**Տեղեկատվական տեխնոլոգիաների հարցարան 1**

(համակարգչային ցանցերի հիմունքներ և տեղեկատվության պաշտպանության հիմունքներ)

***Քրեական և քրեական դատավարության օրենսդրություն***

1. Հանցակազմի հասկացությունը և տեսակները
2. Հանցագործության հատուկ սուբյեկտը
3. Փողերի լվացումը և դրա տեսակները
4. Պաշտոնատար անձի կողմից իշխանական կամ ծառայողական լիազորությունները կամ դրանցով պայմանավորված ազդեցությունը չարաշահելը կամ լիազորություններն անցնելը
5. Ապօրինի հարստանալը
6. Կաշառք ստանալը և տալը, կաշառքի միջնորդությունը, դրանց տեսակները
7. Պաշտոնեական կեղծիքը
8. Հայաստանի Հանրապետության օրենսդրությամբ սահմանված` հայտարարագիր ներկայացնելու պարտականություն ունեցող անձի կողմից հայտարարագրում կեղծ տվյալներ ներկայացնելը, հայտարարագրման ենթակա տվյալները թաքցնելը կամ հայտարարագիր չներկայացնելը
9. Քննիչը, նրա լիազորությունները
10. Հետաքննության մարմնի լիազորությունները
11. Ապացույցների հասկացությունը, ապացույցների թույլատրելիությունը և դրանց օգտագործման սահմանափակումները
12. Ձերբակալման հասկացությունը, տեսակները, հիմքերը և դատավարական կարգը,
13. Ձերբակալվածի իրավունքները և պարտականությունները
14. Վարույթն իրականացնող մարմին հարկադրաբար ներկայացնելը որպես դատավարական սանկցիա
15. Քրեական վարույթ նախաձեռնելը: Քրեական վարույթ նախաձեռնելու առիթները, հիմքերը և կարգը
16. Քրեական հետապնդումը բացառող հանգամանքները
17. Հետաքննություն կատարելու հիմքը, սկիզբն ու ավարտը
18. Խուզարկության և առգրավման կատարման հիմքերը և կարգը
19. Գաղտնի քննչական գործողությունների տեսակները, կատարման հիմքը և պայմանները

***Օպերատիվ-հետախուզական գործունեության օրենսդրություն***

1. **Պետական գաղտնիքի և սահմանափակ տարածման ծառայողական**

**տեղեկության հասկացությունը, գաղտնիության աստիճանները և դրանց հասկացությունները**

1. Պետական գաղտնիք կազմող տեղեկությունների պաշտպանությունը
2. **Տեղեկությունները պետական գաղտնիքի և սահմանափակ տարածման**

**ծառայողական տեղեկության շարքին դասելը**

1. Օպերատիվ-հետախուզական գործունեության հասկացությունը
2. Օպերատիվ-հետախուզական միջոցառման հասկացությունը
3. Օպերատիվ-հետախուզական գործունեության նպատակները
4. Օպերատիվ-հետախուզական գործունեության ընթացքում կիրառվող հատուկ

տեխնիկական մի­ջոցները

1. Օպերատիվ-հետախուզական գործունեության տեղեկատվական ապահովումը

և փաս­տա­թղ­թա­վո­րումը

1. Օպերատիվ-հետախուզական գործունեության արդյունքների ամրագրումը
2. Օպերատիվ-հետախուզական գործունեություն իրականացնող պետական

մարմինները և նրանց գոր­ծառույթները

1. Օպերատիվ-հետախուզական գործունեություն իրականացնող մարմինների

իրավունքները և պարտա­կա­նու­թյուն­նե­րը

1. Օպերատիվ-հետախուզական միջոցառումների տեսակները
2. Օպերատիվ-հետախուզական միջոցառումների անցկացման հիմքերը
3. Օպերատիվ-հետախուզական միջոցառումների անցկացման պայմանները և

դրանց ներկայացվող ընդհանուր պա­հանջ­­ները

1. **Օպերատիվ-հետախուզական միջոցառումների հետևանքով ստացված**

**նյութերի և փաս­տա­թղ­թե­րի հրապարակայնությունը**

1. Հեռախոսային խուսակցությունների վերահսկում օպերատիվ-հետա­խու­զա­

կան միջոցառման անց­կացման ընթացակարգը

1. Օպերատիվ-հետախուզական գործունեության արդյունքների օգտագործումը
2. Դատախազական հսկողությունը օպերատիվ-հետախուզական

գործունեության նկատմամբ

1. Դատարանի թույլտվությամբ իրականացվող օպերատիվ-հետախուզական

միջոցառումների իրավաչափության երաշխիքները

***Համակարգչային ցանցերի հիմունքներ և***

***տեղեկատվության պաշտպանության հիմունքներ***

***1. Համակարգչային ցանցերի բաղադրիչները և մոդելները****.*

1.1 Ցանցերի և տվյալների մշակման համակարգերի հիմնական գաղափարները, սահմանումները և տերմինաբանությունը: Ցանցերի, հանգույցների, համակարգիչների միջև հաղորդագրությունների փոխանցման բազմամակարդակ մոտեցումը։

1.2Բաց համակարգ գաղափարը և միջցանցային փոխհամագործակցման մակարդակները, բաց համակարգերի փոխհամագործակցման էտալոնային OSI մոդելը: TCP/IP էտալոնային մոդելը: OSI և TCP/IP մոդելների համեմատումը:

***2. Ֆիզիկական մակարդակ, ցանցերի տիպային ճարտարապետական որոշումները***.

2.1 Ցանցային քարտ, բազային տոպոլոգիաները` շինա, աստղաձև, օղակաձև, լրիվ, բջիջ, կիրառման եղանակները:

2.2 Կոմբինացված տոպոլոգիաները` աստղ-շինային, աստղ-օղակաձև, կիրառման եղանակները:

2.3 Ethernet տեխնոլոգիան, միջավայրի հասանելիության մեթոդը, բախման` կոլիզիայի երևույթը, հիմնական պարամետրերը տարբեր սպեցիֆիկացիայի մալուխների դեպքում։

2.4 Token Ring տեխնոլոգիան, հիմնական բնութագրերը, բաժանելի միջավայրի հասանելիության մարկերային մեթոդը, մարկեր հասկացողությունը:

2.5 Frame Relay, SMDS և FDDI տեխնոլոգիաները, դրանց առանձնահատկությունները:

***3. Կապուղային մակարդակը*.**

3.1Կապուղային մակարդակի արձանագրությունները, MAC հասցեն:

3.2 ICMP, ARP արձանագրությունները:

3.3 Ցանցի տրամաբանական մասնատման սկզբունքները:

**4. *Ցանցային մակարդակը***.

4.1Հիմնական խնդիրները, արձանագրությունները, IP փաթեթի վերնագրի ձևաչափը։

4.2 Ցանցերում ստատիկ և դինամիկ երթուղավորման սկզբունքները, Երթուղավորման OSPF, RIP, BGP արձանագրությունները:

**5. *Հասցեավորումը ցանցերում.***

5.1 IPv4 հասցեն, դասերը, ենթացանցի դիմակը, մասնավոր IPv4 հասցեները:

5.2 IPv4 և IPv6-ի տարբերությունները, IPv6-ի ձևաչափը:

**6. *Տրանսպորտային մակարդակը***.

6.1UDP արձանագրությունը, դեյտագրամի աշխատանքի սկզբունքը:

6.2 TCP արձանագրությունը, Դեյտագրամի ձևաչափը, աշխատանքի սկզբունքը:

6.3 RTCP, SCTP արձանագրությունները:

6.4 Հոսքերի կառավարման մեխանիզմները։

6.5 http և https արձանագրությունները:

6.6 FTP և SFTP արձանագրությունները:

**7.*Սեանսային, ներկայացուցչական և ծրագրային մակարդակները.***

7.1 Սեանսային և ներկայացուցչական մակարդակի գործառույթները։

* 1. Ծրագրային մակարդակի FTP, Telnet, SMTP, SNMP, DHCP, DNS

արձանագրությունները:

**8. *Ցանցերի տեխնոլոգիաները և դրանց ստանդարտները.***

* 1. Ցանցերի ստանդարտները`IEEE, ITU, ISO և այլն:
  2. Ցանցերի բազմամակարդակ ֆունկցիոնալությունը:

8.3 Fiber Channel ճարտարապետությունը, մակարդակները, ստանդարտները:

**9. *Կոմուտացիան LAN-երում.***

9.1 PPP և HDLC արձանագրությունները, դրանց բաղադրիչները, ֆունկցիաները, ինկապսուլյացիան:

9.2 Կամուրջների կիրառմամբ կոմուտացիայի իրականացում և համեմատում

LAN-երի երկրորդ մակարդակի կոմուտացիայի հետ:

**10. *VLAN տեխնոլոգիան և ստանդարտները***.

10.1 Դասակարգումը, իրականացման տարբերակները` մեկ switch-ով, մի քանի

switch-ով, կամուրջների հենքի վրա:

10.2 Երթուղավորումը VLAN ցանցերի միջև: Ստատիկ և դինամիկ VLAN-ներ և դրանց ստանդարտները: Մասնավոր VLAN-ներ:

**11. *Միջցանցային երթուղավորումը***.

11.1 CIDR տեխնոլոգիան, հասցեների միավորումը (summarization):

11.2 IGRP արձանագրության աշխատանքի նկարագրությունը, IGRP-ի կոնֆիգուրացումը:

11.3 Արտաքին երթուղավորման BGP արձանագրությունը: Երթուղու ընտրությունը BGP-ով: BGP-ի ատրիբուտները (/Weight, Local preference, NextHop, Origin և այլն):

**12. *Տրանսպորտային մակարդակի հոսքային տվյալների արձանագրությունները***

12.1SCTP, Real Time Streaming Protocol(RTSP), Internet Stream Protocol (**ST** and later **ST-II**) հոսքային արձանագրությունները:

12.2 Multipath TCP արձանագրությունը;

***13. Էլեկտրոնային փոստի արձանագրությունները` SMTP, POP3,IMAP4 (RFC 5321), MIME,*** [***S/MIME***](https://ru.wikipedia.org/wiki/S/MIME) ***ձևաչափերը:***

**14.** ***Ձայնային տվյալների փոխանցման տեխնոլոգիաները.***

14.1 H323 արձանագրությունը:

14.2 SIP արձանագրությունը:

**15.**  ***QoS տեխնոլոգիան.***

15.1 Ցանցի գերբեռնվածության հսկում:

15.2 Տվյալների հոսքի անցման արգելանքները, արգելանքների տատանումները, կորստի չափերը:

**16*. Տարածքային բաշխված ցանցերը (ՏԲՑ).***

16.1 ՏԲՑ-երի սարքավորումները: CSU/DSU սարքեր: ՏԲՑ-երը և OSI մոդելը:

**17**. ***Ցանցերի կառավարման հիմնադրույթները.***

17.1 Կառավարվող պարամետրերը և կառավարման սխեման: Կառավարման առաջնային քայլերը:

**18. *Քոմփյութերային ցանցերի կառավարման հիմնադրույթները.***

18.1Քոմփյութերային ցանցերի կառավարման սկզբունքները, առանձնահատկությունները և տեսակները:

18.2 Ցանցերի կառավարման ճարտարապետությունը, [FCAPS](https://ru.wikipedia.org/wiki/FCAPS) մոդելը:

**19. *Քոմփյութերային ցանցերի կառավարման արձանագրությունները.***

19.1SNMP, CMIP, WBEM արձանագրությունները:

19.2 Common Information Model, netconf, Java Management Extensions կառավարման մեխանիզմների նկարագրությունը:

**20. *Հեռահաղորդակցության կառավարումը***.

20.1 Հեռահաղորդակցության կառավարման (Telecommunications Management Network - ITU-T M.3010 TMN) ճարտարապետությունը:

20.2 Քոմփյութերային ցանցերի երկաստիճան և եռաստիճան կառավարման մեխանիզմները:

**21. *Քոմփյութերային ցանցերի ավտոմատացված կառավարումը.***

21.1 Քոմփյութերային ցանցերի ավտոմատացված կառավարման գործիքամիջոցները և համակարգերը:

**22.*Կորպորատիվ քոմփյութերային ցանցերի մշտադիտարկումը.***

22.1 Կորպորատիվ քոմփյութերային ցանցերի մշտադիտարկման հիմունքները:

22.2 Քոմփյութերային ցանցերի թրաֆիկի մշտադիտարկման գործառույթները:

22.3 Քոմփյութերային ցանցերի թրաֆիկի վերլուծության գործիքամիջոցները:

**23. *Քոմփյութերային ցանցերի հեռավար կառավարումը.***

23.1 Քոմփյութերային ցանցերի հեռավար կառավարման առանձնահատկությունները և կազմակերպման սկզբունքները:

**24.** ***Ցանցի բեռնվածքի կառավարումը***.

24.1 Ցանցի բեռնվածքի կառավարման խնդիրները:

24.2 Հավասարաչափ բաշխման ծրագրային գործիքների դասերը և գործառույթները:

**25. *Ցանցի անվտանգության կառավարումը.***

25.1 Տեղեկատվական անվտանգության սպառնալիքները և ռիսկերը, ցանցերի պաշտպանության ապահովման խնդիրները:

25.2 Ցանցային անվտանգության քաղաքականությունը:

1. Տեղեկատվության պաշտպանության գաղափարը :
2. Տվյալներ, տեղեկատվություն և գիտելիք։
3. Տեղեկատվության պաշտպանության հիմնական հասկացությունները:
4. Գաղտնիություն, ամբողջականություն, անհերքելիություն։
5. Տեղեկատվական համակարգերի վրա իրականացվող գրոհները և հնարավոր սպառնալիքները։
6. Տեղեկատվության պաշտպանության հիմնական մարտահրավերները։
7. Տեղեկատվական համակարգերի վրա իրականացվող գրոհները - կոտրում։
8. Տեղեկատվական համակարգերի վրա իրականացվող գրոհները - նմանակում։
9. Տեղեկատվական համակարգերի վրա իրականացվող գրոհները - դիտարկում։
10. Սոցիալական ճարտարագիտություն։
11. Տեղեկատվական համակարգերի վրա իրականացվող գրոհները - սպասարկման մերժում։
12. Խոցելիության ռիսկի նվազեցման քայլեր:
13. Ներխուժման հայտնաբերում։
14. Էթիկական հաքերային ներթափանցում։
15. Վնասակիր ծրագրեր։
16. Վնասակիր ծրագրերից պաշտպանության միջոցները։
17. Սխալներ հայտնաբերող և ուղղող կոդեր։
18. Զույգությունը ստուգող կոդ։
19. Հեմինգի կոդ։
20. Գաղտնագրային պաշտպանության գաղափարը:
21. Գաղտնագրության հիմնական հասկացությունները։
22. Համաչափ և անհամաչափ գաղտնագրային համակարգերի գաղափարը:
23. Պատմական գաղտնագրայի ալգորիթմներ։
24. Ժամանակակից գաղտնագրային ալգորիթմների աշխատանքի սկզբունքները։
25. Թաքնագրային պաշտպանության գաղափարը։
26. Թաքնագրության պատմական և կենցաղային օրինակներ։
27. Ժամանակակից օպերացիոն համակարգերի անվտանգություն։
28. Տեղեկատվության պաշտպանություն չարտոնված մուտքերից։
29. Տվյալների բազաների անվտանգություն։
30. Վեբ անվտանգություն։
31. Օգտագործողների վավերականացում։
32. Վավերականացման տվյալների վրա հիմնված համակարգեր։