწილია. დასავლეთის წამყვანი ქვეყ­ნები უკვე ამზადებენ ინფორმაციული ომის ვიწრო სპეციალისტებს. აშშ-ში, თავდაც­ვის ეროვნულ უნივერსიტეტში მოქმედებს ინფორმაციული ომის და სტრატეგიის სკოლა. კალიფორნიის საზღვაო სკოლაში ინფორმაციული ომის ჯგუფს უკითხავენ ლექციების კურსს: ინფორმაციული ოპერაციების პრინციპები; ფსიქოლოგიური ოპერაციები; ინფორმაციული ომი: დაგეგმარება და შეფასება; ინფორმაციული ომის შეფასება. ინფორმაციული ომს სათანადო ყურადღებას უთმობენ უკიდურესი აღმოსავლეთის ქვეყნები: ჩინეთი, იაპონია, კორეა, ავსტრალია. ინფორმაციული ომის თეორიის სხვადასხვა მიმართულებები განიხილება ამისთვის სპეციალურად შექმნილ ათეულობით სამეცნიერო ჟურნალებში, რეგულარულად ტარდება სამეცნიერო კონფერენციები.

რუსეთმა დაგვიანებით, მაგრამ მანაც დაიწყო ინფორმაციული ომის მიმართულე­ბით მოქმედება. რუსეთის თავდაცვის სამინისტრო ინფორმაციულ-პროპაგანდის­ტულ ცენტრს ქმნის, რომელიც სხვა ამოცანებთან ერთად, მოამზადებს ჰაკერულ შეტევებს მოწინააღმდეგის მედია რესურსებზე. რუსეთის თავდაცვის სამინისტროს ეს გადაწყვეტილება, იყო პასუხი რუსეთის პრეზიდენტის დავალებაზე მოამზადონ წინადადებები იმ სპეციალისტთა ცენტრის შექმნასთან დაკავშირებით, რომლებიც შეძლებენ უთანამედროვესი ტექნოლოგიებით აწარმოონ ინფორმაციული ომის.

საქართველოში 2010 წლის ზაფხულში შეიქმნა ინფორმაციული უსაფრთხოების კვლევებისა და ანალიზის ცენტრი, რომელიც კავკასიის რეგიონში ამ მიმართულებით პირველი ორგანიზაციაა. ცენტრის კვლევის მიმართულებებს წარმოადგენს სხვადას­ხვა სახის ტექნოლოგიური საშიშროების შესწავლა და მათი დეტალური ანალიზი, იქნება ეს კიბერშეტევები, კიბერდანაშაული თუ სხვა.

2012 წლის საგაზაფხულო სესიაზე საქართველოს პარლამენტმა მიიღო კანონი ”ინ-ფორმაციული უსაფრთხოების შესახებ ’’, რომელიც კანონპროექტის სახით იმავე წლის თებერვალს წარედგინა პარლამენტს განსახილველად. კანონი კიბერუსაფ­რთხოების სფეროში ინსტიტუციურ და სამართლებრივ საფუძვლებს და სტანდარ­ტებს აყალიბებს. კანონის თანახმად, სახელმწიფო ავითარებს ერთიან სისტემას, რომლის მიზანია ქვეყნისთვის მნიშვნელოვანი სახელმწიფო თუ კერძო დაწესე­ბულებების ინფორმაციული უსაფრთხოების დაცვა. კანონის შემუშავებაში საქარ­თველოს პარლამენტთან ერთად აქტიურად იყვნენ ჩართულნი საქართველოს ეროვ­ნული უშიშროების საბჭოს აპარატი, საქართველოს იუსტიციის, თავდაცვის, შინაგან საქმეთა სამინისტროების შესაბამისი დეპარტამენტები და მონაცემთა გაცვლის სააგენტო. კანონი მიღებულ იქნა 2012 წლის 5 ივნისს.

თავდაპირველად ტერმინი ”ინფორმაციული ომი” გამოიყენა 1976 წელს *თომას რონამ* თავის ანგარიშში ”იარაღთა სისტემები და ინფორმაციული ომი”, რომელიც განკუთვნილი იყო კომპანია ბოინგისთვის. თ. რონამ მიუთითა, რომ იმ დროისთვის, ინფორმაციული ინფრასტრუქტურა ხდებოდა ამერიკის ეკონომიკის საკვანძო კომპონენტი და ამავდროულად ადვილ, ნაკლებად დაცულ სამიზნედ, როგორც საომარ, ასევე მშვიდობიან დროს.

ტერმინი - ”ინფორმაციული ომის” ერთიანი დეფინიცია ჯერ კიდევ არაა მიღებუ­ლი, მაგრამ ინტუიციურად მიჩნეულია, რომ ინფორმაციული ომი ეს არის მიზანმი­მართული ქმედებები, ინფორმაციული უპირატესობის მისაღწევად, მოწინააღმდეგე მხარის ინფორმაციის, ინფორმაციული სისტემების და პროცესების დაზიანების სა­შუალებით, ამავდროულად ხდება საკუთარი ინფორმაციის, ინფორმაციული სის­ტემების და პროცესების დაცვა. ინფორმაციული ომის ქვეშ ასევე გულისხმობენ სა­ზოგადოებრივ ცნობიერებაზე ინფორმაციული ზემოქმედების ღონისძიებათა კომ­პლექსს, რათა მოხდეს ადამიანთა ქცევის შეცვლა და მათთვის თავს მოხვევა იმ მიზ­ნებისა, რომელიც მათ ინტერესებში არ შედის. ის რომ, ინფორ­მაციული ნაკადი, რო­მელიც თავს დაატყდება მასიურ ცნობიერებას, უმეტეს შემთხვევაში, იძლევა ადამი­ანის მანიპულაციის საშუალებას, მეცნიერულადაა შესწავლილი და ამ ტიპის კვლე­ვებში ქართველ მეცნიერებსაც აქვთ გამოქვეყნებული შედეგები. მეორის მხრივ საჭი­როა ასეთივე ინფორმაციული ზემოქმედებისგან თავის დაცვა.

რადგანაც სახელმწიფოების ინფორმაციული რესურსები ხშირად ხდებიან შეტე­ვისა და თავდაცვის ობიექტები, სახელმწიფო იძულებულია ინფორმაციულ ტექნო­ლოგიებს დაუთმოს დიდი ყურადღება. შესაბამისად ინფორმაციული ომის თეორიაში კვლევების დიდი რაოდენობა მიძღვნილია ინფორმაციის, ინფორმაციული სისტემე­ბისა და პროცესების უსაფრთხოებისადმი.

ინფორმაციული უსაფრთხოების მნიშვნელობა სახელმწიფო დონეზე დღესდღე­ობით საკანონმდებლო და აღმასრულებელი ხელისუფლების ყურადღების ცენტრშია. ამასთან ადამიანს უხსოვარი დროიდან, ისტორიაულად გაცნობიერებული ჰქონდა სიტყვის, როგორც ინფორმაციის მატარებლის ზემოქმედების სიმძაფრე, რაზეც მეტ­ყველებს ხალხურ ზეპირსიტყვიერებაში, ანდაზებში თუ ლიტერატურაში დამკვიდ­რებული ტერმინები და ცნებები: ’შეძახილმა ხე გაახმოო”, ”ენით დაკოდილი” და სხვა. ქრისტიანული რელიგიის თანახმად კი ”პირველითგან იყო სიტყუაჲ, და სიტ­ყუაჲ იგი იყო ღმრთისა თანა, და ღმერთი იყო სიტყუაჲ იგი” *(იოვანეს სახარება. თავი ი, 1*), ამდენად უფლის სიტყვის ძალით შეიქმნა ყოველი ზეგარდმო, ანუ ჯერ უფლის მიერ იყო ნათქვამი სიტყვა და ამის შემდეგ მოხდა ამ სიტყვებში არსებული ინფორმა­ციის მატერიალიზება, მისი რეალიზაცია. და რადგანაც, ქრისტიანული რელიგიის თანახმად, ადამიანი უფალმა თავის ხატებად შექმნა, სრულიად მისაღებია იმის დაშ­ვება, რომ ადამიანის მიერ წარმოთქმულ სიტყვებსაც, გააჩნდეთ თუნდაც მცირე, მაგრამ, მაინც რაღაც დონის მიზანმიმართული ძალა. მით უფრო, რომ ძველ აღთქმაში უფალი ადამიანს უკრძალავს სიტყვის არასათანადო, სხვისთვის საზიანოდ გამოყენე­ბას: ”ცრუ ხმები არ დაყარო, ბოროტმოქმედს არ დაუჭირო მხარი ცრუ მოწმობით” (*გამოსვლა თ. 23.1*) , მეცხრე მცნებაში კი ნათქვამია -” არა ცილისწამო მოყუასსა შენსა წამებითა ცრუჲთა”. ”ცრუ ხმა”, ანუ თანამედროვე გაგებით დეზინფორმაცია, ძველ დროშიც, მცირე კომუნიკაციების პერიოდშიც კი ადამიანზე უარყოფითი ზემოქმე­დების საშუალებას წარმოადგენდა. გაცილებით მეტია თანამედროვე ეპოქაში, ყოვ­ლისმომცველ ინფორმაციულ სივრცეში მყოფ ადამიანზე ”ცრუ ხმების” - დეზინფორ­მაციის, როგორც ინფორმაციული ომის ერთ-ერთი შემადგენელი ნაწილის, ნეგატიური ზემოქმედების ხარისხი.

ინფორმაციული ტექნოლოგიების ეპოქაში, სადაც ადამიანი მუდმივად და ტოტა­ლურად განიცდის ინფორმაციულ ზეწოლას, აქტუალურია ინფორმაციული ზემოქ­მედების პროცესების შესწავლა, მათ შორის იმისთვისაც, რომ მოხერხდეს თავის დაც­ვა პერმანენტულად მიმდინარე ინფორმაციული ომში. სწორედ ამის შესახებ საუბ­რობს თავის საშობაო ეპისტოლე-ში 2010 წელს *უწმიდესი და უნეტარესი, სრულიად საქართველოს კათოლიკოს-პატრიარქი ილია მეორე* : ”კაცობრიობა ახალი ტიპის და­პირისპირებაზე - ინფორმაციულ ომზე გადავიდა და იგი ძირითადად, მასმედიის საშუალებით ხორციელდება. აშკარაა, რომ ჩვენს წინააღმდეგ სხვადასხვა მიმართუ­ლებით მიმდინარეობს ინფორმაციული ომი**,** და ამ ყოველივეს შესაბამისი საშუალე­ბებითვე უნდა გაეცეს პასუხი” .

აღნიშნული მიზნის მისაღწევათ ინფორმაციული ომის შესწავლა მათემატიკური მეთოდებით წარმოადგენს ძალზედ პერსპექტიულ მიმართულებას. კერძოდ კი ინ­ფორმაციული ომის მათემატიკური მოდელირება, რომელიც გულისხმობს მათემა­ტიკური თანაფარდობებით მოდელის შექმნის ეტაპს, შემდგომ მისი ალგორითმი­ზაციის ეტაპს და ბოლოს შესაბამისი პროგრამების შედგენის ეტაპს, წარმოადგენს კვლევებისთვის მეტად მოქნილ, უნივერსალურ და არაძვირ ინსტრუმენტს, მეთოდს. მათემატიკური მოდელირების ეს ტრიადა იძლევა საშუალებას გამოთვლითი ექსპე­რიმენტების ჩატარებით მოხდეს მოდელის ადეკვატურობის შეფასება რეალობასთან, და დადებითი დასკვნის შემდეგ შესაძლებელია მოდელზე სხვადასხვა ექსპერიმენ­ტის ჩატარება, რათა მიღებულ იქნას შესასწავლი ობიექტის რაოდენობითი და ხარის­ხობრივი მახასიათებლები.

ინფორმაციული ომის სხვადასხვა კომპონენტის აღწერა მათემატიკური აპარატით და მისი შესწავლა წარმოადგენს მეცნიერთა მზარდი ინტერესის სფეროს. ამ მხრივ სხვადასხვა ტიპის მათემატიკური მოდელირების გამოყენება მიმდინარეობს რამდე­ნიმე მიმართულებით. მაგალითად, აღსანიშნავია ინფორმაციული ზემოქმედების მოდელის აგებისთვის კავშირის არხებით ინფორმაციის გადაცემის მათემატიკური თეორიის გამოყენება. ამ მოდელის საშუალებით განხორციელებულია კონკრეტული ინფორმაციული ზემოქმედების ეფექტურობის შეფასების მცდელობა. გრაფთა და თამაშთა თეორიის გამოყენებით შედგენილია საინფორმაციო ქსელების და ინფორ­მაციული ომის მოდელები. მათში იძებნება შერეული სტრატეგიები დაპირისპირებუ­ლი მხარეებისთვის. სტრატეგიები ძირითადად გათვლილია, როგორც ფიზიკური, ასევე პროგრამული (ვირუსები, ტროიანები, კიბერშეტევები) ზემოქმედების საშუ­ალებით ინფორმაციული ინფრასტრუქტურის მწყობრიდან გამოყვანაზე, ან მათ დაცვაზე.

რატომ გახდა ჩვენს დროში ინფორმაცია, მისი უსაფრთხოება, ასეთი ყურადღების ქვეს?

თანამედროვე სამყაროს წარმოდგენა კომუნიკაციისა და გამოთვლითი ტექნი­კის საშუალებების გარეშე შეუძლებელია. ინფორმაციული ტექოლოგიები ვითარ­დება ძალზედ სწრაფად და ისინი მოიცავს ადამიანური შემოქმედების კიდევ უფრო ფარ­თო არეალს. ამდენად, ინფორმაციული ტექნოლოგიების უსაფრთხოება მათი ფუნ­ქციონირების უზრუნველყოფის უმნიშვნელოვანეს საკითხს წარმოადგენს. ინფორ­მაცია წარმოადგენს ცნობებს, რომლებიც მიიღება გამოკვლევების, შესწავლის ან განსწავლის შედეგად; სიახლეს, ფაქტებს, მონაცემებს; ბრძანებეს ან მონაცემთა წარ­მოდგენის სიმბოლოებს (კავშირის საშუალებებში ან კომპიუტერზე); ცოდნას (შეტყო­ბინება, ექსპერიმენტული მონაცემები, გამოსახულებები), რომლებიც ცვლი­ან ფიზი­კური ან გონებრივი გამოცდილების შედეგად მიღებულ კონცეფციას. უსაფრთხოება განისაზღვრება, როგორც თავისუფლება საფრთხეთაგან, დაცულობა. თუ გავაერთი­ანებთ ამ ორ ცნებას, მივიღებთ ინფორმაციული უსაფრთხოების განსაზღვრას, რომე­ლიც წარმოადგენს არასანქცირებული გამოყენების, ბოროტად გამოყენების, ცნობე­ბის, ფაქტების, მონაცემების ან აპარატურული საშუალებების შეცვლის ან მათ წვდო­მაზე მტყუნების აღმოფხვრის მიზნით მიღებულ ზომებს.

ზემოთქმულიდან გამომდინარე ინფორმაციული უსაფრთხოება არ უზრუნ­ველ­ყოფს აბსოლუტურ დაცვას. ინფორმაციული უსაფრთხოება არის გამაფრთ ხილებელ მოქმედებათა ერთობლიობა, რომელიც საშუალებას იძლევა დაცულ იქნას ინფორ­მაცია და მოწყობილობები საფრთხეთაგან, რომელიც მოსალოდნელია მათი სუსტი ადგილების გამოყენებით.

კომუნიკაციები და ინფორმაციული ტექნოლოგიები ქმნის ერთ მთლიანობას, რა­საც განსაკუთრებით ხელი შეუწყო ინტერნეტის ქსელის გამოყენებამ, რომელიც კო­მუნიკაციის გლობალური და საყოველთაო გარემო გახდა. კომპიუტერებისა და კომ­პიუტერული ქსელების რიცხვის ზრდამ, ქსელური ტექნოლოგიების და ინტერნეტის ტექნოლოგიების უფრო ფართო გამოყენებამ მნიშვნელოვნად გააფართოვა არა მხო­ლოდ მომხმარებლები და მათი ერთმანეთთან ურთიერთობათა საშუალებები, არა­მედ გაზარდა ქსელური ბიზნეს-პროცესების რეალიზაციის შესაძლებლობები. ორ­განიზაციებს, კომპანიებს და რიგით მომხმარებლებს ყოველდღიურ საქმიანობაში ინტერნეტ-ტექნოლოგიების გამოყენების შესაძლებლობა მიეცათ. ინტერნეტ-ტექნო­ლოგიების მზარდ შესაძლებლობებთან ერთად იზრდება მონაცემების დაკარგვის რისკი, ასევე რეპუტაციის და ფინანსური დანაკარგები. სტატისტიკა უჩვენებს, რომ ყოველწლიურად იზრდება კომპიუტერული დამნაშავეების მიერ მიყენებული ფი­ნანსური ზარალი. აქედან გამომდინარე ორგანიზაციებს, კომპანიებს და რიგით მომ­ხმარებლებს უხდებათ გამოყონ დრო და საშუალებები ინფორმაციისა და ქსე­ლური რესურსების უსაფრთხოების დაცვის უზრუნველსაყოფად. თანამედროვე განაწილე­ბული კომპიუტერული სისტემების დაცვა არ შეიძლება შემოისაზღვროს დაცვის მხოლოდ ორგანიზაციული ზომებისა და ფიზიკური საშუალებების გამოყენებით.

ინფორმაციული ტექნოლოგიების ფუნქციონირების უსაფრთხოებისათვის აუცი­ლებელია ქსელის დაცვის მექანიზმებისა და საშუალებების გამოყენება, რომლებიც უძრუნველყოფს კომპიუტერული სისტემების, პროგრამული უზრუნველყოფისა და მონაცემების **კონფიდენციალობას, მთლიანობასა და წვდომადობას.**

უკანასკნელ ათწლეულში მნიშვნელოვნად გაფართოვდა ინფორმაციული უსაფ­რთხოების უძრუნველყოფის საშუალებები. მრავალი სხვადასხვა ორგანიზაცია ჩა­ერთო დაცვის უზრუნველყოფის ამოცანების გადაწყვეტაში. ინფორმაციული უსაფ­რთხოება მოიცავს უსაფრთხოების მრავალ ასპექტს. საიმედო დაცვა წარმოადგენს დაცვის ყველა საშუალების და მეთოდის გაერთიანებას. საიმედო ფიზიკური დაცვა საჭიროა მატერიალური აქტივების – ქაღალდის მატარებლების და სისტემების და­ცულობის უზრუნველსაყოფად. კომუნიკაციის დაცვა (**COMSEC)** უზრუნველყოფს ინ­ფორმაციის გადაცემის უსაფრთხოებას. გამოსხივების დაცვა (**EMSEC)** საჭიროა, თუ მოწინააღმდეგეს აქვს მძლავრი აპარატურა კომპიუტერული სისტემებიდან ელექ­ტრონული ემისიის წასაკითხად. კომპიუტერული უსაფრთხოება (**COMPUSEC**) საჭი­როა კომპიუტერულ სისტემებში წვდომის მართვისათვის, ხოლო ქსელის უსაფრთხო­ება (**NETSEC)** – ლოკალური ქსელის დაცვისათვის. დაცვის ყველა სახეობა ერთობ­ლივად უზრუნველყოფს ინფორმაციულ უსაფრთხოებას (**INFOSEC**).

**ინფორმაციული უსაფრთხოების უზრუნველყოფის ამოცანები**

ინფორმაციის ცნება დღეისდღეობით გამოიყენება საკმაოდ ფართოდ და მრავალმხრივად. უზარმაზარი ინფორმაციული ნაკადი მოედინება ადამიანების გარშემო. შეიძლება ითქვას, რომ XXI საუკუნე არის ინფორმაციული საუკუნე. ამავე დროს იზრდება ინფორმაციაზე ბო­როტმოქმედება, ამდენად წარმოიშვა ინფორმაციის დაცვის აუცილებლობაც. გამოცდილება გვიჩვენებს, რომ ამ ტენდენციასთან საბრძოლველად საჭიროა ინფორმაციული რესურსების დაცვის პროცესის მიზანმიმართული ორგანიზაცია, რაშიც უნდა მონაწილეობდნენ პროფე­სიონალი სპეციალისტები, ადმინისტრაცია, თანამშრომლები და მომხმარებლები, რაც აამაღ­ლებს საკითხის ორგანიზაციულ მხარეს. გამოცდილება გვიჩვენებს, რომ:

− ინფორმაციული უსაფრთხოების უზრუნველყოფა არ შეიძლება იყოს ერთჯერადი აქტი. ეს უწყვეტი პროცესია, რომელიც მდგომარეობს დაცვის სისტემის სრულყოფისა და განვითა-

რებისათვის უფრო რაციონალური მეთოდების, ხერხებისა და გზების დაფუძნებასა და რეალიზაციაში, დაცვის სისტემის მდგომარეობის განუწყვეტელ კონტროლში, სისტემის სუსტი ადგილების გამოვლენაში.

− ინფორმაციის უსაფრთხოება უნდა იყოს უზრუნველყოფილი სისტემის ყველა სტრუქ­ტურულ ელემენტზე და ინფორმაციის დამუშავების ტექნოლოგიური ციკლის ყველა ეტაპზე.

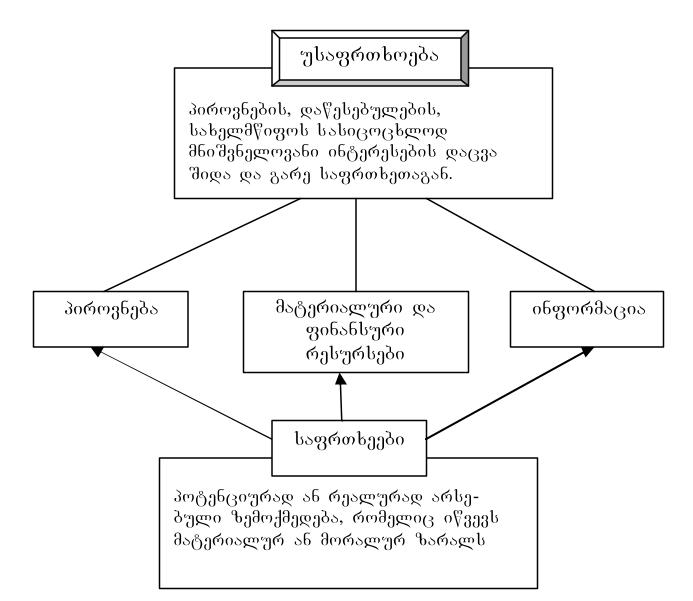
− მნიშვნელოვანი ეფექტი მიიღწევა მაშინ, როცა გამოყენებული მეთოდი, საშუალება და მიღებული ზომები ერთიანდება მთლიან ორგანიზმად – ინფორმაციის დაცვის სისტემად (იდს). ამავე დროს სისტემის ფუნქციონირება უნდა იყოს კონტროლირებადი, განახლებადი და შევსებადი, გარე და შიდა პირობების ცვლილების მიხედვით.

− იდს უნდა აკმაყოფილებდეს ინფორმაციის უსაფრთხოების მოთხოვნილ დონეს, რის­თვისაც საჭიროა მომხმარებელთა მომზადება და მათ მიერ ინფორმაციის დაცვისათვის

გამიზნული ყველა წესის დაცვა. დაგროვილი გამოცდილების გათვალისწინებით იდს

შეიძლება განისაზღვროს როგორც სპეციალური ორგანოების, საშუალებების, მეთოდების და მიღებული ზომების ერთობლიობა, რომელიც უზრუნველყოფს ინფორმაციის დაცვას შიდა და გარე საფრთხეთაგან.

ინფორმაციული უსაფრთხოების ზოგადი სქემა წარმოდგენილია ნახ. 1.1.1.-ზე.



**ნახ. 1.1.1. ინფორმაციული უსაფრთხოების ზოგადი სქემა**

**ინფორმაციის დაცვა სისტემური მიდგომის თვალ საზრისით უნდა აკმაყოფილებდეს გარკვეულ მოთხოვნებს. ინფორმაციის დაცვა უნდა იყოს:**

− **უწყვეტი.** ეს მოთხოვნა გამომდინარეობს იქედან, რომ ბოროტმოქმედები ეძებენ მომენტს, თუ როგორ აუარონ გვერდი მათი ინტერესების სფეროში მყოფი ინფორმაციის დაცვას;

-**გეგმიური**. დაგეგმვა ხორციელდება თითოეული სამსახურის მიერ თავის კომპე­ტენციის სფეროში მყოფი ინფორმაციის დაცვის დეტალური გეგმის დამუშავებაში, დაწესე­ბულების (ორგანიზაციის) საერთო მიზნების გათვალისწინებით;

− **მიზანმიმართული**. უნდა იქნას დაცული კონკრეტული მიზნების ინტერესებში და არა ყველაფერი;

− **კონკრეტული**. დაცვას ექვემდებარება კონკრეტული მონაცემები, რომლის დანაკარგიც ორგანიზაციას მიაყენებს განსაზრვრულ ზარალს;

− **აქტიური**, გარკვეული ხარისხით;

− **საიმედო**. დაცვის მეთოდები და ფორმები საიმედოდ უნდა კეტავდეს დასაცავ საიდუმ­ლოებებზე წვდომის შესაძლო გზებს, მათი წარმოდგენის ფორმის, გამოხატვის ენისა და ფიზიკური მატარებლის სახეობის (რომელზეც ისინი არიან მიმაგრებულნი) მიუხედავად.

**− უნივერსალური.** ითვლება, რომ გაჯონვის არხის სახეობის ან არასანქცირებული წვდომის ხერხის მიხედვით იგი უნდა გადაიკეთოს კარგად გააზრებული და საკმარისი სასუალებებით, ინფორმაციის ხასიათის, ფორმისა და სახეობის მიუხედავად;

**− კომპლექსური.** ინფორმაციის დაცვისათვის, ყველა სტრუქტურულ ელემენტში უნდა იქ­ნას მიღებული დაცვის ყველა სახე და ფორმა სრული მოცულობით. დაუშვებე­ლია მხოლოდ ცალკეული ფორმის ან ტექნიკური საშუალების გამოყენება;

***გამოცდილება უჩვენებს, რომ ინფორმაციის დაცვის სისტემა (იდს) უნდა აკმაყოფილებდეს შემდეგ მოთ ხოვნებს:***

− მოიცავდეს ინფორმაციული ქმედების მთელ ტექნოლოგიურ კომპლექსს;

− იყოს გათვალისწინებული ცვლილებებისა და დამატებების შეტანა;

− იყოს არასტანდართული, განსხვავებული. დაცვის საშუალებების არჩევა არ უნდა იყოს გათვლილი ბოროტმოქმედის მცირედ შესაძლებლობებზე;

− იყოს მარტივი ტექნიკური მომსახურეობის თვალსაზრისით და მოხერხებული მომხმარე­ბელთა მიერ ექსპლოატაციის თვალსაზრისით;

− იყოს საიმედო. ტექნიკური საშუალების ნებისმიერი გატეხვა არის ინფორმაციის გაჟონვის არაკონტროლირებადი არხების გაჩენის მიზეზი;

− იყოს კომპლექსური, მთლიანი.

**იდს-ს მიმართ განსაზღვრულია გარკვეული მოთხოვნები:**

− ცხადად იყოს განსაზრვრული მომხმარებლის უფლებები გარკვეული სახის ინფორმაციის წვდომაზე;

− წაუყენოს მომხმარებელს მინიმალური უფლება, რომელიც ჭირდება დაკისრებული სამუ­შაოს შესასრულებლად;

− აღრიცხოს კონფიდენციალურ ინფორმაციაზე მიმართვის ან მიმართვაზე მცდელობის შემთხვევები;

− უზრუნველყოს კონფიდენციალური ინფორმაციის ხარისხის შეფასება;

− დაცვის საშუალებების მთლიანობის კონტროლის უზრუნველყოფა და მომენტალური რეა­გირება დაცვის საშუალებების მწყობრიდან გამოსვლისას.

იდს-ს, ისე როგორც ნებისმიერი სისტემას, უნდა ჰქონდეს გარკვეულად საკუთარი უზ­რუნველყოფა, რომელზე დაყრდნობითაც იგი შეასრულებს თავის მიზნობრივ ფუნქციას. აქედან გამომდინარე, იდს-ს შეიზლება ჰქონდეს:

− უფლებრივი უზრუნველყოფა, რომელსიც შედის ნორმატიული დოკუმენტები, მდგო­მარე­ობები, ინსტრუქციები, სახელმძღვანელოები;

− ორგანიზაციული უზრუნველყოფა; იგულისხმება, რომ ინფორმაციის დაცვის რეალი­ზაცია ხორციელდება გარკვეულ სტრუქტურულ ერთეულებზე, როგორიცაა: დოკუმენტების დაცვის სამსახური, ტექნიკური საშუალებების დაცვის სამსახური;

ინფორმაციულ-ანალიტიკური საქმიანობა და სხვა;

− აპარატურული უზრუნველყოფა;

− ინფორმაციული უზრუნველყოფა. იგი მოიცავს ცნობებს, მონაცემებს, მაჩვენებლებს, პარა­მეტრებს, რომელიც საფუძვლად უდევს იმ ამოცანების გადაწყვეტას, რომელიც უზრუნ­ველ­ყოფს სისტემის ფუნქციონირებას.

− პროგრამული უზრუნველყოფა. მათ მიეკუთვნება სხვადასხვა ინფორმაციული, სააღ­რიცხვო, სტატისტიკური პროგრამები, რომელიც უზრუნველყოფს სხვადასხვა გაჟონვის არხის საფრთხეთა და ასევე კონფიდენციალური ინფორმაციის წყაროებზე არასანქცი- რებული წვდომის გზების შეფასებას.

− მათემათიკური უზრუნველყოფა. გვთავაზობს მათემათიკური მეთოდების გამოყენებას სხვადასხვა გამოთვლებისათვის, რომლებიც დაკავშირებულია ბოროტმოქმედთა ტექნი­კური საშუალებების საფრთხეთა შეფასებასთან, ასევე, დაცვისათვის საჭირო ზონებისა და ნორმების შეფასებასთან.

− ლინგვისტური უზრუნველყოფა. მოიცავს ინფორმაციის დაცვის სფეროში სპეციალის­ტებისა და მომხმარებლების საკონტაქტო სპეციალური ენობრივი სასუალებების ერთობ­ლიობას.

− ნორმატიულ -მეთოდური უზრუნველყოფა, რომელშიც შედის ინფორმაციის დაცვის ფუნქციის შემსრულებელი ორგანოების, სამსახურების, საშუალებების მოქმედებათა ნორმები და რეგლამენტები.

უსაფრთხოების სისთემა წარმოადგენს სპეციალური ორგანოების, სამსახურების, საშუ­ალებების, მეთოდების და ღონისძიებების ერთობლიობას, რომელიც უზრუნველყოფს პიროვნების, დაწესებულების, სახელმწიფოს სასიცოცხლოდ მნისვნელოვანი ინტერე­სე­ბის დაცვას შიდა და გარე საფრთხეთაგან.

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 – CERT.GOV.GE (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**

საქართველოს სისხლის სამართლის კოდექსი

[მუხლი 157. პირადი ან ოჯახური საიდუმლოს ხელყოფა](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426&lang=ge)

1. პირადი ან ოჯახური საიდუმლოს უკანონოდ მოპოვება, შენახვა ან გავრცელება, რამაც მნიშვნელოვანი ზიანი გამოიწვია, −

ისჯება ჯარიმით ანდა გამასწორებელი სამუშაოთი ვადით ერთ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.

2. პირადი ან ოჯახური საიდუმლოს უკანონოდ გამოყენება ანდა გავრცელება ამა თუ იმ ხერხით გავრცელებულ ნაწარმოებში, მასობრივი მაუწყებლობით ან სხვა საჯარო გამოსვლისას, რამაც მნიშვნელოვანი ზიანი გამოიწვია, −

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) [(ამოღებულია – 25.05.2012, №6326);](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1672037)

დ) იმის მიერ, ვისაც სამსახურებრივი მდგომარეობის, პროფესიული საქმიანობის ან სხვა გარემოების გამო ევალებოდა ამ საიდუმლოს დაცვა, −

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.

[საქართველოს 2006 წლის 28 აპრილის კანონი №2937 – სსმ I, №14, 15.05.2006 წ., მუხ.90](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=952)

[*საქართველოს 2012 წლის 25 მაისის კანონი №6326 – ვებგვერდი, 12.06.2012წ.*](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1672037)

|  |  |  |
| --- | --- | --- |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |

**[მუხლი 158. კერძო კომუნიკაციის საიდუმლოების დარღვევა](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426&lang=ge)**

1. კერძო საუბრის უნებართვო ჩაწერა ან მიყურადება, აგრეთვე კომპიუტერულ სისტემაში ან სისტემიდან კერძო კომუნიკაციისას გადაცემული კომპიუტერული მონაცემის ან ამგვარი მონაცემის მატარებელი ელექტრომაგნიტური ტალღების უნებართვო მოპოვება ტექნიკური საშუალების გამოყენებით, –

ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით იმავე  ვადით.

2. კერძო კომუნიკაციის ჩანაწერის, ტექნიკური საშუალებით მოპოვებული ინფორმაციის ან კომპიუტერული მონაცემის 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.

**შენიშვნა:**

1. ამ მუხლის მიზნებისთვის „კომპიუტერული მონაცემი“, „კომპიუტერული სისტემა“ და „უნებართვო“ განიმარტება [ამ კოდექსის XXXV თავით](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426#part_387) გათვალისწინებული დეფინიციების შესაბამისად.

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

[საქართველოს 2006 წლის 28 აპრილის კანონი №2937 – სსმ I, №14, 15.05.2006 წ., მუხ.90](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=952)

[*საქართველოს 2010 წლის 24 სექტემბრის კანონი №3619 - სსმ I, №51, 29.09.2010 წ., მუხ.332*](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1027497)

|  |  |  |
| --- | --- | --- |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |

[მუხლი 159. პირადი მიმოწერის, ტელეფონით საუბრის ან სხვაგვარი ხერხით შეტყობინების საიდუმლოების დარღვევა](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426&lang=ge)

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, –

ისჯება ჯარიმით ან თავისუფლების აღკვეთით ვადით სამ წლამდე, თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევით ვადით სამ წლამდე.

[თავი XXXV](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426&lang=ge)

**კიბერდანაშაული**

[*საქართველოს 2010 წლის 24 სექტემბრის კანონი №3619 - სსმ I, №51, 29.09.2010 წ., მუხ.332*](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1027497)

|  |  |  |
| --- | --- | --- |
|  |  |  |

**[მუხლი 284. კომპიუტერულ სისტემაში უნებართვო შეღწევა](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426&lang=ge)**

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.

[საქართველოს 2000 წლის 5 მაისის კანონი №292 – სსმ I, №18, 15.05.2000 წ., მუხ.45](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1720)

[საქართველოს 2000 წლის 30 ივნისის კანონი №458 – სსმ I, №27, 17.07.2000 წ., მუხ.83](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=17182)

[საქართველოს 2006 წლის 28 აპრილის კანონი №2937 – სსმ I, №14, 15.05.2006 წ., მუხ.90](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=952)

[საქართველოს 2008 წლის 19 მარტის კანონი №5940 – სსმ I, №8, 28.03.2008 წ., მუხ.47](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=20872)

[*საქართველოს 2010 წლის 24 სექტემბრის კანონი №3619 - სსმ I, №51, 29.09.2010 წ., მუხ.332*](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1027497)

|  |  |  |
| --- | --- | --- |
|  |  |  |

**[მუხლი 285. კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426&lang=ge)**

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](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426#part_213) 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.

[საქართველოს 2000 წლის 30 ივნისის კანონი №458 – სსმ I, №27, 17.07.2000 წ., მუხ.83](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=17182)

[*საქართველოს 2010 წლის 24 სექტემბრის კანონი №3619 - სსმ I, №51, 29.09.2010 წ., მუხ.332*](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1027497)

|  |  |  |
| --- | --- | --- |
|  |  |  |

**[მუხლი 286. კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426&lang=ge)**

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.

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

[საქართველოს 2000 წლის 30 ივნისის კანონი №458 – სსმ I, №27, 17.07.2000 წ., მუხ.83](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=17182)

[საქართველოს 2006 წლის 28 აპრილის კანონი №2937 – სსმ I, №14, 15.05.2006 წ., მუხ.90](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=952)

[საქართველოს 2010 წლის 24 სექტემბრის კანონი №3619 - სსმ I, №51, 29.09.2010 წ., მუხ.332](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1027497)

[მუხლი 320. სახელმწიფო საიდუმლოების გახმაურება](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426&lang=ge)

1. სახელმწიფო საიდუმლოების განზრახ გახმაურება ან გახმაურება იმის მიერ, ვინც ასეთი საიდუმლოება იცოდა თავისი სამსახურებრივი მდგომარეობის გამო ან ვისაც ის გაანდეს, თუ არ არის [ამ კოდექსის 313](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426#part_415)-ე ან [314-ე მუხლით](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426#part_416) გათვალისწინებული ქმედების ნიშნები, –

ისჯება თავისუფლების აღკვეთით ვადით სამიდან ხუთ წლამდე, თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევით ვადით სამ წლამდე.

2. იგივე ქმედება, რამაც გამოიწვია საქართველოს ინტერესისათვის მძიმე შედეგი, –

ისჯება თავისუფლების აღკვეთით ვადით ხუთიდან რვა წლამდე, თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევით ვადით სამ წლამდე.

[საქართველოს 2000 წლის 30 ივნისის კანონი №458 – სსმ I, №27, 17.07.2000 წ., მუხ.83](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=17182)

[საქართველოს 2006 წლის 28 აპრილის კანონი №2937 – სსმ I, №14, 15.05.2006 წ., მუხ.90](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=952)

|  |  |  |
| --- | --- | --- |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |

[მუხლი 321. სახელმწიფო საიდუმლოების დაცვის წესის დარღვევა](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426&lang=ge)

1. სახელმწიფო საიდუმლოების შემცველი დოკუმენტისადმი ან საგნისადმი მოპყრობის წესის განზრახ ან გაუფრთხილებლობით დარღვევა, რამაც ასეთი დოკუმენტის ან საგნის დაზიანება, განადგურება ან დაკარგვა გამოიწვია, –

ისჯება თავისუფლების აღკვეთით ვადით **სამ წლამდე, თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევით ვადით სამ წლამდე.**

2. იგივე ქმედება, რამაც გამოიწვია სახელმწიფო საიდუმლოების გახმაურება ან სხვა მძიმე შედეგი, –

ისჯება თავისუფლების აღკვეთით **ვადით ორიდან ექვს წლამდე,** თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევით ვადით სამ წლამდე.

[საქართველოს 2000 წლის 30 ივნისის კანონი №458 – სსმ I, №27, 17.07.2000 წ., მუხ.83](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=17182)

[მუხლი 324](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426&lang=ge)[1](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426&lang=ge)[. კიბერტერორიზმი](https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16426&lang=ge)

1. კიბერტერორიზმი, ესე იგი კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის საშიშროებას, 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.