**ლექცია II.** **ინფორ­მაციული რესურსების კლასიფიკაცია. კონფიდენციალური ინფორმაცია და სახელმწიფო საიდუმლოება.**

ინფორმაციული რესურსი სტრუქტურული, საგნობრივი გაგებით წარმოადგენს მასივს ან ცალკეულ დოკუმენტს, სხვა, ვიზუალურად აღქმად ობიექტს, რომელიც მოიცავს განსაზღრული ნიშნის ან კრიტერიუმის მიხედვით ფორმირებულ ცნობებს (ინფორმაციას).

პირველადი ინფორმაცია ასახავს პირველადი წყაროს, შექმნის (აღძვრის) სფეროს სპეციფიკას. არის ინფორმაცია, რომელიც ბუნებრივ პირობებში დამოუკიდებლად წარმოიშვება, ასევე არის ინფორმაცია სხვადასხვა სოციალური პროცესის რაოდენობრივი და ხარისხობრივი მაჩვენებლების შესახებ. ისინი ქმნიან ”გადაღებული ინფორმაციის” კლასს. ამ ნიშნის მიხედვით კონცენტრირებული ინფორმაციული რესურსი შეიძლება დახასიათდეს, როგორც ბუნებრივი, სოციალურ-ეკონომიკური. მაგალითად, ინფორმაცია მოსახლეობის რაოდენობის შესახებ.

ინფორმაციული რესურსების სხვა კლასს ქმნის ცნობები, მონაცემები, რომლებიც მიღებულია ხელოვნურად ნებისმიერი შემოქმედებითი სამუშაოს სამეცნიერო-კვლევითი საქმიანობის

პროცესსი. მსგავსი ინფორმაცია იქმნება ადამიანის ინტელექტუალური შემოქმედების შედე­გად. ამ დროს იქმნება არა მარტო მეორადი ინფორმაცია, რომელიც მიღებულია უკვე არსე­ბული ინფორმაციის გადამუშავებით, არამედ სრულიად ახალი, რომლის შესახებაც ჯერ ცნო­ბილი არ არის კაცობრიობისათვის. საუბარია აღმოჩენებზე, სხვადასხვა სოციალური და ბუნებრივი პროცესის პროგნოზებზე.

დამოუკიდებელი მნიშვნელობა აქვს ინფორმაციული რესურსების კლასიფიკაციას მისი გამოყენების სფეროების მიხედვით, რომელსაც საფუძვლად უდევს მომხმარებლის ინტერესები, როგორიცაა: განათლების მიღება, ფიზიკური პირის პროფესიული მომზადება.

როგორც წესი, მიმდინარეობს ინფორმაციული რესურსების ფორმირება იმ სუბიექტების მოთხოვნათა გათვალისწინებით, რომლებიც გამოიყენებენ უკვე დაგროვილ რესურსებს. ფორმირდება საერთო, სპეციალიზებული ბიბლიოთეკები, არქივები, ინფორმაციის სხვადასხვა ფონდი, ინფორმატიზაციის პირობებში ეს წყაროები, ინფორმაციული რესურსების საცავები გადაჰყავთ ელექტრონულ ფორმაში, იქმნება ელექტრონული საინფორმაციო სისტემები.

ინფორმაცია შეიძლება იყოს სრულიად განსხვავებული სუბიექტების რესურსი: ცალკეული პირის (მოქალაქის), იურიდიული პირის, სახელმწიფო ორგანოს, ადგილობრივი თვითმმართველობის ორგანოების, საზოგადოებრივი ორგანიზაციების. ეს სუბიექთები აწარმოებენ, ქმნიან გარკვეულ ინფორმაციულ პროდუქტს და იყენებენ მათ სხვადასხვა სახით. დღევანდელ პერიოდში განსაკუთრებულ მნიშვნელობას იძენს ინფორმაციულ რესურსებისადმი კორპორაციული, სახელმწიფოთაშორისო და გლობალური ინტერესები.

ზოგადად ინფორმაციული რესურსები შეიძლება დავყოთ დარგობრივი პრინციპით და წარმოდგენის ფორმის მიხედვით.

ინფორმაციულ რესურსებს მიეკუთვნება: ბიბლიოთეკის რესურსები, არქივის რესურსები, სამეცნიერო-ტექნიკური ინფორმაცია, სამართლებრივი ინფორმაცია, სახელმწიფო სტრუქტურის ინფორმაცია, დარგობრივი ინფორმაცია, ფინანსურ-ეკონომიკური ინფორ-

მაცია, ინფორმაცია ბუნებრივი რესურსების შესახებ, საწარმო-დაწესებულებების ინფორმაცია.

თანამედროვე ადმიანმა კარგად უნდა გააცნობიეროს, თუ რამდენად მნიშვნელოვანია საიდუმლოება მის ცხოვრებაში. ეს უფლება განსაზღვრულია კონსტიტუციით. სწორედ დემოკრატიაც ამ პინციპებზეა აგებული. თუნდაც არჩევნებში დაცული უნდა იყოს ბიულეტენის გასაიდუმლოება. მრავალ ქვეყანაში არის კანონები, რომლებიც იცავენ ადამიანის პირად ცხოვრებას. არის კანონები, მონაცემების დაცვაზე (Data Protection Act ).

ორგანიზაციები, რომლებიც აგროვებენ პერსონალურ მონაცემებს, უნდა იყვნენ დარეგისტრირებული მთავრობაში და უზრუნველყონ ზომები მათი ბოროტად გამოყენების წინააღმდეგ. მათ არა აქვთ უფლება შეაგროვონ, გამოიყენონ და გაავრცელონ კერძო ხასიათის ინფორმაცია იმათთან შეუთანხმებლად, ვის საკუთრებასაც წარმოადგენს აღნიშნული ინფორმაცია.

ორგანიზაციებმა, ასევე, უნდა შეატყობინონ კერძო პირებს ინფორმაციის შეგროვების მიზეზებზე, უზრუნველყონ მათზე წვდომა, გაასწორონ უზუსტობები და დაიცვან ეს ინფორმაცია უუფლებო წვდომისაგან. ადამიანებს აქვთ უფლება ნახონ მათზე შეგროვებული პერსონალური მონაცემები და გაასწორონ მათში დაშვებული ხარვეზები. ადამიანებს აქვთ უფლება იცოდნენ, თუ რისთვის არის შეგროვებული ეს ინფორმაცია და დარწმუნდნენ, რომ იგი არ გაიყიდება სხვა მიზნებისათვის.

ამავე დროს ადამიანებს უფლება აქვთ უარი განაცხადონ ნებისმიერი სახის ცნობის გაცემაზე, თუ მათ ამის სურვილი არა აქვთ. გარკვეული დროით გასაიდუმლოებას საჭიროებს მთავ-

რობაც. ნებისმიერი ქვეყნის ინტერესები საჭიროებს სხვა ქვეყნების ინტერესებზე თვალყურის დევნებას. ამიტომაც მთავრობა დაინტერესებულია შეინახოს განსაზრვრული ინფორმაცია

სხვა სახელმწიფოებისაგან მალულად. ამ საიდუმლოებთაგან მნიშვნელოვანია სამხედრო საიდუმლოებანი: სტრატეგიები და ტაქტიკა, შეიარაღება, ჯარის გადაადგილება.

კონფიდენციალური ინფორმაციის საფრთხედ ითვლება ინფორმაციულ რესურსებზე პოტენციური ან რეალურად შესაძლო მოქმედებები, რომლის შედეგადაც ხდება დასაცავი ინფორმაციის არასამართლებრივი დაუფლება. ასეთი მოქმედებები შსეიძლება იყოს:

− კონფედენციალური ინფორმაციის გაცნობა სხვადასხვა გზითა და ხერხით მისი მთლიანობის დარღვევის გარეშე.

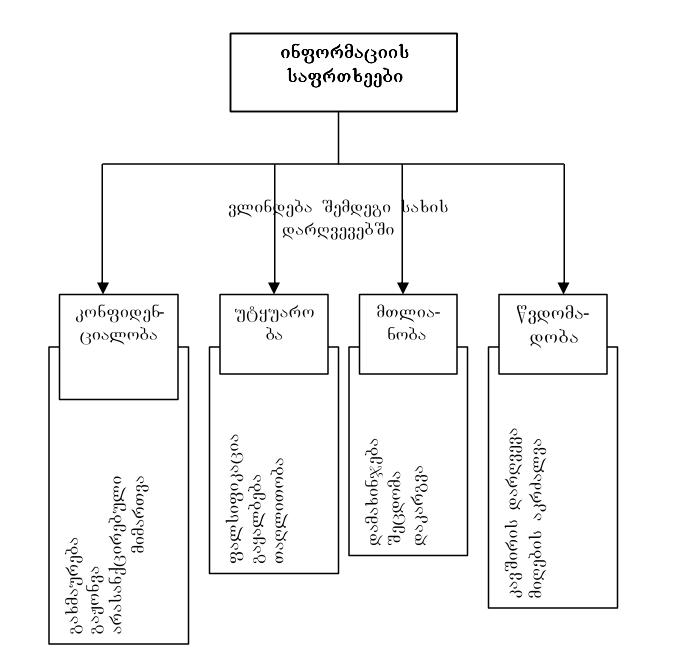
− ინფორმაციის მოდიფიკაცია, შემადგენლობისა და შინაარსის, როგორც ნაწილობრივი, ასევე მნისვნელოვანი ცვლილება.

− ინფორმაციის დარღვევა (განადგურება), როგორც ვანდალური აქტი, მატერიალური ზარალის მიყენების მიზნით. საერთო ჯამში ინფორმაციის მიმართ კანონსაწინაარმდე-

გო მოქმედებები იწვევს მისი კონფიდენციალობის, მთლიანობის, უტყუარობის და წვდომადობის დარღვევას.

თითოეული საფრთხე, რომელიც ვლინდება ნახ.2.1.-ზე მოცემულ დარღვევებში, მოიცავს განსაზღვრულ ზარალს - მორალურს ან მატერიალურს, ხოლო დაცვა და საწინაარმდეგო

ქმედებები ამცირებს მას მნისვნელოვნად ან ნაწილობრივ. თუმცა ეს ყოველთვის არ ხერხდება. ამის გათვალისწინებით საფრთხეები შეიძლება კლასიფიცირდეს კლასტერების სახით, რომელიც მოცემულია ნახ.2.1.-ზე.



**ნახატი 2.1. ინფორმაციის საფრთხეთა გამოვლენა**

საფრთხე, მიყენებული ზარალის მიხედვით, შეიძლება იყოს: უკიდურესი, რომლის შედეგადაც ფირმა შეიძლება გაკოტრდეს; მნიშვნელოვანი, მაგრამ არ გამოიწვიოს გაკოტრება; უმნიშვნელო, რომლის შედეგადაც ფირმას შეუძლია გარკვეული დროის შემდეგ გააკეთოს კომპენსირება;

გაჩენის მიზეზების მიხედვით: სტიქიური უბედურებები; გამიზნული უბედურებები;

მიყენებული ძარალის ხასიათის მიხედვით: მატერიალური; მორალური;

შემოქმედებების ხასიათის მიხედვით: აქტიური; პასიური;

ობიექტთან მიმართებაში: შიდა; გარე;

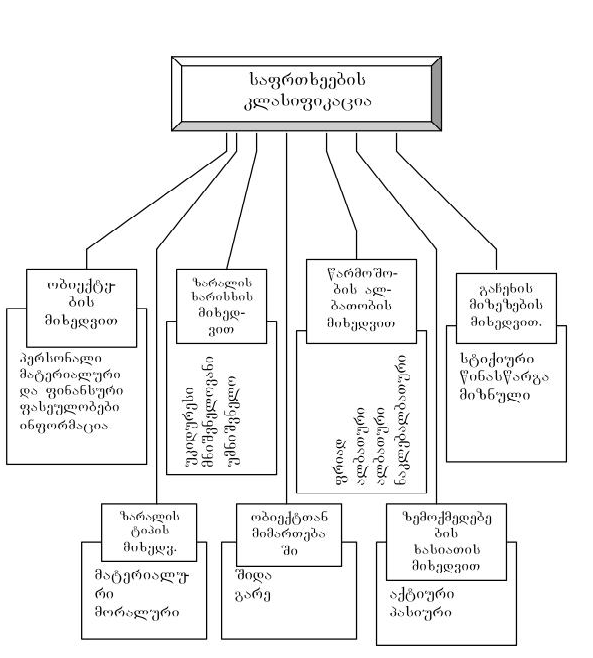
გარე საფრთხეების წყაროებს წარმოადგენს: არაკეთილსინდისიერი კონკურენტები; დამნაშავე ჯგუფები ან ფორმირებები; ადმინისტრაციულ-მმართველი აპარატის ცალკეული პირები და ორგანიზაციები. შიდა საფრთხეების წყაროები შეიძლება იყოს: დაწესებულების ადმინისტრაცია; პერსონალი; საწარმოო და შრომითი საქმიანობის უზრუნველყოფის ტექნიკური საშუალებები.

შიდა და გარე საფრთხეების თანაფარდობა საშუალოდ შეიძლება შემდეგი სახით დახასიათდეს:

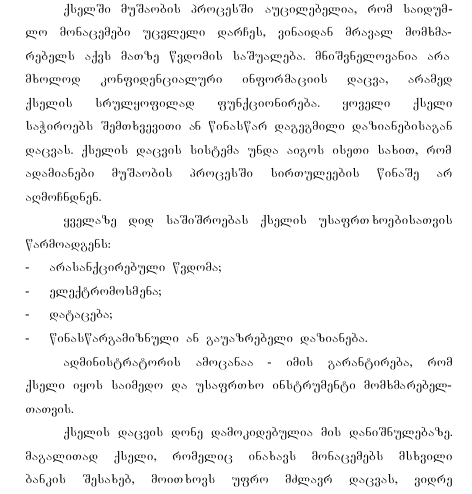
− საფრთხეთა 82% ხორციელდება ფირმის საკუთარი თანამშრომლების მიერ, მათი პირდაპირი ან შუალედური მონაწილეობით;

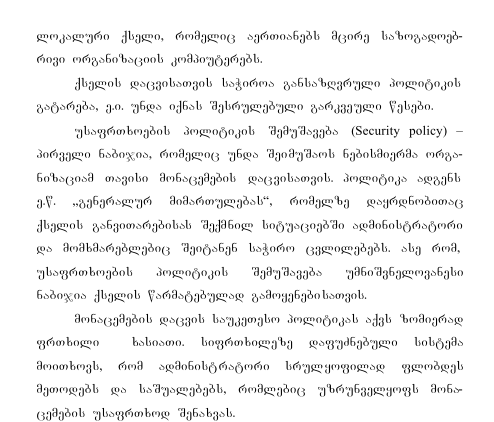
− 17% ხორციელდება გარედან;

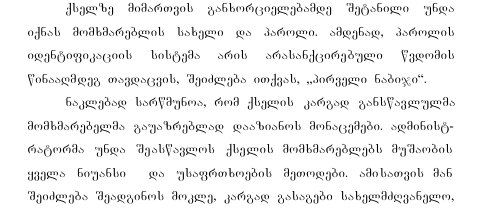
− 1% ხორციელდება შემთხვევითი პირების მიერ.

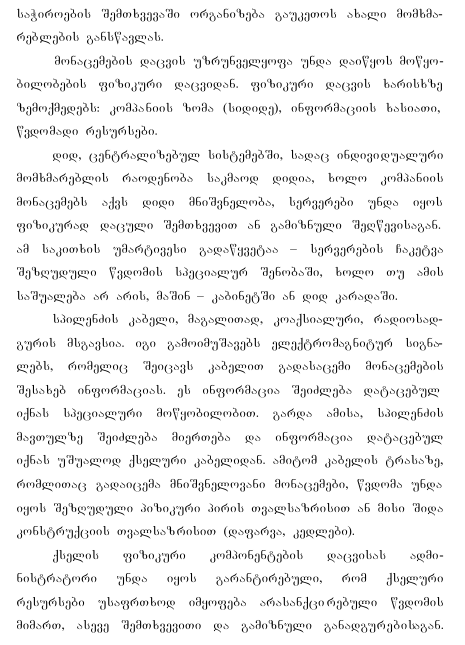


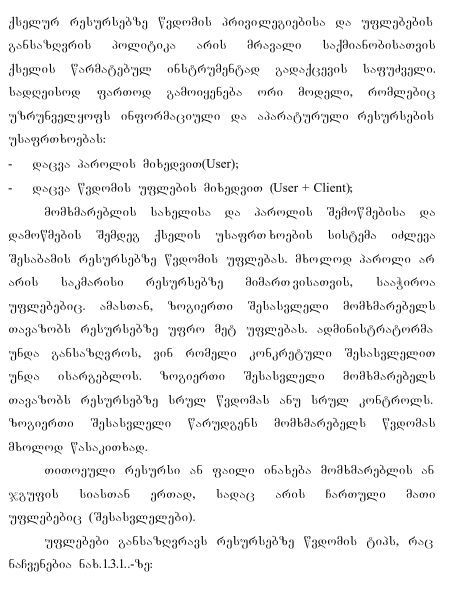
**ნახ. 2.2. საფრთხეების კლასიფიკაცია**

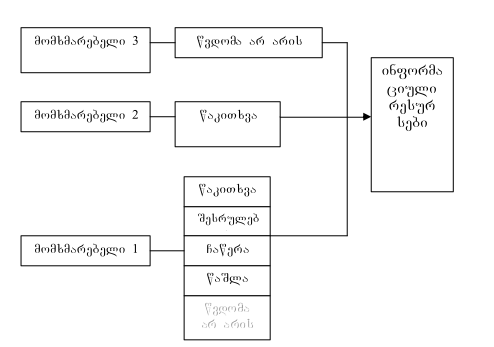
****

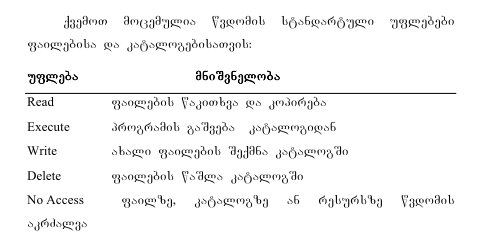
****

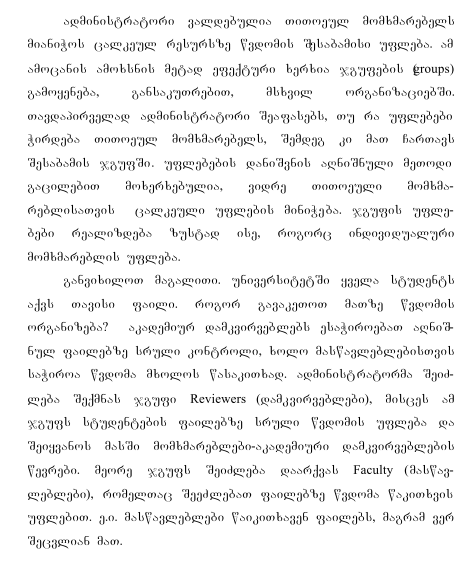
****

****

****

****

****

****



**საქართველოს ეროვნული უსაფრთხოების კონცეფცია**

**საქართველოს ეროვნული ინტერესები**

**12. კიბერუსაფრთხოების განმტკიცება:** საქართველოსთვის მეტად მნიშვნელოვანია ინფორმაციული სივრცის უსაფრთხოება და ელექტრონული ინფორმაციის დაცულობა. ინფორმაციული ტექნოლოგიების სწრაფ განვითარებასთან ერთად იზრდება მათზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულება. ამის გათვალისწინებით, დიდი მნიშვნელობა ენიჭება კიბერდანაშაულთან ბრძოლას და კიბერსივრცეში დივერსიული აქტებისგან თავდაცვას.

**საქართველოს წინაშე არსებული საფრთხეები, რისკები და გამოწვევები**

**8. კიბერსაფრთხეები:** ინფორმაციულ ტექნოლოგიებზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულებასთან ერთად იზრდება ის გამოწვევები, რომლებიც საქართველოს ინფორმაციული სივრცის დაცვასთანაა დაკავშირებული. 2008 წლის რუსეთ-საქართველოს ომის დროს რუსეთის ფედერაციამ საქართველოს წინააღმდეგ, სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, მიზანმიმართული და მასობრივი კიბერთავდასხმები განახორციელა. ამ კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სახმელეთო, საჰაერო და საზღვაო სივრცეების დაცვა.

**საქართველოს უსაფრთხოების პოლიტიკის ძირითადი მიმართულებები**

**13. კიბერუსაფრთხოების პოლიტიკა**

საქართველოს მიზანია, შექმნას ინფორმაციული უსაფრთხოების ისეთი სისტემა, რომლის დროსაც ნებისმიერი კიბერთავდასხმის საზიანო შედეგები მინიმუმამდე იქნება შემცირებული და ასეთი თავდასხმის შემდეგ უმოკლეს დროში გახდება შესაძლებელი ინფორმაციული ინფრასტრუქტურის ფუნქციონირების სრული აღდგენა.

საქართველო დიდ მნიშვნელობას ანიჭებს საიდუმლო ინფორმაციის უსაფრთხოების უზრუნველყოფას და სახელმწიფოს საინფორმაციო სისტემების დაცვას. იგი ქმნის შესაბამის საკანონმდებლო ბაზას და ინფრასტრუქტურას, რომელიც აუცილებელია ინფორმაციული ტექნოლოგიების გასაუმჯობესებლად და ინფორმაციის დაცულობის უზრუნველსაყოფად.

კიბერუსაფრთხოების უზრუნველყოფისათვის დიდი მნიშვნელობა ენიჭება საქართველოს მეგობარ ქვეყნებთან თანამშრომლობას და მათი გამოცდილების გაზიარებას.