

SUHBAT JARAYONIDA BERILADIGAN NAMUNAVIY SAVOLLAR TO‘PLAMI

I BLOK. Mamlakatda o‘z sohasiga oid amalga oshirilayotgan islohotlarning mohiyati va ahamiyatini tushunish bo‘yicha savollar:

1. Respublikamizda davlat xavfsizligini ta‘minlashda kiberxavfsizlikning o‘rni qanday?
2. O‘zbekiston Respublikasi Kiberxavfsizlik to‘g‘risidagi qonunning mazmun-mohiyatini tushuntirib bering.
3. O‘zbekistonda Respublikasida axborot xavfsizligi va kiberxavfsizlikni ta‘minlashda hozirgi kunda amalga oshirilayotgan ishlar nimalardan iborat?
4. Kiberjinoyatchilik deganda nima tushuniladi va kibermakonda yuzaga kelishi mumkin bo‘lgan qanday kiberjinoyatlar bor?
5. Kiberxavfsizlik obyekti hamda kiberxavfsizlik subyekti nimalarni o‘z ichiga oladi?
6. Tashkilotning axborot xavfsizlik siyosati qaysi me‘yoriy hujjatga asoslanib ishlab chiqiladi?
7. O‘zbekistonda Respublikasida kiberxavfsizlik sohasida vakolatli davlat organi va uning asosiy vazifalari nimadan iborat?
8. Kiberxavfsizlikni ta‘minlash deganda nima tushuniladi?
9. Kiberhujumlarning qanday turlari mavjud va uni amalga oshirishda umumiy maqsad nimadan iborat bo‘lishi mumkin?
10. Axborotni muhofaza qilish, axborot xavfsizligi konsepsiyasi nima?
11. Axborot xavfsizligi va axborotni himoyalash tushunchalarini bir-biridan farqi nimadan iborat?
12. Kiberxavfsizlikning ta‘minlanganlik darajasini baholash deganda qanday jarayon tushuniladi?
13. Kiberxavfsizlik hodisalari kim tomonidan tekshiriladi hamda bunda qanday chora-tadbirlar amalga oshiriladi?
14. Muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta‘minlashning asosiy yo‘nalishlari nimalardan iborat?
15. Muhim axborot infratuzilmasi nima, hamda uning obyekti va subyektlarini nimalar tashkil etadi?

II BLOK. Bakalavriat ta'lim yo'nalishini tanlashda motivatsiya (soha kasbining mohiyati va ijtimoiy ahamiyatini tushunish, unga doimiy qiziqish ko'rsatish) bo'yicha savollar

1. Nima uchun aynan axborot xavfsizligi sohasini tanladingiz? Ushbu soha nimasi bilan sizni o'ziga jalb qildi?
2. Respublikamizda axborot xavfsizligi sohasida milliy dasturiy mahsulotlarni ishlab chiqarishga qaratilgan chora-tadbirlarni qanday baholaysiz?
3. O'zbekiston Respublikasi kibermakonida kiberxavfsizlikni ta'minlaganlik darajasi haqida nimalar bilasiz?
4. Hozirgi kunda axborot va kiberxavfsizlik ta'minlash qay darajada muhim deb hisoblaysiz? Misollarda tushuntirib bering.
5. Mana hozirgi kunda Internet tarmog'ida, ijtimoiy tarmoqlarda kiberjinoyatlarni soni ortganligi haqida ko'plab xabarlar tarqalmoqda, bunga sizning fikringiz qanday?
6. Kiberjinoyatchilarni undayotgan motivatsiya haqida nimalar ayta olasiz? Kiberjinoyatlarni amalga oshirishning maqsadlari nimadan iborat?
7. Nima sababda hozirgi kunda axborot va kiberxavfsizlikni ta'minlashga qaratilgan hatti harakatlar oshmoqda, ijtimoiy tarmoqlarda, televideniya shu yo'nalishdagi roliklar ko'paymoqda?
8. Raqamlashtirish jarayonlari ortgan sari kiberxavfsizlikka bo'lgan talab ham ortib bormoqda. Bunga asosiy sabab nima deb o'ylaysiz?
9. Hozirgi kundagi kiberxavfsizlik sohasidagi qonunchilikda bu sohani tartibga soluvchi yetarlicha qonunlar ishlab chiqilgan deb hisoblaysizmi?
10. Soha korxonalaridan kiberxavfsizlikni ta'minlash maqsadida xorijda ishlab chiqarilgan dasturiy mahsulotni joriy qilish maqsadga muvofiqmi yoki milliy dasturiy mahsulotni? Javobingizni izohlang.
11. O'zbekiston Respublikasining Qonuni "Kiberxavfsizlik to'g'risida" qonunni asosiy vazifasi nimadan iborat?
12. Kiberxavfsizlikni ta'minlashni amalga oshiruvchi tashkilotlarning asosiy vazifasi nimadan iborat va ular qanday turdagi xizmatlarni taqdim etmoqda?
13. Respublikamizda faoliyat yuritayotgan Kiberxavfsizlik sohasidagi qanday davlat va xususiy korxonalar va tashkilotlarni bilasiz?
14. Kiberxavfsizlik, kiberhujum va kiberhimoya tushunchalariga ta'rif bering?
15. Tashkilotlarda axborot xavfsizligi siyosatini joriy etish kerakmi? Axborot xavfsizligi siyosati qanday afzalliklarni beradi?

III BLOK. Shaxsiy-kasbiy xususiyatlar:

1. Axborot xavfsizligi mutaxxasisi qanday mas'uliyatlarni o'z zimmasiga olishi lozim?
2. Hozirgi kunga qadar qanday yutuqlarga erishdingiz? Eng asosiy yutug'ingiz sifatida nimani hisoblaysiz?
3. Axborot xavfsizligi xodimi qanday xarakter xususiyatlariga ega bo'lishi kerak? Sizda ushbu fazilatlarning qaysi biri bor?
4. Qaysidir muammo chiqqanda mustaqil qaror qabul qilishni afzal ko'rasizmi yoki birovlarining fikri siz uchun muhimmi?
5. Aynan axborot xavfsizligi yo'nalishini tanlaganingizdan qanday maqsad ko'zlayapsiz? Bunda siz uchun nima muhim?
6. Siz axborot xavfsizligi bo'yicha qaysidir sohada ishlaganmisiz?
7. Axborot xavfsizligi sohasida faoliyat yurituvchi tashkilotlar haqida nimalar bilasiz? Ularning vazifasini tushuntirib bersangiz?
8. Sizningcha axborot xavfsizligi sohasida faoliyat yurituvchi xodim uchun qaysi bilim sohalarini bilish muhim deb hisoblaysiz?
9. Axborot xavfsizligi sohasida ta'lim olishingizni kim maslahat berdi? Ular shu sohada ishlashadimi yoki o'zingiz mustaqil qiziqqanmisiz?
10. Universitetni tugatganingizdan keyingi rejalaringiz nimadan iborat?
11. Axborot xavfsizligi sohasi o'rganish uchun hozirda biror amaliy ish qilyapsizmi? Dasturlashni o'rganyapsizmi yoki chet tilini o'rganyapsizmi?
12. Ta'lim olgan texnikumda axborot xavfsizligi sohasida qanday fanlarni o'qigansiz?
13. Kiberjinoyatchilikdan aziyat chekkanmisiz, yoki yaqin tanishlaringiz ushbu turdagi jinoyat bilan jabrlanganmi?
14. Axborot xavfsizligi sohasini rivojlantirishning dolzarb ekanligini so'ngi yuz bergan voqealar bilan izohlay olasizmi?
15. Nima deb o'ylaysiz qanday bilim va ko'nikmaga ega bo'lgan abuturiyentlar oliy ta'lim muassasasida o'qishni davom ettirishi kerak?
16. Agar siz talabalikka qabul qilinmasangiz, keyingi rejalaringiz qanday bo'ladi?
17. Hozirgi kunda chet tilini bilish, ayniqsa IT sohasida juda muhim hisoblanadi, buning sababi nimada deb o'ylaysiz?

IV BLOK. Axborot xavfsizligi mutaxassisligi bo'yicha:

1. Axborot xavfsizligi tushunchasiga izoh bering?
2. Axborot xavfsizligini ta'minlashning asosiy vazifalari nimalardan iborat?
3. Axborot uchun foydalanuvchanlikning muhimligi?
4. Axborotni yaxlitligini ta'minlash deganda nimani tushunasiz?
5. Axborot xavfsizligida xavflarni boshqarish deganda nimani tushunasiz?
6. Axborotni himoyalashning asosiy yo'nalishlari qaysilar?
7. Tizimli fikrlash nima va u nima uchun zarur?
8. Axborot xavfsizligi va axborotni himoyalash tushunchalarini bir-biridan farqi?
9. Kiberxavfsizlikning bilim sohalari va ularning asosiy xususiyatlari nimalardan iborat?
10. Kiberxavfsizlikda inson omilini misollar yordamida tushuntiring?
11. Tahdid va zaiflik tushunchalariga izoh bering.
12. Shaxsiy ma'lumotlar nima? Ular qanday himoya qilinishi zarur?
13. Kriptografiyaning asosiy tushunchalariga: shifrlash, deshifrlash, kalit, shifr, ochiq matn, shifrmtn, alifbo, izoh bering.
14. Elektron tijorat xavfsizligi?
15. Kodlash va shifrlash tushunchalarining bir – biridan farqini ayting.
16. Kriptografiya va steganografiyaning o'zaro farqini ayting?
17. Simmetrik kriptografiya nima va uning axborotni himoyalashdagi o'rni haqida gapiring.
18. Ochiq kalitli kriptografiyaga izoh bering va uning axborotni himoyalashdagi o'rni haqida gapiring?
19. Xesh funksiya nima, ularga qo'yilgan talablar va uni axborot himoyalashdagi o'rni?
20. Internet-banking, mobil-banking tushunchlari.
21. Kriptografik akslantirishlar: o'rniga qo'yish va o'rin almashtirish nima?
22. Diskni va faylni shifrlash usullarining bir-biridan farqi nimadan iborat?
23. Web saytlarga bo'ladigan DOS hujumni tushuntiring.
24. Qog'oz ko'rinishidagi ma'lumotlarni xavfsiz yo'q qilish usullari va ularning xususiyatlari?
25. Ma'lumotlarni yaxlitligini ta'minlash usullari haqida ayting.
26. Ruxsatlarni nazoratlashning asosiy tushunchalariga: identifikasiya, autentifikasiya va avtorizasiya, izoh bering.
27. Elektron raqamli imzo va xabarlarni autentifikatsiyalash kodlarining bir-biridan farqi hamda o'xshash tomonlarini ayting?
28. Identifikatsiya nima?
29. Elektron raqamli imzoning axborot xavfsizligidagi rolini tushuntiring.

30. Autentifikatsiya nima? Bir faktorli va ko'p faktorli autentifikatsiyaga misol keltiring.

31. Foydalanishni boshqarish matrisasi, ACL va C-list tushunchalarini tushuntiring?

32. Elektron ko'rinishdagi ma'lumotlarni yo'q qilish usullari va ularning xususiyatlari.

33. Parolga asoslangan autentifikatsiya usuli va uning afzallik/kamchiliklarini ayting.

34. Foydalanishni mantiqiy boshqarish deganda nimani tushunasiz?

35. Axborotning fizik himoyasi va uning muhimligini tushuntiring.

36. Tahdid, zaiflik va hujum tushunchalariga izoh bering?

37. Tarmoq qurilmalarining: tarmoq kartasi, repitor, xab, svitch, router, ko'priklar, shlyuzlar, asosiy vazifasini ayting.

38. Asosiy tarmoq protokollari va ularning vazifalarini ayting.

39. Tarmoq viruslari va antivirusli himoyalash muammolari.

40. Zararli dasturiy vositalarga asoslangan hujumlarning asosiy maqsadi nima va ularga misollar ayting.

41. Zaxira nusxalash nima va uning turlarini sanang.

42. Ma'lumotlarni yo'qolishiga olib keluvchi asosiy sabablarni ayting.

43. Zararli dasturlar nima va ularning asosiy turlarini sanang.

44. Kompyuter viruslari nima va ularga misollar ayting.

45. Kiberjinoyatni amalga oshirishdan ko'zlangan maqsadlarni ayting?

46. Kiberetika tushunchasiga izoh bering va ularga misollar keltiring?

47. Zararli dasturlar va ularning klassifikatsiyasini keltiring.

48. Tarmoq xavfsizligiga qaratilgan hujum turlari va ularga izoh bering?

49. Axborot xavfsizligi siyosati nima va uning asosiy vazifasi nimadan iborat?

50. O'zbekiston Respublikasining Jinoyat kodeksida kiberjinoyatchilikka oid qanday bandlar mavjud?

СБОРНИК ВОПРОСОВ, ЗАДАВАЕМЫХ ВО ВРЕМЯ СОБЕСЕДОВАНИЯ ПРИ ПОСТУПЛЕНИИ В ЛИЦЕЙ.

I БЛОК. Вопросы для определения характера и значения реформ в стране по данной сфере:

1. Какова роль кибербезопасности в обеспечении государственной безопасности в нашей республике?
2. Объясните суть закона о кибербезопасности Республики Узбекистан.
3. Какие работы ведутся в настоящее время по обеспечению информационной безопасности и кибербезопасности в Республике Узбекистан?
4. Что такое киберпреступность и какие виды киберпреступлений могут происходить в киберпространстве?
5. Что такое объект и субъект кибербезопасности?
6. На основании какого нормативного документа разрабатывается политика информационной безопасности организации?
7. В чем заключаются основные задачи компетентного государственного органа в сфере кибербезопасности в Республике Узбекистан?
8. Что такое кибербезопасность?
9. Какие бывают виды кибератак и в чем заключается общая цель их реализации?
10. Дать пояснение выражениям: защита информации, информационной безопасности.
11. В чем заключается разница между понятиями информационной безопасностью и защитой информации?
12. Что подразумевается под процессом оценки уровня обеспечения кибербезопасности?
13. Кто расследует процесс кибербезопасности и какой план мероприятий ими предусматривается?
14. Каковы основные направления обеспечения объектов кибербезопасности как основной информационной инфраструктуры?
15. Что такое важная информационная инфраструктура, каковы ее объекты и субъекты?

II БЛОК. Вопросы мотивации при выборе направления образования бакалавриата (понимание сути и социальной значимости профессии, постоянный интерес к ней)

1. Объяснить причину выбора сферы информационной безопасности. Чем привлекла Вас данная сфера?

2. Ваша оценка плану мероприятий, разработанного на основе национальной программы в сфере информационной безопасности в нашей республике.

3. Что вы знаете о степени кибербезопасности в киберпространстве Республики Узбекистан?

4. Что вы думаете об уровне обеспечения информации и кибербезопасности в настоящее время? Приведите примеры.

5. Сейчас в Интернете и социальных сетях много сообщений о росте количества киберпреступлений, что вы думаете по этому поводу?

6. Что вы можете сказать о мотивах, которые движут киберпреступниками? В чем заключается цели повышения роста киберпреступлений?

7. Почему в наши дни растет число информационных и кибербезопасных сообщений, а также возрастают ролики в социальных сетях и на телевидении?

8. С ростом цифровизации растет и спрос на кибербезопасность. Что, по - вашему, является основной причиной этому?

9. Считаете ли вы, что в современном законодательстве в сфере кибербезопасности разработано достаточно законов, регулирующих эту сферу?

10. Целесообразно ли внедрение программного продукта зарубежного производства в целях обеспечения кибербезопасности от предприятий отрасли или национальное программное обеспечение? Объясните свой ответ.

11. В чем главная задача Закона Республики Узбекистан «О кибербезопасности»?

12. В чем заключается основная задача организаций, осуществляющих обеспечение кибербезопасности, и какие виды услуг они предоставляют?

13. Какие вы знаете государственные и частные предприятия и организации в сфере кибербезопасности, действующие в нашей республике?

14. Дать определения к понятиям кибербезопасности, кибератаки и киберзащиты?

15. Следует ли внедрять политику информационной безопасности в организациях? Какие преимущества дает политика информационной безопасности?

III БЛОК. Личностно-профессиональные особенности:

1. Каким обязанностям должен обладать специалист по информационной безопасности?

2. Ваши достижения в настоящее время. Какое из достигнутых достижений является главным?

3. Какими чертами характера должен обладать сотрудник службы информационной безопасности? Какими из этих качеств обладаете вы?

4. При возникновении той или иной проблемы вы опираетесь на собственное самостоятельное решение, или же для вас важно мнение других?

5. Какую цель вы преследуете при выборе направления информационной безопасности? В чем заключается важность вашего выбора?

6. В какой сфере информационной безопасности вы работали?

7. Что вы знаете об организациях, служащих в сфере информационной безопасности? Объясните, в чем заключается их обязанность?

8. Какие области знаний вы считаете важными для сотрудника, работающего в сфере информационной безопасности?

9. Кто посоветовал вам получить образование в области информационной безопасности? Работают ли они в этой сфере или вы сами интересовались ею самостоятельно?

10. Каковы ваши планы после окончания университета?

11. Делаете ли вы в настоящее время что-то практическое для изучения области информационной безопасности? Учитесь программировать или изучаете иностранный язык?

12. Какие предметы в области информационной безопасности вы изучали в техникуме, где учились?

13. Были ли вы жертвой киберпреступности или кто-то из ваших знакомых пострадал от такого рода преступлений?

14. Можете ли вы объяснить актуальность развития сферы информационной безопасности последними событиями?

15. Какие знания и навыки, по вашему мнению, должны иметь абитуриенты, продолжающие обучение в вузе?

16. Если вас не примут в качестве студента, каковы ваши дальнейшие планы?

17. В наше время знание иностранного языка очень важно, особенно в сфере IT, как вы думаете, в чем причина этому?

IV БЛОК. По специальности «Информационная безопасность»:

1. Объясните понятие информационной безопасности?
2. Каковы основные задачи информационной безопасности?
3. Важность использования информации?
4. Что вы подразумеваете под целостностью информации?
5. Что вы подразумеваете под управлением риска в информационной безопасности?
6. Каковы основные направления защиты информации?
7. Что такое системное мышление и зачем оно нужно?
8. В чем разница между понятиями информационная безопасность и защита информации?
9. Каковы знания в области кибербезопасности и их основные аспекты?
10. Объясните человеческий фактор в кибербезопасности на примерах.
11. Объяснить понятия угрозы и уязвимости.
12. Что такое личная информация? Как их следует защищать?
13. Дать понятия основным выражениям криптографии: шифрование, дешифрование, ключ, шифр, открытый текст, зашифрованный текст, алфавит.
14. Безопасность электронной коммерции?
15. Объясните разницу между кодированием и шифрованием?
16. В чем разница между криптографией и стеганографией?
17. Обсудите, что такое симметричная криптография и ее роль в информационной безопасности.
18. Дать понятия открытой криптографии с ключом и её роль в информационной безопасности.
19. Что такое хеш-функция, ее требования и роль в информационной безопасности?
20. Дать понятия выражениям: интернет-банкинг, мобильный банкинг.
21. Криптографическое отражение: его замена и своп.
22. В чем разница между шифрованием диска и шифрованием файлов?
23. Объясните DOS-атаку на веб-сайтах.
24. Как уничтожить бумажные данные и их значимость?
25. Расскажите о способах обеспечения целостности данных.
26. Объясните основные понятия контроля разрешений: идентификация, аутентификация и авторизация.
27. Каковы различия и сходства между цифровыми подписями и кодами аутентификации сообщений?
28. Что такое идентификация?
29. Объяснить роль электронной цифровой подписи в обеспечении информационной безопасности.
30. Что такое аутентификация? Приведите примеры однофакторной и многофакторной аутентификации.
31. Объясните концепции матрицы контроля использования, ACL и C-списка?
32. Способы уничтожения электронных данных и их значимости. Способы уничтожения электронных данных и их особенности.

33. Объяснить метод закодированной аутентификации и его преимущества/недостатки.
34. Что вы подразумеваете под логическим управлением использования?
35. Объяснить физическую защиту информации и ее важность?
36. Объясните понятия угрозы, уязвимости и нападения?
37. Назовите основные функции сетевых устройств: сетевая карта, репитер, концентратор, коммутатор, маршрутизатор, мосты, шлюзы.
38. Назовите основные сетевые протоколы и их функции.
39. Сетевые вирусы и проблемы антивирусной защиты.
40. Каковы основные цели атак с использованием вредоносных программ и приведите примеры.
41. Перечислите, что такое резервное копирование и его виды.
42. Перечислите основные причины потери данных.
43. Перечислите, что такое вредоносное ПО и его основные виды.
44. Что такое компьютерные вирусы и приведите примеры.
45. Каковы предпосылки возникновения киберпреступности?
46. Объясните понятие кибернетики и приведите примеры?
47. Перечислите вредоносные программы и их классификацию.
48. Виды атак на сетевую безопасность и дать этим видам объяснение.
49. Что такое политика информационной безопасности и какова ее основная цель?
50. Какие статьи о киберпреступности есть в Уголовном кодексе Республики Узбекистан?