INTERNATIONAL JOURNAL OF RECENTLY SCIENTIFIC RESEARCHER'S THEORY

ELEKTRON HUKUMAT TIZIMIDA AXBOROT XAVFSIZLIGINI TA'MINLASH VOSITALARI VA USULLARI

Mardiyev Azamat Sag'dulla o'gli
O'zbekiston Milliy universiteti Jizzax filiali
Kompyuter ilimlari va dasturlash texnalogiyalari yo'nalishi (1-b magistr)

Annotatsiya: *Maqolada elektron hukumat tizimlarida axborot xavfsizligini ta'minlashning ahamiyati, ayniqsa, bugungi raqamli davrda ushbu tizimlardan tobora ko'proq foydalanilayotganligi muhokama qilinadi. Maqolada elektron hukumat tizimining xavfsizligini ta'minlash uchun mavjud bo'lgan turli xil vositalar va usullar, jumladan autentifikatsiya protokollari, shifrlash texnologiyalari, xavfsizlik devorlari, hujumlarni aniqlash tizimlari, antivirus dasturlari, zaiflikni baholash va penetratsion testlar haqida so'z boradi. Unda ta'kidlanganidek, xavfsiz elektron hukumat tizimiga ega bo'lish aholi ishonchini oqlash va davlat xizmatlarining uzluksiz ishlashini ta'minlashda muhim ahamiyatga ega. Kuchli xavfsizlik protokollariga sarmoya kiritish orqali davlat idoralari elektron tizimlari xavfsizligini yaxshilashi, xavflarni kamaytirishi va maxfiy ma'lumotlarni himoya qilishi mumkin.*

Abstract: *The article discusses the importance of ensuring information security in e-government systems, especially in today's digital era, when these systems are increasingly used. The article discusses the various tools and techniques available to secure an e-government system, including authentication protocols, encryption technologies, firewalls, intrusion detection systems, anti-virus software, vulnerability assessments, and penetration testing. As it was noted, having a secure e-government system is important for justifying public trust and ensuring uninterrupted operation of public services. By investing in strong security*

protocols, government agencies can improve the security of their electronic systems, reduce risks, and protect sensitive information.

Аннотация: *В статье рассматривается важность обеспечения информационной безопасности в системах электронного правительства, особенно в сегодняшнюю цифровую эпоху, когда эти системы используются все чаще. В статье обсуждаются различные инструменты и методы, доступные для обеспечения безопасности системы электронного правительства, включая протоколы аутентификации, технологии шифрования, брандмауэры, системы обнаружения вторжений, антивирусное программное обеспечение, оценки уязвимостей и тестирование на проникновение. Как было отмечено, наличие защищенной системы электронного правительства важно для оправдания общественного доверия и обеспечения бесперебойной работы государственных услуг. Инвестируя в надежные протоколы безопасности, государственные учреждения могут повысить безопасность своих электронных систем, снизить риски и защитить конфиденциальную информацию.*

Kirish so'zlar: *Elektron hukumat, raqamli xavfsizlik, globallashuv, inson omili, davlat xizmatlari, axborot tizimlari, maxfiy ma'lumotlar*

Key words: *Electronic government, digital security, globalization, human factor, public services, information systems, confidential information*

Ключевые слова: *Электронное правительство, цифровая безопасность, глобализация, человеческий фактор, государственные услуги, информационные системы, конфиденциальная информация.*

Elektron hukumat tizimi fuqarolarga davlat xizmatlari va ob'ektlaridan tez va qulay foydalanishni ta'minlash uchun mo'ljallangan innovatsion platformadir. Foydalanuvchilar ma’lumotlari zararli hujumlar va ruxsatsiz kirishdan xavfsiz va xavfsiz bo‘lishini ta’minlash muhim. Elektron hukumat tizimida axborot xavfsizligini ta'minlashning bir qancha vositalari va usullari mavjud. Birinchidan, tizimga faqat vakolatli shaxslar kirishini ta'minlash uchun kuchli autentifikatsiya protokollari amalga oshirilishi mumkin. Ikkinchidan, shifrlash texnologiyalari maxfiy ma’lumotlarning himoyalanganligini va xakerlar yoki ruxsatsiz shaxslar tomonidan buzilmasligini ta’minlash uchun ishlatilishi mumkin. Bundan tashqari, ruxsatsiz kirishni oldini olish va maxfiy ma'lumotlarning oshkor etilishini oldini olish uchun xavfsizlik devorlari, hujumlarni aniqlash tizimlari va antivirus dasturlari o'rnatilishi mumkin. Bundan tashqari, potentsial zaifliklarni aniqlash va xavfsizlikni buzish xavfini kamaytirish uchun muntazam ravishda zaifliklarni baholash va kirish testlarini o'tkazish mumkin. Nihoyat, foydalanuvchilarga yaxshi xavfsizlik amaliyotlarini o‘rgatish va foydalanuvchi xatosini oldini olish uchun foydalanuvchilarni o‘qitish va o‘qitish mumkin. Umuman olganda, elektron hukumat tizimida axborot xavfsizligini ta'minlash vositalari va usullari fuqarolarga xavfsiz va xavfsiz davlat xizmatlarini ko'rsatishda hal qiluvchi ahamiyatga ega. Ushbu chora-tadbirlarni amalga oshirish orqali elektron hukumat tizimi ishonchli, samarali va samarali ishlashi mumkin. Hozirgi raqamli asrda elektron hukumat tizimlari tobora ommalashib bormoqda va keng tarqalmoqda. Ushbu tizimlar turli davlat xizmatlaridan oson foydalanish imkonini beradi va shaxsiy, moliyaviy va boshqa muhim ma’lumotlarni o‘z ichiga olgan katta hajmdagi maxfiy ma’lumotlarni boshqarish uchun muhim ahamiyatga ega. Ushbu elektron hukumat tizimlaridan foydalanish ortib borayotgani sari kiberhujumlar va ruxsatsiz kirishdan himoya qilish uchun mustahkam xavfsizlik choralariga bo‘lgan ehtiyoj har qachongidan ham muhimroq bo‘lib bormoqda. Elektron hukumat tizimida

axborot xavfsizligini ta'minlashning turli vositalari va usullari mavjud. Asosiy usullardan biri kuchli autentifikatsiya protokollarini amalga oshirishdir. Bu tizimga faqat to'g'ri hisob ma'lumotlariga ega bo'lgan vakolatli shaxslar kirishini ta'minlaydi. Autentifikatsiya protokollari parollar, ikki faktorli autentifikatsiya va biometrik ma’lumotlarni o‘z ichiga olgan turli chora-tadbirlarni o‘z ichiga olishi mumkin.

Axborot xavfsizligini ta'minlashning yana bir muhim jihati - maxfiy ma'lumotlarni himoya qiluvchi shifrlash texnologiyalaridan foydalanish. Shifrlash ma’lumotlarga faqat vakolatli xodimlar kirishi va xakerlar yoki boshqa ruxsatsiz shaxslar tomonidan tutib olinmasligi yoki buzilmasligini ta’minlaydi. Xavfsizlik devorlari, bosqinlarni aniqlash tizimlari va antivirus dasturlari ruxsatsiz kirishni oldini olish va maxfiy ma'lumotlarni tajovuzkor hujumlardan himoya qilish uchun ishlatilishi mumkin. Xavfsizlik devorlari tarmoq tizimlari va tashqi tarmoqlar o‘rtasida to‘siq vazifasini o‘taydi, buzg‘unchilikni aniqlash tizimlari esa fishing urinishlari va ruxsatsiz kirishni aniqlash va oldini olish uchun tarmoq trafigini nazorat qiladi.

Xavfsiz elektron hukumat tizimiga ega bo‘lish aholi ishonchini saqlash va davlat xizmatlarining uzluksiz ishlashini ta’minlashda muhim ahamiyatga ega. Yuqorida ko'rsatilgan vositalar va usullarni o'z ichiga olgan holda, davlat muassasalari o'zlarining elektron tizimlari xavfsizligini yaxshilashlari, xavflarni kamaytirishlari va maxfiy ma'lumotlarni himoya qilishlari mumkin. Elektron hukumat tizimlaridan foydalanish o‘sishda davom etar ekan, kiberhujumlarning oldini olish va maxfiy ma’lumotlarni himoya qilish uchun mustahkam xavfsizlik protokollariga sarmoya kiritish muhim.

Xulosa. Xulosa qilib aytadigan bo'lsak, mustahkam va xavfsiz elektron hukumat tizimiga ega bo'lishning ahamiyatini, ayniqsa, bugungi raqamli asrda

ortiqcha baholab bo'lmaydi. Elektron hukumat tizimlaridan foydalanish ortib borayotganligi sababli, davlat idoralari maxfiy ma'lumotlarni himoya qilish va kiberhujumlarning oldini olish uchun kuchli xavfsizlik choralariga sarmoya kiritishlari juda muhimdir. Autentifikatsiya protokollari, shifrlash texnologiyalari, xavfsizlik devorlari, tajovuzlarni aniqlash tizimlari, antivirus dasturlari, zaifliklarni baholash va kirish testlarini joriy etish davlat idoralari elektron tizimlari xavfsizligini yaxshilash va jamoatchilik ishonchini saqlash usullaridan biridir. Axborot xavfsizligiga ustuvor ahamiyat berish orqali davlat organlari o‘z xizmatlarining uzluksiz ishlashini ta’minlashi va fuqarolarning manfaatlarini himoya qilishi mumkin.

Foydalanilgan adabiyotlar:

1. O’zbekiston Respublikasining “Elektron hukumat to’g’risida”gi Qonuni (2015 yil 9 dekabr № O’RQ—395)
2. Kovalyova L.N. Mnogofaktornoye prognozirovaniye na osnove ryadov dinamiki.-M.: Statistika, 1980.-104 s.
3. Ergashev A. X. Mavhum jarayonlarni matematik modellashtirish.- Qarshi: Nasaf, 2000.-103 b.
4. Frenkel A.A. Prognozirovaniye proizvoditelnosti truda: metodы i modeli. –M.: Ekonomika, 2007.-214 s.
5. S.S.Qosimov. Axborot texnologiyalari. O’quv qo’llanma. Toshkent . “Aloqachi”, 2006-y