AXBOROTNI HIMOYALASH KONSEPSIYASI

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:*Axborotni himoyalash konsepsiyasi, axborotni nusxalash, saqlash, uzatish va foydalanish jarayonlarida uning xavfsizligini ta'minlashga yo'naltirilgan tizim va usullar to'plamidir. Bu konsepsiya ma'lumotlarni hujjatlardan, tarmoq orqali yuboriladigan xabar va ma'lumotlardan, shaxsiy ma'lumotlardan va boshqalardan himoya qilishni o'z ichiga oladi.*

Axborotni himoyalash konsepsiyasi yordamida, ma'lumotlar himoyalashning asosiy tamoyillaridan, masalan, konfidensiallik (ma'lumotlarning maxfiylik), bozorlik (ma'lumotlarning to'g'ridan-to'g'ri va to'liq bo'lishi) va integritet (ma'lumotlar bilan o'zgarishlarni aniqlash va ularga zarar yetkazishni oldini olish) bo'yicha xavfsizlikning ta'minlanishi hedeflangan.

Axborotni himoyalash konsepsiyasi tizimlarning ma'lumotlar bilan ishlash jarayonlarini, foydalanuvchilar orqali ma'lumotlarga kirishni, ularning kimligini tasdiqlashni va ma'lumotlarni himoya qilishni ta'minlashda asosiy qoidalarni va usullarni belgilaydi. Bu konsepsiya ma'lumotlarni shifrlash, autentifikatsiya protsesslari, nukusliklardan himoya, xavfsizlik ta'limi va tahlil, hujumlar va xavfsizlik holatlarini tahlil qilish va xavfsizlik siyosatini tashkil etish kabi muhim aspektlarni o'z ichiga oladi.

Axborotni himoyalash konsepsiyasi, korporativ tarmoqlar, internet-xizmat provayderlari, elektron biznes tizmlari va boshqa axborot tizimlari uchun asosiy bo'lib, ma'lumotlarni himoya qilish, tizimlarning xavfsizligini ta'minlash va foydalanuvchilarga xavfsizlikni ta'lim berishning muhim qismidir. Bu konsepsiya tizimlarga yuqori darajada xavfsizlik darajasini ta'minlash, hujumlar va nukusliklardan himoya qilish va foydalanuvchilarning ma'lumotlarga ishonchini oshirishga yordam beradi.

Kalit so'zlar: *Konfidensiallik,I ntegritet,Autentifikatsiy a,Shifrlash,Xavfsizlikta'limi,X avfsizlikan alizi Hujumlardan himoya,Ma'lumotlar tarqatish, Xavfsizlik siyosati,Vulnerabili tetlar.*

Abstract:*The concept of information protection is a set of systems and methods aimed at ensuring the safety of information in the process of copying, storing, transmitting and using it. This concept includes the protection of data from documents, messages and data sent over the network, personal data, etc.*

Using the concept of information protection, the main principles of data protection, for example, confidentiality (the confidentiality of data), marketability (the directness and completeness of data) and integrity (the It is aimed to provide security in terms of "identifying changes with data and preventing damage to them).

The concept of information protection defines the basic rules and methods for ensuring the processes of data processing of systems, access to data by users, confirmation of their identity and data protection. This concept includes important aspects such as data encryption, authentication processes, breach protection, security education and analysis, analysis of attacks and security situations, and the organization of security policies.

The concept of information security is fundamental to corporate networks, Internet service providers, e-business systems, and other information systems, and is an important part of data protection, system security, and user security education. This concept helps to provide systems with a high level of security, protect against attacks and malfunctions, and increase users' confidence in information.

Keywords:*Confidentiality, Integrity, Authentication, Encryption, Security Education, Security Analysis, Attack Protection, Data Distribution, Security Policy, Vulnerabilities.*

Gidronsiy bir afzallikni tashkil etayotgan barcha tarmoqlarda yuqori darajada axborotni himoya qilish muhim ahamiyatga ega. Hozirgi zamonaviy dunyoda tarmoq xavfsizligi kuchayib bormoqda va xavfsizlik muammolari hamda hujumlarni bartaraf etishda yanada ko'p muammolar va kamchiliklar paydo bo'lishi mumkin. Axborotni himoyalash konsepsiyasi, tizimlarning xavfsizligini ta'minlash, ma'lumotlarni himoya qilish, shaxsiy ma'lumotlarning maxfiyligini ta'minlash, hujumlar bilan kurashish va xavfsizlik siyosatini belgilash kabi muhim maqsadlarga yo'naltirilgan. Bu maqolada, axborotni himoyalash konsepsiyasining asosiy istiqbollari va ulardan qanday foydalanish haqida tafsilotlar beriladi.

Ma'lumotlarni shifrlash

Ma'lumotlarni shifrlash, axborotni himoya qilishning asosiy tamoyillaridan biridir. Shifrlash, ma'lumotlarni maxfiylik va konfidensiallikning asosiy belgisi sifatida himoya qilishda katta ahamiyatga ega. Shifrlash protokollari va algoritmlari, ma'lumotlarni yopishmasliklar va nukusliklardan himoya qilish uchun foydalaniladi. Bu protokollar va algoritmlar yordamida ma'lumotlar o'zgartirilganda, o'zgartirilganligini aniqlash va uni amalga oshirishning faqatgina ruxsat berilgan hodisalarda mumkin bo'lishini ta'minlash mumkin.

Identifikatsiya va autentifikatsiya

Identifikatsiya va autentifikatsiya, foydalanuvchilar va tizimlar orasidagi hamkorlikni boshqarishning asosiy qismlaridan biridir. Foydalanuvchilar tizimga kirish va ularga kirish ruxsatini berish uchun identifikatsiya va autentifikatsiya protsesslaridan o'tkazishlari talab qilinadi. Identifikatsiya, foydalanuvchini aniqlovchi ma'lumotlarni kiritishni va autentifikatsiya esa foydalanuvchining kimligini tasdiqlashni o'z ichiga oladi. Identifikatsiya va autentifikatsiya protsesslarining xavfsizligi, tizimlarda hujum va foydalanuvchi sababli xavfsizlik muammolari bilan kurashishda kerak.

Axborotni himoyalash konsepsiyasi (AHK) - bu maqsadga muvofiq ma'lumotlarni muvaffaqiyatli va xavfsiz tarzda amalga oshirish uchun o'z ichiga olgan tuzilish, huquqiy asoslar, protseduralar va tizimlarni ta'minlashning umumiy konsepsiyasi. AHK, kompyuter tarmoqqa aloqador ma'lumotlar, ma'lumot omborlari, internet, o'zaro aloqa tarmog'i va boshqa barcha axborot manbalari uchun amal qiladi.

AHK, kompyuter tarmoqlarida ma'lumotlarni himoyalashga qaratilgan tartib va hujumlar qarshi himoya tizimlarini o'rganish bilan boshlanadi. Bunday himoya tizimlarini amalga oshirishda, ma'lumotlar himoyalashida xavfsizlik, integritet va konfidensiallikning ko'rsatilgan standartlarga muvofiq ta'minlanishi kerak.

AHK tizimlarining amal qilishida ikki asosiy tamoyil mavjud: birinchisi, tarmoqdagi xavfsizlik nukusliklarini aniqlash va ularni bartaraf qilish, ikkinchisi, hujumlar va kiber-hujumlar bilan kurashish uchun tizimga xavfsizlik qo'shimchalari. AHK, ma'lumotlarni shifrlash, autentifikatsiya va tarmoqdagi nukusliklarni to'g'rilash uchun barcha ko'rsatmalarni taqdim etadi.

AHK tizimlarining amal qilishi, hech qanday axborotni o'z ichiga olgan tizimda amal qilishning muhim komponenti sifatida qaralganligi bilan, bu tizimlarning ishlashida muvaffaqiyatga erishishning yaxshi usullaridan biri hisoblanadi. AHK, tarmoqdagi ma'lumotlar va tarmoqdagi faoliyatlarga ta'sir ko'rsatadigan barcha imkoniy nukusliklarga qarshi himoya tizimlarini o'rganish, ularga qarshi kurashish va hujumdan himoya tizimlarini amalga oshirishda ko'rsatilgan standartlarni amalga oshirishni ta'minlaydi.

AHK-ni amalga oshirish, tizimlarda tashkil etilgan barcha axborot manbalari uchun muhimdir. Ma'lumotlarni himoyalash, barcha sohalarda qo'llaniladigan maqsadga muvofiq axborotni himoya konsepsiyasining boshqa muhim tushunchalarini tashkil etadi. Bu tushunchalar, tizimlarni xavfsizlikdan himoya qiladi.

Axborotni himoyalash konsepsiyasi - Bizning Digiral Dunyoda Ehtiyacimiz Olan Asosiy Muhofaza

Dasturlash, elektronika va internetning hujjatlar orqali ahamiyatli axborotlar, shaxsiy ma'lumotlar va kompaniya sirli ma'lumotlari o'z ichiga oladi. Bu esa, axborotni himoyalash konsepsiyasining kuchayishini va xavfsizlik muammolari o'rtasidagi zaruriyatni ko'rsatadi.

Axborotni himoyalashning mohiyati, muhim axborotlarni hujjatlarda, serverlarda yoki bulut xizmatlarida xavfsiz saqlash, yetkisiz erişimni oldini olish, axborotni shifrlash,kimlikni tasdiqlash va hackerning sergakini oldini olishni o'z ichiga oladi. Bu asosiy muhofazalar bilan birga, axborotni himoya qilish konsepsiyasi kompaniyalar uchun keyingi afzalliklarni taqdim etadi:

1. Maxfiylikni himoya qilish: Axborotni himoyalash konsepsiyasi, kompaniyalar uchun maxfiy axborotlarni himoya qilishga imkon beradi. Bu, kompaniyalar uchun xavfsizlikdan boshqa, raqamli maxfiylikni ta'minlash imkoniyatini beradi.

2. Kimlikni tasdiqlash: Axborotni himoyalash, axborotga kirishda kimlikni tasdiqlash mehanizmlari orqali yolg'on kirishni oldini olishga imkon beradi. Bu, kompaniya

xodimlariga yolg'onlik bilan kirishni oldini olish va uning joriyligini ta'minlash imkoniyatini beradi.

3. Veri g'oyasi: Xavfsizlik konsepsiyasi, axborotlarni shifrlash va g'oyaviylashtirishni o'z ichiga oladi. Bu, kompaniya maxfiy ma'lumotlarini xorijiy etkazib berish, hujjatlarni o'zgartirish va shaxsiy ma'lumotlarni yuborish kabi xavfli amallarni oldini olish imkoniyatini beradi.

4. Xavfsizlikni ta'minlashning xususiyatlari: Axborotni himoyalash konsepsiyasi, xavfsizlik o'rnini ta'minlashga xususiyatlar bilan ta'minlanadi. Bu, hech qanday xavfsizlik masalalari paydo bo'lmaganligini anglatadi va kompaniya hamjamiyatiga xavfsizlikni katta ahamiyat berishga imkon beradi.

Axborotni himoyalash, hozirgi kunda IT sohasida juda muhim masalalardan biridir. Bu tizimlar barcha mavzularda xizmat ko'rsatish uchun ishlatiladi, ammo ularning muhim nuqtasi xavfsizligi. O'zimizning shaxsiy ma'lumotlari, bank karta ma'lumotlari, va boshqa maxfiy axborotlarimizni Internet yoki boshqa tarmoqlarda o'tkazganimizda, ularni himoyalashning zaruriyati tushunarli bo'ladi.

Axborotni himoyalash konsepsiyasi, faqat maxfiy axborotlarni himoyalashga o'xshash yo'lga asoslangan emas, balki o'z ichiga boshqa ko'rsatkichlarni ham o'z ichiga oladi. Masalan, bir katta kompaniyada, bitta departament boshqasi tomonidan yuborilgan axborotlarga kirish imkonini olmasligini taminlashda ham axborotni himoyalash konsepsiyasi ishlatiladi.

Axborotni himoyalash konsepsiyasi xavfsizlikni yuqori darajada ta'minlash imkonini beradi. Maxfiy axborotlarimizni xorijiy ta'qib qiluvchilar yoki xakerlar tomonidan o'zlashtirilishidan qochish uchun, bizning ma'lumotlarimizni himoya qilishning ko'p o'rinlari mavjuddir. Bunda, axborotni himoyalash konsepsiyasi yordamida, ma'lumotlarimizni himoya qilish uchun maxsus protokollarni ishlatish mumkin.

Biroq, axborotni himoyalash konsepsiyasini amalga oshirish ham muammo bo'lishi mumkin. Bu tizimlarning yaxshi ishlaydigan xavfsizlik protokollariga ega bo'lishi kerak, ammo, hozirgi kunda, insonlarning o'zlarining maxfiy axborotlarini qanday qilib himoya qilishlarini aniqlashga qodir emaslar. Shuning uchun, axborotni himoyalash konsepsiyasi xavfsizligi ko'paytirish uchun doimiy ravishda yangilanishi lozim.

Tabiiy, axborotni himoyalash konsepsiyasi, verilarni himoya qilish va ularga o'zgartirishsiz kirishga qarshi himoya ta'minlashga asoslangan strategiya va usuldir. Bu, ma'lumotlarni to'g'ri va butunligini saqlayish, faqat ruxsat etilgan shaxslarning ularga kirish imkoniyatini berish, degan ma'noni anglatadi. Buning uchun murakkab himoya chora-tadbirlari va texnologiyalardan foydalaniladi, masalan, kuchli shifrlash algoritmlari, shaxslarni tasdiqlash mehanizmlari, xavfsizlik devorlari, xavfsizlik tushunmasi tizimlari va hokazo. Axborotni himoyalash konsepsiyasining asosiy maqsadi - ma'lumotlarni himoya qilishdir. Bu, ma'lumotlarni to'g'ri, butunligi saqlanib, faqat ruxsat etilgan shaxslar tomonidan kirishga ruxsat berilgan holatda saqlash ma'nolarini o'z ichiga oladi. Bu uchun turli xavfsizlik chora-tadbirlari va texnologiyalardan foydalaniladi, misol uchun kuchli

shifrlash algoritmlari, kimlikni tasdiqlash vositalari, xavfsizlik devorlari, to'qnashuvni aniqlash tizimlari va boshqalar.

Axborotni himoyalash konsepsiyasining bir qancha afzalliklari mavjud. Birinchidan, ma'lumotlar xavfsizligini ta'minlaydi va bu hamkorlarga va mijozlarga muhim ishonch ko'rsatadi. Mijozlar, shaxsiy va moliyaviy ma'lumotlarining himoyalangan bo'lishini biladigan kompaniyani qo'llashadi. Shuningdek, ma'lumot himoyalash qonunlari va tartiblari bilan mos bo'lish, kompaniyalarga qonuniy javobgarliklarini bajarishlariga yordam beradi.

Lekin, axborotni himoyalash konsepsiyasining bir qancha qiyinchiliklari ham mavjud. Birinchidan, bu turiy xavfsizlik chora-tadbirlari uchun to'lov qilish kerak. Maxsus dasturlar va qurilmalar sotib olinishi, xavfsizlik mutaxassislarini ishga olganlik va doimiy yangilanishlar kiritilishi zarur bo'ladi. Bu, kompaniyalarga qo'shimcha xarajatlar keltiradi.

Shuningdek, axborotni himoyalash konsepsiyasi murakkab bo'lishi mumkin. Xavfsizlik protokollari, shifrlash usullari va kimlikni tasdiqlash jarayonlari, texnik bilimlarni himoyalaydi.

Afzalliklari:

1. Veri Himoyasi: Axborotni himoyalash konsepsiyasi, axborotlarni himoya qilish va yetkazib berishning ishonchli va himoyalangan bo'lishini ta'minlaydi. Bu, ma'lumotlarni noaniq kirish, yo'qotish yoki o'zgartirishlardan himoya qiladi.

2. To'g'ridan-to'g'ri xizmat: Xavfsiz axborot tizimlari, o'z foydalanuvchilari uchun etkazib berish jarayonini himoya qilib turadi. Bu, foydalanuvchilar uchun xizmatning ishonchli va ishonchli bo'lishini ta'minlaydi.

3. Ijtimoiy ishonch: Himoyalangan axborot tizimi, mijozlar orasida ishonch va etiborini oshiradi. Mijozlar o'zlarining ma'lumotlarini himoyalangan shirkatlarni afzal ko'radilar va ularga ishonch bilan yondashishadi.

4. Huquqiy to'g'ri kelish: Axborot himoyasini ta'minlash konsepsiyasi, ma'lumot himoyasi va maxfiyligiga rioya qilishga yordam beradi va shirkatlarga qonuniy talablarni bajarmasliklariga yordam beradi.

5. Rekabet avantajlari: Xavfsiz axborot tizimi shirkatlarga rekabet avantajini ta'minlayishi mumkin. Mijozlar, ma'lumotlarining xavfsizligini ta'minlayuvchi shirkatlarni tanlashadi va bu shirkatlar yangi mijozlarni jalb qilish va mavjud mijozlarni o'zlarida saqlashni osonlashtiradi.

Kamchiliklar:

1. Kostnog'tirish: Xavfsizlik chora-tadbirlari, ushbu axborot tizimlarini qurish va saqlash uchun qo'shimcha xarajatlarni talab qiladi. Xususan, kichik tadbirkorlik uchun ushbu xarajatlar yuqori bo'lishi mumkin.

2. Qiyinchilik: Axborot himoyasi, murakkab texnologiyalar, protokollar va tartiblarga ega bo'lishini talab qiladi. Bu, amalga oshirish, boshqarish va yangilash jarayonlarini murakkablashtirishi mumkin.

3. Foydalanuvchi tajribasi: Xavfsizlik chora-tadbirlari, foydalanuvchilarga qo'shimcha xatlar va jarayonlarni talab qilishi mumkin.

XULOSA

Axborotni himoyalash konsepsiyasi, ma'lumotlarni himoya qilish va yetkazib berishning asosiy prinsiplarini o'z ichiga oladi. Bu konsept, axborot sistemlaridagi xavfsizlik muammolarini hal qilish uchun qo'llaniladigan usullar va strategiyalardan iboratdir.

Axborotni himoyalash konsepsiyasining asosiy maqsadi, ma'lumotlar to'g'risidagi, butunligidagi va maxfiyligidagi xavfsizlikni ta'minlashdir. Bu maqsadni erishish uchun quyidagi asosiy tamoyillar va usullar muhim ahamiyatga ega:

1. Kimlik tasdiq etish va huquqiy qo'llanma: Ma'lumotlarga kirishni tasdiq etish uchun foydalanuvchilarning kimlik tasdiq etish va huquqiy qo'llanmani qo'llash zarur. Bu, faqat ruxsat etilgan foydalanuvchilaring ma'lumotlarga kirishi mumkin bo'lishini ta'minlaydi.

2. Ma'lumotni shifrlash: Ma'lumotlar shifrlanishi, ularning o'qilmaydigan shaklga keltirilishi demakdir. Bu usul orqali ma'lumotlar xavfsizlikda saqlanib, uzatilishi mumkin bo'ladi.

3. Xavfsizlik ehtiyojlarini baholash va xavfsizlik duvari: Xavfsizlik ehtiyojlarini aniqlash, tahlil qilish va ularni amalga oshirish uchun xavfsizlik duvarlaridan foydalanish kerak. Xavfsizlik duvarlari, tarmoq trafikini monitoring qiladi va noaniq kirishlarga qarshi himoya ta'minlaydi.

4. Ma'lumotlar tiklanishi va tiklashi: Ma'lumotlar regulyar ravishda tiklanishi va tiklashi, ma'lumot yo'qotilganida ham tiklangan ma'lumotlarni tiklash imkoniyatini beradi.

5. O'zgartirishlar va yangilanishlar: Xavfsizlik hotiralaridagi o'zgarishlar sababli, xavfsizlikni ta'minlash usullarini doimiy yangilab borish zarur. Bu, yangi xavfsizlik og'irligi va muammo darajalariga qarshi himoya ta'minlaydi.

Axborotni himoyalash konsepsiyasi, ma'lumotlarning himoyalashini oshiradi, mijozlarga ishonch va muvaffaqiyat hissiyatini beradi. Shirkatlar uchun rivojlanish imkoniyatlarini oshiradi va yasal talablar bilan muvofiqlikni ta'minlayadi. Biroq, bu konseptning bazi qiyinchiliklari ham mavjud bo’ladi.

FOYDALANILAGAN 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).