**”ინფორმაციული უსაფრთხოების საფუძვლები” -საგანი**

**ტესტი შუალედური გამოცდისთვის, I ვარიანტი**

**IV კურსი, კომპიუტერული მინორი, 29 სტუდენტი;**

**საგნის ხელმძღვანელი - ნუგზარ კერესელიძე**

**1. რას წარმოადგენს ინფორმაციის უსაფრთხოება?**

ა) ინფორმაციის დამალვა

ბ) ინფორმაციის წაშლა

გ) თავისუფლებას საფრთხეთაგან, დაცულობას

 დ) ინფორმაციის არასანქცირებული გამოყენების, ბოროტად გამოყენების, ცნობე­ბის, ფაქტების, მონაცემების ან აპარატურული საშუალებების შეცვლის ან მათ წვდო­მაზე მტყუნების აღმოფხვრის მიზნით მიღებულ ზომებს

**2. რა საჭიროა კიბერუსაფრთხოების განმტკიცება**

ა) ეს მოდაშია

ბ) მსოფლიო პროგრამაა

გ) ინფორმაციული ტექნოლოგიების სწრაფ განვითარებასთან ერთად იზრდება მათზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულება. ამის გათვალისწინებით, დიდი მნიშვნელობა ენიჭება კიბერდანაშაულთან ბრძოლას და კიბერსივრცეში დივერსიული აქტებისგან თავდაცვას.

დ) გაეროსნორმატივია

**3. რითი იცავს სახელმწიფო საიდუმლო ინფორმაციას და სახელმწიფოს საინფორმაციო სისტემას.**

ა) თანამედროვე ტექნიკის შეძენით

ბ) კანონებით

გ) ქმნის შესაბამის საკანონმდებლო ბაზას და ინფრასტრუქტურას, რომელიც აუცილებელია ინფორმაციული ტექნოლოგიების გასაუმჯობესებლად და ინფორმაციის დაცულობის უზრუნველსაყოფად.

დ) მეგობარ ქვეყნებთან თანამშრომლობით

4. **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;

**5. 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.

**6. 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;

**7**. **რომელი ბრძანებით შეიძლება რეესტრში შესვლა:**

 ა) secpol.msc ბ) cmd

გ) dpedit.msc დ) regedit.exe

**8. რეესტრში, HKEY\_USER საქაღალდე შეიცავს:**

ა) ყველა ლოკალური მომხმარებლის უნიკალურ SID იდენტიფიკატორს ბ) მხოლოდ ადმინისტრატორის უნიკალურ SID იდენტიფიკატორს

გ) მხოლოდ სტუმრის უნიკალურ SID იდენტიფიკატორს

დ) ყველა ადმინისტრატორის უნიკალურ SID იდენტიფიკატორს

**9. რამდენი სახის უსაფრთხოების ჯგუფი არსებობენ Windows-ში**

 ა) 5 ბ) 7

 გ) 9 დ) 11

**10. Administrators (ადმინისტრატორები),**

ა) აქვს მრავალი პრივილეგია

ბ)ესაა მძლავრი ჯგუფი, რომელსაც აქვს უფლება სრულად აკონტროლოს სისტემა

გ) უზრუნველყოფს რეპლიკაციების მართვას დომენურ ქსელში

დ) ამ ჯგუფის წევრებს აქვთ შეზღუდული უფლება განკუთვნილი სტუმრებისა და შემთხვევითი მომხმარებლებისათვის

**11. Guests** :

ა) აქვს მრავალი პრივილეგია

ბ)ესაა მძლავრი ჯგუფი, რომელსაც აქვს უფლება სრულად აკონტროლოს სისტემა

გ) უზრუნველყოფს რეპლიკაციების მართვას დომენურ ქსელში

დ) ამ ჯგუფის წევრებს აქვთ შეზღუდული უფლება განკუთვნილი სტუმრებისა და შემთხვევითი მომხმარებლებისათვის

**12. რამდენი ტიპის აღრიცხვის ჩანაწერების შექმნის საშუალებას იძლევაWindows XP**

ა) მხოლოდ კომპიუტერის ადმინისტრატორის ბ) მხოლოდ შეზღუდული

გ) კომპიუტერის ადმინისტრატორის და შეზღუდული დ) არცეთი ამათგანის

**13**. **ადმინისტრატორის რა მონაცემების შეცვლაა შესაძლებელი აღრიცხვის ჩანაწერებში**:

ა) სახელის; სურათის; პასვორდის დაყენება, გაუქმება, შეცვლა; მომხმარებლის ტიპის. ბ) სახელის; სურათის; პასვორდის დაყენება, გაუქმება, შეცვლა; მომხმარებლის ტიპის;

 გ) სურათის,მომხმარებლის აღრიცხვის ჩანაწერების გაუქმება. დ) ყველა ზემოთ ჩამოთვლილის

**14. არა ადმინისტრატორის და არა სტუმრის რა მონაცემების შეცვლაა შესაძლებელი აღრიცხვის ჩანაწერებში**:

ა) სახელის; სურათის; პასვორდის დაყენება, გაუქმება, შეცვლა; მომხმარებლის ტიპის. ბ) სახელის; სურათის; პასვორდის დაყენება, გაუქმება, შეცვლა; მომხმარებლის ტიპის;

 გ) სურათის,მომხმარებლის აღრიცხვის ჩანაწერების გაუქმება. დ) ყველა ზემოთ ჩამოთვლილის

**15**. **როგორ უნდა** **მოვახდინოთ ლოკალური კომპიუტერის უსაფრთხოების პარამეტრების შერჩევა**

ა) Start → Run→ ბრძანების სტრიქონი →gpedit.msc → ok → Windows Setting →Security Setting

ბ) Start → Run →ბრძანების სტრიქონი →gpedit.msc → ok → Computer configuration→ Windows Setting →Security Setting

გ) Start → gpedit.msc → ok → Windows Setting →Security Setting

დ) Start → Run →ბრძანების სტრიქონი →gpedit.msc → ok → Administrative Templates→ Windows Setting →Security Setting

**16.**  **პაროლების პოლიტიკის ჩართვისას შესაძლებელია:**

ა) მოვითხოვოთ პაროლების განუმეორება; პაროლის მოქმედების მაქსიმალური ვადა

ბ) პაროლის მოქმედების მინიმალური ვადა; პაროლის მინიმალური სიგრძე.

გ) პაროლის სირთულე; პაროლების შენახვა უკუ გაშიფრვით

დ) ყველა ზემოთ ჩამოთვლილი

**17. Account Lockout** - **პაროლების გაშიფრის (გატეხვისგან) დაცვის პოლიტიკა:**

ა) ყველა ქვემოთ ჩამოთვლილ შემთხვევებში.

ბ) მიეთითება ზღვრული რაოდენობა სისტემაში წარუმატებული შესვლის, რის შემდეგაც ჩაირთვება ბლოკირების ფუნქცია - Account Lockout threshold.

გ) მიეთითება დრო რომლის განმავლობაში იქნება დაბლოკილი სისტემა, სისტემაში წარუმატებული შესვლებს მცდელობებს შორის - Account Lockout counter after.

დ) დაბლოკავს განსაზღვრული (მითითებული) დროით აღრიცხვის ჩანაწერებს სისტემაში წარუმატებული შესვლის შემდეგ - Account Lockout duration.

**18. აუდიტის პოლიტიკით უსაფრთხოების თვალსაზრისით დაფიქსირდება;**

ა)აღრიცხვის ჩანაწერების სისტემაში შესვლის აუდიტი; აღრიცხვის ჩანაწერების მართვის აუდიტი; კატალოგთა სამსახურის წვდომის აუდირი.

ბ) სისტემაში შესვლის მოვლენათა აუდიტი; ობიექტების წვდომის აუდიტი; პოლიტიკის შეცვლის აუდიტი.

გ) პრივილეგიების გამოყენების აუდიტი; პროცესების მიყურადების აუდიტი; სისტემური მოვლენების აუდიტი.

დ) ყველა ზემოდ ჩამოთვლილი.

**19. მომხმარებლების ჯგუფში ჩართვისათვის, ავირჩიოთ:**

ა) Start → Control panel → Administrative Tools → Computer Management→ System Tools→ Local users and groups

ბ) Start → Control panel → Administrative Tools → Computer Management→ System Tools→Shared Folder

გ) Start → Control panel → Administrative Tools → Computer Management→ Disk management

დ) Start → Control panel → Administrative Tools → Computer Management→Storage →Disk management

**20.** **რისი უფლება აქვს არქივის ოპერატორებს** **(Backup Operators);**

ა) ნებისმიერი ოპერაციის ჩატარების

ბ) ფაილებისა და ფოლდერების დაცვითი პარამეტრების შეცვლის, როცა საქმე ეხება რეზერვულ კოპირებას და აღდგენას

გ) ქსელის პარამეტრების ცვლილების

დ) ლოკალურ სისტემასთან მიერთების, შორი წვდომის საშუალებით

**21. რა სქემით ხდება აუდიტის მითითება :**

ა) Start » Audit Policy » Administrative Tools » Local Security Setting » Local Policies » Control Panel

ბ) Start »Control Panel » Audit Policy » Local Security Setting » Local Policies » Administrative Tools

გ)Start »Control Panel » Administrative Tools » Local Security Setting » Local Policies » Audit Policy

დ) Start »Control Panel » Administrative Tools » Audit Policy » Local Security Setting » Local Policies

**22.რომელ აუდიტს ჩართავს ეს ქმედება Start »Control Panel » Administrative Tools » Local Security Policy » Local Policies » Audit Policy » Audit process tracking**

ა) ყოველი გაშვებული პროცესის აუდიტს.

ბ) უფლებების ყოველი გამოყენების აუდიტს.

გ) აღრიცხვის ჩანაწერში შეტანილი ცვლიცებების აუდიტს.

დ) ნებისმიერი ობიექტისადმი, რომელთაც აქვთ ცხრილი *(SA*CL), წვდომის აუდიტი.

**23. რომელი სავალდებულო ჩანაწერების ჟურნალებია მოვლენათა დათვალიერების პროგრამაში:**

ა) ყველა ქვემოთ ჩამოთვლილი ბ) გამოყენებითი

გ) უსაფრთხოების დ) სისტემური

**24**. **რა შედეგს მოგვცემს:**  **Start » Control Panel » Administrative Tools » Event Viewer**

ა) გაიხსნება გამოყენებითი ჩანაწერების ჟურნალი

ბ) გაიხსნება მოვლენათა დათვალიერების პროგრამა

გ) დაიხურება მოვლენათა დათვალიერების პროგრამა

დ) დაიხურება გამოყენებითი ჩანაწერების ჟურნალი

**25. სად შეიძლება შემოწმდეს, ჩაირთო თუ არა კომპიუტერი ამა თუ იმ დროს**

ა) მოვლენათა დათვალიერების პროგრამის უსაფრთხოების ჟურნალში

ბ) მოვლენათა დათვალიერების პროგრამის სისტემურ ჟურნალში

გ) მოვლენათა დათვალიერების პროგრამის გამოყენებით პროგრამების გაშვების ჟურნალში

დ) არცერთ ზემოთ ჩამოთვლილში

**26. როგორ მოვახერხოთ ფაილებისა და საქაღალდეების აუდიტის აქტივიზაციის ჩართვა:**

ა) Start » Control Panel » Administrative Tools » Event Viewer » security;

ბ) Start » Control Panel » Administrative Tools »Local Security Policy » Local Policies » Audit Policy » Audit object access » Success | Failure;

გ) Start » Control Panel » Administrative Tools »Local Security Policy » Local Policies » Audit Policy » Audit directory service access » Success | Failure;

დ) Start » Control Panel » Administrative Tools »Local Security Policy » Local Policies » Audit Policy » Audit account management » Success | Failure;

**27. აუცილებელია ფაილებზე და საქაღალდეებზე მარტივი ზო­გადი წვდომის (Simple File Sharing) გამორთვა, რადგანაც ის :**

ა) ნაწილობრივ აჩენს უსაფრთხო­ების (Security) ჩანართს ფაილებისა და საქაღალ­დეების თვისებების (Properties) დიალო­გურ ჩანართში.

ბ) აჩენს უსაფრთხო­ების (Security) ჩანართს ფაილებისა და საქაღალდეების თვი­სებების (Properties) დიალო­გურ ჩანართში.

გ) არ აჩენს უსაფრთხო­ების (Security) ჩანართს ფაილებისა და საქაღალდეების თვისებების (Properties) დიალო­გურ ჩანართში.

დ) არ აჩენს უსაფრთხო­ების (Security) ჩანართს ფაილებისა და საქაღალდეების თვისებების (Properties) დიალო­გურ ჩანართში.

**28. კონკრეტული საქაღალდეზე ან ფაილზე წვდომის აუდიტის ჩასართავად აუცილებელი მოქმედებები:**

ა) Start » Windows Explorer» კონკრეტული Folder|file გამოყოფა (გამუქება) » File » Properties » Security

ბ) Windows Explorer» კონკრეტული Folder|file გამოყოფა (გამუქება)» File » Security » Properties

გ) Windows Explorer» კონკრეტული Folder|file გამოყოფა (გამუქება) » File » Properties » Security

დ) Start » Windows Explorer» File » Properties » Security

**29**. **კონკრეტულ საქაღალდეზე ან ფაილზე ახალი მომხმარებლის განსაზღვრული უფლებების წვდომის აუდიტის ჩასართავად აუცილებელი მოქმედებები Auditing ჩანართიდან:**

ა) Edit » Audit Entry » არჩეული ტიპის აუდიტის მონიშვნა » ok

ბ) მომხმარებლის ან ჯგუფის გამოყოფა (გამუქება) » Edit » Audit Entry » არჩეული ტიპის აუდიტის მონიშვნა » ok

გ) მომხმარებლის ან ჯგუფის გამოყოფა (გამუქება) » Edit » Audit Entry » არჩეული ტიპის აუდიტის მონიშვნა

 დ) მომხმარებლის ან ჯგუფის გამოყოფა (გამუქება) » Edit » არჩეული ტიპის აუდიტის მონიშვნა » ok

**30. კეისრის კოდირების სისტემით მიღებულია შიფროტექსტი ”ჯჭთკღჰჭ”. ცნობილია, რომ შიფრის გასაღები მოთავსებულია ინტერვალში [-6;6], რისი ტოლია იგი:**

 ა) 3 ბ) 2,9

გ) -4 დ) 4