Axborot xavfsizligi sohasiga oid xalqaro va milliy me'yoriy-huquqiy baza

Zamonaviy raqamli dunyoda axborot xavfsizligini ta'minlash uchun xalqaro va milliy qonunchilik asoslari

1-bob: Axborot xavfsizligi nima va uning ahamiyati

Axborot xavfsizligi asoslari

Maxfiylik

Ma'lumotlarning ruxsatsiz kirish va oshkor qilinishdan himoyalanishi

Yaxlitlik

Axborotning to'g'riligi va to'liqligi saqlanishi

Mavjudlik

Kerakli vaqtda ma'lumotlarga kirish imkoniyati

Raqamli transformatsiya davrida shaxsiy, korporativ va davlat ma'lumotlarini himoya qilish har qachongidan ham muhimroq ahamiyat kasb etmoqda. Axborot xavfsizligi – bu texnologiya, qonunchilik va madaniyat uyg'unligini talab qiluvchi kompleks jarayon.

Xalqaro hamkorlikning roli

Global muammo

Kiberjinoyatlar va axborot tahdidlari davlat chegaralarini tan olmaydi. Bugungi kunda bir mamlakat resurslariga boshqa qit'adan hujum qilish mumkin.

- Transnatsional kiberjinoyatlar
- Ma'lumotlar oqimining xalqaro xarakteri
- Umumiy xavfsizlik standartlari zarurati

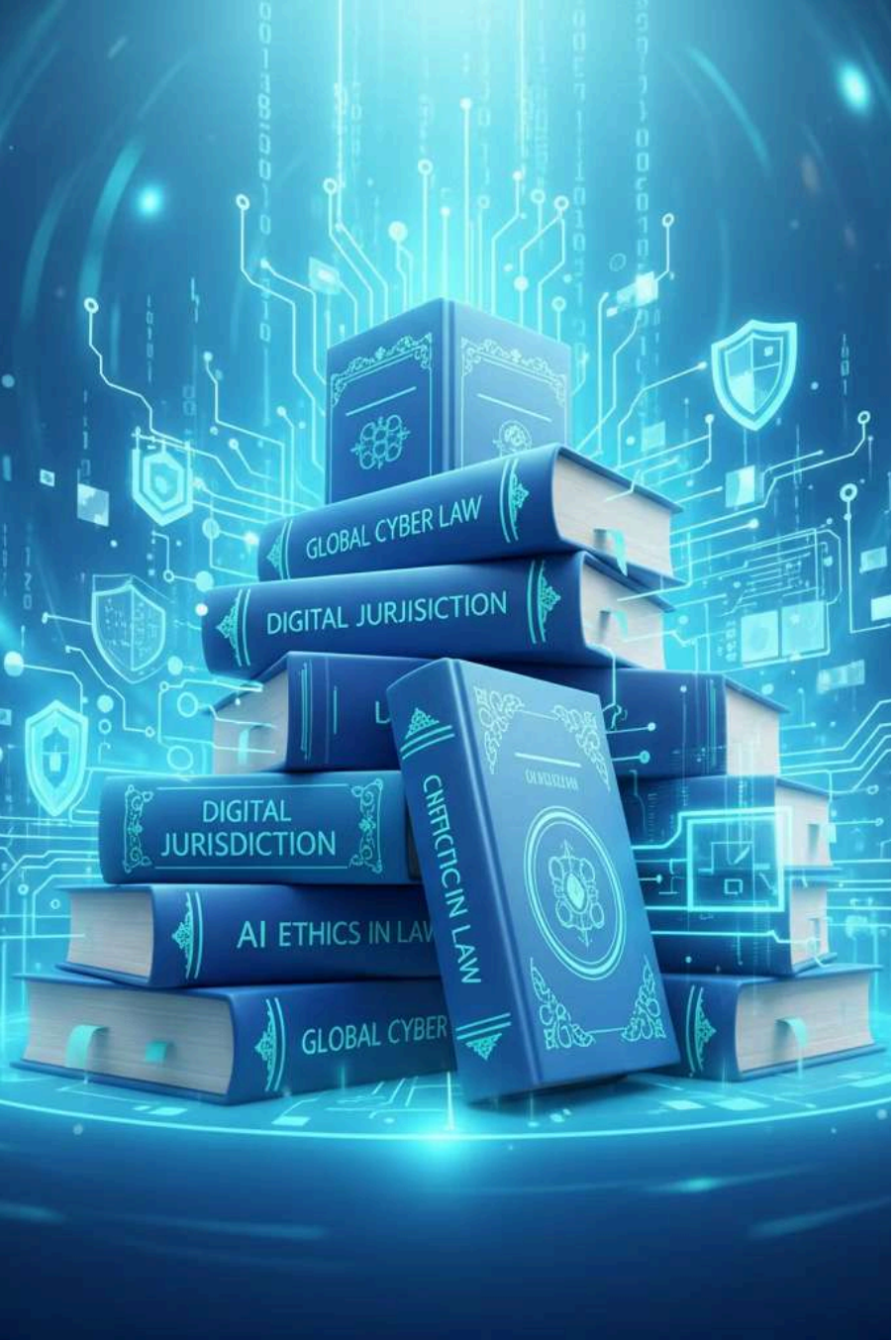
Hamkorlik mexanizmlari

Xalqaro tashkilotlar va ikki tomonlama shartnomalar orqali mamlakatlar o'rtasida axborot xavfsizligi bo'yicha hamkorlik amalga oshirilmoqda.

- BMT va OECD rezolyutsiyalari
- Regional xavfsizlik tashkilotlari
- Texnik standartlar va protokollar

Axborot xavfsizligi chegaralari yo'q

Zamonaviy kibertahdidlar global xarakterga ega bo'lib, xalqaro hamkorlik va yagona standartlarni talab qiladi



2-bob: Xalqaro me'yoriy-huquqiy hujjatlar

Kiberxavfsizlik va axborot himoyasida asosiy xalqaro hujjatlar

1

BMT rezolyutsiyalari

Birlashtirgan Millatlar Tashkiloti kiberxavfsizlik bo'yicha bir qancha muhim rezolyutsiyalarni qabul qilgan. Ular davlatlararo hamkorlik, axborot almashinuvi va milliy qonunchilikni uyg'unlashtirish bo'yicha asoslarni belgilaydi.

2

Budapesht konvensiyasi

2001-yilda qabul qilingan Kiberjinoyatchilikka qarshi konvensiya – bu sohadagi birinchi va eng muhim xalqaro shartnoma. U kompyuter jinoyatlarini ta'qib qilish va xalqaro hamkorlikni yo'lga qo'yish mexanizmlarini o'rnatadi.

3

OECD tavsiyalari

Iqtisodiy Hamkorlik va Taraqqiyot Tashkiloti ma'lumotlarni himoya qilish, shaxsiy hayotni saqlash va raqamli xavfsizlik bo'yicha bir qator tavsiyalar ishlab chiqqan. Bu tavsiyalar ko'plab mamlakatlar uchun yo'naltiruvchi asos hisoblanadi.

Imperativ, dispozitiv va tavsiyaviy tartibga solish usullari

Imperativ tartibga solish

Majburiy qonunlar va qat'iy talablar. Misol: Yevropa Ittifoqining GDPR qonuni, AQShning CFAA (Computer Fraud and Abuse Act) qonuni. Bu qonunlar aniq jazo va majburiyatlarni belgilaydi.

Dispozitiv tartibga solish

Shartnomaviy erkinlik va tomonlarning kelishuvi. Misol: AQShning E-SIGN qonuni, ICANN UDRP jarayonlari. Tomonlar o'zaro kelishuvlar asosida munosabatlarni tartibga soladi.

Tavsiyaviy tartibga solish

Eng yaxshi amaliyotlar va ko'rsatmalar. Misol: OECD tavsiyalari, IETF RFC standartlari, ISO sertifikatlari. Majburiy emas, lekin keng qo'llaniladigan standartlar.

Xalqaro hamkorlik – kiberxavfsizlik kaliti

Davlatlar, xalqaro tashkilotlar va texnologiya kompaniyalari o'rtasidagi samarali hamkorlik axborot xavfsizligini ta'minlashning asosiy omilidir

3-bob: O'zbekiston Respublikasining milliy me'yoriy-huquqiy bazasi

Asosiy qonunlar va normativ hujjatlar

"Axborotlashtirish to'g'risida"gi qonun

Axborot texnologiyalarini rivojlantirish, axborot resurslarini shakllantirish va ulardan foydalanish tartibini belgilaydi. Elektron hujjat aylanishi va raqamli xizmatlar asosini tashkil etadi.

"Shaxsiy ma'lumotlarni himoya qilish to'g'risida"gi qonun

Fuqarolarning shaxsiy ma'lumotlari yig'ilishi, saqlanishi va qayta ishlanishini tartibga soladi. GDPR talablariga moslashtirilgan milliy qonunchilik bazasini yaratadi.

"Davlat siri to'g'risida"gi qonun (2024)

2024-yil 27-dekabrda qabul qilingan yangi qonun davlat sirini tashkil etuvchi ma'lumotlarni aniqlash, tasniflash va himoya qilish tartibini yangicha belgilaydi.

Prezident qarorlari va hukumat farmoyishlari

2025-yilgi muhim qarorlar

Prezident qarori № ПП-153 axborot texnologiyalari yordamida sodir etilgan jinoyatlarga qarshi kurashni kuchaytirish bo'yicha kompleks choralarni belgilaydi.

- Kiberjinoyatlar bilan kurash mexanizmlarini takomillashtirish
- Davlat organlarining texnik salohiyatini oshirish
- Xalqaro tajribani o'rganish va joriy qilish
- Fuqarolarni xabardor qilish dasturlari

Kiberxavfsizlikni mustahkamlash bo'yicha yangi tashabbuslar milliy raqamli infratuzilmani himoya qilish va fuqarolarning ishonchini oshirishga qaratilgan.

Milliy qonunchilik – mustaqillik va xavfsizlik asosi

O'zbekistonning axborot xavfsizligi sohasidagi zamonaviy qonunchilik bazasi xalqaro standartlarga muvofiq holda rivojlanmoqda

4-bob: Shaxsiy ma'lumotlarni himoya qilish va kiberxavfsizlik

Shaxsiy ma'lumotlar himoyasining xalqaro va milliy asoslari

GDPR standartlari

Yevropa Ittifoqining Umumiy Ma'lumotlarni Himoya Qilish Reglamanti (GDPR) shaxsiy ma'lumotlar himoyasida global standart hisoblanadi va kuchli ta'sir ko'rsatadi.

O'zbekiston qonunchiligi

Milliy qonunchilik GDPR prinsiplaridan kelib chiqqan holda mahalliy xususiyatlarni hisobga oladi va fuqarolar huquqlarini himoya qilishga qaratilgan.

2023-2024 yillardagi kiberjinoyatlar statistikasi diqqatga sazovor: O'zbekistonda 58,8 ming kiberjinoyat qayd etilgan bo'lib, ularning 97,7 foizi bank kartalari bilan bog'liq. Bu raqamlar raqamli savod va xavfsizlik madaniyatini oshirish zarurligini ko'rsatadi.

Kiberxavfsizlikda tashkilotlar va davlat organlarining roli

01

Uzinfocom

O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi axborot xavfsizligi siyosatini ishlab chiqish va amalga oshirishda yetakchi rol o'ynaydi.

02

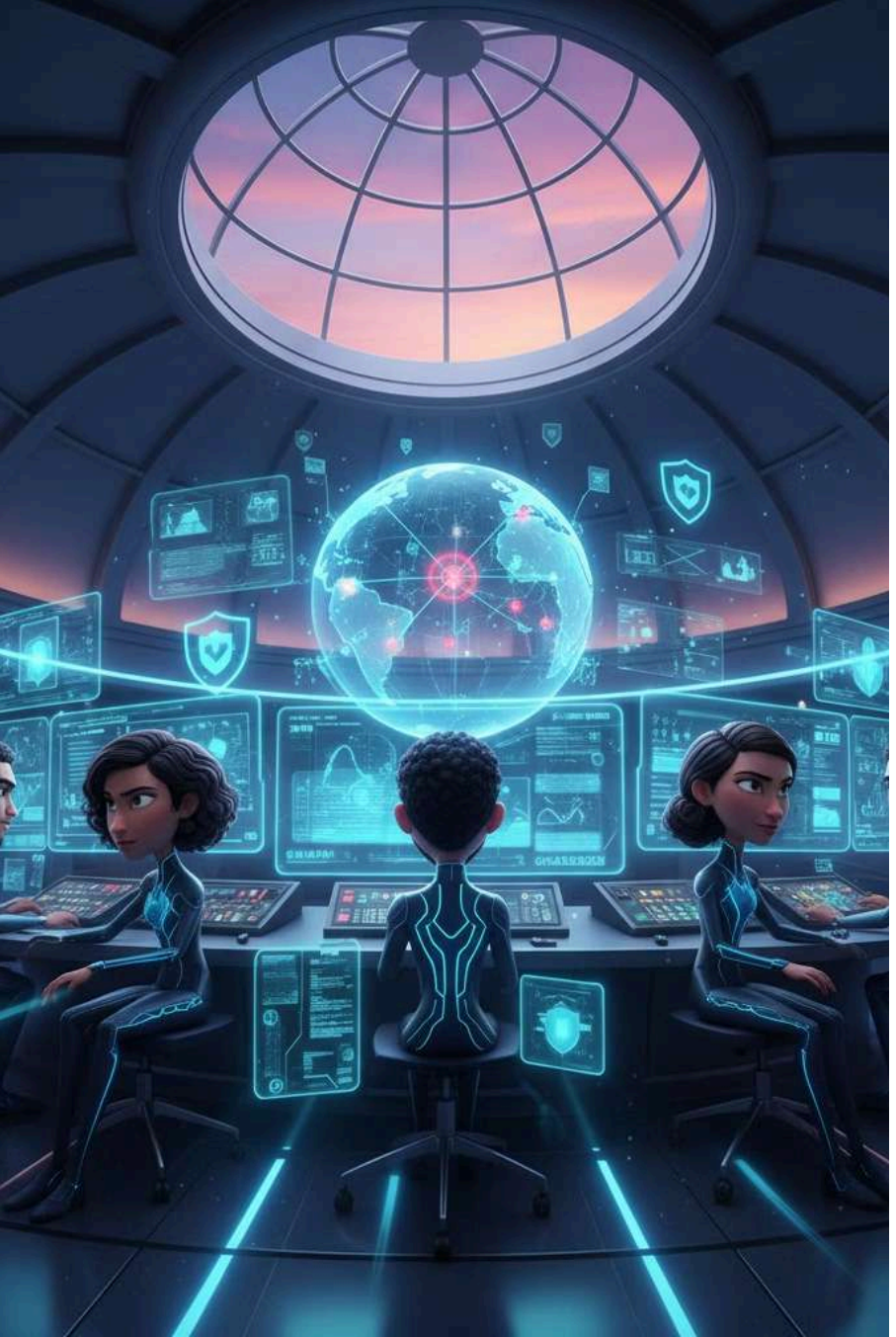
UZSOC monitoring

O'zbekiston Kiberxavfsizlik Operativ Markazi (UZSOC) 24/7 rejimida milliy infratuzilmani monitoring qiladi, tahdidlarni aniqlaydi va ularga javob beradi.

03

Mass Communications Center

Ommaviy kommunikatsiyalar markazi internet kontentini nazorat qilish, qonunga xilof ma'lumotlarni bloklash va fuqarolar xavfsizligini ta'minlash vazifalarini bajaradi.



Kiberhujumlarga qarshi kurashda mutaxassislar

Malakali kiberxavfsizlik mutaxassislari milliy infratuzilmani himoya qilish va tahdidlarga tezkor javob berishda hal qiluvchi ahamiyatga ega

5-bob: Axborot xavfsizligi sohasidagi javobgarlik va nazorat

Qonunbuzarliklar uchun javobgarlik turlari

Ma'muriy javobgarlik

Nisbatan yengil qonunbuzarliklar uchun qo'llaniladi:

- Jarima to'lovlari (jismoniy va yuridik shaxslar uchun)
- Litsenziyani to'xtatib turish yoki bekor qilish
- Ma'lumotlar bazasiga kirish huquqini cheklash
- Ogohlantirishlar va tuzatish buyruqlari

Internet resurslari va kontent egalari o'z platformalarida qonunga muvofiq tartibni ta'minlash majburiyatiga ega.

Jinoiy javobgarlik

Og'ir qonunbuzarliklar uchun jinoiy jazo belgilanadi:

- Kompyuter tizimlariga noqonuniy kirish
- Ma'lumotlarni o'g'irlash yoki buzish
- Kibershoximarj va moliyaviy firibgarlik
- Davlat sirini oshkor qilish
- Kritik infratuzilmaga hujum

Jazo muddati jinoyatning og'irligiga qarab 3 yildan 15 yilgacha ozodlikdan mahrum qilishni tashkil qilishi mumkin.

Kontentni bloklash va olib tashlash tartibi

Ariza topshirish

Qonunga xilof kontent topilganda davlat organlari yoki fuqarolar Mass Communications Center ga ariza yuboradi

1

Tekshirish jarayoni

Markaz mutaxassislari kontentni tekshiradi, qonun hujjatlariga muvofiqligini baholaydi va qaror qabul qiladi

2

Bloklash qarori

Agar qonunbuzarlik aniqlansa, resurs egasiga ogohlantirish yuboriladi va muayyan muddat ichida kontentni olib tashlash talab qilinadi

3

Amalga oshirish

Agar resurs egasi o'z majburiyatini bajarmasa, internet provayderlariga resursni bloklash to'g'risida buyruq yuboriladi

4

Xalqaro platformalar bilan munosabatlar ko'pincha murakkab bo'ladi, chunki ular boshqa yurisdiksiyalarda joylashgan. Shu sababli xalqaro hamkorlik mexanizmlarini rivojlantirish muhim ahamiyatga ega.

Qonunga xilof kontentga kirish bloklangan

Kontentni bloklash fuqarolar xavfsizligi va qonun ustuvorligini ta'minlashning muhim vositasidir

6-bob: Davlat siri va axborot xavfsizligi

"Davlat siri to'g'risida"gi qonunning asosiy jihatlari

Davlat sirining ta'rifi

Davlat siri – bu ochiq bo'lishi davlat xavfsizligi, mudofaa qobiliyati, tashqi siyosat va iqtisodiy manfaatlarga zarar yetkazishi mumkin bo'lgan himoyalangan ma'lumotlar.

Maxfiylik darajalari

Ma'lumotlar uch toifaga bo'linadi: "O'ta maxfiy", "Maxfiy" va "Maxfiylik belgisi". Har bir toifa uchun alohida himoya choralari va kirish tartibi belgilangan.

Himoya choralari

Davlat sirini tashkil etuvchi ma'lumotlarni himoya qilish uchun tashkiliy, texnik va huquqiy choralar kompleksi qo'llaniladi. Maxfiy hujjatlar bilan ishlash maxsus xonalarda amalga oshiriladi.

Kirish huquqi va javobgarlik

Davlat siriga kirish faqat maxsus ruxsatnoma asosida amalga oshiriladi. Davlat sirini oshkor qilish jinoiy javobgarlikka sabab bo'ladi va og'ir jazo bilan jazalanadi.

Davlat sirini himoya qilishda tashkilotlarning majburiyatlari

Texnik choralar

- Maxfiy ma'lumotlar uchun alohida tarmoq va serverlar
- Shifrlash tizimlari va kriptografik muhofaza
- Fizik kirish nazorati tizimlari
- Video kuzatuv va signalizatsiya
- Maxsus dasturiy ta'minot va antivirular
- Ma'lumotlarni zaxiralash va himoya qilish

Tashkiliy choralar

- Xodimlarni maxfiylik bo'yicha o'qitish va sertifikatlash
- Maxfiy hujjatlar bilan ishlash tartibini belgilash
- Ichki nazorat va audit tizimini joriy etish
- Ruxsatnomalar berish va kirish huquqlarini boshqarish
- Hodisalarni qayd etish va tekshirish
- Tashqi auditorlar bilan muntazam tekshiruvlar

Ruxsatnoma va sertifikatlash tartiblari davlat tomonidan nazorat qilinadi. Tashkilotlar muntazam ravishda tekshiruvdan o'tadi va me'yorlarga muvofiqligini tasdiqlovchi sertifikatlar oladi.

Maxfiy hujjatlar bilan ishlash

Davlat sirini tashkil etuvchi ma'lumotlar bilan ishlash maxsus tartib va qat'iy nazorat ostida amalga oshiriladi

7-bob: Axborot xavfsizligi sohasida xalqaro standartlar va sertifikatlash

ISO/IEC 27001 va boshqa xalqaro standartlar

ISO/IEC 27001

Axborot xavfsizligi boshqaruv tizimlari (ISMS) uchun eng mashhur xalqaro standart. Tashkilotlarga ma'lumotlarni himoya qilish uchun tizimli yondashuvni joriy etishga yordam beradi va xavflarni boshqarishni ta'minlaydi.

ISO/IEC 27002

Axborot xavfsizligi nazorat choralari bo'yicha ko'rsatmalar to'plami. 114 ta nazorat chorasi orqali tashkilotlar o'z xavfsizlik siyosatini shakllantirishi mumkin.

ISO/IEC 27017 va 27018

Bulut xizmatlari uchun maxsus standartlar. 27017 bulut xavfsizligi nazoratlarini, 27018 esa bulutdagi shaxsiy ma'lumotlarni himoya qilishni tartibga soladi.

NIST Cybersecurity Framework

AQSh Milliy Standartlar va Texnologiyalar Instituti tomonidan ishlab chiqilgan. Kiberxavfsizlikni boshqarish uchun keng qo'llaniladigan ramka hisoblanadi.

Sertifikatlash jarayonlari tashkilotlarning xalqaro standartlarga muvofiqligini tasdiqlaydi va mijozlar ishonchini oshiradi.

Milliy standartlar va ularning xalqaro mosligi

Xalqaro standartlarni o'rganish

O'zbekiston ISO/IEC standartlarini milliy sharoitlarga moslashtirib, O'zDSt (O'zbekiston Davlat Standarti) sifatida qabul qiladi

Mahalliy xususiyatlarni hisobga olish

Milliy qonunchilik, madaniy xususiyatlar va texnologik rivojlanish darajasi inobatga olinadi

Tatbiq etish va nazorat

Standartlar majburiy yoki tavsiya etilgan tartibda joriy qilinadi, tashkilotlar sertifikatlanadi

Yangilash va takomillashtirish

Xalqaro tajriba almashinuvi orqali standartlar muntazam yangilanadi va takomillashtiriladi

O'zbekiston O'rta Osiyo davlatlari, MDH mamlakatlari va xalqaro tashkilotlar bilan faol hamkorlik qiladi. Tajriba almashinuvi, qo'shma loyihalar va o'quv dasturlari orqali milliy axborot xavfsizligi salohiyati oshirilmoqda.

Sertifikatlangan axborot xavfsizligi markazi

Xalqaro standartlarga muvofiq sertifikatlangan markazlar yuqori darajadagi xavfsizlik va ishonchni ta'minlaydi

8-bob: Amaliy misollar va so'nggi yangiliklar

2024-2025 yillardagi kiberxavfsizlik hodisalari

AQSh: Kritik infratuzilmaga hujum

2024-yil fevralda AQShning neft va gaz sanoatiga qarshi keng ko'lamli kiberhujum amalga oshirildi. Change Healthcare tibbiy ma'lumotlar bazasiga hujum 100 million bemorning shaxsiy ma'lumotlarini xavf ostiga qo'ydi.

Yaponiya: Davlat tuzilmalariga hujum

2024-yil may oyida Yaponiya hukumat tarmog'iga katta kiberhujum qayd etildi. Tashqi kuchlar davlat siriga oid ma'lumotlarni o'g'irlashga harakat qildi, ammo tez javob berish natijasida zarar minimal darajada qoldi.

Germaniya: Moliyaviy sektor tahdidi

2024-yil avgustda Germaniyaning yirik banklariga DDoS hujumlari uyushtirildi. Xizmatlar bir necha soatga to'xtatildi va millionlab mijozlar ta'sir ko'rdi.

O'zbekistonda vaziyat

O'zbekistonda kiberjinoyatchilikning o'sish tendentsiyasi kuzatilmoqda. 2023-2024 yillarda 58,800 ta kiberjinoyat qayd etilgan bo'lib, ularning aksariyati moliyaviy firibgarlik va bank kartalari bilan bog'liq. Davlat organlari raqamli savodxonlikni oshirish va fuqarolarni xabardor qilish dasturlarini kuchaytirmoqda.

Yangi texnologiyalar va qonunchilikdagi o'zgarishlar

Kriptografiya va elektron imzo

O'zbekistonda elektron raqamli imzo (ERI) tizimi keng joriy etilmoqda. Yangi kriptografik algoritmlar va protokollar milliy xavfsizlik talablariga moslashtirilgan.

- Milliy kriptografik standartlar rivojlanishi
- Kvant xavfsizligiga tayyorgarlik
- Blokcheyn texnologiyalarining tatbiqi

Raqamli identifikatsiya

Biometrik autentifikatsiya va mobil ID tizimlari davlat xizmatlariga xavfsiz kirish va fuqarolarning shaxsini tasdiqlash uchun joriy qilinmoqda.

- Yuz va barmoq izi tanish tizimlari
- Mobil ilovalarda xavfsiz autentifikatsiya
- Raqamli hujjatlar va elektron pasportlar

Kiberxavfsizlik bo'yicha treninglar

Doimiy ta'lim va malaka oshirish zamonaviy kibertahdidlarga qarshi kurashning muhim qismidir

9-bob: Xulosa va kelajak istiqbollari

Axborot xavfsizligini ta'minlashda qonunchilikning roli

Qonunchilik mustahkamligi

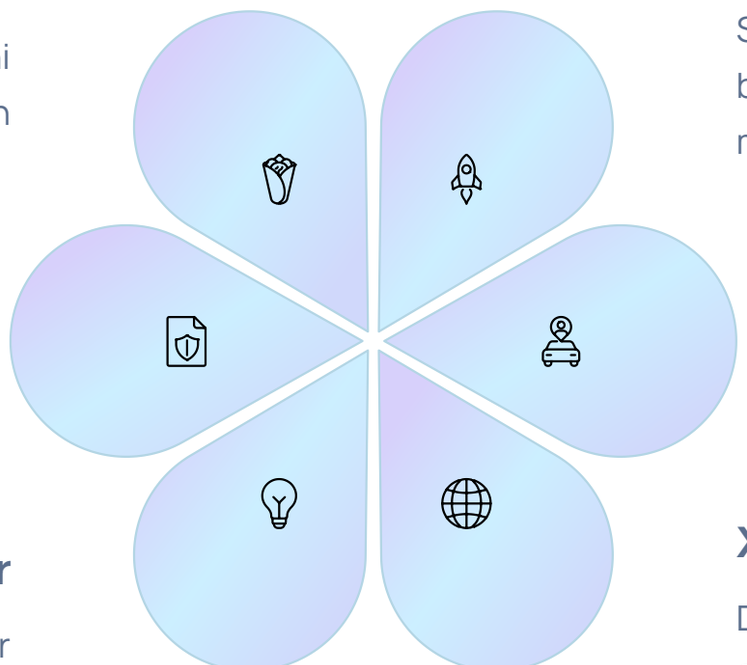
Milliy va xalqaro me'yoriy-huquqiy bazani doimiy yangilash va takomillashtirish

Proaktiv yondashuv

Tahdidlarni oldindan aniqlash va oldini olishga qaratilgan proaktiv strategiyalar

Innovatsiyalar

Ilmiy tadqiqotlar va innovatsion yechimlar orqali kiberxavfsizlik salohiyatini oshirish



Texnologik rivojlanish

Sun'iy intellekt, kvant texnologiyalari va blokcheyn kabi yangi texnologiyalarga moslashish

Xavfsizlik madaniyati

Fuqarolar va tashkilotlarda raqamli savod va kiberxavfsizlik madaniyatini shakllantirish

Xalqaro hamkorlik

Davlatlar, tashkilotlar va kompaniyalar o'rtasida samarali hamkorlik mexanizmlarini kengaytirish

Axborot xavfsizligi – bu faqat texnologiya masalasi emas, balki jamiyat, iqtisodiyot va davlat xavfsizligining ajralmas qismidir. Kelajakda sun'iy intellekt, Internet of Things (IoT) va kvant kompyuterlari kabi yangi texnologiyalar yangi imkoniyatlar bilan birga yangi tahdidlarni ham keltirib chiqaradi. Shu sababli, qonunchilik, texnologiya va xalqaro hamkorlikning uyg'un rivojlanishi barqaror va xavfsiz raqamli kelajakni ta'minlashning yagona yo'lidir.