

TOSHKENT KIMYO XALQARO UNIVERSITETINING AXBOROT XAVFSIZLIGI KONSEPSIYASI

I. Umumiy qoidalar

1. Ushbu Toshkent Kimyo xalqaro universitetining (keyingi o‘rinlarda — TKXU) axborot xavfsizligi konsepsiyasi TKXU axborot tizimida axborotni shakllantirish, qayta ishlash, uzatish va saqlash jarayonida axborot xavfsizligini ta’minlash strategiyasini belgilaydi.
2. TKXU axborot xavfsizligi konsepsiyasi (keyingi o‘rinlarda — Konsepsiya) axborotni himoya qilishning maqsadlari, vazifalari, tamoyillari va asosiy choralarini belgilovchi asosiy hujjat hisoblanadi.
3. Konsepsiyaning amal qilishi TKXU axborot tizimidan foydalanish huquqiga ega bo‘lgan barcha xodimlar va foydalanuvchilarga tatbiq etiladi.
4. Ushbu Konsepsiyada quyidagi atama va ta’riflar qo‘llaniladi:
 - **Avtorizatsiya** — foydalanuvchiga kirish huquqlarini berish;
 - **Autentifikatsiya** — foydalanuvchining haqiqiylikini tasdiqlash;
 - **Tashqi ma’lumot uzatish kanallari** — TKXU xodimlari nazoratida bo‘lmagan ma’lumot uzatish kanallari;
 - **Sirlar** — alohida ahamiyatga ega ma’lumotlar;
 - **Demilitarizatsiyalangan zona** — axborot tizimida ma’lumotlarni bir kirish darajasidan boshqasiga uzatish uchun yaratiladigan, zonada bajariladigan operatsiyalar xususiyatiga qarab axborot xavfsizligiga nisbatan o‘ziga xos talablarga ega bo‘lgan maxsus zona (VLAN);
 - **hujjatlashtirilgan axborot** — moddiy jismda qayd etilgan, uni identifikatsiya qilish imkonini beruvchi rekvizitlarga ega axborot;
 - **axborotni himoya qilish** — axborot xavfsizligiga tahdidlarning oldini olish va ularning oqibatlarini bartaraf etish choralari;
 - **axborot** — manbalari va taqdim etilish shaklidan qat’i nazar shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to‘g‘risidagi ma’lumotlar;
 - **TKXU axborot tizimi** — TKXU texnik va dasturiy vositalarining ularning alohida va birgalikda ishlashiga qo‘yiladigan talablarni hisobga olgan holdagi majmui;
 - **maxfiy axborot** — foydalanish cheklangan hujjatlashtirilgan axborot;

- **axborotdan ruxsatsiz foydalanish** — kirishni cheklashning belgilangan qoidalarini buzgan holda axborotdan foydalanish;
- **axborot tizimiga xizmat ko'rsatuvchi xodimlar** — axborot tizimini kuzatib borish (qo'llab-quvvatlash) uchun mas'ul xodimlar majmui;
- **axborot tizimi foydalanuvchisi** — ish joyidan qat'i nazar axborot tizimiga ulanuvchi, unda axborotni qabul qiluvchi yoki uzatuvchi shaxs;
- **axborot xavfsizligiga tahdid** — axborot tizimi foydalanuvchilari yoki egalariga bevosita yoki bilvosita zarar yetkazishi mumkin bo'lgan, axborot tizimiga qasddan yoki qasddan bo'lmagan ta'sir ko'rsatishning potentsial imkoniyati;
- **tarmoqni jismoniy ajratish** — ma'lumot uzatish tarmog'ini apparat vositalari bilan o'zaro bog'lanmagan bir nechta mustaqil tarmoqlarga ajratish;

II. Konsepsiyaning maqsadi va vazifalari

5. Konsepsiyaning asosiy maqsadi TKXU axborot tizimining axborot xavfsizligini ta'minlash sohasida umumiy strategiyani shakllantirishdan iborat.
6. Konsepsiyaning asosiy vazifalari quyidagilardan iborat:
 - axborot xavfsizligini ta'minlash tizimini qurishning asosiy tamoyillarini shakllantirish;
 - axborot xavfsizligini ta'minlash tizimining faoliyat ko'rsatishiga qo'yiladigan asosiy talablarni shakllantirish;
 - axborot xavfsizligini ta'minlash tizimini joriy etishning tashkiliy-uslubiy bazasini shakllantirish;
 - axborot xavfsizligini ta'minlash tizimini rivojlantirish imkonini beruvchi ustuvor yo'nalishlarni belgilash.

III. Konsepsiyaning asosiy tamoyillari

7. Konsepsiya quyidagi tamoyillarga asoslanadi:
 - g'ayriqonuniy muomalada bo'lishi TKXUga zarar yetkazishi mumkin bo'lgan har qanday axborotni himoya qilish;
 - axborot xavfsizligini ta'minlash tizimining O'zbekiston Respublikasi qonunchiligi talablariga muvofiqligi;
 - TKXUning amaldagi tashkiliy tuzilmasi va axborot xavfsizligini ta'minlash choralari joriy etish ustuvorligini hisobga olgan holda axborot xavfsizligini ta'minlash tizimini bosqichma-bosqich rivojlantirish;
 - TKXU axborot tizimi xodimlari va foydalanuvchilarining axborot xavfsizligi sohasida yetarli darajada xabardorligi va o'qitilishini ta'minlash;

- axborot xavfsizligini ta'minlash tadbirlarini moliyalashtirishning samarali tizimini yaratish.

IV. Konsepsiyani shakllantirishning huquqiy asoslari

8. Konsepsiyaga muvofiq ishlab chiqilgan normativ hujjatlar qonunchilik talablariga, shuningdek TKXUning axborot xavfsizligi bo'yicha hujjatlariga muvofiq bo'lishi kerak.
9. Umuman olganda, TKXU axborot xavfsizligi tizimlarini tashkil etishda TKXU tomonidan qabul qilingan axborot texnologiyalari va axborot xavfsizligi sohasidagi standartlar qo'llaniladi.
10. TKXU tegishli xodimlarning qonunchilik hujjatlari, shuningdek axborot texnologiyalari va axborot xavfsizligi sohasidagi standartlar bilan tanishib chiqishini ta'minlaydi.

V. Himoya obyektlari va xavflarni baholash

11. TKXU axborot tizimi himoya qilinishi lozim bo'lgan axborot birgalikda foydalaniladigan yagona axborot-telekommunikatsiya tarmog'iga birlashtirilgan taqsimlangan tizimdir.
12. TKXU axborot tizimining faoliyat ko'rsatishini ta'minlash va uni kuzatib borish Raqamli texnologiyalar markazi (keyingi o'rinlarda — RTM) tomonidan amalga oshiriladi.
13. TKXU axborot tizimida aylanib yuruvchi axborot quyidagi darajalarga bo'linadi:
 - TKXU axborot tizimidagi foydalanish cheklangan axborot;
 - TKXU axborot tizimidagi ommaviy axborot.
14. Maxfiy axborotga quyidagilar kiradi:
 - xodimlarning shaxsga doir ma'lumotlari;
 - xizmat axboroti;
 - buyruqlar bilan cheklangan axborot.
15. Ichki ommaviy axborotga xodimlar tomonidan o'z lavozim majburiyatlarini bajarish doirasida TKXU axborot tizimida shakllantiriladigan va foydalaniladigan axborot kiradi, foydalanish cheklangan ichki axborotga taalluqli axborot bundan mustasno.
16. TKXU axborot tizimida axborot xavfsizligiga asosiy tahdidlar quyidagi ko'rinishlarda namoyon bo'ladi:
 - axborotni ruxsatsiz oshkor qilish, uning sizib chiqishi, o'g'irlanishi;

- axborotni ruxsatsiz bloklash yoki yo‘q qilish, texnologik jarayonlarni buzish, axborot tizimi ishini izdan chiqarish, axborot tizimining axborot va dasturiy vositalarini buzish;
- axborotni buzib ko‘rsatish, almashtirish, soxtalashtirish;
- tizimdagi nosozliklar.

17. Kelib chiqish xususiyatiga ko‘ra axborot xavfsizligiga tahdidlar quyidagi guruhlariga bo‘linadi:

a) sun‘iy tahdidlar, ular o‘z navbatida quyidagilarga bo‘linadi:

- **qasddan bo‘lmagan tahdidlar:** axborotni yig‘ish, qayta ishlash va uzatishning belgilangan reglamentlarini, shuningdek axborot xavfsizligi talablarini xato, tasodifiy, o‘ylamasdan, g‘arazli niyat va manfaatdorlik maqsadisiz buzish hamda vaqt va resurslarning samarasiz sarflanishiga, foydalanish cheklangan axborotning oshkor bo‘lishiga, qimmatli axborotning yo‘qolishiga yoki alohida ishchi stansiyalar, quyi tizimlar yoki butun axborot tizimi ish qobiliyatining buzilishiga olib keluvchi shaxslarning boshqa harakatlari;
- **qasddan qilingan tahdidlar:** g‘arazli maqsadlarda, uchinchi shaxslarning majburlashi bilan, yomon niyatda sodir etilgan buzilishlar va axborotni yig‘ish, qayta ishlash va uzatishning belgilangan reglamentlarini, shuningdek axborot xavfsizligi talablarini boshqacha buzish hamda vaqt va resurslarning samarasiz sarflanishiga, foydalanish cheklangan axborotning oshkor bo‘lishiga, qimmatli axborotning yo‘qolishiga yoki alohida ishchi stansiyalar, quyi tizimlar yoki butun axborot tizimi ish qobiliyatining buzilishiga olib keluvchi shaxslarning boshqa harakatlari;

b) tabiiy tahdidlar:

- tabiiy ofatlar, tabiiy kataklizmlar va boshqalar natijasida yuzaga kelgan dasturiy-texnik vositalarning ishdan chiqishi, avariylari va nosozliklari.

18. Foydalanish cheklangan ichki axborotni o‘z ichiga olgan apparat-dasturiy komplekslardan foydalanishga faqat axborotni himoya qilish bo‘yicha zarur choralar ko‘rilganidan keyin ruxsat beriladi. Himoya qilish tartib-taomillari va muhandislik-texnik choralari quyidagilarga yo‘naltirilgan bo‘lishi kerak:

- tahdidning oldini olish yoki axborot xavfsizligiga tahdid ta‘sirini lokallashtirish;
- zarur hollarda axborot tizimining ish qobiliyatini tiklash.

19. Har bir axborot, shuningdek foydalanish cheklangan ichki axborotning har bir turi uchun foydalanish mumkin bo‘lish muddatlari belgilanishi kerak.

20. Axborotni bir kirish darajasidan boshqa darajaga o‘tkazish uchun tegishli tartib-taomillar va demilitarizatsiyalangan zonalar yaratilishi kerak.

VI. Axborot xavfsizligiga tahdidlarga qarshi kurashish yo'llari

21. Axborot xavfsizligining talab etiladigan darajasini ta'minlashga qaratilgan asosiy choralar quyidagilarga bo'linadi:
 - jismoniy himoya choralari;
 - tashkiliy himoya choralari;
 - muhandislik-texnik himoya choralari.
22. Jismoniy himoya choralari potensial buzg'unchilarning axborot tizimi komponentlari va himoya qilinadigan axborotga kirib borishi mumkin bo'lgan yo'llarda jismoniy to'siqlar yaratish uchun maxsus mo'ljallangan turli mexanik, elektron, elektron-mexanik qurilmalar va inshootlarni, shuningdek vizual kuzatuv va qo'riqlash signalizatsiyasining texnik vositalarini qo'llashga asoslanadi.
23. TKXU axborot tizimining asosiy komponentlari joylashgan binolar va xonalarni jismoniy himoya qilish qo'riqlash xizmati kuchlari tomonidan amalga oshiriladi.
24. Xonalarni jismoniy himoya qilish choralari quyidagilarni ta'minlashi kerak:
 - himoya qilinadigan obyektga begona shaxslarning kirib kelishining oldini olish;
 - axborot tizimining asosiy komponentlari joylashgan himoya qilinadigan obyekttni kecha-kunduz kuzatib borish;
 - himoya qilinadigan obyektlarga tashrif buyuruvchi har bir shaxsni identifikatsiya qilish, tashriflar to'g'risidagi ma'lumotlarni o'z ichiga olgan jurnal yuritish;
 - favqulodda holatlarda himoya qilinadigan obyektga kirib borish va unga kirishning barcha mumkin bo'lgan yo'llarini to'sish.
25. Tashkiliy (ma'muriy) himoya choralari axborot xavfsizligiga tahdidlarni amalga oshirish imkoniyatini iloji boricha qiyinlashtiradigan yoki istisno etadigan yoxud ular amalga oshirilgan taqdirda yo'qotishlar hajmini kamaytiradigan tarzda ma'lumotlarni qayta ishlash tizimining faoliyat ko'rsatish jarayonini, axborotdan foydalanishni, xizmat ko'rsatuvchi xodimlarning faoliyatini, shuningdek foydalanuvchilarning axborot tizimi bilan o'zaro hamkorligini tartibga soladi.
26. Yuqori boshqaruv darajasida ko'riladigan tashkiliy choralarning asosiy maqsadi axborot xavfsizligi sohasida qarorlar qabul qilish va hujjatlar ishlab chiqishdan iborat bo'lib, ular jumladan quyidagilarni nazarda tutadi:
 - zarur inson va moliyaviy resurslarni ajratish;
 - axborot xavfsizligi holatini muntazam tekshirib borish;
 - TKXU axborot xavfsizligini ta'minlashga qaratilgan tadbirlarni amalga oshirish.

27. TKXU quyidagilarning tartibini belgilovchi yo'riqnomalar, nizomlar va boshqa normativ hujjatlarni ishlab chiqadi:

- foydalanish cheklangan ichki axborotga kirish huquqini berish;
- apparat-dasturiy vositalarga xizmat ko'rsatish, ularni modifikatsiya qilish, tegishli kirish toifasiga mos apparat vositalarini ta'mirlash;
- axborot tizimida ma'lumotlar bazalarini yuritish;
- foydalanuvchilar tomonidan axborot tizimidan foydalanish;
- ichki ommaviy axborotga kirish huquqini berish;
- xizmat ko'rsatuvchi xodimlar tomonidan axborot tizimini kuzatib borish;
- favqulodda holatlarda choralar ko'rish;
- TKXU xodimlari va boshqa shaxslarga axborot tizimidan foydalanish huquqini berish tasdiqlangan tartibga muvofiq amalga oshirilishi kerak;

28. Axborot tizimining har bir foydalanuvchisi vakolatlari darajasi quyidagi talablarga rioya qilgan holda alohida belgilanadi:

- foydalanuvchilarga faqat ularning xizmat vazifalariga kiradigan axborotga kirish huquqini berish;
- foydalanuvchilarga axborot tizimiga kirish huquqini berish jarayonida «aniq ruxsat etilmagan vakolat va huquqlar taqiqlangan hisoblanadi» tamoyiliga rioya qilinadi;
- axborot tizimini ma'muriyatlash va kuzatib borish operatsion tizim va ma'lumotlar bazasini boshqarish tizimi ma'murlari, ilova ma'murlari, lokal hisoblash tarmog'i ma'murlari hamda axborot xavfsizligi ma'murlari o'rtasida majburiyatlar, huquqlar va vakolatlarni taqsimlagan holda amalga oshirilishi kerak;
- axborot tizimida ishlashga ruxsat etilgan barcha xodimlar va xizmat ko'rsatuvchi xodimlar ma'lumotlarni avtomatlashtirilgan qayta ishlashning belgilangan tartibini, o'z ixtiyoridagi axborot va apparat-dasturiy vositalarni saqlash, ulardan foydalanish va ularni uzatish qoidalarini buzganlik uchun shaxsan javobgar bo'ladilar;
- Har bir xodim ishga qabul qilinayotganda TKXU axborot tizimida himoya qilinadigan axborot bilan ishlashning belgilangan qoidalariga rioya qilish va ularni buzganlik uchun javobgarlik to'g'risidagi Kelishuv-majburiyatni imzolashi kerak;

29. TKXU axborot tizimida ma'lumotlar bazasini yuritish bo'yicha barcha operatsiyalar, ma'lumotlar bazasidagi har qanday o'zgarishlar, ma'lumotlar bazasi foydalanuvchilari (shu jumladan xizmat ko'rsatuvchi xodimlar) tarkibi va vakolatlarining o'zgarishi tasdiqlangan tartibga muvofiq amalga oshirilishi kerak.

30. Ma'lumotlar bazalaridagi axborotning saqlanishi tasdiqlangan texnologik yo'riqnomalarga muvofiq elektron arxivni har kuni yuritishni tashkil etish orqali ta'minlanadi. Bunda quyidagi talablarga rioya qilish zarur:

- ma'lumotlar bazasini arxivlash dasturiy kompleks va yordamchi boshqaruv vositalarini hisobga olgan holda to'liq hajmda amalga oshiriladi;
- elektron arxivlarni energiyaga bog'liq bo'lmagan tashqi axborot tashuvchilarda saqlashni tashkil etish;
- elektron arxivlarning tiklash uchun yaroqliligini aniqlash maqsadida ularni rejali yoki rejadan tashqari tekshirishni tashkil etish;
- asosiy ma'lumotlarni qayta ishlash markazidan uzoqda joylashgan, faol ma'lumotlarni qayta ishlash tizimlarini to'liq yoki qisman takrorlovchi zaxira ma'lumotlarni qayta ishlash tizimini tashkil etish.

31. TKXU axborot tizimida apparat-dasturiy vositalarga xizmat ko'rsatish va ularni modifikatsiya qilishning barcha jarayonlari, shuningdek yangi apparat-dasturiy vositalar, quyi tizimlarni foydalanishga topshirish hamda texnik va dasturiy vositalar, quyi tizimlar konfiguratsiyasidagi barcha o'zgarishlar faqat tasdiqlangan tartib asosida amalga oshirilishi kerak.

32. TKXUning barcha apparat va dasturiy vositalari belgilangan tartibda kirish darajasi bo'yicha toifalarga ajratilishi kerak (tegishli apparat-dasturiy vositalar yordamida saqlanadigan va qayta ishlanadigan axborot uchun talab etiladigan kirish darajasi belgilanishi va u tegishli apparat va dasturiy vositalarga berilishi kerak).

33. Apparat-dasturiy vositalarning konfiguratsiyasi foydalanuvchilar zimmasiga yuklatilgan majburiyatlarga hamda axborotning xususiyati va kirish darajasidan kelib chiqqan holda axborot xavfsizligi talablariga mos kelishi kerak.

34. Xodimning majburiyatlariga kirmaydigan axborot (dasturiy vositalar, o'yinlar, filmlar, kliplar va boshqalar) TKXU axborot tizimiga ulangan apparat-dasturiy vositalarda saqlanmasligi, aniqlangan taqdirda esa darhol o'chirilishi kerak.

35. Muhandislik-texnik himoya choralari TKXU axborot tizimi tarkibiga kiruvchi, axborotni himoya qilish funksiyalarini (mustaqil ravishda yoki boshqa vositalar bilan birgalikda) bajaruvchi turli elektron qurilmalar va maxsus dasturlardan foydalanishga asoslanishi kerak.

36. Axborot xavfsizligining amaldagi talablari va tartib-taomillariga rioya qilingan taqdirda axborotni himoya qilishning muhandislik-texnik choralari quyidagilarni ta'minlashi kerak:

- TKXU axborot tizimida aylanib yuruvchi axborotning mavjudligi, yaxlitligi va maxfiyligini;

- axborot tizimiga kirishni nazorat qilish va barcha hodisalarni qayd etishni; axborot tizimi resurslaridan oqilona foydalanishni;
- axborot xavfsizligini ta'minlash tizimining yaxlitligi va ish qobiliyatini;
- axborot xavfsizligiga tahdidlarni aniqlash va ularning oldini olishni;
- ma'lumotlarni zaxiralash va tiklashni.

37. Muhandislik-texnik himoya choralari o'z ichiga quyidagilarni olishi kerak:

- foydalanuvchilar (shu jumladan ma'murlar) va axborot tizimi elementlarini (ishchi stansiyalar, terminallar, ma'lumotlar bazasi elementlari va boshqalar) identifikatsiya va autentifikatsiya qilish vositalari, axborot tizimiga kirishni cheklash va nazorat qilish vositalari;
- axborot tizimining uzluksiz ishlashini ta'minlovchi vositalar;
- axborotni arxivlash va saqlash vositalari;
- axborotni himoya qilishning antivirus vositalari;
- axborotni himoya qilishning boshqa zamonaviy dasturiy va apparat vositalari.

38. Foydalanuvchilarni autentifikatsiya qilish axborotning xususiyati va kirish toifasiga qarab parollardan foydalanish asosida amalga oshirilishi kerak.

39. Axborot tizimiga kirishni cheklash vositalari foydalanuvchini axborot tizimi tomonidan tanib olinganidan keyin uni avtorizatsiya qilishi kerak.

40. Foydalanuvchini avtorizatsiya qilish kirishni cheklashni amalga oshirishning quyidagi mexanizmlaridan foydalangan holda amalga oshirilishi kerak:

- atribut sxemalari, ruxsatlar ro'yxatlari va boshqalardan foydalanishga asoslangan tanlab kirishni boshqarish;
- axborotning maxfiylik belgilari va foydalanuvchilarning kirish darajalaridan foydalanishga asoslangan vakolatli kirishni boshqarish;
- ishonchli dasturiy ta'minotning yopiq muhitini ta'minlash;

41. Kirishni cheklashning texnik vositalari yagona kirishni nazorat qilish tizimining tarkibiy qismi bo'lishi kerak.

42. TKXU axborot tizimi uzluksiz ishlashni ta'minlovchi vositalarni (tizimning takrorlovchi elementlari, uzluksiz quvvat manbalari, elektr generatorlari va boshqalar) o'z ichiga olishi kerak.

43. Axborot tizimining uzluksiz ishlashini ta'minlovchi vositalarga qo'yiladigan asosiy talablar quyidagilardan iborat:

- axborot tizimining asosiy uzeli, elektr ta'minoti ishdan chiqqanda, o'chganda (yoqilganda) avtomatik ravishda javob qaytarish va belgilangan vaqt davomida axborot tizimining uzluksiz ishlashini ta'minlash;

44. Axborotni arxivlash va saqlash vositalari zarur hollarda axborotni tiklash yo'li bilan axborot tizimining ishonchli ishlashini ta'minlashi kerak.
45. TKXU axborot tizimida elektron arxiv yuritishni tashkil etishga qo'yiladigan asosiy talablar quyidagilardan iborat:
- elektron arxivlash va zaxira nusxalash ishlarini olib borish bo'yicha mas'ul xodimni tayinlash;
 - arxivlangan ma'lumotlarni ishonchli saqlash;
46. TKXU axborot tizimida axborotni antivirus himoyasini tashkil etishga qo'yiladigan asosiy talablar quyidagilardan iborat:
- litsenziyalangan antivirus dasturiy ta'minotidan foydalanish;
 - doimiy antivirus tekshiruvini tashkil etish;
 - axborot tizimining ma'muriy qismida (serverlar va boshqalar) ham, foydalanuvchi qismida (foydalanuvchilarning shaxsiy kompyuterlari) ham antivirus dasturiy ta'minotining antivirus bazalari (signaturalar ro'yxati) dolzarbligini avtomatik yoki qo'lda yangilash orqali ta'minlash;
 - antivirus tizimining ish qobiliyatini muntazam tekshirishni tashkil etish;
 - axborot tizimida kompyuter viruslari tarqalish manbasini aniqlashni tashkil etish;

VII. Konsepsiyani amalga oshirish

47. Konsepsiyani amalga oshirish uchun quyidagilar zarur:
- a) axborotning xususiyati va toifasiga qarab axborotni himoya qilishning ko'p qatlamli tizimini qo'llash:
- himoyaning birinchi qatlami — axborot tizimining apparat-dasturiy vositalariga kirishni jismoniy cheklash;
 - himoyaning ikkinchi qatlami — foydalanuvchini identifikatsiya va autentifikatsiya qilish;
- b) foydalanuvchilarga axborot xavfsizligi bo'yicha qonunchilik talablaridagi ularga bevosita taalluqli o'zgarishlarni yetkazish;
48. Axborot xavfsizligi bo'linmasi zimmasiga quyidagi funksiyalar yuklanadi:
- foydalanuvchilarning axborot tizimiga kirishini nazorat qilish, shu jumladan parollarni o'rnatish va davriy almashtirish;
 - axborot tizimi ma'lumotlar bazalarining zaxira nusxalari saqlanishini, axborot xavfsizligi tizimlari ma'lumotlar bazasini yaratish va saqlashni nazorat qilish;

IX. YAKUNLOVCHI QOIDALAR

49.Konsepsiya muntazam ravishda qayta ko‘rib chiqilishi va yangilanishi lozim.

50.O‘zgartirishlar TKXU rahbariyati tomonidan tasdiqlanadi.

Strategik rivojlanish va raqamlashtirish
bo‘yicha prorektor _____

U.A. Vosiqov

Raqamli texnologiyalar markazi
rahbari/direktori _____

I.G. Li