**”ინფორმაციული უსაფრთხოების საფუძვლები” -საგანი**

**ტესტი შუალედური გამოცდისთვის, II ვარიანტი**

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

**საგნის ხელმძღვანელი - ნუგზარ კერესელიძე**

**1.** **რას უზრუნველყოფს** **ინფორმაციის უსაფრთხოება**

ა)კონფიდენციალობას, მთლიანობასა და წვდომადობას. ბ) აუთენტურობას

გ) დაცულობას დ) საიმედოობას

**2. კიბერუსაფრთხოების პოლიტიკაა**

ა) არ დაუშვას ჰაკერული შეტევები

 ბ) 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.

გ) შექმნას უ­საფრთხოების სისტემა

დ) ინფორმაციული ინფრასტრუქტურის ფუნ­ქციონირება

**3. ქსელური სენსორია**

ა) პროგრამული უზრუნველყოფა

ბ) ინფორმაციული ტექნოლოგია

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

დ) აპარატი

**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. 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 სუბიექტის დაჯარიმება

**6. 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

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

 ა) secpol32.msc ბ) regedt32.exe

გ) dpedit32.msc დ) cmd32

**8. SID იდენტიფიკატორის დროითი ხანდრძლივობა**

ა) SID იდენტიფიკატორი იშლება კომპიუტერის ყოველ გამორთვისას

ბ) SID იდენტიფიკატორი იქმნება კომპიუტერის ყოველი ჩართვისას და იშლება კომპი­უტერის ყოველ გამორთვისას

გ) SID იდენტიფიკატორი იქმნება მომხმარებლის ახალი აღრიცხვის ჩანაწერის შექმნის­თანავე და არსებობს მისი წაშლის მომენტამდე

 დ) SID იდენტიფიკატორი იქმნება მომხმარებლის ახალი აღრიცხვის ჩანაწერის შექმნის­თანავე და აკომპიუტერის ყოველ გამორთვამდე

**9. დამატებით რამდენი სახის უსაფრთხოების ჯგუფები შექმნა შეიძლება Windows-ში**

 ა) არ შეიძლება ბ) ერთის

 გ) სამი დ) ნებისმიერი

**10.Users (მომხმარებლები)**:

ა) აქვს მრავალი პრივილეგია

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

გ) ესაა შეზღუდული უფლებების ნაკრები ისეთი მომხმარებლებისათვის, რომელთაც არ ეძლევათ სისტემის ადმინისტრირების უფლება

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

**11. როგორ შევქმნათ ახალი მომხმარებლის აღრიცხვის ჩანაწერები**

 ა) start →control panel→user accounts→manage Accounts→Create a password for your Accounts

 ბ) start → control panel → user accounts → next

 გ) start → control panel → user accounts → Create New Accounts→სახელის შეყვანა→next

დ) start → control panel → user accounts →manage Accounts → Change your Accounts

**12. როგორ შევცვალოთ მომხმარებლის აღრიცხვის ჩანაწერებში მონაცემები**:

ა) start → control panel → user accounts → change an account→ შესაბამის პიქტოგრამაზე დაწკაპუნებით

ბ) start → control panel → user accounts → or pick an account to change ნაწილში შესაბამის პიქტოგრამაზე დაწკაპუნებით

გ) ორივე შემოთ ჩამოთვლილი საშუალებით

დ) არცერთი ზემოთ ჩამოთვლილი საშუალებით

**13. 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

**14. როცა ხდება მომხმარებლის აღრიცხვის ჩანაწერების გაუქმება, მაშინ მომხმარებლის მიერ შექმნილი ფაილები:**

ა) ავტომატურად ნადგურდება ბ) ავტომატურად უცვლელად რჩება

გ) გვეკითხებიან - შევინახოთ სამუშაო მაგიდა და ფაილები ”ჩემი დოკუმენტებიში” , თუ გავანადგუროთ

დ) არცერთი ზემოდ ჩამოთვლილი

**15. პაროლების პოლიტიკის ჩართვა**

ა) Start → Run →ბრძანების სტრიქონი →gpedit.msc → ok → Computer configuration→ Windows Setting →Security Setting→ Account Policies→ Password policy

ბ) Start → Run →ბრძანების სტრიქონი →gpedit.msc → ok → Administrative Templates→ Windows Setting →Security Setting→ Account Policies→ Password policy

გ) Start → gpedit.msc → ok → Windows Setting →Security Setting→ Account Policies→ Password policy

დ) Start → Run →ბრძანების სტრიქონი →gpedit.msc → ok → Windows Setting →Security Setting →Account Policies→ Password policy

**16. პაროლების გაშიფრის (გატეხვისთვის) დაცვისთვის ირჩევენ:**

ა) Start → Run ბრძანების სტრიქონი →gpedit.msc → ok → Administrative Templates→ Windows Setting →Security Setting→ Account Policies → Account Lockout

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

გ) Start → Run ბრძანების სტრიქონი →gpedit.msc → ok → Windows Setting →Security Setting →Account Policies→ Account Lockout

დ)Start → gpedit.msc → ok → Windows Setting →Security Setting→ Account Policies→ Password policy → Account Lockout

**17. აუდიტის პოლიტიკის ჩასართავად საჭიროა:**

ა) Start → Run→ ბრძანების სტრიქონი →gpedit.msc → ok → Computer configuration→ Windows Setting →Security Setting→ local Policies → Audit Policy

ბ) Start → control panel → Administrative Tools → local Security Policy→ local Policies→ Audit Policy

გ) Start → Run→ ბრძანების სტრიქონი →secpol.msc → local Policies→ Audit Policy

დ) ყველა ზემოთ ჩამოთვლილი შემთხვევები.

**18. მომხმარებლისათვის უფლებების მინიჭებისთვის საჭიროა** **Administrative Tools-იდან:**

ა) local Security Policy→ local Policies→ User Right Assignment

ბ) local Security Policy→ local Policies→ Security Options → Assignment

გ) local Security Policy→ local Policies→Public key Policies

დ) ყველა ზემოდ ჩამოთვლილი

**19. Windows-ში სტანდარტული ჯგუფების რაოდენობა არის:**

ა) 7 ბ) 8

გ) 9 დ) 10

**20. გამოცდილ მომხმარებელთა ჯგუფში ახალი წევრის ჩართვისას:**

ა) Computer Management→ System Tools→ Local users and groups→Users→Power User→ add→advanced→ok→ok

ბ) Computer Management→ System Tools→ Local users and groups→group→Power User→ add→advanced→ok

გ) Computer Management→ System Tools→ Storage→group→Power User→ add→advanced→ok→ok

დ) Computer Management→ System Tools→ Local users and groups→group→Power User→ add→advanced→ok→ok

**21. როგორ ჩავრთოთ აღრიცხვის ჩანაწერში შეტანილ ცვლიცებების აუდიტი.**

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

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

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

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

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

ა) დოქტორ ვები ბ) მაიკროსოფტ ოფისის დიაგნოსტიკა

გ)მაიკროსოფტ ოფისის სესიები დ) არც ერთი ზემოთ ჩამოთვლილი

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

ა) გაიხსნება მოვლენათა დათვალიერების პროგრამის უსაფრთხოების ჟურნალი

ბ) დაიხურება მოვლენათა დათვალიერების პროგრამის უსაფრთხოების ჟურნალი

გ) დაიხურება მოვლენათა დათვალიერების პროგრამის სისტემური ჟურნალი

დ) გაიხსნება მოვლენათა დათვალიერების პროგრამის სისტემური ჟურნალი

**24. რომელი ჟურნალის, რა ტიპის დეტალური ჩანაწერია მოცემული ამ ნახატზე**



ა) სისტემური, წარმატებული ბ) სისტემური, წარუმატებელი

გ) გამოყენებითი, წარუმატებელი დ) უსაფრთხოების, წარმატებული

**25. შესვლის წარუმატებული მცდელობის სიმბოლოა**

ა)  ბ) 

გ)  *დ*)

**26. რომელი ფაილური სისტემის საქაღალდეებისა და ფაილების აუდიტია შესაძლებელი:**

ა) FAT ბ) NTFS

გ) FAT32 დ) არც ერთის

**27.** **ფაილებზე და საქაღალდეებზე მარტივი ზო­გადი წვდომის (Simple File Sharing) გამოსართავად:**

 ა) start » accessories »Folder Options» view» User simple file sharing (Recommended) გამორთეთ

ბ) start » accessories » Windows Explorer» view» User simple file sharing (Recommended) გამორთეთ » ok

გ) start » accessories » Windows Explorer» Tools»Folder Options» view» User simple file sharing (Recommended) გამორთეთ » ok

დ) start » accessories » Windows Explorer» Tools»Folder Options» view» User simple file sharing (Recommended) გამორთეთ

**28**. **კონკრეტულ საქაღალდეზე ან ფაილზე ახალი მომხმარებლის წვდომის აუდიტის ჩასართავად აუცილებელი მოქმედებები Security ჩანართიდან:**

 ა) Advanced » Advanced Security Setting » Add » Select User Or group » ახალი მომხმარებლის ან ჯგუფის ჩაწერა » ok

ბ) Advanced » Advanced Security Setting » Auditing » Select User Or group » ახალი მომხმარებლის ან ჯგუფის ჩაწერა » ok

გ) Advanced » Advanced Security Setting » Auditing » ახალი მომხმარებლის ან ჯგუფის ჩაწერა » ok

დ) Advanced » Advanced Security Setting » Auditing » Add » Select User Or group » ახალი მომხმარებლის ან ჯგუფის ჩაწერა » ok

**29. სად შეესაბამება მიმართვის უფლებები და მოქმედებები:**

ა) Read & execute - აძლევს უფლებას ჩაწეროს ფაილში და გაუშვას პროგრამები შესრულებაზე

ბ) Write - უფლებას არ აძლევს არჩეულ მომხმარებელს და ჯგუფს შექმნას ფაილები

გ) Modify - აძლევს უფლებას შეცვალოს მიმართვა და საკუთრება ფაილზე

დ) Full Control - ამყარებს სრულ კონტროლს ფაილებზე და საქაღალდეებზე

**30.** **კეისრის კოდირების სისტემით დაშიფრულია პაროლი ”იმაზლზ”. რომელი შეიძლება იყოს შიფროტექსტი და შიფრის გასაღები:**

ა) ეთჯგზგ; k=-4 ბ) ლოგინი; k=2

გ) პუზნრნ; k=6 დ) ყველა