Emro Science and Education
Open-access scientific journal
Journal homepage: https://journal.emro.uz

OPEN ACCESS

CONFERENCE PAPER OPEN ACCESS

Vol. 1 No. 3 (2024) · “Hududlarni ijtimoiy-iqtisodiy rivojlantirish dasturlarini moliyalashtirish tendensiyalari” mavzusidagi respublika il...

loyihasi amalga oshiriladi. Loyiha amalga oshirilishi natijasida 20 nafar yangi ish o‘rinlari yaratiladi hamda 10 mlrd.so‘mlik sanoat mahsulotlari ishlab chiqariladi.

Xulosa qilib aytganda tumanning ijtimoiy iqtisodiy rivojlanishi va aholini ijtimoy himoya qilish kambag’allikni qisqartirish shuningdek xotin qizlarni ijtimoiy qo’llab quvvatlash ko’rsatkichlari davr talablariga mosdir.

Foydalanilgan adabiyotlar ro’yhati

1. Me’yoriy hujjatlar to’plami 2022-2024.
2. Pahtaobod tumani statistik ma’lumotlari.
3. https://stat.uz/uz/matbuot-markazi/qo-mita-yangiliklar/51693-milliy-statistikani-rivojlantirish-ustuvor-vazifa

O’ZBEKISTONDA AXBOROT HAVFSIZLIGI

Abduqayumov Jaloliddin Jo‘rabek og‘li
TDIU Andijon fakulteti
Iqtisodiyot talim yo‘nalishi 60/23 guruh talabasi
Kurbonov Jasurbek Pozilovich
TDIU Andijon fakulteti
“Mutaxassislik fanlari” kafedrasi mudiri, PhD

Annotatsiya: *Ushbu maqolada bugungi kunning dolzarb masalalaridan biri bo‘lgan axborot xavfsizligini ta’minlash, turli xil axborot xujumlaridan saqlanish yuzasidan taxliliy ma’lumotlar bayon etilgan.*

Kalit so‘zlar: *xavfsizlik, axborot, dasturiy ta’minot, internet, parol, kiberxavfsizlik.*

Hozirgi kunda axborot xavfsizligini taminlash tobora dolzarb muammoga aylanib bormoqda chunki borgan sayin axborotga bo‘lgan tahdidlar ortib bormoqda. Misol uchun dunyoning yirik banklariga bo’layotgan xakerlarning hujumlari, bank mijozlarning plastik kartalaridan noqonuniy pul yechib olishlar, davlat idoralaridagi tizimlarga bo’layotgan tajovuzlarni misol qilishimiz mumkin. Bilamizki, axborot eng qimmatli narsalardan biri hisoblanadi. Axborot xavfsizligi nimaga kerak deganda axborotni boshqargan odam dunyoni boshqaradi bu yaqqol ko’rinib turibdi. Chunki, bir yolg’on axborot bilan butun bir jamiyatning hayotini yaxshilash yoki barbod qilib yuborish mumkin. Hamda hozirgi kunda asosan qurolli urushlar emas, balki axborot urushi avj olgan davrda yashamoqdamiz. Bundan tashqari eng kuchli qurol bu ma’naviy qurol hisoblanadi. Bu quroldan foydalanish uchun esa axborot katta ro’l o’ynaydi.

Davlat, harbiylar, korporatsiyalar, moliya institutlari, tibbiyot muassasalari va xususiy korxonalar o‘z xodimlari, mijozlari, mahsulotlari, tadqiqotlari va moliyaviy natijalari haqida doimiy ravishda katta miqdordagi maxfiy ma’lumotlarni to‘playdi.

Published: 17.05.2024

Cite this article: Abduqayumov Jaloliddin Jo‘rabek o‘g‘li, Kurbonov Jasurbek Pozilovich (2024). O‘zbekistonda axborot havfsizligi. Emro Science and Education, 1(3). https://journal.emro.uz/public/maqola/115

© 2024 The Author(s). Published by Emro Science and Education. This is an open access article.

Agar bunday ma’lumotlar raqobatchilar yoki kiberjinoyatchilar qo‘liga tushib qolsa, bu tashkilot va uning mijozlari uchun keng qamrovli huquqiy oqibatlarga, tuzatib bo‘lmas moliyaviy va ayanchli yo‘qotishlarga olib kelishi mumkin.

Bugungi dunyoda internetdan foydalanishining kengayishi bilan birga kiber-hujumlar ham o'sib bormoqda. Shu sababli axborot xavfsizligini ta’minlash birinchi navbatdagi vazifadir. Axborot xavfsizligini taminlash quyidagi foydalarni ta'minlaydi:

1.Muhim ma’lumotlar xavfsizligini ta’minlash: bu bilan, shaxsiy ma'lumotlar, korxona, davlat ma’lumotlari hamda va boshqa maxfiy axborotlarni hakkerlar hujumlaridan va xavfsizlik muammolaridan himoya qilish mumkin.

2. Xavfsizlikni ta'minlash orqali mijozlar va boshqalarning ishonchi: Foydalanuvchilar va kompaniyalar xavfsizlikni ta'minlash orqali o'zlarini himoya qilish, shuningdek, ma'lumotlarni to'g'ri xisoblash bilan birga, xavfsizlik muammolari, hujumlar va tahdidlarga bo’lgan xujumlar qarshisida ishonchga sazovor bo’ladi.

3. To'g'ri hisoblanadiganlik: Xavfsizlikni ta'minlash orqali, ma'lumotlar noto'g'ri ko'rsatilish, ochilish yoki o'zgartirishiga hamda buzib kirishga qarshi himoya yahshilanadi, bu esa axborotlarni to'g'ri va xavfsiz foydalanishga olib keladi.

Axborot xavfsizligi har qanday davlatda, jumladan, O‘zbekistonda ham muhim jihat hisoblanadi. Bizning hukumat axborotni himoya qilish muhimligini tushungan holda kiberxavfsizlik choralarini kuchaytirish choralarini ko'rib kelmoqda.

O‘zbekiston Mudofaa vazirligi huzuridagi Axborot xavfsizligi agentligi mamlakatimizda axborot tizimlari va tarmoqlari xavfsizligini ta’minlash uchun mas’ul hisoblanadi. U kiber tahdidlarning oldini olish, hodisalarni aniqlash va ularga javob berish, shuningdek, tashkilotlar va shaxslarga axborot xavfsizligi masalalari bo'yicha yo'l-yo'riq va yordam ko'rsatishga qaratilgan.

Axborot xavfsizligini ta'minlash uchun shaxslar va tashkilotlar amalga oshirishi mumkin bo'lgan bir qancha muhim qadamlar mavjud. Ushbu choralar maxfiy ma'lumotlar, tizimlar va tarmoqlarni ruxsatsiz kirish, kiber tahdidlar va ma'lumotlar buzilishidan himoya qilishga yordam beradi.

Axborot xavfsizligini ta'minlash uchun quyidagilarga e’tibor berilishi lozim:

Kuchli va murakkab parollarni qo'llash: buning uchun raqam va harf birikmalari aralashgan parollardan foydalanish. Shuningdek parollarni tugilgan sanalar va ism shariflarga o’xshash bo’lmayotganligiga e’tibor berish kerak. Bundan tashqari parollarning ketma-ket va bir xil bo’lishidan saqlanish samarali.

Foydalanadigan har bir hisob yoki xizmat uchun noyob parollardan foydalaning. Bir nechta platformalarda bir xil paroldan foydalanishdan saqlaning. Shungingdek bitta platformadan hamda faqat bitta akauntdan foydalaning. Agar har hil platformalarda masalan: kompyuter, telefon, planshet va boshqalardan foydalamsangiz ularning har biriga o’zgacha parol qo’ying. Bir xillikdan saqlaning.

Parollaringizni muntazam ravishda o'zgartiring, har haftada bir necha bor o’zgartirishlarni amalga oshiring ayniqsa hukumatga tegishli, shaxsiy hisob raqamingiz, bank yoki elektron pochta kabi nozik hisoblar uchun bu ishlarni

muntazam amalga oshiring. Parollaringizni har doim yangilash uchun eslatmalarni o'rnating.

Axborot xavfsizligini ta'minlash uchun dasturiy ta'minotni yangilab turish juda muhimdir. Sizning dasturiy ta'minotingiz yangilanishini ta'minlash uchun quyidagi qadamlar mavjud:

Yangilashdan oldin zaxira nusxasini yarating. Katta dasturiy ta'minot yangilanishlarini amalga oshirishdan oldin, yangilash jarayonida muammolar yuzaga kelganda ma'lumotlar yo'qolishining oldini olish uchun muhim ma'lumotlaringizni zaxiralang. Ularni isonchli joylarga bir nechta nusxalarini saqlabn qoying. Buning uchun fleshka, chip, kampyuter va boshqa gadjetlardan foydalaning.

So'nggi xavfsizlik tahdidlari va dasturiy ta'minot zaifliklari haqida xabardor bo'ling. Xavfsizlik axborotnomalariga obuna bo'ling, xavfsizlik bloglarini kuzatib boring va dasturiy ta'minot ishlab chiqaruvchilarining xavfsizlik ogohlantirishlariga e'tibor bering. Har doim axborot xavfsizligiga qarshi chiqarilayotgan xujumlarni kuzatib boring.

Xodimlarni kiberxavfsizlik bo'yicha ilg'or tajribalarga o'rgatish tashkilotning umumiy xavfsizlik holatini mustahkamlash uchun muhim ahamiyatga ega.

Xodimlarni kuchli parollar muhimligi, parolni muntazam ravishda o'zgartirish va parol menejerlaridan foydalanish haqida o'rgating. Bunda o’zingiz ham faol bong va birgalikda o’rganing. Iloji boricha ko'p faktorli autentifikatsiyadan (MFA) foydalanishni rag'batlantiring.

Xodimlar uchun kiberxavfsizlik bo'yicha treningga sarmoya kiritib, tashkilotlar xavfsizlik bo'yicha xabardorlik madaniyatini shakllantirishi, muvaffaqiyatli kiberhujumlar ehtimolini kamaytirishi va nozik ma'lumotlar va kompaniya aktivlarini samarali himoya qilishga qodir mustahkam ishchi kuchini yaratishi mumkin. Kiberxavfsizlikdan xabardorlik va treninglar bugungi raqamli landshaftda mustahkam kiberxavfsizlik strategiyasining asosiy komponentlari hisoblanadi.

Axborotga kirishni cheklang. Axborotga kirishni cheklash maxfiy ma'lumotlarni himoya qilish va ruxsatsiz kirishning oldini olishda hal qiluvchi ahamiyatga ega. Muntazam ravishda xavfsizlikni baholashni amalga oshirish va ushbu bosqichlarni bajarish orqali siz xavfsizlik xatarlarini faol ravishda aniqlashingiz va bartaraf etishingiz, tashkilotingizning kibertahdidlarga chidamliligini oshirishingiz va tizimlaringiz va ma’lumotlaringizni potentsial buzilishlardan himoya qilish uchun mustahkam xavfsizlik holatini saqlab qolishingiz mumkin.

Xulosa: Hozirgi kunda va bundan buyon axborot xavfsizligi dolzarb mavzu bo’lib qolaveradi chunki yildan yilga axborotga bo’lgan extiyojimiz ortib bormoqda va dunyo axborot asrida yahsamoqda. O’zimiz va jamiyat uchun ham bu mavzuga befarq qaramasligimiz talab etiladi. Xulosa o’rnida axborot xavfsizligini taminlash uchun yuqorida sanab o’tilgan ishlardan tashqari yana har birimizdan o’zimiz va jamiyatning rivoji uchun bunga befarq bo’lmasligimiz talab etiladi.