

O‘RTA MAXSUS VA PROFESSIONAL TA’LIM TASHKILOTLARI PEDAGOG KADRLARINI ATTESTATSIYADAN O‘TKAZISH UCHUN AXBOROT XAVFSIZLIGI FANIDAN MALAKA TEST SINOVI TOPSHIRIQLARI SPETSIFIKATSIYASI

I. Maqsad

Mazkur test varianti tafsilotining maqsadi kasbiy ta’lim fanlarini bilish darajasini baholashning malaka toifalarini berish test tizimi doirasida Axborot xavfsizligi fani talabgorlarining bilim darajasini aniqlash va sertifikatlash uchun qo‘llaniladigan test varianti formati (topshiriqlar soni, turi, vaqt me’yori), fan mazmuni tarkibi, kognitiv ko‘nikma darajalari, baholash mezonlari va talabgorlarning tayyorgarlik darajasiga qo‘yiladigan talablarni belgilashdan iborat.

II. Me’yoriy asoslar

1.O‘zbekiston Respublikasi Vazirlar Mahkamasining 2021-yil 17-sentyabrdagi **“Maktabgacha, umumiy o‘rta, o‘rta maxsus, professional va maktabdan tashqari ta’lim tashkilotlari pedagog kadrlarini attestatsiyadan o‘tkazish tartibini takomillashtirish chora-tadbirlari to‘g‘risida”**gi 572-sonli Qarori.

III. Baholash qamrovi: mazmun sohalari

Axborot xavfsizligi

1. Axborot xavfsizligi konsepsiyasi. Axborot xavfsizligi tushunchasi;
2. Identifikatsiya, autentifikatsiya va avtorizatsiya tushunchalari;
3. Kriptografiya tushunchasi. Stenografiya. Simmetrik va assimetrik shifrlash tizimlari;
4. Kompyuter viruslari va antiviruslar, Zararli dasturlar;
5. Tarmoq xavfsizligi. Tarmoqlararo Ekran texnologiyasi, IDS tizimi;
6. Elektron raqamli imzo (e-imzo), Maxsus shifrlash algoritmlari (RSA,DES, El-Gamal);

IV. Baholanadigan mazmun sohalar va konstuktlar

T/r	Mazmun sohalar	Konstruktlar	Ulushi (%)	Testlar soni
1	Axborot xavfsizligi konsepsiyasi. Axborot xavfsizligi tushunchasi	Axborot xavfsizligi konsepsiyasi va axborot xavfsizligi tushunchasi bo'limida axborot tizimlarini himoya qilish jarayonlarini samarali tashkil etish maqsadida axborot xavfsizligi asosiy tushunchalari, prinsip va kontsepsiyalarini o'rganish, ma'lumotlarni himoya qilishning zamonaviy usullari va texnologiyalarini o'zlashtirish, axborot resurslarining xavfsizligini ta'minlash, tizimlarda xavfsizlik siyosati va normativ talablarni hisobga olgan holda amaliy ko'nikmalarni rivojlantirish, innovatsion IT-metod va dasturiy vositalardan foydalanish kompetensiyalarini shakllantirish, axborot tizimlarining barqaror, samarali va xavfsiz ishlashini ta'minlash uchun zarur nazariy bilim va amaliy ko'nikmalarga ega bo'ladi.	12.5 %	5 ta
2	Identifikatsiya, autentifikatsiya va avtorizatsiya tushunchalari	Identifikatsiya, autentifikatsiya va avtorizatsiya tushunchalari bo'limida axborot tizimlarida foydalanuvchilarni aniqlash va kirish huquqlarini boshqarish jarayonlarini samarali tashkil etish maqsadida identifikatsiya, autentifikatsiya va avtorizatsiya tushunchalari, usullari va texnologiyalarini o'rganish, foydalanuvchilarni tizimga kiritish va ularga ruxsat berish jarayonlarini boshqarish, axborot xavfsizligi talablarini hisobga olgan holda amaliy ko'nikmalarni rivojlantirish, innovatsion IT-metod va dasturiy vositalardan foydalanish kompetensiyalarini shakllantirish, axborot tizimlarining barqaror, ishonchli va xavfsiz ishlashini ta'minlash uchun zarur nazariy bilim va amaliy ko'nikmalarga ega bo'ladi.	12.5 %	5 ta
3	Kriptografiya tushunchasi. Stenografiya. Simmetrik va assimetrik shifrlashtizim lari	Kriptografiya tushunchasi, stenografiya, simmetrik va assimetrik shifrlashtizimlar bo'limida axborot xavfsizligini ta'minlash jarayonlarini samarali tashkil etish maqsadida kriptografiya asoslari, stenografiya va ma'lumotlarni yashirish usullarini o'rganish, simmetrik va assimetrik shifrlash tizimlarining ishlash prinsiplari va amaliy qo'llanilishini o'zlashtirish, ma'lumotlarni himoya qilish va	32.5 %	13 ta

		uzatish jarayonlarini xavfsiz tashkil etish, axborot tizimlarida kriptovositlardan foydalanish bo'yicha amaliy ko'nikmalarni rivojlantirish, innovatsion IT-metod va dasturiy vositalardan foydalanish kompetensiyalarini shakllantirish, axborot tizimlarining barqaror, ishonchli va xavfsiz ishlashini ta'minlash uchun zarur nazariy bilim va amaliy ko'nikmalarga ega bo'ladi.		
4	Kompyuter viruslari va antiviruslar, Zararli dasturlar	Kompyuter viruslari va antiviruslar, zararli dasturlar bo'limida axborot tizimlarini himoya qilish jarayonlarini samarali tashkil etish maqsadida turli kompyuter viruslari, zararli dasturlar (malware, trojan, ransomware va boshqalar) xususiyatlari va tarqalish usullarini o'rganish, tizimni viruslardan va zararli dasturlardan himoya qilish usullari, antivirus dasturlarining ishlash prinsiplari va konfiguratsiyasini o'zlashtirish, xavfsizlik siyosati va normativ talablarni hisobga olgan holda amaliy ko'nikmalarni rivojlantirish, innovatsion IT-metod va dasturiy vositalardan foydalanish kompetensiyalarini shakllantirish, axborot tizimlarining barqaror, ishonchli va xavfsiz ishlashini ta'minlash uchun zarur nazariy bilim va amaliy ko'nikmalarga ega bo'ladi.	15 %	6 ta
5	Tarmoq xavfsizligi. Tarmoqlararo Ekran texnologiyasi, IDS tizimi	Tarmoq xavfsizligi, tarmoqlararo ekran texnologiyasi, IDS tizimi bo'limida axborot tizimlari va tarmoqlarni himoya qilish jarayonlarini samarali tashkil etish maqsadida tarmoq xavfsizligi asoslari, tarmoqlararo ekran (firewall) texnologiyalari va ularning ishlash prinsiplari, shuningdek IDS (Intrusion Detection System) tizimlari va ularni tarmoqda qo'llash usullarini o'rganish, tarmoq trafikini monitoring qilish va tahdidlarni aniqlash amaliyotini o'zlashtirish, xavfsizlik siyosati va normativ talablarni hisobga olgan holda amaliy ko'nikmalarni rivojlantirish, innovatsion IT-metod va dasturiy vositalardan foydalanish kompetensiyalarini shakllantirish, tarmoq tizimlarining barqaror, samarali va xavfsiz ishlashini ta'minlash uchun zarur nazariy bilim va amaliy ko'nikmalarga ega bo'ladi.	17.5 %	7 ta

6	Elektron raqamli imzo (e-imzo), Maxsus shifrlash algoritmlari (RSA,DES, El-Gamal)	Elektron raqamli imzo (e-imzo) va maxsus shifrlash algoritmlari (RSA, DES, El-Gamal) bo'limida axborot tizimlarida ma'lumotlarni himoya qilish jarayonlarini samarali tashkil etish maqsadida elektron raqamli imzo (e-imzo) tushunchasi, ishlash prinsiplari va qo'llanilishini o'rganish, RSA, DES, El-Gamal kabi simmetrik va assimetrik shifrlash algoritmlarining xususiyatlari, ishlash texnologiyasi va amaliy qo'llanilishini o'zlashtirish, ma'lumotlarni uzatish va saqlash jarayonlarida xavfsizlikni ta'minlash, axborot tizimlarida kriptovositalardan foydalanish bo'yicha amaliy ko'nikmalarni rivojlantirish, innovatsion dasturiy va texnologik yechimlardan foydalanish kompetensiyalarini shakllantirish, axborot tizimlarining barqaror, ishonchli va xavfsiz ishlashini ta'minlash uchun zarur nazariy bilim va amaliy ko'nikmalarga ega bo'ladi.	10 %	4 ta
---	---	--	------	------

V. Baholanadigan kognitiv ko'nikmalar va taqsimoti

T/r	Kognitiv daraja	Izohi	Ulushi (%)
1.	Bilish	Fanga doir nazariy ma'lumotni, atama va qoidalarni eslab qolish, tushunish, nazariy jihatdan tahlil qila olish	17.5 %
2.	Qo'llash	O'zlashtirgan nazariy bilim va tushunchalarni yangi kontekstlarda (ta'limiy, muammoli vaziyat va pedagogik-psixologik holatlarda) ishlata olish	52.5 %
3.	Mulohaza qilish	Muayyan faktlar, dalillar va normalarni mantiqiy bog'liq tarzda tahlil qilib, jarayonlarning ketma-ketligini farqlab, vaziyatni analiz qilib, xulosalar chiqara olish	30 %

VI. Test turlari va taqsimoti

T/r	Test turi	Izohi
1.	Y1	To'rtta variantdan bittasi to'g'ri bo'lgan muqobil javobli yopiq test
2.	Y2	Tartiblangan bir nechta javoblardan to'g'rilarni topishni talab qiladigan muqobil javobli yopiq test
3.	Y3	Moslashtirishni talab qiladigan yopiq test
4.	Y4	Gap yoki jarayonlarni to'g'ri ketma-ketlikda joylashtirish talab etiladigan yopiq test

VII. Baholash mezonlari va ajratilgan vaqt

Test topshiriqlari umumiy 80 ball bilan baholanadi.

Har bir to'g'ri javob 2 ball, noto'g'ri javob esa 0 ball bilan baholanadi.

VIII. Imtihon tartibi

Taqiqlangan vositalar: imtihon vaqtida mobil telefon, aqlli soat, planshet yoki elektron eslatmalardan foydalanish qat'iyan man etiladi.

Axloq va intizom: nusxa ko'chirish, yordam so'rash yoki yordam berish, imtihon davomida gaplashish, ruxsatsiz chiqish kabi holatlar taqiqlanadi.

Nazoratchi qoidabuzarlikni aniqlaganda, uni rasmiylashtirib, tinglovchini testdan chetlashtiradi va natijasi bekor qilinadi.

IX. Inklyuziya va moslashtirish

Alohida ta'limga ehtiyoji bor talabgorlar uchun qo'shimcha 15 % vaqt beriladi. Shuningdek, topshiriqlarning berilish shakli va turi ham ularga mos va qulay shaklda taqdim etiladi.

Ko'rish sohasida imkoniyati cheklangan talabgorlar savollarni o'qib berishi uchun maxsus texnik yordamchi bilan kelishiga ruxsat etiladi, faqat savolning to'g'ri javobini aytishi mumkin emas.

X. Tavsiya etilgan adabiyotlar

1. Sh.B.Sayfullayev. Axborot xavfsizligi. Toshkent 2021
2. Informatika va axborot texnologiyalari. 10-11-sinf. P.Long, S.Lawrey, V.Ellis. "Cambridge University Press". 2023
3. E.Sh. Nazirova. A.Nematov, Sh.B. Abidova. Web dasturlash va dizayn. O'quv qo'llanma Zamin Nashri 2021 yil.
4. B.N.Shomirzayev. Internet ilovalarini ishlab chiqish. Toshkent "Turon nashriyoti" 2023 yil.
5. S.Sh.Yo'ldoshev. Sh.I. Razzoqov Dasturlash. Toshkent "Zamin nashriyoti" 2021 yil.
6. Axborot texnologiyalari asoslari. Mirzayev A.E. Xalilov S.p, Naim N.A. Toshkent -2021
7. Informatika va axborot texnologiyalari. 9-sinf. M.Fayziyeva. "Nashriyot uyi tasvir". 2020
8. Informatika va axborot texnologiyalari. 10-sinf. F.Fayziyeva, D.Sayfurov va b. "Respublika ta'lim markazi". 2021
9. Informatika va axborot texnologiyalari. 11-sinf. N.Xaytullayeva, F.Fayziyeva va b. "Respublika ta'lim markazi". 2021.

10. Mamajonov R,Y. Qosimov F,Sh, Haydarova M.Y "Operatsion tizimlar" o'quv qo'llanma
11. Shaxsiy kompyuter va ofis qurilmalariga texnik xizmat ko'rsatish Yaxshiboyev R.E, Siddiqov B.N Toshkent : "Tafakkur avlodi" 2022 yil
12. Kompyuter tizimlari va tarmoqlari A.A.Kaxxarov, Yu.Sh Avazov Toshkent 2022.
13. Gaipnazarov T.S, Irgasheva D.Y Ma'lumotlar ombori. Toshkent-2014,
14. G.Rahimova; G. Jo'raqulova. Ma'lumotlar bazisini boshqarish tizimlari. Toshkent -2024 yil.
15. A.Boqiyev, Ma'lumotlar bazasi, Toshkent-2001
16. Kompyuter tarmoqlarini administratorlash X.Djumanov. K.T.Abdurashidova. S.Botirov Zamin Nashr -2021