«Tasdiqlayman»
Abu Rayhon Beruniy nomidagi
UrDU rektori v.v.b. _____S.U.Xodjaniyazov

SUHBAT JARAYONIDA BERILADIGAN NAMUNAVIY SAVOLLAR TO‘PLAMI

60610300 – Axborot xavfsizligi ta’lim yo‘nalishi bo‘yicha

1. **Mamlakatda o‘z sohasiga oid amalga oshirilayotgan islohotlarning mohiyati va ahamiyatini tushunish.**

1. Axborot xavfsizligi sohasida mamlakatda olib borilayotgan islohotlar qanday asosiy yo‘nalishlarni qamrab oladi?
2. Axborot xavfsizligi strategiyasining asosiy maqsadlari nimalardan iborat?
3. Davlatning raqamli transformatsiya jarayonida axborot xavfsizligi islohotlari qanday rol o‘ynaydi?
4. O‘zbekistonda axborot xavfsizligini tartibga soluvchi asosiy qonun va normativ hujjatlar qaysilar?
5. Milliy axborot xavfsizligi tizimini rivojlantirishda xalqaro tajribadan foydalanishning ahamiyati nimada?
6. Axborot xavfsizligi islohotlarida davlatning strategik maqsadi nima?
7. “Axborotlashtirish to‘g‘risida”gi Qonun axborot xavfsizligi bo‘yicha qanday asosiy talablarni belgilaydi?
8. Axborot xavfsizligini ta’minlash bo‘yicha davlat organlari vakolatlari qanday taqsimlangan?
9. O‘zbekistonda kiberxavfsizlik markazlari va CERT/CSIRT tuzilmalari qaysi vazifalarni bajaradi?
10. Maxfiy ma’lumotlarni himoya qilish bo‘yicha normativ hujjatlarning amaliy ahamiyati nimada?
11. Axborot xavfsizligi islohotlarida davlat-xususiy sektor hamkorligi qanday amalga oshiriladi?
12. Kiberjinoyatlarni tergov qilish va oldini olish bo‘yicha qanday qonunchilik choralarini bilasiz?
13. Milliy tarmoq infratuzilmasini himoya qilishda qanday texnik islohotlar amalga oshirilmoqda?
14. Davlat axborot tizimlarida kriptografik himoya vositalaridan foydalanish talablari qanday belgilangan?
15. Kiberxavfsizlik bo‘yicha milliy monitoring tizimi qanday ishlaydi?
16. Axborot tizimlarini sertifikatlash va attestatsiyadan o‘tkazishning maqsadi nima?
17. Raqamli hukumat (e-Government) loyihalarida axborot xavfsizligi qanday integratsiya qilinmoqda?
18. Milliy ma’lumotlar markazlarida xavfsizlikni oshirish uchun qanday texnologiyalar qo‘llanilmoqda?
19. Axborot xavfsizligi bo‘yicha malakali mutaxassislarni tayyorlash davlat islohotlarida qanday o‘rin tutadi?

20. Universitetlarda kiberxavfsizlik fanlarini o‘qitishning milliy strategiyaga qo‘shgan hissasi qanday?

21. Axborot xavfsizligi bo‘yicha ilmiy-tadqiqot ishlari davlat siyosatida qanday qo‘llab-quvvatlanadi?

22. Mutaxassislar uchun xalqaro sertifikatlash (CISSP, CEH, ISO 27001) dasturlarini rivojlantirishning ahamiyati nimada?

23. Davlat xodimlari uchun axborot xavfsizligi bo‘yicha muntazam treninglarning maqsadi nima?

24. Yosh mutaxassislar uchun milliy grant va stipendiyalar axborot xavfsizligi sohasida qanday rag‘batlantiradi?

25. O‘zbekiston qaysi xalqaro kiberxavfsizlik tashkilotlari bilan hamkorlik qiladi?

26. Xalqaro kiberxavfsizlik standartlarini (ISO, NIST, ITU) joriy etish mamlakat xavfsizligiga qanday ta’sir qiladi?

27. Transchegaraviy kiberjinoyatlarga qarshi kurashda xalqaro hamkorlikning roli nimada?

28. Mamlakatlararo axborot almashinuvida xavfsizlikni ta’minlash mexanizmlari qanday ishlaydi?

29. Xalqaro tajriba asosida O‘zbekistonda kiberxavfsizlik siyosatini takomillashtirish misollari keltiring.

30. O‘zbekistonning xalqaro kiberxavfsizlik reytinglaridagi o‘rni islohotlar samaradorligi haqida qanday ma’lumot beradi?

2. Bakalavriat ta’lim yo‘nalishini tanlashda motivatsiya (soha kasbining mohiyati va ijtimoiy ahamiyatini tushunish, unga doimiy qiziqish ko‘rsatish)

1. Axborot xavfsizligi sohasining jamiyat va davlat uchun asosiy ahamiyati nimada?
2. Nega zamonaviy dunyoda axborot xavfsizligi strategik soha hisoblanadi?
3. Axborot xavfsizligi sohasi qaysi asosiy yo‘nalishlarni o‘z ichiga oladi?
4. Kiberxavfsizlik va axborot xavfsizligi o‘rtasidagi farq nimada?
5. Axborot xavfsizligi bo‘yicha mutaxassislar qanday asosiy vazifalarni bajaradi?
6. Kiberhujumlarning iqtisodiy va ijtimoiy oqibatlari nimalardan iborat?
7. Axborot xavfsizligi fuqarolarning shaxsiy hayoti daxlsizligini qanday ta’minlaydi?
8. Davlatning axborot tizimlarini himoya qilish nima uchun muhim?
9. Raqamli iqtisodiyot rivojida axborot xavfsizligi qanday rol o‘ynaydi?
10. Sog‘liqni saqlash, moliya va ta’lim sohalarida axborot xavfsizligining ahamiyatini misollar bilan tushuntiring.
11. Xalqaro kiberxavfsizlik hamkorligining ijtimoiy foydasi nimada?
13. Siz axborot xavfsizligi sohasini tanlashga nima sabab bo‘ldi?
14. Axborot xavfsizligi bo‘yicha ishlash siz uchun qanday shaxsiy qoniqish keltiradi?

15. Ushbu sohada muvaffaqiyat qozonish uchun qanday shaxsiy fazilatlar zarur deb hisoblaysiz?
16. Axborot xavfsizligi sohasida ishlashning eng qiziqarli jihatlari nimalar?
17. Kiberxavfsizlik bo‘yicha yangi texnologiyalarni o‘rganishga bo‘lgan ishtiyoqingizni qanday baholaysiz?
18. Ushbu sohada ilmiy-tadqiqot ishlari olib borishga qiziqasizmi?
19. Kelajakda axborot xavfsizligi mutaxassislariga talab ortishiga sabab bo‘ladigan omillar qaysilar?
20. Axborot xavfsizligi bo‘yicha xalqaro sertifikatlarga ega bo‘lishning foydasi nimada?
21. Sun’iy intellekt va kiberxavfsizlikning o‘zaro bog‘liqligi qanday rivojlanmoqda?
22. Bulutli texnologiyalarda axborot xavfsizligini ta’minlashning murakkab jihatlari qaysilar?
23. IoT (Buyumlar interneti) qurilmalarida xavfsizlikni ta’minlash nima uchun dolzarb?
24. Kelajakda axborot xavfsizligi sohasida qanday yangi tahdidlar paydo bo‘lishi mumkin?

3. **Shaxsiy-kasbiy xususiyatlar (o‘qishga qobiliyat, kasbiy vazifalarni hal qilishda amaliy faoliyat, intizomlilik, hamjihatlik, mas’uliyatlilik, qaror qabul qilishda mustaqillik darajasi, shaxsiy yutuqlar mavjudligi, shuningdek, o‘z ustida ishlash va ijodkorlik qobiliyatlari)**

1. Kriptografiya bo‘yicha yangi algoritmni o‘zlashtirishda qanday yondashuvni qo‘llasiz?
2. Kiberxavfsizlik bo‘yicha xalqaro standartlarni (ISO 27001, NIST) o‘rganish darajangizni qanday baholaysiz?
3. So‘nggi 12 oyda o‘zingiz o‘rgangan eng dolzarb kiberxavfsizlik texnologiyasi qaysi?
5. Tarmoqdagi zaifliklarni aniqlashda qaysi skanerlash vositalarini qo‘llaysiz?
6. Kiberhujum yuz berganda hodisaga javob berish (Incident Response) bosqichlarini qanday ketma-ketlikda bajarishingizni tushuntiring.
7. Digital forensics jarayonida dalillarni to‘plash va saqlash bo‘yicha qanday choralarni bilasiz?
8. Axborot tizimini himoyalash uchun ishlab chiqqan yoki takomillashtirgan yechimingiz bo‘lganmi?
9. Xavfsizlik siyosatiga barcha xodimlarning rioya qilishini jamoada qanday nazorat qilasiz?
10. Penetratsion test o‘tkazishda jamoa ichida vazifalarni qanday taqsimlaysiz?
11. Vaqt cheklangan sharoitda tarmoqni himoya qilish choralari ustuvorligini qanday belgilaysiz?
12. Hamkasblar bilan ishlash jarayonida xavfsizlik bo‘yicha kelishmovchilik yuzaga kelsa, uni qanday hal qilasiz?
13. Kiberxavfsizlik bo‘yicha qaror qabul qilishda qanday risk tahlili usullaridan foydalanasiz?
14. Foydalanuvchi ma’lumotlari sizib chiqish xavfi aniqlansa, birinchi navbatda qanday chorani ko‘rasiz?

15. Zaiflikni tuzatish yoki uni vaqtincha cheklash bo‘yicha qaror qabul qilgan tajribangizni tushuntiring.
16. Kutilmagan DDoS hujumida mustaqil qaror qabul qilish bo‘yicha qanday rejangiz bor?
17. Axborot xavfsizligi bo‘yicha yangi hujum ssenariylarini aniqlash uchun qanday ijodiy yondashuvlardan foydalanasiz?
18. Xavfsizlik tizimini yaxshilash uchun ishlab chiqqan noodatiy texnik yechimingizni tasvirlab bering.
19. Soha bo‘yicha xalqaro konferensiya, vebinar yoki onlayn kurslardan qaysilarida ishtirok etgansiz?
20. Kelajakda axborot xavfsizligi sohasidagi o‘z yutuqlaringizni qanday amaliy loyihalarda qo‘llashni rejalashtiryapsiz?

4. Tanlangan bakalavriat ta’lim yo‘nalishi sohasidagi bilim va kasbiy ko‘nikmalarning mavjudligi

1. Axborot xavfsizligining uch asosiy tamoyili (CIA triadasi) nimani anglatadi?
2. Axborot xavfsizligida maxfiylik (Confidentiality) qanday ta’minlanadi?
3. Axborot yaxlitligi (Integrity) tushunchasiga misol keltiring.
4. Mavjudlik (Availability) tamoyilini buzuvchi hodisaga misol bering.
5. Kiberxavfsizlik va axborot xavfsizligi o‘rtasidagi asosiy farq nimada?
6. Axborot xavfsizligidagi asosiy tahdid turlari qaysilar?
7. Ijtimoiy muhandislik (Social Engineering) nima va uning turlari qaysilar?
8. Axborot xavfsizligi siyosati (Security Policy) nimani o‘z ichiga oladi?
9. “Defense in Depth” (Ko‘p qatlamli himoya) strategiyasining mohiyatini tushuntiring.
10. Xavf tahlili (Risk Assessment) jarayonining asosiy bosqichlarini sanab bering.
11. Firewall qanday ishlaydi va uning asosiy turlari qaysilar?
12. IDS va IPS tizimlari o‘rtasidagi farq nimada?
13. VPN texnologiyasining maqsadi va ishlash prinsipi qanday?
14. TCP/IP modelining xavfsizlik bilan bog‘liq qatlamlari qaysilar?
15. DDoS hujumi nima va undan himoyalanish usullarini ayting.
16. MAC filtering nima va qachon qo‘llaniladi?
17. VLAN texnologiyasi xavfsizlikka qanday hissa qo‘shadi?
18. Port skanerlash (Port Scanning) nima va qanday aniqlanadi?
19. Zero Trust arxitekturasi qanday ishlaydi?
20. HTTPS protokoli HTTP’dan qaysi jihatlari bilan farq qiladi?

21. Simmetrik va assimetrik shifrlash o‘rtasidagi farq nima?
22. AES algoritmi qanday ishlaydi?
23. RSA algoritmining ishlash prinsipini tushuntiring.
24. Hash funksiyasi nima va uning xavfsizlikdagi roli nimada?
25. SHA-256 va MD5 o‘rtasidagi farqlarni tushuntiring.
26. Digital Signature (Raqamli imzo) nima va qachon qo‘llaniladi?
27. Public Key Infrastructure (PKI) qanday ishlaydi?
28. X.509 sertifikati nima uchun kerak?
29. Ko‘p faktorli autentifikatsiya (MFA) nima va qaysi usullarini bilasiz?
30. Kriptografik kalitlarni boshqarishdagi eng yaxshi amaliyotlarni sanab bering.
31. Operatsion tizim xavfsizlik mexanizmlarini sanab bering.
32. Windows OS’da foydalanuvchi huquqlarini qanday boshqarish mumkin?
33. Linux’da fayl ruxsatlari (chmod) qanday ishlaydi?
34. Zaxira nusxa olish (Backup) strategiyalari qaysilar?
35. Virtualizatsiya xavfsizligi bo‘yicha asosiy tahdidlar nimalar?
36. Bulutli xizmatlarda (Cloud) xavfsizlikni ta’minlashning asosiy choralarini ayting.
37. IoT qurilmalarida eng ko‘p uchraydigan zaifliklar qaysilar?
38. SCADA tizimlari xavfsizligining o‘ziga xos jihatlarini tushuntiring.
39. Antivirüs va EDR tizimlari o‘rtasidagi farq nimada?
40. Log fayllarini tahlil qilish xavfsizlik monitoringida qanday rol o‘ynaydi?
41. Phishing hujumi nima va uni qanday aniqlash mumkin?
42. SQL Injection nima va undan himoyalanish usullarini ayting.
43. Cross-Site Scripting (XSS) nima va uning turlari qaysilar?
44. Malware turlari qaysilar va ularga misollar keltiring.
45. Ransomware hujumi qanday ishlaydi va unga qarshi qanday chora ko‘riladi?
46. Zero-Day zaiflik nima?
47. Insider Threat (Ichki tahdid) nima va uni kamaytirish usullari qaysilar?
48. Kiberhujum ssenariysini modellashtirish nima uchun kerak?
49. Penetratsion test (PenTest) nima va uning bosqichlarini sanab bering.
50. Red Team va Blue Team yondashuvlari o‘rtasidagi farq nimada?

Axborot xavfsizligi kafedrasi mudiri: **dots. T.R.Xudayberganov**