AXBOROT HIMOYASINING STRATEGYASI VA ARXITEKTURASI

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 himoyasining strategiyasi va arxitekturasi, bir tashqi va ichki tahlillar yig'indisi hisoblanadi va tizimni hech kim tomonidan kirishga imkon bermaydigan xavfsizlikni ta'minlash uchun kerakli yo'nalishlarni aniqlaydi. Bu strategiya va arxitektura, ma'lumotlar sistemining boshqarishini, axborot resurslarining himoyalanishini, xavfsizlikning ta'minlanishini va uning zararlilarga qarshi qilinishini o'z ichiga oladi.Strategiya va arxitektura, quyidagi asosiy xususiyatlarga ega bo'ladi*

1. Kirish nazorati: Axborot himoyasi strategiyasi va arxitekturasi, tizimga kirish va tizimdan chiqishlar uchun nazoratni ta'minlaydi. Bu, autentifikatsiya protsedurasi, parol nazorati, biometrik ma'lumotlar, otentifikatsiya vositalari kabi qurilmalarni o'z ichiga oladi.

2. Ma'lumot himoyasi: Axborot himoyasi strategiyasi va arxitekturasi, ma'lumotlar himoyasini ta'minlashga yordam beradi. Bu, ma'lumotlarning shifrlanishi, xavfsizlik krishtal qatori (SSL) protokollari, ma'lumotlar saqlanadigan serverlarning xavfsizligi va saqlash xavf-xatarlari kabi qo'llanmalar bilan amalga oshiriladi.

3. Xavfsizlik sohalarini aniqlash: Strategiya va arxitektura, tizimdagi xavfsizlik kamchiliklarini aniqlash, ta'limotlarni yig'ish va zararli dasturlarni aniqlash uchun qo'llanmalarni o'z ichiga oladi. Bu, zararli faollanishlarni avtomatik ravishda aniqlash, ushbu faollanishlarni to'xtatish va zararli dasturlarni izoli qilishni o'z ichiga oladigan zararli dastur izlantiruvchilarni o'z ichiga oladi.

4. Talablar va nazorat: Strategiya va arxitektura, axborot himoyasining talablari va nazorat jarayonlarini aniqlaydi. Ushbu talablar tizimga kirish, tizimdan chiqish, ma'lumotlarga kirish va chiqish, ma'lumot almashinuvi va saqlash jarayonlariga ega bo'ladi.

5. Tartibga solish va tartibga solishtirish: Axborot himoyasining strategiyasi va arxitekturasi, ma'lumotlar va tizim elementlarining to'g'ridan-to'g'ri foydalanishini ta'minlaydi.

Kalit so'zlar:*Xavfsizlik, himoya,autentifikatsiya,shifrlash, xavfsizlik nazorati,zararli dasturlar, ma'lumot almashinuvi,nazorat, xavfsizlik protokollari,zararli faollanishlar,shaffoflik,nafazalar, ijtimoiy axborot himoyasi,nizomlash,. xavfsizlik ta'limoti.*

Abstract:*The strategy and architecture of information protection is a set of external and internal analyzes and determines the necessary directions to ensure security that does not allow anyone to access the system. It includes strategy and architecture, information system management, protection of information resources, security and anti-malware.*
Strategy and architecture will have the following key features:

1. Access Control: The information security strategy and architecture provides controls for system logins and logouts. This includes devices such as authentication procedures, password controls, biometrics, and authentication tools.

2. Data protection: Information protection strategy and architecture help ensure data protection. This is done with guidelines such as data encryption, Secure Sockets Layer (SSL) protocols, security of servers where data is stored, and storage risks.

3. Identifying Security Areas: Includes guides to strategy and architecture, identifying system security vulnerabilities, gathering intelligence, and detecting malware. This includes malware scanners that automatically detect malicious activations, stop those activations, and isolate malware.

4. Requirements and controls: The strategy and architecture define information security requirements and control processes. These requirements will have processes for logon, logoff, data access and output, data exchange and storage.

5. Regulation and regulation: The strategy and architecture of information protection ensures the direct use of data and system elements.

Key words:*Security, protection, authentication, encryption, security control, malware, information exchange, control, security protocols, malicious activations, transparency, breaths, social information protection, regulation. security doctrine.*

KIRISH

Axborot himoyasi, bugungi global xavfsizlik ko'lamida muhim ahamiyatga ega bo'lgan mavzu. Axborot tizimlarida o'zgaruvchan texnologiyalar, tashqi va ichki xavfsizlik xavf-xatarlarini oshirib borayotgan va zararlilar uchun potentsial yo'lovchilarni yaratadigan muhitlar mavjud. Bu haqda o'ylash, axborot himoyasining strategiyasi va arxitekturasi muhim bo'lgan ehtimollar yaratdi. Bu maqolada, axborot himoyasining strategiyasi va arxitekturasi haqida o'zbek tilida tushunchani tahlil qilamiz.

Maqsad va Umumiy Tartib:

Axborot himoyasining strategiyasi va arxitekturasi, ma'lumotlarning himoyalanishi va axborot tizimlarining xavfsizligini ta'minlash maqsadida yaratilgan tartibdir. Ushbu strategiya, tizimga kirish, ma'lumot almashinuvi, saqlash, uzatish va tizimdan chiqish jarayonlarida xavfsizlikni ta'minlaydi. Bu muhim tartib, xavfsizlik protokollari, zararli dasturlar, shifrlash, autentifikatsiya va nazoratning bir qator vositalari bilan amalga oshiriladi.

Strategiya va Arxitektura Asosiy Ko'rsatkichlari:

1. Xavfsizlik Protokollari: Axborot himoyasining strategiyasi va arxitekturasi, xavfsizlikni ta'minlash uchun o'rganilgan protokollardan foydalanishni talab qiladi. SSL (Xavfsizlikning Ta'minlanishi uchun Secure Socket Layer) protokollari, ma'lumotlar almashinuvini shifrlab o'tkazish va ta'minlashda muhim ahamiyatga ega.

2. Zararli Dasturlar va Zararli Faollanishlar: Strategiya va arxitektura, zararli dasturlar va zararli faollanishlarni aniqlash, ularga qarshi qilish va ularning zararlarini cheklashda

avtomatik vositalardan foydalanadi. Bu vositalar, zararli kodlar va atakalarni identifikatsiya qilish, tahlil qilish va ularga javob berishga yordam beradi.

3. Ma'lumot Himoyasi: Axborot himoyasining strategiyasi va arxitekturasi, ma'lumotlarni shifrlab olish, maxfiylash, nafaqat tizim ichidagi o'lchovda, balki tashqi aloqalarda ham himoyalanadi.

Axborot himoyasi, bizning hayotimizning har bir sohasida o'z o'rnatilishini ko'rsatib turayotgan ahamiyatli mavzu bo'lib, muammolar va tahlillar yig'indisi hisoblanadi. Bizning kundalik faoliyatimiz, kompyuterlar, mobil qurilmalar, tarmoqlar va internet orqali amalga oshiriladi. Bu esa bizning ma'lumotlarimizning, xavfsizligimizning va xavfsizliklarni ta'minlash strategiyamizning ahamiyatini ko'rsatadi.

Axborot himoyasining strategiyasi va arxitekturasi, tizimni tashqi va ichki xavfsizlikga qarshi himoya qilish, ma'lumotlar almashinuvi va saqlashning himoyalashini ta'minlashga yo'naltirilgan. Bu strategiya va arxitektura, bizning tizimlardagi xavfsizlik xavf-xatarlarini, zararli faollanishlarni va ma'lumotlarimizga kirishga urinishni to'xtatish uchun zarur qo'llanmalarni o'z ichiga oladi.

Biroq, strategiya va arxitekturani to'g'ri rivojlantirish uchun dastlab bizning xavfsizlik ehtiyojlarni tahlil qilish zarur. Bunda bizning tizimlardagi muhim ma'lumotlarni, shu jumladan foydalanuvchilar haqidagi ma'lumotlarni, tizimga kirish protsedurini, ma'lumotlar almashinuvi va saqlashni hisobga olamiz.

Strategiya va arxitekturani belgilashda quyidagi asosiy ko'rsatuvlar ahamiyatga ega:

1. Tahlil: Axborot himoyasining strategiyasi va arxitekturasi belgilanishidan oldin, tahlil qilish zarur. Bu maqsad bilan bizning tizimimizning xavfsizlik holatini, muhim foydalanuvchilarimiz va ularga tegishli ma'lumotlarni identifikatsiya qilish uchun tahlil qilamiz.

2. Xavfsizlik protokollari: Xavfsizlikni ta'minlash uchun xavfsizlik protokollari va standartlari ishlatiladi. Bu protokollar, shifrlash, autentifikatsiya, yetkazib berish va to'xtatishning turli ko'rsatkichlarini o'z ichiga oladi.

3. Xavfsizlik sohalarini ta'riflash: Strategiya va arxitektura, tizimdagi xavfsizlik sohalarini aniqlaydi. Bu shaxsiy ma'lumotlarga kirish, tizim ustidan foydalanuvchilar nazor

Axborot himoyasi har qanday tashkilotda juda muhimdir, chunki hozirgi zamon ma'lumotlar va internet dunyosida, hamma tashkilotlarda o'z mijozlari yoki foydalanuvchilari bilan aloqalar o'rnatilgan. Bu aloqalar orqali mijozlar, tashkilotlarning faoliyatini oshirishi, ma'lumotlar almashish va ularga kirish uchun avvalgi davrlarga nisbatan ko'proq imkoniyatlarga ega bo'lishdi. Shuning uchun, axborot himoyasi muhimdir, chunki, hujjatlar, ma'lumotlar, ishonchli axborot, mijozlar haqida maxfiy axborot va boshqa ma'lumotlar kabi ko'plab ma'lumotlar mavjud.

Axborot himoyasining strategiyasi va arxitekturasi tashkilotning xavfsizlikni ta'minlash va maxfiylikni saqlashning tizimi va protsedurasi sifatida tan olish uchun keraklidir. Strategiya va arxitektura, tashkilotning axborot tizimini qayta ko'rgan, uni rivojlantirgan va

maxfiylikni ta'minlash uchun zarur elementlarni qo'shgan strategiya va arxitektura standartlaridir.

Axborot himoyasining strategiyasi va arxitekturasi, ma'lumotlarni yaxshilash, qo'llash va tarqatish uchun imkon beradi. Bu strategiya va arxitektura, tashkilotning qo'shimcha axborot himoyasi talablari bilan tan olinishi kerak. Bunday talablar tashkilotning xavfsizlik, yozuvchilarining ma'lumotlari bilan ishlash va yig'ilish qobiliyatini oshirish, tizim nazorati va ma'lumot almashinuvi kabi tizimlar uchun zaruriy bo'ladi.

Axborot himoyasining strategiyasi va arxitekturasi yaxshi nazorat tizimini ta'minlash uchun ham keraklidir. Nazorat tizimlari, tizimda yuzaga keladigan xavfsizlik muammo va hujjatlarni aniqlash va hal qilishga imkon beradi. Ma'lumot almashinuvi, zararli dasturlarni aniqlash, xavfsizlikning oshirilishi, xavfsizlikning nazorati va xavfsizlikni ta'minlash uchun zarur barcha protseduralar va vositalar ko'rsatiladi.

Bular hammasi, axborot himoyasining strategiyasi va arxitekturasi talablari bilan tan olinadi. Ma'lumot almashinuvi tizimlarida, xavfsizlikning yuqori darajasini ta'minlash uchun zaruriy bo'lgan barcha vositalar kiradi.

"Axborot Himoyasining Strategiyasi va Arxitekturasi: Ma'lumotlar Xavfsizligini Ta'minlash"

Axborot himoyasi bugungi kunda bizning hayotimizning asosiy bir qismiga aylandi. Aholi, tashkilotlar va hukumatlar har kuni millionlab odamlar tomonidan ishlatilayotgan axborot tizimlariga bog'liq ma'lumotlarni himoya qilishga e'tibor qaratmoqda. Bu kabi ma'lumotlar, shaxsiy axborotlar, korporativ ma'lumotlar, va davlat sirli axborotlarini o'z ichiga oladi. Shuning uchun, axborot himoyasining strategiyasi va arxitekturasi muhim ahamiyatga ega.

Axborot himoyasining strategiyasi va arxitekturasi, axborot tizimlarini, ma'lumotlarini, va ulardan foydalanuvchilarni himoya qilishga yo'naltirilgan jamoatchilik tadbirlarining jamiyati hisoblanadi. Ushbu strategiya va arxitektura, tizimga kirish, ma'lumot almashinuvi, saqlash, va tarqatish jarayonlarini himoya qilish uchun to'g'ridan-to'g'ri qo'llanmalar, usullar va protokollar jamiyatini qo'llab-quvvatlaydi.

Axborot himoyasi strategiyasi va arxitekturasi bazi muhim qo'llanmalarni o'z ichiga oladi. Birinchi navbatda, autentifikatsiya protseduralari va vositalari foydalanuvchilar tomonidan tizimga kirishni tasdiqlash uchun ishlatiladi. Bu protseduralar parollar, biometrik ma'lumotlar yoki boshqa usullar yordamida haqiqiylikni aniqlayishni ta'minlaydi.

Ikkinchi navbatda, ma'lumotlar himoyasi o'rniga shifrlash protokollari qo'llaniladi. Shifrlash usullari yordamida ma'lumotlar elektronik ravishda shifrlanib, faqatgina ma'lumotni tushunishiga ega bo'lganlar uchun oqish va tushirish imkonini beradi. Bunda SSL (Xavfsizlik katagi tashqi protokoli) protokolining muhim ahamiyati mavjud.

Uchinchi navbatda, xavfsizlik nazorati strategiyasi va arxitekturasi ma'lumotlarni himoya qilishga yo'naltirilgan xususiyatlarga ega. Ushbu nazorat jarayonida tizimga kirishlarni kuzatish, anomaliyalarni aniqlash va zararli dasturlarni to'xtatish muhim ahamiyatga ega.

"Axborot Himoyasining Strategiyasi va Arxitekturasi" Axborot himoyasi, bugungi kunda bizning hayotimizning asosiy qismi bo'ldi. Biz har kuni o'z ma'lumotlarimizni, identitetimizni, moliyaviy ma'lumotlarimizni va boshqa shaxsiy axborotlarimizni kompyuterlarda, telefonda yoki internet orqali saqlaymiz. Bu esa bizga yuqori darajada xavfsizlik va himoya talab qiladi. Shunday qilib, axborot himoyasining strategiyasi va arxitekturasi hayotimizdagi ma'lumotlarni nazorat qilish, himoyalash va xavfsizligini ta'minlashga yo'naltirilgan bo'lishi shart.

Axborot himoyasi strategiyasi va arxitekturasi, xavfsizlik sohasidagi eng yaxshi amaliyotlarni jamlagan va ularga amal qilishni o'rganishda muhim bo'ladi. Bu strategiya va arxitektura, ma'lumotlarga kirish huquqini cheklash, ma'lumotlarni shifrlash, autentifikatsiya protseduralarini o'rnatish va zararli faollanishlarni aniqlashni o'z ichiga oladi.

Strategiya va arxitekturada ma'lumotlarni shifrlashga katta ahamiyat beriladi. Shifrlash usullari orqali, ma'lumotlar maxfiy tarzda saqlanadi va faqatgina moslashtirilgan shaxslar uchun o'qimaydi. Bunda, tarqatuvchilar yoki noqonuniy shaxslar ma'lumotlarga kirishga urinishni to'xtatiladi. Autentifikatsiya protsedurasi esa foydalanuvchilarning haqiqiyligini tasdiqlaydi. Bu, parollar, biometrik ma'lumotlar, kimlikni tasdiqlovchi sertifikatlar va boshqa autentifikatsiya vositalarini o'z ichiga oladi.

Zararli faollanishlarni aniqlash ham muhim tizim qismi hisoblanadi. Bu faollanishlar, viruslar, malware, hakerlar va boshqa zararli dasturlar orqali tizimni xavfsizligini ogohlantirishi mumkin. Strategiya va arxitektura, zararli faollanishlarni aniqlash, uning tarqatuvchi vositalarni tanishuv etish va ularni isolatsiya qilish jarayonlarini o'z ichiga oladi.

Axborot himoyasining strategiyasi va arxitekturasi shuningdek, tizimga kirish va chiqishlar, ma'lumot almashish jarayonlari, ma'lumotlarni saqlashning xavfsizligi, tizim foydalanuvchilarining xavfsizligini ta’minlaydi.

"Axborot Himoyasining Strategiyasi va Arxitekturasi"

Axborot himoyasi, bizning hozirgi asrning muhim tajribadir. Har kuni katta miqdorda ma'lumotlar yaratiladi, uzatiladi va saqlanadi. Bu ma'lumotlar, shaxsiy ma'lumotlardan korporativ ma'lumotlarga, ilmiy tadqiqotlaridan biznes axborotlariga qadar turli sohalar bo'yicha bo'lishi mumkin. Shuningdek, ma'lumot almashinuvi va tizimlar o'rtasidagi bog'lanish, tarmoq axborotlarining kengayishi va internetning rivojlanishi, axborot himoyasini ham muhim muammo qilmoqda.

Axborot himoyasining strategiyasi va arxitekturasi, bu muammo va xavf-xatarlarga qarshi qilinish uchun xususiy yo'nalishlar va tahlillar yig'indisi hisoblanadi. Bu strategiya va arxitektura, ma'lumotlar, axborot resurslari va tizimlarni himoya qilishning integral qismlari sifatida ishlaydi. Ular, tizimga kirishga urinish, ma'lumotlarni saqlash va ularga kirish, ma'lumot almashinuvi, xavfsizlik monitoringi va zararli faollanishlarni to'xtatish kabi jarayonlarni o'z ichiga oladi.

Birinchi navbatda, tizimga kirish va autentifikatsiya muammolari hal qilinadi. Bu, foydalanuvchilarning kimligini tasdiqlash, parollar, biometrik ma'lumotlar, ikki bosqichli

autentifikatsiya protseduralari va boshqa usullar orqali amalga oshiriladi. Ma'lumotlar himoyasiga muvaffaqiyatli kirish, yoki hujjatlar, ma'lumotlar yoki tizimlarga bo'lgan kirishlar tomonidan talon bo'lish muammosini yechishni ta'minlaydi.

Keyingi bosqichda, ma'lumotlar shifrlanadi va himoyalangan saqlash tizimlari bilan himoyalanadi. Bu, maxfiylik protokollari, SSL (Shifrlangan Soket Layer) kabi xavfsizlik qo'llanmalari va ma'lumotlar saqlash serverlari uchun maxfiylik tamoyillari orqali amalga oshiriladi. Shuningdek, ma'lumotlar almashinuvi jarayonlarida shifrlash, axborotlar o'rtasida yuborish va qabul qilish jarayonlari xavfsizlik protokollariga asoslangan.

Bundan tashqari, strategiya va arxitektura zararli faollanishlarni aniqlash va ular bilan kurashishga imkon beradi.

Axborot himoyasining strategiyasi va arxitekturasi

Axborot himoyasi, bugungi kunda bizning hayotimizning asosiy juzjiga aylanib kelgan muhim muddatli muammoni tashkil etadi. Har kuni o'zimizning shaxsiy ma'lumotlarimiz, tashqi va ichki tadbirlarimiz, pul mablag'larimiz va boshqalar kabi axborotlar orqali munosabatlarni amalga oshirayotganimizga shahodat etamiz. Shuningdek, hukumatlar, korporatsiyalar va boshqalar ham o'z ma'lumotlari va operatsiyalarini xavfsiz va himoyalangan holda saqlash va boshqarishga qiziqish ko'rsatadilar.

Axborot himoyasining strategiyasi va arxitekturasi, axborotni xavfsiz saqlash va uning ta'sirli foydalanishini ta'minlash uchun strategik rejalashtirish va texnik vositalar to'plamini ifodalaydi. Bu strategiya va arxitektura, xorijiy va ichki axborotlarga kirishni cheklash, ma'lumotlarni shifrlash, zararli dasturlarni aniqlash, nazorat va monitoring, foydalanuvchilar autentifikatsiyasi, ma'lumot almashinuvi, saqlash xavf-xatarlari, tarqatish protokollari va ko'plab boshqa jarayonlarni o'z ichiga oladi.

Axborot himoyasi strategiyasi va arxitekturasi, quyidagi asosiy qismatlardan iborat bo'ladi:

1. Tahlil va rivojlantirish jarayonlari: Axborot himoyasi strategiyasi, tashqi va ichki xavfsizlik holatini tahlil qilish, tizimning yaxlitligini o'rganish va uni rivojlantirish uchun kerakli o'zgarishlarni aniqlashni o'z ichiga oladi.

2. Xavfsizlik siyosati: Tashqi va ichki xavfsizlikning belgilangan siyosati va qoidalarini amalga oshirish.

3. Xavfsizlikning boshqa tashqi va ichki bo'limlar bilan integratsiyasi: Tizimdagi barcha bo'limlar o'rtasida xavfsizlikni ta'minlash uchun ko'rsatmalarni va doiralarini aniqlash.

4. Foydalanuvchilar autentifikatsiyasi: Foydalanuvchilar tomonidan tizimga kirishni tasdiqlash uchun xavfsiz autentifikatsiya protseduralarini amalga oshirish.

5. Shifrlash va maxfiylash: Ma'lumotlar va kommunikatsiya tarmog'ining shifrlanishi va maxfiylashining ta'minlanishi

Axborot himoyasining strategiyasi va arxitekturasi

Axborot himoyasi, bugungi kunda bizning hayotimizning jadal o'zgaruvchanligi bilan birga rivojlanayotgan muhim sohalaridan biridir. Xavfsizlikning o'ziga xos o'rniga ega bo'lgan, ma'lumotlarni himoya qilish va ularga kirishni cheklash uchun mo'ljallangan

stratejiya va arxitektura muhimdir. Bu maqolada axborot himoyasining strategiyasi va arxitekturasi haqida tafsilotlar beraman.

Axborot himoyasining strategiyasi, axborot tizimi va tashqi yo'l-yo'riq bilan bog'liq risklarni va xavf-xatarlarni tahlil qilish, ularga qarshi qilish uchun kerakli tahlil va chora-tadbirlarni aniqlash va tizimga kirish, tizimdan chiqish, ma'lumot almashinuvi va saqlash jarayonlarida xavfsizlikni ta'minlashni o'z ichiga olgan strategik qarorlar jamlanmasidir.

Bundan tashqari, axborot himoyasining strategiyasi, ma'lumotlarning himoyalanish darajasini belgilash, himoya standartlarini va qoidalarni belgilash, xavfsizlikning monitoring va nazorat jarayonlarini tartibga solish, ma'lumot almashinuvi va uzatishning xavfsizlik prinsiplarini aniqlash va xavfsizlikning moliyaviy va huquqiy aspektlarini qamrab oladi.

Axborot himoyasining arxitekturasi esa bir xil tizimning muhtasar tavsifidir. Bu arxitektura, tizimga kirish, ma'lumot almashinuvi, saqlash, ma'lumotlar bazasi va tashqi aloqalar bilan bog'liq barcha jarayonlarda xavfsizlikni ta'minlash uchun kerakli xususiyatlarni belgilaydi. Arxitektura, xavfsizlik protokollarini, autentifikatsiya va autorizatsiya vositalarini, shifrlash algoritmlarini, xavfsizlikning ta'limotlarini va zararli dasturlar bilan kurashish vositalarini o'z ichiga oladi.

Axborot himoyasining strategiyasi va arxitekturasi, tashqi va ichki xavfsizlikning ta'minlanishini amalga oshiradi. Ushbu strategiya va arxitektura, ma'lumotlarni himoya qilish, zararli dasturlarni aniqlash, xavfsizlikning nazorat va tartibga solishni ta'minlash kabi muhim vazifalarni o'z ichiga oladi.

Axborot himoyasining strategiyasi va arxitekturasi bilan bog'liq kalit so'zlar quyidagilardir:

1. Xavfsizlik: Strategiya va arxitektura asosiy maqsadiga erishish uchun xavfsizlikni ustunligi bilan ta'minlayadi.

2. Himoya: Strategiya va arxitektura, ma'lumotlar himoyasini ta'minlash, maxfiylash va qo'llab-quvvatlashga yo'naltirilgan.

3. Autentifikatsiya: Kirish huquqini va haqiqiylikni tasdiqlash uchun protseduralar va vositalar.

4. Shifrlash: Ma'lumotlarni shifrlash orqali himoyalash usuli.

5. Xavfsizlik nazorati: Tizimga kirishlarni nazorat qilish, nazoratni oshirish va anomaliyalarni aniqlash.

6. Zararli dasturlar: Zararli va noqonuniy dasturlarni aniqlash va uning ta'sirini cheklash.

7. Ma'lumot almashinuvi: Ma'lumotlarni xavfsiz tarzda almashish, saqlash va uzatish.

8. Nazorat: Tizimdagi xavfsizlik holatlarini monitoring qilish va tez-tez o'zgartirishlarni identifikatsiya qilish.

9. Xavfsizlik protokollari: Xavfsizlikning ta'minlanishini amalga oshirish uchun o'rganilgan protokollar va standartlar.

10. Zararli faollanishlar: Zararli faollanishlarni to'xtatish, ta'limotlarni yig'ish va o'chirish uchun xavfsizlik tahlillari va vositalari.

11. Shaffoflik: Tizimga kirishlarni anonim va shaffof ravishda bajarish.

12. Nafazalar: Tizimga kirish, foydalanuvchilar va ma'lumotlar uchun nafazalar.

13. Ijtimoiy axborot himoyasi: Ma'lumotlarni ijtimoiy xavfsizlik va axborot himoyasi prinsiplari asosida himoyalash.

14. Nizomlash: Ma'lumotlar va tizim elementlarining tartib va nizomini ta'minlash.

15. Xavfsizlik ta'limoti: Tizim foydalanuvchilariga xavfsizlik sohalarida ta'lim berish.

Bu kalit so'zlar, axborot himoyasining strategiyasi va arxitekturasining muhim ko'rsatkichlarini ta'riflashda ishlatilishi mumkin.

Axborot himoyasining strategyasi va arxitekturasi qullayliklari va kamchiliklari.

Axborot himoyasining strategiyasi va arxitekturasi, bir nechta qullayliklarga va kamchiliklarga ega. Ularni quyida ko'rib chiqamiz:

***Qullayliklar**:*

1. Ma'lumotlarning Himoyalangan Saqlash: Axborot himoyasining strategiyasi va arxitekturasi, ma'lumotlarni himoyalash va muhofaza qilish imkoniyatini beradi. Bu, foydalanuvchilar uchun ma'lumotlarning xavfsiz saqlash imkonini yaratadi.

2. Xavfsizlikning Ta'minlanishi: Strategiya va arxitektura, tizimning xavfsizligini yuqori darajada ta'minlaydi. Xavfsizlik protokollari, autentifikatsiya usullari va zararli dasturlar bilan kurashish, zararli faollanishlarni aniqlash va ularga qarshi qilish kabi qo'llanmalardan foydalaniladi.

3. Ma'lumot almashinuvi va biriktirish: Axborot himoyasining strategiyasi va arxitekturasi, ma'lumot almashinuvini va biriktirishni samarali va xavfsiz amalga oshirishga yordam beradi. Bu, ma'lumot almashinuvini himoyalash, ma'lumotlar bazalarini nazorat qilish va muhofaza qilish, ma'lumotlar o'rtasidagi almashishni himoyalash kabi muammolarni hal qilishni ta'minlaydi.

4. Nazorat va Javobgarlik: Strategiya va arxitektura, tizimning nazorat va javobgarlikni oshirishga imkon beradi. Xavfsizlik tahlillari, anomaliyalarni aniqlash, zararli faollanishlarni to'xtatish va zararli dasturlarni identifikatsiya qilish kabi vositalardan foydalanish orqali tizimning xavfsizlik holatlarini nazorat qilish va ularga tez va samarali javob berish imkonini beradi.

1. Xavfsizlikni Ta'minlash: Axborot himoyasining strategiyasi va arxitekturasi, ma'lumotlarni shifrlash, autentifikatsiya va nazoratning bir qator vositalari bilan himoyalashni talab qiladi. Ushbu tartib tizimlarga xavfsiz kirish imkoniyatini ta'minlaydi.

2. Atakalarni To'xtatish: Strategiya va arxitektura, zararli kodlarni aniqlash, tahlil qilish va ularga javob berishda qulay vositalardan foydalanadi. Bu sayda, ma'lumotlarni to'g'ridan-to'g'ri ochishga harakat qilish, shifrlash va maxfiylashni talab qilish kabi xavfsizlikni ta'minlaydigan vositalar kiritilgan.

3. Yuqori Darajadagi Ma'lumot Xavfsizligi: Axborot himoyasining strategiyasi va arxitekturasi, ma'lumot almashinuvi, saqlash, uzatish va tizimdan chiqish jarayonlarida

yuqori darajadagi xavfsizlikni ta'minlaydi. Bu tartib, ma'lumotlarni shifrlab olish va maxfiylash bilan bir qatorda, yaxshi nazorat va ko'rsatma bilan birlikda yoritadi.

g narxi katta bo'lishi mumkin.

Kamchiliklar:

1. Komplekslik: Axborot himoyasining strategiyasi va arxitekturasi kompleks bo'lib, uning tashqi va ichki qurilmalarning xavfsizlik talablari va zarur resurslarni talab qiladi. Ushbu komplekslik, tizimni o'rnatish, sozlash va boshqarish jarayonlarini murakkablashtirishi mumkin.

2. Xavfsizlik Vaqt-so'atlari: Strategiya va arxitekturani amalga oshirish va xavfsizlikni ta'minlash, qo'ng'iroq qiladigan vaqt, resurs va xarajatlarni talab qiladi. Xavfsizlikni o'zgartirish va yangilash jarayonlari tizimni band qiladi.

1. Texnologik Moddalar: Axborot himoyasining strategiyasi va arxitekturasi, tezroq o'zgaruvchan axborot tizimlari uchun ancha keng imkoniyatlarni taklif qiladi. Bunday tizimlarda xavfsizlikni ta'minlash va xavfsizlikni aniqlash qiyinlashadi.

2. Narx: Xavfsizlikni ta'minlashning ko'p vositalarini sotib olish, ulardan foydalanish, ma'lumotlar uchun qulay bo'lsa-da, bu vositalarning xafini ortiradi.

Bugungu kunda'' Axborot himoyasining strategyasi va arxitekturasi'' ga kiritilayor

tgan yangicha o'zgarishlar.

"Axborot Himoyasining Strategiyasi va Arxitekturasi" bo'yicha Bugungi Kunda Kiritilgan Yangilanishlar

Axborot himoyasi sohasida tez-tez yangilanishlar amalga oshiriladi, chunki zararlilarning va xavfsizlikga qarshi kurashadigan sovg'alarni yaratishlari ham doimiy ravishda davom etadi. Bugungi kunda "Axborot Himoyasining Strategiyasi va Arxitekturasi" sohasida quyidagilarni kiritilgan yangilanishlar ko'riladi:

1. Yagona Kirish Tizimi: Bizning zamonaviy dunyomizda, yagona kirish tizimlari, masalan, parol o'rniga biometrik identifikatsiya (qo'l izi, yuz tanishligi) va boshqalar kabi yangi texnologiyalar keng tarqalgan. Bu, foydalanuvchilar uchun xavfsiz va qulay kirishni ta'minlashga imkon beradi.

2. Sun'iy Intellekt va Machine Learning: Sun'iy intellekt (SI) va ma'lumotlar tahlili texnologiyalari, zararli faollanishlarni aniqlash va ularga qarshi kurashishning o'zlashtirilgan usullarini rivojlantirishda o'rnatilmoqda. Bu, zararli faollanishlarni oldini olish va xavfsizlikni oshirishning yanada efektiv usullarini beradi.

3. Bulut Computerning Kengayishi: Bulut kompyuterlik xizmatlarining ommalashtirilishi, tashqi serverlar va ma'lumotlar bilan ishlashda yangi imkoniyatlarni yaratmoqda. Axborot himoyasining strategiyasi va arxitekturasi bu yangilanishlarga mos keladigan xavfsizlik protokollari va ko'rsatkichlarni o'zgartirishni talab qiladi.

4. Internet of Things (IoT): IoT qurilmalari sonining kengayishi bilan, qurilmalar orasidagi ma'lumot almashinuvi va ularga xavfsizlikni ta'minlash ham muhim bo'lgan mavzular bo'ldi. Axborot himoyasining strategiyasi va arxitekturasi, IoT vositalarini

himoyalash, ulardan kelib chiqadigan xavfsizlik risklarini minimalizlash, xavfsizlikni oshirishni ham o'z ichiga oladi.

5. Birlashtirilgan Xavfsizlik Tizimlari: Xavfsizlikning barcha tizimlar bo'yicha integratsiyasi va birlashtirilgan xavfsizlik tizimlari, kamchiliklarni oshiradi va o'rganilgan usullar yordamida ma'lumotlar almashinuvini va xavfsizligi muvaffaqiyatli ravishda ta'minlaydi.

Axborot himoyasining strategyasi va axborot himoyasining arxitekturasi ikkalasining farqi nimada?

Axborot himoyasining strategiyasi va axborot himoyasining arxitekturasi ikkisi ham axborot himoyasining asosiy qismlari bo'lib, bir-biriga bog'liq, ammo ularga turli turdagi vazifalar va tushunchalar taalluqli.

Axborot Himoyasining Strategiyasi:

Axborot himoyasining strategiyasi, bir tashqi tashkilot yoki kompaniyaning umumiy axborot himoyasi to'g'risidagi qarorlar va o'tishlarni belgilaydi. Ushbu strategiya, axborot himoyasining maqsadlarini, prinsiplarini va hujjatlarini belgilayadi. Strategiya, xavfsizlik maqsadlarini aniqlovchi, qo'llanuvchilar va so'nggi foydalanuvchilarni himoyalashning yo'nalishlarini ko'rsatuvchi va axborot himoyasi bilan bog'liq vazifalarni belgilaydigan hujjatlarni o'z ichiga oladi.

Axborot himoyasining arxitekturasi:

Axborot himoyasining arxitekturasi, bir axborot tizimining yoki tarmog'i yoki bir axborot sohasining yaratishini va ishlab chiqishini belgilaydi. Ushbu arxitektura, axborot tizimining o'rganishini, xavfsizlikni ta'minlashni, ma'lumot almashinuvini, saqlash va uzatish jarayonlarini tartibga soluvchi qurilmalar, protokollar va vositalarni o'z ichiga oladi. Arxitektura, tizimni qurish, ta'mirlash va yangilash jarayonlarida xavfsizlikni ta'minlayuvchi, tizimning yuqori darajadagi ma'lumot xavfsizligini ta'minlayuvchi tuzilmalarni belgilayadi.

Bundan tashqari, avvalgi tarjimada belgilangan xususiyatlardan foydalanish orqali, strategiya va arxitektura orasidagi farqlar quyidagicha bo'lishi mumkin:

- Strategiya, umumiy axborot himoyasi to'g'risidagi qarorlar va maqsadlar bilan bog'liq bo'lib, har bir tashkilot yoki kompaniya uchun o'ziga xos bo'lishi mumkin. Arxitektura esa konkret axborot tizimi yoki tarmog'i uchun belgilanadi.

- Strategiya, axborot himoyasining maqsadlarini va asosiy yo'nalishlarini belgilashda keng qo'llaniladi. Arxitektura esa tizimning konkret arxitekturasi, protokollari va vositalarini o'z ichiga oladi.

- Strategiya, axborot himoyasining bunday ko'rsatkichlarini belgilaydi:

Axborot himoyasining strategyasi va arxitekturasi. O’zbekiston respublikasida qanday qo’llanilyapdi?

Axborot himoyasining strategiyasi va arxitekturasi O'zbekiston Respublikasi dasturlash sohasidagi amaliyotlarda va tartibotlarda qo'llaniladi. Axborot himoyasi, O'zbekistonning strategik maqsadlariga mos keluvchi tartibda rivojlanadi va amalga oshiriladi.

O'zbekiston Respublikasida axborot himoyasining strategiyasi, Davlat axborot xizmati tomonidan belgilanadi va amalga oshiriladi. Ushbu strategiya, axborot infrastrukturini rivojlantirish, xavfsizlikni ta'minlash, ma'lumotlar almashinuvi va hujjatlarni boshqarish, ma'lumot tizimlarining integratsiyasi va hamkorliklarni rivojlantirish kabi asosiy yo'nalishlarni o'z ichiga oladi.

O'zbekiston Respublikasida axborot himoyasining arxitekturasi esa har bir axborot tizimi, tarmoq va tizimlar uchun alohida belgilanadi. Ushbu arxitektura, ma'lumot tizimlarining tashqi va ichki xavfsizligini ta'minlash, ma'lumot almashinuvi protokollari va standartlarini belgilash, ma'lumotlar bazalarini tashkil etish va ulardan foydalanish, axborot tizimlarining integratsiyasini va ta'minotini ta'minlash kabi vazifalarni o'z ichiga oladi.

Axborot himoyasining strategiyasi va arxitekturasi O'zbekiston Respublikasida hukumat va dasturiy ta'minot muassasalarining faoliyati, tashqi kompaniyalar, banklar, telekommunikatsiya sohasi va boshqa sohalarda ham qo'llaniladi. Bu tartiblar, O'zbekistonning ma'lumotlarni himoyalash, axborotlararo almashishni rivojlantirish, xavfsizlikni ta'minlash va moliyaviy faoliyatning rivojlanishiga muhim hissa qo'shadi.

Axborot himoyasining strategiyasi va arxitekturasi O'zbekiston Respublikasida O'zbekiston Respublikasi Prezidenti, O'zbekiston Respublikasi Vazirlar Mahkamasi va ilgari tashkilotlar tomonidan muvofiqlashtiriladi va rivojlanishi uchun kerakli qonun hujjatlari va boshqa yo'nalishlar takomillashtiriladi.

O'zbekiston Respublikasida, axborot himoyasi strategiyasi va arxitekturasi, hukumatning "O'zbekiston Respublikasida axborot tizimini takomillashtirish va rivojlantirish chora-tadbirlari to'g'risida"gi qarorlari va "O'zbekiston Respublikasining axborot himoyasi strategiyasi" nomli qarori bilan belgilanadi.

Axorot himoyasi strategiyasi, O'zbekiston Respublikasining "Insonlar uchun yangi elektron xizmatlarni taqdim etish va axborot-kommunikatsiya texnologiyalarini rivojlantirish

bo'yicha davlat dasturi" va "Yoshlar va yoshlarning kreativ g'oyalarini qo'llab-quvvatlashni rivojlantirish bo'yicha Davlat Dasturi"da belgilangan vazifalar va maqsadlar bilan mos keladi.

Arxitektura esa, "O'zbekiston Respublikasi axborot tarmoqlari arxitekturasi" degan qonuniy hujjat asosida belgilanadi. Ushbu arxitektura, axborot tizimining maqsadlarini, qurilish va ishlab chiqish jarayonlarini, xavfsizlikni ta'minlashni va tizimni rivojlantirishni belgilaydi.

Shu bilan birga, O'zbekiston Respublikasida axborot himoyasi strategiyasi va arxitekturasi, hukumatning "O'zbekiston Respublikasida axborot tizimini takomillashtirish va rivojlantirish chora-tadbirlari to'g'risida"gi qarorlari asosida amalga oshiriladi.

XULOSA

Axborot himoyasining strategiyasi va arxitekturasi, ma'lumotlarni xavfsiz qilish, himoyalash va xavfsizlikni ta'minlash maqsadida yaratilgan tartibdir. Ushbu strategiya va arxitektura, zararli dasturlar, atakalar va xavfsizlik xavf-xatarlariga qarshi kurashishga imkon beradi.

Bu tartib, ma'lumot almashinuvi, saqlash, uzatish va tizimdan chiqish jarayonlarida xavfsizlikni ta'minlayadi. Shifrlash, autentifikatsiya, nazorat, zararli dasturlarni aniqlash va ularga qarshi qilish, ma'lumotlarni shifrlab olish va maxfiylash, xavfsizlik protokollari va standartlar bilan bir qatorda amalga oshiriladi.

Axborot himoyasining strategiyasi va arxitekturasi, ma'lumotlar almashinuvi, saqlash va uzatish jarayonlarida yuqori darajadagi xavfsizlikni ta'minlayadi. Bu tartib, zararli faollanishlarni to'xtatish, xavfsizlik ta'limoti, ma'lumotlar almashinuvi uchun nafazalar, ijtimoiy axborot himoyasi prinsiplari va nizomlash asoslarini o'z ichiga oladi.

Shaffoflik, ma'lumotlarning ijtimoiy tarzda almashinuvi va nazorat tizimlari ham axborot himoyasining strategiyasi va arxitekturasining muhim xususiyatlari hisoblanadi.

Axborot himoyasining strategiyasi va arxitekturasi uchun kamchiliklar esa texnologik moddalar, xavfsizlikning qiymatli foydalanuvchilar uchun yuqori narxi kabi faktorlar bo'lib ko'rinadi.

Xulosa qilib aytish mumkinki, axborot himoyasining strategiyasi va arxitekturasi ma'lumotlar himoyasini ta'minlash, zararli faollanishlarni to'xtatish, xavfsizlik protokollari va tizimlarining integratsiyasini o'z ichiga olgan tartibdir. Bu tartib, o'zgaruvchanlik, yangilanishlarga mos kelish va foydalanuvchilarga xavfsizlikni ta'minlashga imkon beradi. Uning kamchiliklari esa texnologik moddalar va xavfsizlikning narxi bo'lib ko'rinadi.

Axborot himoyasi sohasidagi yangi texnologiyalar va zararli faollanishlarning o'sishi bilan, "Axborot Himoyasining Strategiyasi va Arxitekturasi"ni rivojlantirish keng tarqalgan mavzu bo'lib chiqdi. Bu strategiya va arxitektura, xavfsizlikning muhim yo'nalishlarini identifikatsiya qiladi va ularga qarshi kurashish uchun mos keladigan usullarni o'rnatadi.

Bu strategiya va arxitektura quyidagi imkoniyatlarni ta'minlaydi:

1. Yagona Kirish Tizimi: Biometrik identifikatsiya va yagona kirish tizimlari orqali foydalanuvchilar uchun xavfsiz va qulay kirishni ta'minlash.

2. Sun'iy Intellekt va Machine Learning: Zararli faollanishlarni aniqlash va ularga qarshi kurashish uchun sun'iy intellekt va ma'lumotlar tahlili texnologiyalarini qo'llash.

3. Bulut Computerning Kengayishi: Xavfsizlik protokollari va ko'rsatkichlarni o'zgartirishni talab qilgan xavfsizlikning ko'payishi bilan qo'shimcha imkoniyatlarni ta'minlash.

4. Internet of Things (IoT): IoT qurilmalari orasidagi ma'lumot almashinuvi va xavfsizligi ta'minlash.

5. Birlashtirilgan Xavfsizlik Tizimlari: Barcha tizimlarni birlashtirilgan xavfsizlik tizimlariga integratsiya qilish orqali kamchiliklarni o'sirish va xavfsizligi oshirish.

"Axborot Himoyasining Strategiyasi va Arxitekturasi" bu sohada rivojlanayotgan yangiliklarni qo'llab-quvvatlash, xavfsizlikni oshirish, shaxsiy axborotlarni himoyalash, tashqi hamkorliklarda ma'lumot almashinuvi va o'zaro munosabatlarni kuchaytirish uchun muhim o'rin o'z ichiga oladi.

FOYDALANILAGAN ADABIYOTLAR:

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

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

«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.

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

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

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.

Kosimova, A. (2022). MAIN FEATURES OF LANGUAGE LEARNING STRATEGIES. Eurasian Journal of Academic Research, 2(12), 1247-1249.

Kosimova, A. (2022). DRABBLLAR–KICHIK HAJMLI EPIK JANR. In INTERNATIONAL CONFERENCES (Vol. 1, No. 21, pp. 490-493).

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.

Muydinova, N. (2020). DYNAMIC ACTIVITIES FOR SONG IN THE EFL CLASSROOM. In НАУКА И ТЕХНИКА. МИРОВЫЕ ИССЛЕДОВАНИЯ (pp. 11-13).

Муйдинова, Н. (2020). СОСТОЯНИЕ ВДОХНОВЕНИЯ У СПОРТСМЕНОВ. In Психологическое здоровье населения как важный фактор обеспечения процветания общества (pp. 112-113).