INTERNET- XIZMATLAR VA ELEKTRON BIZNES TIZMLARIDA XAVFSIZLIK MUAMMOLARI

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: *Internet-xizmatlar va elektron bines tizmlarida xavfsizlik muammolari barcha dunyoning muhim muammolaridan biridir. Internet va elektron bines tizmlar o'z faoliyati davomida xavfsizlikni ta'minlash uchun ko'p qatlamli usullarni o'z ichiga olgan bo'lsa ham, hozirgi zamonaviy texnologiyalar hamkorlik qilish va ma'lumotlarni himoya qilish uchun katta imkoniyatlar taqdim etadi.*

Xavfsizlik muammolari boshqarishning asosiy sabablari o'zgaruvchan va kuchayuvchan bo'lishi, tarmoq xavfsizlik protokollaridagi nukuslik va yopishmasliklar, xavfsizlikning yuqori darajada yetarli bo'lmagani, shaxsiy ma'lumotlarni himoya qilmaganlik, hakerlik va kiber-hujumlar, botnetlar va yomonligi ortib borgan sayyohliklar kabi sabablarga qarshi kelib chiqadi.

Hozirgi texnologik imkoniyatlar bilan ham shaxsiy ma'lumotlarni himoya qilish uchun muhim tahlil va kengaytirilgan qo'llanmalar mavjud. Bu qo'llanmalar orqali tarmoq protokollaridagi nukusliklar, xavfsizlik ko'rsatkichlari, identifikatsiya va autentifikatsiya usullari, shifrlash va shifrlashni yechish, dasturlar va tizimlarni yangilashlarini ta'minlash uchun xavfsizlikning qanday ta'minlanganligi, hujumning aniqlash va ta'lim qilish, xavfsizlik holatlarida ishlash va rivojlantirish uchun ko'p qatlamli usullar bilan ta'minlanadi.

Bundan tashqari, shaxsiy xavfsizlikning amaliy komponentlari ham mavjud. Bu komponentlarning biri - foydalanuvchilarning xavfsizlik sohalarida xavfsizlik siyosatlarini o'rganish va amalga oshirish imkoniyatlari. Foydalanuvchilar parollarini himoya qilish, haqiqiy foydalanuvchini aniqlovchi usullarni ishlatish, to'g'ridan-to'g'ri ma'lumotlarni kiriting va xavfsizlik sohalarida ma'lumotlarni saqlash xavfsizligini ta'minlash imkoniyatlari bilan tanishishi kerak.

Jamiyat va korporatsiyalar ham muhim xavfsizlik masalalari bilan shug'ullanadilar. Xavfsizlik kengaygan kompyuter va tarmoq vositalari, mobil qurilmalar, IoT vositalari, bulut kompyutering tizimlari

Kalit so’zlar:*Hakerlik,Kiber-hujumlar, Xavfsizlik protokollari. Nukuslik va yopishmaslik, Shaxsiy ma'lumotlarning himoyalash, Xavfsizlik siyosati, Identifikatsiya va autentifikatsiya,Shifrlash, Botnetlar, Xavfsizlik ta'limi, Xavfsizlik tahlil va taqdimoti, Xavfsizlik nukusligi,Ma'lumotlarni to'g'ridan-to'g'ri amalga oshirish,Xavfsizlikning darajasi, Xavfsizlikning echim topishi*

Annotation:*Security problems in Internet services and e-commerce systems are one of the most important problems of the whole world. Even though the Internet and e-*

commerce systems incorporate multi-layered methods to ensure security during their operation, today's modern technologies offer great opportunities for collaboration and data protection.

The main reasons for managing security issues are changing and evolving, flaws and gaps in network security protocols, highly inadequate security, lack of privacy protection, hacking and cyber-attacks, botnets, and increasingly malicious traffic. comes against.

Even with today's technological capabilities, there are important analysis and advanced guidelines for protecting personal data. These manuals cover flaws in network protocols, security metrics, identification and authentication methods, encryption and decryption, how security is maintained to ensure software and system updates, attack detection and education, handling security situations, and provides multi-layered methods for development.

There are also practical components of personal security. One of these components is the ability for users to learn and implement security policies in security domains. Users should familiarize themselves with the possibilities of protecting their passwords, using methods that identify the real user, entering data directly, and ensuring the security of data storage in security areas.

Communities and corporations are also dealing with important security issues. Security-enhanced computing and networking tools, mobile devices, IoT tools, cloud computing systems

Keywords:*Hacking, Cyber attacks, Security protocols, Defect and non-adhesion, Protection of personal data, Security Policy, Identification and Authentication, Encryption, Botnets, Safety training, Security analysis and presentation, Security defect, Direct Implementation of Data, Level of security, Security solutions*

Xavfsizlik muammolari, internet-xizmatlar va elektron biznes tizmlarida muhim bir muammolardir. Bugungi zamonning so'nggi texnologik ilovalarining yuksalishi bilan birga, hakerlik va kiber-hujumlar ham ko'payib kelmoqda. Bu, shaxsiy ma'lumotlarni, korporativ ma'lumotlarni va tizimlarni himoya qilishni va ularga muvofiq xavfsizlikni ta'minlashni qiyinlashtiradi.

Birinchi muammolardan biri xavfsizlik protokollari va ularga xos nukusliklar va yopishmasliklardir. Internet protokollarida nukusliklar va yomonliklar bo'lishi mumkin, bu esa hujumlarni yanada osonlashtiradi. Bunday nukusliklar va yopishmasliklar yuzasidan, tarmoq xavfsizlik sohasida yuqori darajada yuqori samaradorlikka ega protokollar va texnologiyalar ishlab chiqilishi kerak.

Shaxsiy ma'lumotlarning himoyalash ham xavfsizlikning muhim bir qismidir. Foydalanuvchilarning shaxsiy ma'lumotlari, shuningdek, korporativ ma'lumotlar, foydalanuvchilarning identifikatorlari va parollarini himoya qilish kerak. Autentifikatsiya va identifikatsiya usullari, qo'llanmalar orqali foydalanuvchilarni haqiqiy foydalanuvchilar bilan farqini aniqlashga yordam berishi kerak.

Hakerlik va kiber-hujumlar internet-xizmatlar va elektron biznes tizmlarining muammolari bilan bog'liq eng muhim tashviqlardan biridir. Hujumlar, tizimlarga kirishni urushga olib chiqarish, ma'lumot olish yoki o'chirish, tizimlar orqali foydalanuvchilarni qo'llab-quvvatlash uchun ishlatish kabi yo'llar orqali amalga oshiriladi. Bu hujumlar, tizimlar va xavfsizlik protokollaridagi nukusliklardan foydalanish, botnetlar yordamida ta'lim qilinadi va ulardan foydalaniladi. Tizimlarni hujumdan himoya qilish uchun hujumning aniqlanishi, to'g'ridan-to'g'ri tanishish va o'z vaqtida harakat qilish imkoniyatlari kritik ahamiyatga ega.

Xavfsizlik siyosati, korporatsiyalar va foydalanuvchilar uchun bir qatorda belgilanishi kerak. Bu, tizimlarga kirish va ma'lumotlarni yuborish jarayonida xavfsizlikni amal

Bugungi kunda, elektronik tarmoqlar va internet-xizmatlar dunyoda biznes, kommunikatsiya, siyosat va axborot almashinuvini o'zida jamlaydi. Shu bilan birga, tarmoq xavfsizligi tizimlar va foydalanuvchilar uchun katta muhim ahamiyatga ega. Xavfsizlikning yo'qolishlari, hakerlar, botnetlar va kiber-hujumlar kabi muammolarga duch kelishi mumkin va bu haqda yetarli tushunchaga ega bo'lgan barcha tashkilotlar xavfsizlikni ta'minlashga harakat qilishga majbur.

Bu mavzuga bag'ishlangan professional maqolalar keng ko'lamda yozilgan va ular yozuvchilar tomonidan tarmoq xavfsizligini ta'minlash uchun ko'p yonalarni ko'rsatishadi. Bular orasida xavfsizlikning nima ekanligi, xavfsizlikni ta'minlashni qanday amalga oshirish, xavfsizlik tizimlari va ularning samarali ishlashini ta'minlash, hakerlik va botnetlar kabi xavfsizlik muammolari bilan qanday kurashish kabi ko'plab mavzular mavjud.

Xavfsizlikni ta'minlash uchun qo'llaniladigan usullar va vositalar ham mavjud. Bu usullar shifrlash, autentifikatsiya, identifikatsiya, kalit bilan nusxalanish, xavfsizlik ta'limi va monitoringlar kabi vositalarni o'z ichiga oladi. Hozirgi zamon davomida ko'plab tashkilotlar xavfsizlikni ta'minlashga xarajatlarni oshirishga tayyorlar va xavfsizlik tizimlarini yaxshilash uchun xavfsizlik tahlil va taqdimoti bo'yicha xizmat ko'rsatadilar.

Shuningdek, xavfsizlikni ta'minlashga ko'plab tashkilotlar avval, o'ziga xos xavfsizlik siyosatini belgilashni va amalga oshirishni qaror qilishadi. Bu siyosatlar tashkilot tarmoqlari uchun xavfsizlikni ta'minlash, foydalanuvchilar uchun ma'lumotlarni himoya qilish, kiber-hujumlarga qarshi kurashish, xavfsizlikni ta'minlash uchun zarur bo'lgan resurslarni belgilash kabi ko'plab xususiyatlarga ega bo'ladi.

Agar xavfsizlik tizimlari yaxshi ishlayotgan bo'lsa, tashkilotlar o'z xavfsizlik darajasini oshirishadi va tashkilotlarining ma'lumotlari ham xavfsizlikni

Internet-xizmatlar va elektron biznes tizmlarida xavfsizlik muammolari, bugungi zamonning muhim va kuchayuvchan masalalardan biridir. Qurilmalar, tarmoqlar, dasturlar va internet-xizmatlarining kengayganligi bilan birga, muammolar va xavfsizlik himoyasi bo'yicha muvaffaqiyatsizliklarning yuqori ehtimoli mavjud.

Shaxsiy ma'lumotlarni himoya qilish, hakerlik, kiber-hujumlar, nukuslik, shifrlash va xavfsizlikning echim topish kabi konseptlar internet-xizmatlar va elektron biznes tizmlarida

qarshi keladigan katta muammolardan faqat bir nechasi. Bu muammolar bilan mukofotlashish uchun muvaffaqiyatli xavfsizlik siyosati, protokollar, tizimlar va identifikatsiya tizimlari zarur bo'ladi.

Birinchi muammolardan biri shaxsiy ma'lumotlarni himoya qilishdir. Internet-faqatgina shaxsiy ma'lumotlarni o'zgartirish va ulardan foydalanish imkonini beradi, lekin bu ma'lumotlar zararli elemntlarning hujumlariga oziq-ovqat bo'lishi mumkin. Bunday hujumlar, identifikatsiya ma'lumotlarini, moliyaviy ma'lumotlarni yoki shaxsiy ma'lumotlarni olishga harakat qilishi mumkin. Bu sababli, shaxsiy ma'lumotlarni himoya qilishning yuqori darajadagi ko'maklashishini talab qilish zarur.

Hujumlar va hakerlik internet-xizmatlari va elektron biznes tizmlarida ko'plab muammolarga olib keladi. Hakerlar o'zlarining foydalanish yo'li bo'lmagan tarmoqqa kirish uchun xavfsizlikni buzishga harakat qilishadi. Bu hujumlar, sistemlarga ziyon yetkazish, identifikatsiya ma'lumotlarini olish, tizimga zarar yetkazish va hokazo shakllarda bo'lishi mumkin. Bunday hujumlar foydalanuvchilar uchun xavfsizlik riskini oshirishi bilan birga, korporatsiyalar uchun ham axborotni himoya qilish muammolarini ortga soladi.

Kiber-hujumlar ham muhim xavfsizlik muammolaridan biridir. Ular tarmoqni yopish, ma'lumotlarni olish, tizimlarni zarar yetkazish va xavfsizlik protokollaridagi nukusliklardan foydalanishni o'z ichiga oladi. Botnetlar kiber-hujumlarni kuchaytirish uchun ko'p

Xavfsizlik, internet-xizmatlar va elektron biznes tizmlarida aholi, korporatsiyalar, va tizim administratorlari uchun muhim bir muammolardan biridir. Xavfsizlik muammolari, hakerlik guruhlarining qonuniy yoki qonuniy olmaydigan faoliyati, kiber-hujumlar, shaxsiy ma'lumotlarning himoyalashining ta'minlanmaganligi va shaxsiy ma'lumotlarni himoya qilish tizimlari bo'lmaganligi kabi sabablarga asoslanadi. Bu muammolar, tizimlarga zarar yetkazuvchi programmalarni yuborish, identifikatsiya va autentifikatsiya muammosi, nukuslik va yopishmasliklar, tarmoq protokollari orqali ma'lumotlarni to'g'ridan-to'g'ri amalga oshirishning ta'minlanmaganligi, shifrlash usullaridagi nukusliklar va yomonliklar, tizim administratorlari va foydalanuvchilarning xavfsizlik sohalarida ko'proq ta'lim olishi va qo'llab-quvvatlashi talablari kabi tashkil etilishi mumkin.

Profesional maqolada, internet-xizmatlar va elektron biznes tizmlarida xavfsizlik muammolari haqida quyidagi eng muhim nuqtalarni yozish mumkin:

1. Identifikatsiya va autentifikatsiya usullari: Xavfsizlikning asosiy qismi, shaxsiy ma'lumotlarni himoya qilish, yani foydalanuvchining haqiqiyligini aniqlovchi identifikatsiya va autentifikatsiya usullarini o'z ichiga oladi. Bu usullar, parol, biometrik ma'lumotlar, ikkilashuvli autentifikatsiya, tekshiruvli kirishlar kabi ko'plab muhim tizimlardan iborat bo'lishi kerak.

2. Shifrlash: Ma'lumotlarni himoya qilish uchun shifrlash usullari keng qo'llaniladi. Shifrlash, ma'lumotlarni noma'lum shaxslardan himoya qilish uchun o'zgaruvchanlik qiluvchi matematik algoritmlarini qo'llashni o'z ichiga oladi. Bu usul tarmoqda o'tkazilayotgan ma'lumotlarni himoya qilishga yordam beradi.

3. Tarmoq xavfsizlik protokollari: Tarmoqda axborotlar uzatilayotgan va qabul qilinayotgan paytlarda xavfsizlikni ta'minlash uchun xavfsizlik protokollaridan foydalaniladi. Bu protokollar, axborotlar yuborish va qabul qilish jarayonlarida n

Internet-xizmatlar va elektron biznes tizmlarida xavfsizlik muammolari, korporatsiyalar, foydalanuvchilar va tizim ishchi taraflar uchun ahamiyatli va kuchli masalalardan biridir. Bu muammolar, xavfsizlik protokollari, shaxsiy ma'lumotlarning himoyalash, hakerlik, kiber-hujumlar, identifikatsiya, autentifikatsiya, shifrlash va shifrlashni yechish, botnetlar, xavfsizlik siyosati, xavfsizlik ta'limi, tahlil va taqdimot, nukuslik, ma'lumotlarni to'g'ridan-to'g'ri amalga oshirish va xavfsizlikning darajasi kabi bir nechta bo'limlarda o'zgaruvchanlik va kuchayuvchanlikni o'z ichiga oladi.

Xavfsizlik protokollari, tarmoq xavfsizligi uchun yuqori darajada muhimdir. Bu protokollar orqali ma'lumotlar tasiriqlarida nukuslik va yopishmaslikni ta'minlash maqsadga muvofiq bo'ladi. Shaxsiy ma'lumotlarning himoyalash esa, foydalanuvchilar tomonidan taqdim etilgan ma'lumotlarning to'g'ridan-to'g'ri amalga oshirilishi, shifrlanishi va haqiqiy foydalanuvchilarni aniqlovchi identifikatsiya va autentifikatsiya usullari orqali amalga oshiriladi.

Hakerlik va kiber-hujumlar internet va elektron biznes tizmlarining asosiy xavfsizlik muammolaridan biridir. Hakerlar va kiber-hujum guruhlari tarmoqqa hujum qilish, ma'lumotlarni to'plash, ma'lumotlarga nusxa olish va tarmoqdagi nukusliklardan foydalanish kabi zararli faoliyatlarni amalga oshirishadi. Bu tufayli korporatsiyalar va foydalanuvchilar uchun xavfsizlik kuchayishining zarur bo'lganligini tushuntish zarur.

Identifikatsiya va autentifikatsiya usullari foydalanuvchilar uchun yuqori darajada muhimdir. Bu usullar foydalanuvchilar haqiqiyligini aniqlovchi va ularga tizimga kirishga ruxsat beruvchi tahlillar bilan bog'liq. Shifrlash esa ma'lumotlarni himoya qilishning asosiy qismidir.

Misol:

Internet-xizmatlar va elektron biznes tizmlarida xavfsizlik muammolari ko'plab turli shakllarda yuzaga kelishi mumkin. Quyidagi misollar, xavfsizlik muammolarining bir nechta turlari bilan bog'liq:

1. Hakerlik va kiber-hujumlar: Hakerlar tarmoq xavfsizligini buzish uchun turli xil vositalardan foydalanishi mumkin. Masalan, bir tizim yoki veb-saytga do'stonasiz kirish, tarmoqni buzish, ma'lumotlarni olish yoki o'chirish kabi hujumlar.

2. Phishing: Bu muammo shaxsiy ma'lumotlarni olish uchun g'alati veb-saytlarni yaratish orqali foydalanuvchilarni qo'llab-quvvatlashga qonuniy asosda orqali qoldirish bilan bog'liq. Phishing xavfsizlikni buzganidan so'ng, shaxsiy ma'lumotlar hujumchilar tomonidan foydalanish uchun olishadi.

3. Malware va viruslar: Bu muammolarda, zararli dasturlar, viruslar yoki malumotlarni buzish uchun yaratilgan programmalarga tizimga kirish mumkin. Bunday dasturlar va viruslar tizimga zarar yetkazish, ma'lumotlarni olish va unda qandaydir turdagi operatsiyalarni amalga oshirish uchun foydalaniladi.

4. DDoS hujumlari: DDoS (Distributed Denial of Service) hujumlarida, katta miqdorda so'rovlar tarmoqqa yuboriladi, shuning natijasida tarmoq xizmatlari to'g'risida bekor qilinish yuzaga keladi. Bu hujumlarda, tarmoq xavfsizlik protokollari va resurslarni ta'minlovchi vositalar tomonidan muhofaza qilinmaganlik hisobga olinadi.

5. Identifikatsiya va autentifikatsiya muammolari: Shaxsiy ma'lumotlarni tekshirish, haqiqiy foydalanuvchilarni aniqlovchi usullar xavfsizlik muammolariga olib keladi. Identifikatsiya va autentifikatsiya protokollaridagi xatolar yoki nufuzli hakerlar tizimga yasalganlikni oshirishi mumkin.

6. Ma'lumotlarni himoya qilish protokollari: Xavfsizlik protokollari va shifrlash algoritmlaridagi nukusliklar va yopishmasliklar ma'lumotlarning himoyasiga ta'sir etishi mumkin.

XULOSA

Internet-xizmatlar va elektron biznes tizmlarida xavfsizlik muammolari, hozirgi zamonaviy dunyoda katta ahamiyatga ega muhim muddalardan biridir. Bu muammolar korporatsiyalar, foydalanuvchilar va tizim ishchi taraflar uchun xavfsizlikning jiddiy va davlatlararo darajasini oshirishni talab qiladi.

Xavfsizlik muammolari o'zgaruvchan va kuchayuvchan bo'lishi tufayli internet-xizmatlar va elektron biznes tizmlarida shaxsiy ma'lumotlarni himoya qilish, tarmoq xavfsizlik protokollaridagi nukuslik va yopishmasliklar, hakerlik, kiber-hujumlar, botnetlar va xavfsizlikning yuqori darajada yetarli bo'lmaganligi kabi muhim vazifalar bilan bog'liq.

Bu muammolarni hal qilish uchun, tizimlarda yuqori darajada xavfsizlikning ta'minlanishi, xavfsizlik siyosati va protokollarining qo'llanilishi, identifikatsiya va autentifikatsiya usullari, shifrlash va shifrlashni yechish protokollari, xavfsizlik ta'limi va sensibilizatsiya, xavfsizlik tahlil va taqdimotlar, yomonliklar haqida xabar beruvchi tizimlar va xavfsizlik sohasida yangiliklardan xabardorlik kabi chora-tadbirlar kerak.

Xavfsizlikning yuqori darajada muhim bo'lishi tufayli, korporatsiyalar va foydalanuvchilar tashabbuskorlik va qo'llab-quvvatlashni talab qiladi. Bu masalada, foydalanuvchilar parollarini himoya qilish, haqiqiy foydalanuvchini aniqlovchi usullarni ishlatish, ma'lumotlarni to'g'ridan-to'g'ri kiriting, tizimlarni yangilashlar bilan sa'y qilish, hujumlar va nukusliklarni aniqlash va aniqlagan xavfsizlik holatlarida ishlash muhimdir.

Xavfsizlik muammolari internet-xizmatlar va elektron biznes tizmlarining iste'molchilari uchun haqiqiy bir muammodir. Biroq, xavfsizlik protokollari, usullari va yangiliklar bilan, bu muammolarni bartaraf etish va tizimlar va ma'lumotlarni himoya qilish mumkin.

FOYDALANILAGAN ADABIYOTLAR:

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

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

14. «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.

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

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

17. 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.

18. Kosimova, A. (2022). MAIN FEATURES OF LANGUAGE LEARNING STRATEGIES. Eurasian Journal of Academic Research, 2(12), 1247-1249.
19. Kosimova, A. (2022). DRABBLLAR–KICHIK HAJMLI EPIK JANR. In INTERNATIONAL CONFERENCES (Vol. 1, No. 21, pp. 490-493).
20. 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.
21. Muydinova, N. (2020). DYNAMIC ACTIVITIES FOR SONG IN THE EFL CLASSROOM. In НАУКА И ТЕХНИКА. МИРОВЫЕ ИССЛЕДОВАНИЯ (pp. 11-13).
22. Муйдинова, Н. (2020). СОСТОЯНИЕ ВДОХНОВЕНИЯ У СПОРТСМЕНОВ. In Психологическое здоровье населения как важный фактор обеспечения процветания общества (pp. 112-113).