AXBOROT XAVFSIZLIGINING SIYOSATI

Jumaboyev Javlonbek Sherqul o’g’li
Po’latov Doston Normurod o’g’li
Roziqov Abdug’ani Ilhomjon o’g’li
Hasanov Murodillo Azim o’g’li

Annotatsiya:*Axborot xavfsizligi, modern dunyoda muhim bir muammoga aylanadi. Axborot tizimlari, zararli faollanishlardan, ma'lumot sovurishdan va hujjatlar bilan hamda xavfsizlikka o'rtacha xavf ko'rsatish imkoniyatlari bilan ta'sirchan bo'lgan shaxslardan himoyalash talablari keltiriladi. Axborot xavfsizligining siyosati, bir tashqi tashkilot yoki davlatning axborot tizimlarini va ma'lumotlarni himoyalash uchun belgilangan strategiyalarni va qo'llanmalarni belgilaydi.Axborot xavfsizligining siyosati, foydalanuvchilar va axborot resurslariga zararli ta'sir ko'rsatishdan himoyalash uchun kerakli tartib va qo'llanmalarni belgilaydi. Bu siyosat, hukumatlar, korxonalarga, tashkilotlarga va boshqa axborotni qo'llab-quvvatlovchi tashkilotlarga qarshi kurashishda muhimdir.Axborot Xavfsizligining Siyosati Quyidagi Yo'nalishlarni O'z Ichiga Oladi*

1. Xavfsizlikni ta'minlashning asosiy tamoyillari: Axborot tizimlarida xavfsizlikni oshirish uchun asosiy tamoyillar va standartlar joriy etiladi. Bunda xavfsizlik protokollari, shifrlash algoritmlari, kirish tizimlari va boshqa xavfsizlikning muhim tushunchalari keng tarqalgan bo'ladi.

2. Xavfsizlik risklarini tahlil qilish: Axborot tizimlaridagi xavfsizlik risklarini aniqlash, shu jumladan, zararli programmalarning identifikatsiyasi, hujjatlarni himoya qilish, foydalanuvchilar ma'lumotlarining himoyasi, tarmoqlarni himoyalash va xavfsizlik ko'nikmalari bilan bog'liq xavfsizlik risklarini tahlil qilishni o'z ichiga oladi.

3. Xavfsizlikning texnik va tashkiliy tomonlari: Xavfsizlikning o'rganishini va o'zgarishlarni belgilash uchun, texnik va tashkiliy qo'llanmalarni joriy etish, xavfsizlikni ta'minlash uchun kerakli vositalarni, texniklar va infratuzilmani amalga oshirishni o'z ichiga oladi.

4. Huquqiy muhofaza va nazorat: Axborot xavfsizligining siyosati, foydalanuvchilar va axborot tizimlariga zararli faollanishlarni oldini olish kerak.

Bu annotatsiyada, axborot xavfsizligi siyosati haqida bilgilar beriladi. Axorot xavfsizligi siyosati, bir mamlakat yoki tashqi tashkilotning axborot tizimlarini xavfsizlikka qarshi himoya qilish va axborotga kirishga harakat qiluvchi kishilar va tashkilotlar uchun qo'llanma va qonunlardan iborat bo'lgan umumiy qo'llanmalar va qonunlar jamlanmasidir.

Bu siyosatning maqsadi, axborot tizimlarida yuzaga keladigan xavfsizlik xatarlarini tushuntirish, ularga qarshi kurashish va ularga qarshi himoya qilish, xavfsizlikni ta'minlash va axborotni qo'llab-quvvatlashdir.

Axorot xavfsizligi siyosati, sayyoraliklar, tashqi tashkilotlar va fuqarolarning axborot tizimlariga erishishi, tizimdan foydalanishi, o'z ma'lumotlarini saqlashishi va ularga

xavfsizligini ta'minlash uchun asosiy muhimat hisoblanadi. Siyosatning bajarilishida, axborot tizimlarining xavfsizligi uchun zarur bo'lgan qo'llanmalar va xavfsizlikni ta'minlash bo'yicha texnikalar amalga oshiriladi.

Axorot xavfsizligi siyosati hamma tashqi tashkilotlar va fuqarolar uchun zarurdir. Ushbu siyosat sayyoraliklarni, tashqi tashkilotlarni va fuqarolarni xavfsizlikga oid xabarlardan xabardor qilishi va ularga muhim ma'lumotlarni o'zgartirishlari kerak bo'lgan axborot tizimlarida xavfsizlikni ta'minlash uchun kerakli maslahatlar va yondashuvlar beradi.

Kalit so'zlar:*Xavfsizlik,risk tahlili,xavfsizlik standartlari,xavfsizlikning butunligi,xavfsizlik nazariyasi,huquqiy qo'llanmalar, xavfsizlik niyati,xavfsizlik monitorinigi,tashqi tashkilotlar bilan hamkorlik,tashqi tashkilotlar bilan hamkorlik,xavfsizlik tarbiyasi.*

Abstract:*Information security becomes an important problem in the modern world. Information systems are required to be protected against malicious activations, information leakage, and exposure to documents and individuals with moderate security risk capabilities. An information security policy defines the strategies and guidelines for protecting the information systems and data of an external organization or country.*

The policy of information security defines the necessary procedures and guidelines to protect users and information resources from harmful effects. It is important to fight against politics, governments, businesses, organizations and other organizations that support information.

The policy of information security includes the following directions:

1. Basic principles of security: Basic principles and standards are introduced to improve security in information systems. It covers security protocols, encryption algorithms, access systems, and other important security concepts.

2. Security Risk Analysis: Identifying security risks in information systems, including security risk analysis related to malware identification, document protection, user data protection, network protection, and security skills .

3. Technical and organizational aspects of security: It includes the implementation of the necessary tools, techniques and infrastructure to ensure security, to define security studies and changes, to introduce technical and organizational manuals.

4. Legal protection and control: Information security policy should prevent harmful activations to users and information systems.

This annotation provides information about the information security policy. A national security policy is a set of general guidelines and laws for people and organizations trying to protect information systems of a country or foreign organization against security and access information.

The purpose of this policy is to explain, combat, and protect against security threats to information systems, to ensure security, and to support information.

Akhorot's security policy is of primary importance to the access, use, storage and security of information systems by aliens, external organizations and citizens. In the implementation of the policy, the necessary guidelines for the security of information systems and security techniques are implemented.

Akhorot security policy is necessary for all external organizations and citizens. This policy informs stakeholders, external organizations, and citizens of security-related messages and provides them with the necessary advice and approaches to ensure security in information systems that need to change critical information.

Key words:*Security, risk analysis, security standards, security integrity, security theory, legal guidelines, security intent, security monitoring, cooperation with external organizations, cooperation with external organizations, security education*.

KIRISH

Axborot xavfsizligi siyosati, bir tashkilot yoki mamlakatning axborot tizimlarida xavfsizlikni ta'minlashga oid amalga oshiriladigan qo'llanmalar va qonunlar jamlamasidir. Kirish qismida axborot xavfsizligi siyosatining asosiy qismlari va muhim nuqtalari ko'rsatiladi. Quyidagi kalit so'zlar va ifodalar, axborot xavfsizligi siyosati kirish qismida foydalanilishi mumkin:

1. Maqsad va maqsadlar: Axborot xavfsizligi siyosati o'z maqsadlari va ulardan kutib turgan natijalarni belgilayadi.

2. Qo'llashuvchilar: Siyosatda tashkilotingizning xavfsizlik bo'yicha mas'ul bo'lgan shaxslar va tashkilot birliklari ko'rsatiladi.

3. Xavfsizlik prinsiplari: Siyosatda amal qiluvchi asosiy prinsiplar, masalan, konfidensiallik, butunlik, mavjud bo'lish, amalni bajarganlik va boshqalar, ko'rsatiladi.

4. Xavfsizlikning asosiy yo'nalishlari: Siyosatning asosiy yo'nalishlari va ustuvor vazifalari ifodalangan.

5. Xavfsizlikning qo'llanmasi: Xavfsizlikni ta'minlashda qo'llanadigan qo'riqnomalar, standartlar, protseduralar va usullar ko'rsatiladi.

6. Xavfsizlikni oshirish: Siyosatda tashkilotning xavfsizlikni oshirish uchun qo'llaniladigan chora-tadbirlar va strategiyalar ko'rsatiladi.

7. Riskni tahlil qilish: Xavfsizlikning ta'minlanishi uchun tizimdagi xavf va xavfsizlik xatarlarining tahlili va boshqarilishi.

8. Xavfsizlikni ta'minlash usullari: Axborot tizimlaridagi xavfsizlikni ta'minlash uchun amalga oshiriladigan texnikalar, vositalar, vositalarni monitoring qilish usullari va boshqalar ko'rsatiladi.

9. Xavfsizlik kafolatlari: Siyosatda xavfsizlikni ta'minlash uchun tashkilotning qanday kafolatlar berishini belgilash mumkin, masalan, xavfsizlik sertifikatlari, kengaytirilgan kimyo emasligi (PKI), xavfsizlik politalari va boshqalar.

Axborot xavfsizligi siyosati, tashkilotlarning axborot tizimlarida yozuvlar, ma'lumotlar va kommunikatsiya uchun ta'minlangan himoya muhofazasini ta'minlash uchun belgilangan

strategiyalar, protseduralar va qo'llanmalardir. Bu siyosat, axborot tizimlaridagi xavf va xavfsizlik xatarlarining tahlili, xavfsizlik standartlari va qoidalar, axborot tizimlari uchun huquqiy qo'llanmalar, xavfsizlik nazariyasi va tizimning xavfsizligi uchun belgilangan qarorlarni o'z ichiga oladi.

Axborot xavfsizligi siyosati, tashkilotning xavfsizlik niyatiga muvofiq tuziladi. Ushbu siyosat tashkilotingizning axborot tizimlarida xavfsizlikga e'tiborini qaratish uchun xavfsizlik monitorinigini, xavfsizlikni oshirish uchun tashqi tashkilotlar bilan hamkorlik va axborot almashinuvini ta'minlashni, tizimdan foydalanuvchilarga xavfsizlikni o'rgatish va ularni xavfsiz foydalanishga o'rgatishni o'z ichiga oladi.

Axborot xavfsizligi siyosati tashkilotning xavfsizlikni ta'minlashda muhim ahamiyatga ega bo'ladi. Bu siyosatni to'g'ri tuzish tashkilotning ma'lumotlarining himoyalangan va xavfsizligini ta'minlashiga yordam beradi.

1. Xavfsizlik: Axborot tizimlarida yozuvlar, ma'lumotlar va kommunikatsiya uchun ta'minlangan himoya muhofazasi.

2. Risk tahlili: Xavfsizlikni ta'minlash uchun axborot tizimlaridagi xavf va xavfsizlik xatarlarining tahlili.

3. Xavfsizlik standartlari: Xavfsizlikni ta'minlash uchun belgilangan standartlar, protokollar va qoidalar.

4. Xavfsizlikning butunligi: Xavfsizlikni ta'minlash uchun to'liq muhimatlarni o'z ichiga olgan tizim yoki tarmoq.

5. Xavfsizlik nazariyasi: Xavfsizlikning asosiy prinsiplari, printsipiyalar va o'zaro aloqalar.

6. Huquqiy qo'llanmalar: Axorot tizimlarining xavfsizligini ta'minlash uchun belgilangan qonunlar, qarorlar va muhimatlarning jamlanmasi.

7. Xavfsizlik niyati: Tashkilotingizning xavfsizlikga berilgan e'tibori va xavfsizlikni o'z ichiga olgan qarorlar to'plami.

8. Xavfsizlik monitorinigi: Axborot tizimlaridagi xavfsizlik holatini nazorat qilish va e'tibor bilan kuzatish.

9. Tashqi tashkilotlar bilan hamkorlik: Xavfsizlikni oshirish uchun tashqi tashkilotlar bilan hamkorlik va axborot almashinuvini ta'minlash.

10. Xavfsizlik tarbiyasi: Tizimdan foydalanuvchilarga xavfsizlikni ta'lim berish va ularni xavfsiz foydalanishga o'rgatish.

Bu kalit so'zlar, axborot xavfsizligi siyosati bo'yicha muhim tushuncha va asosiy mavzularni ifoda qilishda ishlatiladi. Ular axborot tizimlarini xavfsiz va himoyalanuvchi qilishda ahamiyatga ega bo'ladi.

Axborot xavfsizligining siyosati, tashkilotning axborot tizimlarida yozuvlar, ma'lumotlar va kommunikatsiya uchun ta'minlangan himoya muhofazasini ta'minlash uchun belgilangan strategiyalar, protseduralar va qo'llanmalardan iboratdir.

Bu siyosatning asosiy maqsadi, axborot tizimlaridagi xavf va xavfsizlik xatarlarini tushuntirish, ularga qarshi kurashish va ularga qarshi himoya qilish, xavfsizlikni ta'minlash

va axborotni qo'llab-quvvatlashdir. Ushbu siyosat tashkilotning xavfsizlik niyatiga muvofiq tuziladi va xavfsizlikning butunligi, risk tahlili, xavfsizlik standartlari, huquqiy qo'llanmalar, xavfsizlik nazariyasi va tashkilotning xavfsizlik monitorinigi kabi muhim qo'llanmalarni o'z ichiga oladi.

Axborot xavfsizligining siyosati tashkilotning axborot tizimlarini xavfsiz va himoyalangan qilishga intiladi. Ushbu siyosat tashkilotning tizimlarga kirish tizimlarini, ma'lumotlarni shifrlash va himoyalashni, xavfsizlik protokollari va sozlashlarni, tizimdan foydalanuvchilarga xavfsizlikni o'rgatishni o'z ichiga oladi.

Axborot xavfsizligining siyosati tashkilotning xavfsizlikni ta'minlash va tashkilotni axborot xavfsizligi konsepsiyasi bilan muvofiqlashtirish uchun joriy qilingan qo'llanmalar, standartlar va qonunlardan iboratdir. Bu siyosat tashkilotga axborot tizimlarini muhofaza qilish uchun kerakli bo'lgan qarorlar va jarayonlarni belgilaydi.

Axborot xavfsizligi, hozirgi vaqtda tashkilotlar uchun muhim muammolardan biridir. Bu muammolarni yechish uchun esa tashkilotlarning axborot xavfsizligi siyosati kerak. Bu siyosat axborot tizimlarida foydalanuvchi yoki tashkilot ma'lumotlari uchun ta'minlangan himoya va muhofaza tadbirlari jihatidan belgilangan strategiyalar, protseduralar va qo'llanmalardan iborat.

Tashkilotning axborot xavfsizligi siyosati, tashkilotning axborot tizimlarida yozuvlar, ma'lumotlar va kommunikatsiya uchun ta'minlangan himoya muhofazasini ta'minlashga yordam beradi. Bu siyosat, tashkilotning axborot tizimlaridagi xavf va xavfsizlik xatarlarining tahlili, xavfsizlik standartlari va qoidalar, axborot tizimlari uchun huquqiy qo'llanmalar, xavfsizlik nazariyasi va tizimning xavfsizligi uchun belgilangan qarorlarni o'z ichiga oladi.

Axborot xavfsizligi siyosati, tashkilotning xavfsizlik niyatiga muvofiq tuziladi. Ushbu siyosat tashkilotingizning axborot tizimlarida xavfsizlikga e'tiborini qaratish uchun xavfsizlik monitorinigini, xavfsizlikni oshirish uchun tashqi tashkilotlar bilan hamkorlik va axborot almashinuvini ta'minlashni, tizimdan foydalanuvchilarga xavfsizlikni o'rgatish va ularni xavfsiz foydalanishga o'rgatishni o'z ichiga oladi.

Axborot xavfsizligi siyosati, tashkilotning xavfsizlikni ta'minlashda muhim ahamiyatga ega bo'ladi. Bu siyosatni to'g'ri tuzish tashkilotning ma'lumotlarining himoyalangan va xavfsizligini ta'minlashiga yordam beradi. Shuningdek, bu siyosat tashkilotda ma'lumotlarning yo'qolishiga qarshi qarorlar chiqarish, hujjatlarning himoyalangan saqlashini ta'minlash, xavfsiz foydalanuvchi imkoniyatlarini oshirish va tashkilotni axborot tizimlari orqali kuchliroq qilishga yordam beradi.

Axborot xavfsizligining siyosati, bir tashkilotning axborot tizimlarini yozuvlar, ma'lumotlar va kommunikatsiya uchun xavfsizlashtirishning belgilangan qoida va qarorlar jamlanmasidir. Bu maqolada, axborot xavfsizligi siyosati mavzusida O'zbek tilida ma'lumotlar taqdim etaman.

Axborot xavfsizligi siyosati, tashkilotning axborot tizimlarini hujjatlar, ma'lumotlar va kommunikatsiya uchun maxsus protokollar va xavfsizlik standartlari asosida himoya qilishni

ta'minlaydi. Bu siyosatning asosiy maqsadi, axborot tizimlaridagi xavfsizlik xatarlarini tushunish, ularga qarshi kurashish va ularga himoya qilishni o'z ichiga oladi.

Siyosatning amaliyati davomida, axborot tizimlaridagi xavfsizlikni ta'minlash uchun xavfsizlikning turli aspektlari ko'rib chiqiladi. Bu aspektlar tashkilotning xavfsizlik niyatiga muvofiq belgilangan xavfsizlik standartlarini, xavfsizlik protseduralarini, tizimlar uchun huquqiy qo'llanmalarni va axborot xavfsizligi nazariyasini o'z ichiga oladi.

Axborot xavfsizligi siyosati, xavfsizlikning butunligini ta'minlash, xavfsizlikning monitoringini amalga oshirish, tashqi tashkilotlar bilan hamkorlik va axborot xavfsizligi tarbiyasini o'z ichiga oladi. Bu siyosat tashkilotlar uchun muhimdir, chunki u axborot tizimlarini xavfsiz va himoyalangan qilishda katta ahamiyatga ega bo'ladi.

"Axborot xavfsizligining siyosati" deb nomlangan maqolada axborot xavfsizligi siyosati haqida o'zbek tilida ma'lumotlar beriladi.

Axborot xavfsizligi siyosati, tashkilotlarning axborot tizimlarida yozuvlar, ma'lumotlar va kommunikatsiya uchun ta'minlangan himoya muhofazasini ta'minlashga yo'l qo'yadigan qo'llanmalar va qonunlardan iborat bo'ladi. Bu siyosat tashkilotning axborot tizimlaridagi xavf va xavfsizlik xatarlarini tahlil qilish, xavfsizlik standartlari va qoidalar belgilash, xavfsizlikga oid huquqiy qo'llanmalar, xavfsizlik nazariyasi va tizimning xavfsizligini ta'minlashga doir qarorlar asosida shakllanadi.

Axborot xavfsizligi siyosati, tashkilotning xavfsizlik niyatiga muvofiq rivojlanadi. Ushbu siyosat tashkilotning axborot tizimlaridagi xavfsizlik holatini kuzatish, xavfsizlikni oshirish uchun tashqi tashkilotlar bilan hamkorlik va axborot almashinuvini ta'minlash, tizimdan foydalanuvchilarga xavfsizlikni o'rgatish va ularni xavfsiz foydalanishga o'rgatishni o'z ichiga oladi.

Axborot xavfsizligi siyosati, tashkilotning axborot tizimlaridagi xavfsizlikni ta'minlashda muhim ahamiyatga ega bo'ladi. Bu siyosat tashkilotning ma'lumotlarining himoyalangan va xavfsizligini ta'minlash uchun qo'llanmalarni va qarorlarni o'z ichiga oladi.

Axborot xavfsizligi siyosati, bir tashkilotning axborot tizimlarida yozuvlar, ma'lumotlar va kommunikatsiya uchun ta'minlangan himoya muhofazasini ta'minlashning belgilangan qoidalar, strategiyalar va protseduralar to'plamidir. Ushbu siyosat, tashkilotning xavfsizlik niyatiga asoslangan va axborot xavfsizligini ta'minlashda kritik ahamiyatga ega.

Axborot xavfsizligi siyosati, axborot tizimlarida yuzaga kelishi mumkin bo'lgan xavf va xavfsizlik xatarlarini tushuntirish, ularga qarshi kurashish va ularni zaharlantirish uchun kerakli qo'llanmalar, standartlar va protokollar bilan birgalikda amalga oshiriladi. Bu siyosatning asosiy maqsadi, axborot tizimlaridagi xavfsizlik muammolarini oldini olish, yonli maslahatlar va xavfsizlikni ta'minlash usullarini belgilab, tashkilotning axborot tizimlarini hujjatlar, ma'lumotlar va kommunikatsiya yordamida himoyalashni ta'minlashdir.

Axborot xavfsizligi siyosati tashkilotning xavfsizlik bilan bog'liq maqsadlarini, qo'llanish va amalga oshirish jarayonlarini, xavfsizlik tarkibini va tartibini belgilaydi. Ushbu siyosat tashkilotning axborot tizimlaridagi xavfsizlikni oshirish, muomalada yuqori darajada

himoya qilish va foydalanuvchilarga xavfsizlikni ta'minlashda muhim ahamiyatga ega bo'ladi.

Axborot xavfsizligi siyosati, axborot tizimlarini yaxshi tashkil etish, yoshlarni xavfsizlik tamoyillari bilan ta'lim berish, xavfsizlikni oshirish uchun so'nggi texnologiyalardan foydalanish, xavfsizlik monitorinigini amalga oshirish, tashqi tashkilotlar bilan hamkorlik qilish va xavfsizlikni oshirishdagi eng yangi usullarni taklif etish kabi qo'llanmalarni o'z ichiga oladi.

Bu maqolada axborot xavfsizligi siyosati, tashkilotning axborot tizimlaridagi xavfsizlikni ta'minlashda o'rniga keladigan maslahatlar va qo'llanmalar haqida tushuntirilgan. Ushbu siyosatning amalga oshirilishi tashkilotning axborot tizimlarini xavfsiz va himoyalaydi.

"Axborot xavfsizligining siyosati" mavzusida O'zbek tilida professional maqola quyidagicha bo'lishi mumkin:

"Axborot Xavfsizligi: Huquqiy, Texnikaviy va Tashkiliy Aspektlari"

Kirish: Bu maqolada, axborot xavfsizligining siyosati mavzusidagi muhim tartibotlar va muammoniyatlarni tahlil qilinadi. Axborot tizimlaridagi o'lchamli o'zgarishlar va internet foydalanuvchilarining ko'payishi bilan birga xavfsizlik muammosi ham kengaymoqda. Maqolada, axborot xavfsizligi siyosatining asosiy mazmuni, huquqiy aspektlari, texnikaviy imkoniyatlari va tashkiliy muammolari ko'rib chiqiladi.

Huquqiy Aspektlar

Maqolada axborot xavfsizligi siyosatining asosiy huquqiy qo'llanmalari, axborot to'g'risidagi qonunlar, foydalanuvchilar huquqlari va shaxsiy ma'lumotlarni himoya qilish prinsiplari tahlil qilinadi. Shuningdek, axborot xavfsizligi bilan bog'liq bo'lgan davlat va tashkiliy organlarning vazifalari va huquqiy maslahatlar ham ko'rib chiqiladi.

Texnikaviy Aspektlar

Bu qismda, axborot tizimlarida foydalaniladigan xavfsizlik texnikalari, shifrlash protokollari, foydalanuvchi identifikatsiya va autentifikatsiya usullari kabi muhim masalalar ko'rib chiqiladi. Texnikaviy muammolar, hakerlik guruhlarining hujumlaridan himoya ta'minlash, tarmoqni monitoring qilish va xavfsizlik holatini baholash kabi mavzular ham tahlil qilinadi.

Tashkiliy Muammolar

Maqolada axborot xavfsizligi siyosati o'rganish, amalga oshirish va ta'lif qilish jarayonida tashkiliy muammolar ham ko'rib chiqiladi. Bu, axborot xavfsizligi bilan bog'liq bo'lgan xodimlar tayyorlash, axborot xavfsizligini amalga oshirish uchun tashkiliy usullarni o'rganish va xavfsizlik insidentlariga tez reagirov qilish kabi muhim masalalarni o'z ichiga oladi.

Axborot Xavfsizligining Siyosati Qullayliklari Va Kamchiliklari

Axborot xavfsizligi, bir tizim, jumladan kompyuterlar, telefonlar, ağlar, internet va boshqalar orqali almashinuvni amalga oshiruvchi axborotning xavfsizligi va himoya qilishga

qarashlarni o‘z ichiga oladi. Bu axborot xavfsizligining siyosati qullanishlari va kamchiliklari mavzusida bir necha muhim nuqtalarni ko‘rsatadi:

Qullayliklari

1. Ma’lumot himoyasi: Axborot xavfsizligi siyosati, ma’lumotlarni himoya qilish va so‘nggi texnologiyalardan kelib chiqadigan xavf-xatarlarga qarshi himoya qilishga yo‘naltirilgan. Bu, foydalanuvchilar, tashqi yozuvchilar yoki hukumat tashkilotlari tomonidan yetkazib berilgan ma’lumotlarning xavfsizligini ta’minlashda juda muhimdir.

2. Internet to‘g‘risidagi ishlarni kuchaytirish: Xavfsizlik siyosati, internet tarmog‘ining ishlashini yanada kuchaytirishga yordam beradi. Foydalanuvchilar internetni xavfsizlikdagi o‘zaro aloqalar, onlayn xaridlar, ma’lumot almashish, ijtimoiy tarmoqda faol bo‘lish va boshqalar kabi imkoniyatlardan foydalanishlari mumkin bo‘ladi.

3. Malakali xorijiy investitsiyalar: Axborot xavfsizligining yuqori darajada bo‘lishi bir mamlakatga xorijiy investitsiyalar keltirishni ko‘proq qiladi. Ilova korxonalari va startaplar xavfsizlik talablarini qo‘llab-quvvatlash orqali xorijiy investorlarning diqqatini jalb etishlari mumkin.

axborot xavfsizligining siyosati, bir qancha qullayliklarga ega bo‘ladi

1. Ma'lumot himoyasi: Axborot xavfsizligi siyosati, ma'lumotlarni himoya qilish va muvaffaqiyatli bo‘lgan tizimlar, platformalar va tarmoqlar orqali foydalanuvchilar, tashqi yozuvchilar, korxonalarni va hukumatlarni xavfsizlantirishga imkon beradi. Bu, shaxsiy ma'lumotlarning, ish ma'lumotlarining, kompaniya sirli ma'lumotlarning va milliy ma'lumotlarining himoyalashini ta'minlaydi.

2 Ijtimoiy aloqalar va ishbilarmonlik: Xavfsizlik siyosati, mijozlar va korxonalarning bir-biriga ishonch va axborot almashishini kuchaytiradi. Agar foydalanuvchilar, tashqi partnerlar va mijozlar tizimlar yoki kompaniyalar tomonidan ta'minlangan axborotlarni xavfsiz his etishlari mumkin bo'lsa, ular o'zlarini muvaffaqiyatli hamkorliklarga yo'naltirishlari va ishbilarmonlikni rivojlantirishlari osonlashadi.

3. Yutuqlash va ishlab chiqish kuchini oshirish: Axborot xavfsizligi siyosati, innovatsiyalar va yangiliklarni qayta ishlab chiqish jarayonini yutuqlashtiradi. Bizneslar, tizimlar va sohasida faol ishlash uchun axborotlarni xavfsiz his etishlari, foydalanuvchilarning ishonchini oshiradi va axborot almashishini kuchaytiradi. Bu esa yangi xizmatlar, ilovalar va texnologiyalarni ishlab chiqish va tartibga solishga imkon beradi.

4. Barcha sohalarda qo'llanish: Xavfsizlik siyosati barcha sohalarda qo‘llaniladi. Sizning shaxsiy telefon, kompyuter, internet tarmog‘ingiz, shuningdek korxona, bank va hukumat tizimlari hammasi axborot xavfsizligiga rioya qilishi lozim bo‘ladi. Bu, biznes, ishbilarmonlik, shaxsiy hayot, ta'lim, tibbiyot va boshqalar kabi sohalarda qullab-quvvatlashni ta'minlaydi.

5. Xavfsizlik bilan bog'liq huquqlar va shartlar: Xavfsizlik siyosati, axborot xavfsizligi bilan bog'liq huquqlar va shartlar to'g'risidagi qoidalar va qonunlarni ta'minlaydi. Bu, foydalanuvchilarga x

Kamchiliklari

1. Foydalanuvchilar erkinligi va g‘oyalarining tahdidlanishi: Axborot xavfsizligi siyosati, foydalanuvchilarning erkinligi va g‘oyalarining tahdidlanishi mumkinligini yaratishi mumkin. Hukumatlar yoki tashkiy korxonalarning axborotlariga kirish uchun uning erkinligini cheklash uchun xavfsizlik muhofazasi orqali foydalanuvchilarni cheklashlari mumkin.

2. Xavfsizlik va commodification bo‘g‘indorligi: Axborot xavfsizligi siyosati yoriqsizliklarni to‘ldirishga imkon beradi. Xavfsizlik vositalari, xavfsizlik texnologiyalari va himoya xizmatlari ishlab chiqarish tarmog‘i, ximoyalaydi.

Axborot xavfsizligining siyosati, quyidagi kamchiliklarga ega bo'lishi mumkin:

1. Foydalanuvchilar erkinligi va g'oyalarining tahdidlanishi: Agar axborot xavfsizligi siyosati juda qat'iy va cheklangan bo'lsa, bu foydalanuvchilar uchun erkinlik va g'oyalarining tahdidlanishiga olib kelishi mumkin. Agar foydalanuvchilar ma'lumotlarini himoya qilish uchun katta cheklanishlarni qabul qilishlari kerak bo'lsa, ularning axborot erkinligi va maxfiyliklari haqida talablarini buzish uchun foydalanish erkinligi cheklanishi mumkin.

2. Innovatsiyalarni to'xtatish: G'oya kiritish va yangi innovatsiyalar yaratishning muhim qismi, xavfsizlikni talab qilish va qo'llashdir. Agar xavfsizlik siyosati ortiqcha cheklanishlarga yo'l qo'ysa, bu yangi ilovalarni ishlab chiqish va o'rnatish jarayonini qiyinlashtirishi mumkin. Bu esa innovatsiya va sarmoya kiritishga negativ ta'sir qilishi mumkin.

3. Kirish va huquqni cheklash: Xavfsizlik siyosati, tashki kirishlarni cheklash va shaxsiy ma'lumotlarga kirishni cheklashga yo'l qo'ymoq maqsadida ishlatilishi mumkin. Bu esa axborotlarga oson kirishni to'xtatishi va mijozlar uchun uzok va kuchli autentifikatsiya va huquqiy cheklovlar yaratishi mumkin. Buning natijasida, foydalanuvchilar kirish jarayonida yengillikka ega bo'lmaydilar.

4. Moliyaviy va texnikaviy to'xtovsizlik: Xavfsizlikni ta'minlash uchun qo'llaniladigan texnikaviy vositalar va himoya usullari kengayganidek, bu jarayonning moliyaviy to'xtovsizlikni oshirishi mumkin. Xavfsizlik texnikalarini, xavfsizlik xizmatlarini va axborot sohasida mutaxassislar ishlarini tezlashtirish uchun moliyaviy resurslar va xarajatlar talab qiladi.

5. Tizimlar uchun ko'proq mas'uliyat: Xavfsizlik siyosati o'z ichiga tizimlarni va tashqi xavfsizlikni ta'minlashga oid qonunlar va qoidalar bilan ko'p mas'uliyatni solishni talab qiladi.

O’zbekiston Respublikasida “ Axborot xavfsizligining siyosati” qay tarzda qo’llaniladi.

O'zbekiston Respublikasida "Axborot xavfsizligining siyosati"ning amalga oshirilishi davlatning bir necha tartibga solinadigan qonunlar, nizomlar, vaqtlar va hukumat tomonidan tasdiqlangan strategiyalar asosida amalga oshiriladi. Bu siyosatning amalga oshirilishi O'zbekistonning axborot sohasida xavfsizlikni ta'minlash, ma'lumotlarni himoya qilish va muvaffaqiyatli tizimlar yaratishga qaratilgan tashkil etuvchi ishlar bilan birga amalga oshiriladi.

O'zbekiston Respublikasidagi "Axborot Xavfsizligining Siyosati"Ning Asosiy Yo'nalishlari Quyidagilardir

1. Xavfsizlik qonunlari va huquqiy asoslar: Axborot xavfsizligining siyosati, O'zbekiston Respublikasidagi axborot tizimlarining va xizmatlarning xavfsizlikni ta'minlash uchun qoidalar va nizomlar jadvalidini o‘z ichiga oladi. Bunda axborot xavfsizligi, axborotlar himoyasi, foydalanuvchilar huquqlari va boshqalar kabi mavzularni qamrab olgan qonunlar va qarorlar joriy etiladi.

2. Xavfsizlik tizimlarini ishlab chiqish va rivojlantirish: Axborot xavfsizligining siyosati O'zbekiston Respublikasida xavfsizlikning muvaffaqiyatli tashkil etilishi, sohalarda yaxshi xavfsizlik tizimlarini rivojlantirish va joriy etishga yo'naltiriladi. Bunda xavfsizlikni ta'minlash uchun yangi texnologiyalar, xavfsizlik vositalari, himoya tadbirlari va xavfsizlik kengaytirish sohalari rivojlantirilishi keng ko‘lamda o‘zlashtiriladi.

3. Axborot sohasida xavfsizlik bilan bog'liq xizmatlarni ta'minlash: Axborot xavfsizligining siyosati orqali, O'zbekistonda axborot sohasida xavfsizlik bilan bog'liq xizmatlarni ta'minlash, shuningdek, axborotni xavfsiz o‘tkazuvchi tashkilotlarni litsenziyalash va monitoring qilish amalga oshiriladi. Bu xizmatlar, xavfsizlik konsaltinqchilar, xavfsizlik xizmat provayderlari va shaxsiy axborot xavfsizligini ta'minlash sohasida faoliyat yurituvchi boshqa tashkilotlarni o‘z ichiga oladi.

O'zbekiston Respublikasida "Axborot xavfsizligining siyosati" Qonuni 2018 yil 10 iyunda qabul qilingan va 2021 yilning 1 iyunidan buyon kuchga kirgan.

Bu qonun, axborot xavfsizligining ta'minlash va himoyalash sohasidagi muammolarni hal qilish maqsadida yaratilgan va uning asosiy maqsadi O'zbekiston Respublikasida axborot xavfsizligining yuqori darajada ta'minlanishi va maxfiylikni ta'minlashdir.

Qonun, axborot tizimlarida foydalanuvchilar ma'lumotlarini maxfiy ko'rishni talab qiladi va bu maqsad uchun axborot tizimlarida foydalaniladigan qurilmalarning, vositalarning va texnologiyalar yoki xavfsizlik ta'minoti shakllarining qat'iylik bilan tekshirilishi va yaxshi holatga olib kelinishini talab qiladi.

Qonun Shu Jumladan Quyidagi Masalalarni Muqobil Qiladi

- Axborot tizimlari va foydalanuvchilar maxfiylikni ta'minlash;
- Maxfiylik xavfsizligini ta'minlash uchun zarur bo'lgan axborot tizimlarining, vositalarning, qurilmalar va texnologiyalarni yaratish va rivojlantirish;
- Axborot tizimlarida xavfsizlikni ta'minlashda foydalaniladigan vositalar va yondashuvlar;
- Xavfsizlikni ta'minlashda xizmat ko'rsatuvchilarning, foydalanuvchilarning va ma'lumotlarning xavfsizligini ta'minlashning qulayligi va ishonchliligi
- Xavfsizlikni ta'minlash bo'yicha o'qituvchi materiallar va o'quv dasturlar tayyorlash.

"Axborot xavfsizligining siyosati" qonuni O'zbekiston Respublikasida xavfsizlikni ta'minlashga doir qonunlar va qoidalar bilan birgalikda ishlab chiqilgan va o'zining ayriliqchaligi va majburiyatlari mavjud.

O'zbekiston Respublikasida "Axborot Xavfsizligining Siyosati" Quyidagi Tarzda Qo'llaniladi

1. Ma'lumot himoyasi: O'zbekiston Respublikasi "Axborot xavfsizligining siyosati" maqsadi, shaxsiy ma'lumotlarni, korporativ ma'lumotlarni, tashqi yozuvchilar va tashqi tizimlardan kelib chiqadigan ma'lumotlarni himoya qilishni ta'minlashdir. Ushbu siyosat orqali, ma'lumotlarni himoya qilish, ma'lumotlarga kirishni cheklash, ma'lumotlarni ifodalash va ma'lumotlarni uzatish vaqtini cheklashning qoidalarini o'z ichiga oladi.

2. Xavfsizlik sohasida qonunlar va qoidalar: O'zbekiston Respublikasi "Axborot xavfsizligining siyosati", axborot xavfsizligi sohasida amal qiladigan qonunlar, qoidalar va normativ hujjatlarni tasdiq etishni o'z ichiga oladi. Bu siyosat, xavfsizlikni ta'minlash uchun kerakli huquqiy mehanizmalarni va tartibotlarni ta'minlaydi.

3. Axborot xavfsizligini ta'minlash tashkilotlari: O'zbekiston Respublikasi "Axborot xavfsizligining siyosati" orqali, axborot xavfsizligini ta'minlash, monitoring qilish va to'xtatishning huquqiy va texnikaviy tashkilotlari belgilanadi. Bu tashkilotlar, axborot xavfsizligi sohasidagi tartibotlarni amalga oshirish, muammolar va xavfsizlik vaziyatlarini analiz qilish, vaqtni o'tkazish va javobgarliklarni bajarish bilan murojaat qilishni o'z ichiga oladi.

4. Foydalanuvchilar bilgilendirish va ta'limi: O'zbekiston Respublikasi "Axborot xavfsizligining siyosati" bilan, foydalanuvchilarni axborot xavfsizligi haqida ma'lumotlarni bilib olish va xavfsizlik talablarini tushunish bo'yicha ta'limga erishish ta'minlanadi. Bu orqali, foydalanuvchilar o'z axborotlarini xavfsiz saqlash va axborot almashish jarayonida to'g'ri amalga oshirishga imkon beriladi.

5. Xavfsizlikni nazorat qilish va rivojlantirish: O'zbekiston Respublikasi "Axborot xavfsizligining siyosati" xavfsizlikni nazorat qiladi.

XULOSA

Axborot xavfsizligining siyosati, O'zbekiston Respublikasi tomonidan belgilangan qonunlar, qoidalar, va tartibotlardan iboratdir. Bu siyosatning asosiy maqsadi, axborotlar va ma'lumotlar himoyalashini, xavfsizlikni ta'minlashni, foydalanuvchilar va tashqi tizimlardan kelib chiqadigan axborotlarni himoya qilishni ta'minlashdir.

O'zbekiston Respublikasi "Axborot xavfsizligining siyosati"ning asosiy qullayliklari quyidagilar bo'lishi mumkin:

1. Ma'lumot himoyasi: Siyosat maqsadi, shaxsiy ma'lumotlarni, korporativ ma'lumotlarni va tashqi yozuvchilar yoki tizimlardan kelib chiqadigan ma'lumotlarni himoya qilishni ta'minlashdir. Bu, foydalanuvchilar va korporativ tashkilotlar uchun ma'lumotlarning maxfiylik va xavfsizligini ta'minlashni ta'minlaydi.

2. Xavfsizlik tashkilotlari: "Axborot xavfsizligining siyosati" orqali, xavfsizlikni ta'minlash, monitoring qilish va to'xtatishning huquqiy va texnikaviy tashkilotlari belgilanadi. Bu tashkilotlar, axborot xavfsizligi sohasidagi tartibotlarni amalga oshirish, muammolar va xavfsizlik vaziyatlarini analiz qilish, vaqtni o'tkazish va javobgarliklarni bajarish bilan murojaat qilishni o'z ichiga oladi.

3. Foydalanuvchilar bilgilendirish va ta'limi: Siyosat orqali, foydalanuvchilarni axborot xavfsizligi haqida ma'lumotlarni bilib olish va xavfsizlik talablarini tushunish bo'yicha ta'limga erishish ta'minlanadi. Bu, foydalanuvchilarni axborotlarini xavfsiz saqlash va axborot almashish jarayonida to'g'ri amalga oshirishga imkon beradi.

4. Xavfsizlikni nazorat qilish va rivojlantirish: "Axborot xavfsizligining siyosati" axborot xavfsizligini nazorat qilish va rivojlantirishning asosiy qo'llaniladigan qoidalarini belgilaydi. Bu, xavfsizlik muammolarini aniqlash, ularni to'xtatish va mustahkamlash bo'yicha texnikaviy va huquqiy usullarni o'z ichiga oladi.

Axborot xavfsizligi, bugungi kunda bizning hayotimizda hamda iqtisodiyotimiz, siyosatimiz va ijtimoiy tizimimizning muhim qismi bo'lgan muhim muddalodir. Bu sababli, O'zbekiston Respublikasi "Axborot xavfsizligining siyosati"ni belgilab, axborotlarni himoya qilish, axborot xavfsizligi sohasida qonunlar va qoidalar o'rnatish, xavfsizlikni ta'minlash tashkilotlarini belgilash, foydalanuvchilarni ta'lim berish va axborot xavfsizligini nazorat qilish va rivojlantirish bo'yicha harakat qilishni maqsad qilgan.

Bu siyosatning muhim qullayliklari quyidagilar bo'ladi: ma'lumot himoyasi, qonunlar va qoidalar, xavfsizlikni ta'minlash tashkilotlari, foydalanuvchilar bilgilendirish va ta'limi, xavfsizlikni nazorat qilish va rivojlantirish.

Buning bilan birga, bu siyosatning kamchiliklari ham mavjud, masalan, bu siyosatning amal qilishi va bajarilishi uchun kerakli finansal resurslar yetarli emasligi, xavfsizlik tashkilotlarining yetersizligi va foydalanuvchilarning axborot xavfsizligiga qarshi ko'p yuzli va umumiy xatolar bilan ishlashlari mumkin. Shuningdek, qonun va qoidalar o'zgartirilganda, axborot xavfsizligi tashkilotlari, foydalanuvchilar va shaxslar uchun yangi huquqiy va texnikaviy tartibotlarni o'rganishga zarur bo'ladi.

Barcha bu muammolarga qarshi kurashish uchun, axborot xavfsizligi sohasidagi xalqaro hamkorliklar bilan ishlash, xavfsizlikning sarmoya bo'lishi, nazorat tizimlarini rivojlantirish va huquqiy tartibotlarni yangilash, shuningdek, foydalanuvchilarni axborot xavfsizligi sohasida ta'lim berish va bilgilendish hamda xavfsizlikning joriy vaziyatini nazorat qilish kabi harakatlar amalga oshirilishi kerak.

FOYDALANILGAN ADABIYOTLAR:

1. «Axborot texnologiyasi. Ma’lumotlami kriptografik muho- fazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari» O‘zbekiston Davlat standard. 0‘z DSt 1092:2005.

2. «Axborot texnologiyasi. Axborotlami kriptografik muhofazasi. Ma’lumotlami shifrlash algoritmi» 0‘zbekiston Davlat standard. 0‘zDSt 1105:2006

3. «Axborot texnologiyasi. Ochiq tizimlar o‘zaro bogMiqligi. Elek tron raqamli imzo ochiq kaliti sertifikati va atribut sertifikatining tuzil- masi» 0‘zbekiston Davlat standarti. 0‘zDSt 1108:2006.

4. С.В. Симонов. Анализ рисков в информационнмх систе- мах. Практические советь! // Конфидент. -2001. -№2.

5. S.S.Qosimov. Axborottexnologiyalari. 0‘quvqoMlanma. - T.: «Aloqachi», 2006.

6. S.K.G‘aniyev, M.M. Karimov. Hisoblash sistemalari va tar- moqlarida informatsiya himoyasi. Oliy o‘quv yurt.talab. uchun o‘quv qoMlanma. —Toshkent Davlat texnika universiteti, 2003.

7. Kosimova, A. (2022). MAIN FEATURES OF LANGUAGE LEARNING STRATEGIES. Eurasian Journal of Academic Research, 2(12), 1247-1249.
8. Kosimova, A. (2022). DRABBLLAR–KICHIK HAJMLI EPIK JANR. In INTERNATIONAL CONFERENCES (Vol. 1, No. 21, pp. 490-493).
9. Usmonova, D. S., & Muydinova, N. U. Phraseological Units with Proper Nouns in the English and Uzbek Languages. International Journal on Integrated Education, 4(2), 370-374.
10. Muydinova, N. (2020). DYNAMIC ACTIVITIES FOR SONG IN THE EFL CLASSROOM. In НАУКА И ТЕХНИКА. МИРОВЫЕ ИССЛЕДОВАНИЯ (pp. 11-13).
11. Муйдинова, Н. (2020). СОСТОЯНИЕ ВДОХНОВЕНИЯ У СПОРТСМЕНОВ. In Психологическое здоровье населения как важный фактор обеспечения процветания общества (pp. 112-113).