ქვიზი 2

**1. რა არის ინფორმაციული უსაფრთხოება?**

ა) 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;

ბ) ქმედება, რომელიც ხელს უშლის იმას, 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;

გ) ინფორმაციული სისტემა, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის;

დ*)* საქმიანობა, რომელიც უზრუნველყოფს ინფორ­მაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას;

**2. რა არის ინფორმაციული უსაფრთხოების პოლიტიკა?**

ა) კანონით ”ინფორმაციული უსაფრთხოების შესახებ”, გათვალისწინებული ნორმებისა და პრინციპების, აგრეთვე პრაქტიკის  ერთობლიობა, რომელიც ემსახუ­რება ინფორმაციული უსაფრთხოების უზრუნველყოფას და შეესაბამება მისი დაცვის სფეროში დადგენილ საერთაშორისო სტანდარტებს

ბ) 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

გ*)* კანონით ”ინფორმაციული უსაფრთხოების შესახებ”, 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

დ) კანონით ”ინფორმაციული უსაფრთხოების შესახებ”, საქართველოს სხვა ნორმატიული აქტებითა და საერთაშორისო შეთანხმებებით გათვალისწინებული ნორმებისა და პრინციპების, აგრეთვე პრაქტიკის  ერთობლიობა, რომელიც ემსახუ­რება ინფორმაციული უსაფრთხოების უზრუნველყოფას, ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას;

3. **რა არის კიბერსივრცე?**

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

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

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

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

**4. რა არის კიბერშეტევა?**

ა) 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;

 ბ) ინფორმაციული ომი, 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;

გ) დივერსიული აქტი, 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;

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

**5. რას წარმოადგენს კომპიუტერული ინციდენტი** **?**

ა) 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

ბ) ინფორმაციული უსაფრთხოების პოლიტიკის რეალურ ან პოტენციური დარღვევას, რომელიც ხორციელდება კიბერშეტევით და იწვევს ინფორმაციის  უნებართვო წვდომას, გამჟღავნებას, დაზიანებას ან შეფერხებას ან ინფორმაციული რესურსის მიტაცებას

გ) ინფორმაციული უსაფრთხოების პოლიტიკის რეალური ან პოტენციური დარღვევა, რომელიც ხორციელდება ინფორმაციული ტექნოლოგიის გამოყენებით და იწვევს ინფორმაციის მიტაცებას

 დ) ინფორმაციული უსაფრთხოების პოლიტიკის რეალურ ან პოტენციური დარღვევას, რომელიც ხორციელდება ინფორმაციული ტექნოლოგიის გამოყენებით და იწვევს ინფორმაციის  უნებართვო წვდომას, გამჟღავნებას, დაზიანებას ან შეფერხებას ან ინფორმაციული რესურსის მიტაცებას

**6.** **რას წარმოადგენს კრიტიკული ინფორმაციული სისტემა**

ა)ინფორმაციული სისტემას, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის

ბ) ინფორმაციული სისტემას, რომლის ფუნქციონირება მნიშვნელოვანია ქვეყნის სოციალური, თავდაცვისათვის ან/და მორალური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის

გ) ინფორმაციული სისტემასა და კანონთა ნუსხას, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის

დ) ინფორმაციული სისტემას, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის და საიმედოობასთვის

**7. ვინ თუ რას წარმოადგენს კრიტიკული ინფორმაციული სისტემის სუბიექტი**

ა) პრეზიდენტი, სახელმწიფო ორგანო ან იუ­რიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათ­ვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნე­ბისათვის.

ბ)პრეზიდენტი, პრემიერი, პარლამენტის თავმჯგომარე, სახელმწიფო ორგანო ან იუ­რიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათ­ვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნე­ბისათვის

გ)სახელმწიფო ორგანო ან იუ­რიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათ­ვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნე­ბისათვის.

დ) პრემიერი-მინისტრი, სახელმწიფო ორგანო ან იუ­რიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათ­ვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნე­ბისათვის

**8. კონფიდენციალური ინფორმაცია** **ა**

ა) 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 და კანონი პირადი მონაცემების შესახებ.

ბ) ინფორმაცია, რომლის კონფიდენციალურო­ბის, მთლიანობის ან ხელმისაწვდომობის ხელყოფას, სავარაუდოდ, მოჰყვება კრი­ტიკული ინფორმაციული სისტემის სუბიექტის ფუნქციებისათვის მნიშვნელოვანი ზიანი.

გ) 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.

დ) 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

**9. შინასამსახურებრივი გამოყენების ინფორმაცია**

ა) 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

ბ) 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.

გ) ინფორმაცია, 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.

დ) ინფორმაცია, 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 და კანონი პირადი მონაცემების შესახებ.

**10.** **ინფორმაციული აქტივი**  **არის**

ა) ინფორმაციული რესურსი, სტრუქტურული, საგნობრივი გაგებით წარმოადგენილი მასივი ან ცალკეული დოკუმენტი, სხვა, ვიზუალურად აღქმად ობიექტი, რომელიც მოიცავს განსაზღრული ნიშნის ან კრიტერიუმის მიხედვით ფორმირებულ ცნობებს (ინფორმაციას)

ბ) 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.

გ) ინფორმაციული რესურსი - სტრუქტურული სახით წარმოადგენილი მასივი ან ცალკეული დოკუმენტი, სხვა, ვიზუალურად აღქმად ობიექტი, რომელიც მოიცავს განსაზღრული ნიშნის ან კრიტერიუმის მიხედვით ფორმირებულ ცნობებს (ინფორმაციას)

დ) ცალკეული ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომ­ლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია და საციცოცხლოა კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის

**11. ინფორმაციული სისტემა**  **წარმოადგენს**

ა) ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების ნებისმიერი კომბინაცია, რომელიც ხელს უწყობს მოწყვლადობის შემცირებას

 ბ) ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების მიზანმიმართული კომბინაცია, რომელიც ხელს უწყობს მართვას ან/და გადაწყვეტილების მიღებას

გ) ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების მიზანმიმართული კომბინაცია, რომელიც ხელს უწყობს მოწყვლადობის შემცირებას

დ) ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების ნებისმიერი კომბინაცია, რომელიც ხელს უწყობს მართვას ან/და გადაწყვეტილების მიღებას

**12. რა არის ქსელური სენსორი**

ა) პროგრამილი პაკეტი, რომელიც სპეციალურად გამიზნულია ქსელის სეგმენტის მონიტორინგისთვის, ისეთი ქმედებების გამოსავლენად, რომლებიც მიუთითებს ინფორმაციული სისტემის წინააღმდეგ წარმოებულ შეტევაზე ან მასში შეღწევაზე

ბ)აპარატულ-პროგრამული მოწყობილობა, რომელიც სპეციალურად გამიზნულია ქსელის სეგმენტის მონიტორინგისთვის, ისეთი ქმედებების გამოსავლენად, რომლებიც მიუთითებს ინფორმაციული სისტემის წინააღმდეგ წარმოებულ შეტევაზე ან მასში შეღწევაზე

გ) მოწყობილობა, რომელიც სპეციალურად გამიზნულია ქსელის სეგმენტის მონიტორინგისთვის, ისეთი ქმედებების გამოსავლენად, რომლებიც მიუთითებს ინფორმაციული სისტემის წინააღმდეგ წარმოებულ შეტევაზე ან მასში შეღწევაზე

დ) პროგრამული მოწყობილობა, რომელიც სპეციალურად გამიზნულია ქსელის სეგმენტის მონიტორინგისთვის, ისეთი ქმედებების გამოსავლენად, რომლებიც მიუთითებს ინფორმაციული სისტემის წინააღმდეგ წარმოებულ შეტევაზე ან მასში შეღწევაზე

**13. კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხა მტკიცდება და შესაბამისი სუბიექტის კრიტიკულობის კლასიფიცირება დგინდება**

ა) პრემიერ-მინისტრის განკარგულებით

ბ) პრეზიდენტის ბრძანებულებით

გ) კოჰაბიტაციით: ერთობლივად - პრემიერ-მინისტრის განკარგულებით და პრეზიდენტის ბრძანებულები

დ) პარლამენტის დადგენილებით

14. **ინფორმაციული უსაფრთხოების პოლიტიკა უნდა აკმაყოფილებდეს**

ა) 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  სტანდარტიზაციის საერთა­შორისო ორ­განიზაციისა ( ISO) და ინფორმაციული სისტემების აუდიტისა და კონ­ტროლის ასო­ციაციის ( ISACA) მიერ დადგენილი სტანდარტებისა და მოთხოვნების შესაბამისად.

ბ) ინფორმაცი­ული უსაფრთხოების ყველა 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.

გ) ინფორმაცი­ული უსაფრთხოების ზოგიერთ 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.

დ) ინფორმაცი­ული უსაფრთხოების მნიშვნელოვან 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.

**15. ვის წარუდგენს კრიტიკული ინფორმაციული სისტემის სუბიექტი მიღებულ ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამო­ყენების წესებს განსახილველად**

ა) საქართველოს უშიშროების საბჭოს

ბ) მინისტრთა საბჭოს

გ) თავდაცვის სააგენტოს

დ) მონაცემთა გაცვლის სააგენტოს

**16. ვინ და რისთვის ნიშნავს ინფორმაციული უსაფრთხოების მენეჯერს**

ა) საწარმოს დირექტორი

ბ) კრიტიკული ინფორმაციული სისტემის სუბიექტი განსაზღვრავს კონკრეტულ პირს (პირებს) ან თანამშრომელს (თანამშრომლებს), რომელიც (რომ­ლებიც) პასუხისმგებელია (პასუხისმგებელი არიან) კრიტიკული ინფორმაციის სის­ტემის სუბიექტის ინფორმაციული უსაფრთხოების მოთხოვნების შესრულებისათვის (ინფორმაციული უსაფრთხოების მენეჯერი)

გ) კრიტიკული ინფორმაციული სისტემის დირექტორი განსაზღვრავს კონკრეტულ პირს (პირებს) ან თანამშრომელს (თანამშრომლებს), რომელიც (რომ­ლებიც) პასუხისმგებელია (პასუხისმგებელი არიან) კრიტიკული ინფორმაციის სის­ტემის სუბიექტის ინფორმაციული უსაფრთხოების მოთხოვნების შესრულებისათვის (ინფორმაციული უსაფრთხოების მენეჯერი)

დ) საწარმოს ოდეერი

17. **ინფორმაციული უსაფრთხოების მენეჯერის ძირითადი მოვალეობებია**

 ა) ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნების შესრულების ყოველდღიური მონიტორინგი; ინფორმაციული აქტივებისა და მათი წვდომის აღწერა; ინფორმაციული უსაფრთხოების პოლიტიკის შინაუწყებრივი დოკუმენტაციის მომზადება;

 ბ) ინფორმაციული უსაფრთხოების ინციდენტების შესახებ ინფორმაციის შეგროვება და მათზე რეაგირების მონიტორინგი; ინფორმაციული უსაფრთხოების საკითხებზე ანგარიშგება და სხვა სახის ადმინისტრაციული/საორგანიზაციო საქმიანობა

გ) ინფორმაციული უსაფრთხოების ზოგადი და დარგობრივი ტრენინგების ორგანიზება და ჩატარება

დ) ყველა ზემოდ ჩამოთვლილი და სხვა მოვალეობები, რომლებსაც განსაზღვრავს კრიტიკული ინფორმაციული სისტემის სუბიექტი

**18. 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) ზემოთ ჩამოთვლილები და 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.

**19. დახმარების ჯგუფის მოვალეობები არ არის:**

ა) კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა; კომპიუტერული ინციდენტების დროული გამოვლენა;

ბ) კომპიუტერულ ინციდენტებზე რეაგირება და მათზე რეაგირების კოორდინაცია; კომპიუტერული ინციდენტების აღრიცხვა და მათზე რეაგირების პრიორიტეტების დადგენა და კატეგორიზაცია;

გ) კომპიუტერული ინციდენტების ანალიზი; კომპიუტერული ინციდენტების შედეგების გამოსწორებისა და ზიანის მინიმიზაციის პროცესში დახმარების გაწევა; კომპიუტერული ინციდენტების პრევენციისკენ მიმართული ზომების კოორდინაცია და ამგვარი ზომების დანერგვაში დახმარების გაწევა

დ) 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; შესაძლო საფრთხეების შესახებ მომხმარებელთა ფართო წრის გაფრთხილება და მისთვის სათანადო ინფორმაციის მიწოდება; ინფორმაციული უსაფრთხოების საკითხებზე საგანმანათლებლო და ინფორმაციული უზრუნველყოფა; საერთაშორისო დონეზე ინფორმაციული უსაფრთხოების საკითხებში წარმომადგენლობა და კოორდინაცია;

ე) ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნების შესრულებისათვის კრიტიკული ინფორმაციული სისტემის სუბიექტი დაჯარიმება

**20. კომპიუტერული უსაფრთხოების სპეციალისტის მოვალეობა არ არის**

ა) კომპიუტერული სისტემების ყოველდღიური მონიტორინგი და შეფასება;

ბ) კომპიუტერული ინციდენტების იდენტიფიცირება და მათზე რეაგირება

გ) თავიანთ სფეროში ორგანიზაციის თანამშრომელთა კვალიფიკაციის ამაღლების მონიტორინგი

დ) კომპიუტერული ინციდენტებისა და უსაფრთხოების ზომების ანალიზი და ანგარიშგება; დახმარების ჯგუფთან კოორდინაცია;

ქვიზი №2, IV მათემატიკა, ინფ. უსაფ. საფ. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ სახ. გვარი

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

ქვიზი №2, IV მათემატიკა, ინფ. უსაფ. საფ. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ სახ. გვარი

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

ქვიზი №2, IV მათემატიკა, ინფ. უსაფ. საფ. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ სახ. გვარი

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

ქვიზი №2, IV მათემატიკა, ინფ. უსაფ. საფ. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ სახ. გვარი

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

ქვიზი №2, IV მათემატიკა, ინფ. უსაფ. საფ. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ სახ. გვარი

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

ქვიზი №2, IV მათემატიკა, ინფ. უსაფ. საფ. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ სახ. გვარი

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

ქვიზი №2, IV მათემატიკა, ინფ. უსაფ. საფ. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ სახ. გვარი

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |