Zamonaviy axborot almashinuvida raqamli muhitni himoya qilish

Andijon davlat universiteti,
Axborot texnologiyalari va kompyuter injiniringi fakulteti
“Kompyuter injiniringi” yo‘nalishi 3-bosqich talabasi
Xusanboy Odashaliyev Avazbek o‘g‘li

Annotatsiya: *Bugungi o‘zaro bog‘liq dunyoda kompyuter tizimlari va tarmoqlarining xavfsizligi birinchi o'rinda turadi. Kiber tahdidlar yanada murakkablashib, ham shaxslarga, ham tashkilotlarga qaratilgan. Ushbu tahdidlarga qarshi turish uchun turli xil kompyuter xavfsizligi dasturlari ishlab chiqilgan. Ushbu maqolada kompyuter xavfsizligi dasturlarining muhim turlari, ularning funksiyalari va xavfsiz raqamli muhitni saqlashdagi ahamiyati ko‘rib chiqiladi.*

Аннотация: *В современном взаимосвязанном мире безопасность компьютерных систем и сетей выходит на первый план. Киберугрозы становятся все более изощренными и нацелены как на отдельных лиц, так и на организации. Для противодействия этим угрозам были разработаны различные программы компьютерной безопасности. В этой статье рассматриваются важные типы программного обеспечения компьютерной безопасности, их функции и их важность для поддержания безопасной цифровой среды.*

Kalit so‘zlar: *Antivirus, kiberxavfsiz, fishing, xakerlik, identifikator, planshetlar, Firewall, Veb-saytlar, elektron pochta, axloqiy mulohazalar.*

Ключевые слова: *антивирус, кибербезопасность, фишинг, взлом, личность, планшеты, брандмауэр, веб-сайты, электронная почта, этические соображения.*

Kirish

Zamonaviy axborot almashinuvida raqamli muhitni himoya qilish ma'lumotlarning maxfiyligi, kiberxavfsizlik, tartibga rioya qilish, raqamli

savodxonlik va texnologiyalardan axloqiy foydalanishni ta'kidlaydigan yaxlit yondashuvni o'z ichiga oladi. Ma'lumotlarning maxfiyligi va xavfsizligini ta'minlash juda muhim, ya'ni shaxsiy va maxfiy ma'lumotlarni ruxsatsiz kirish va ma'lumotlar buzilishidan himoya qilish uchun shifrlash, xavfsiz aloqa protokollari va ishonchli autentifikatsiya usullaridan foydalanish. Dasturiy ta'minotni muntazam yangilab turish, xavfsizlik devorlarini ishlatish va antivirus dasturlarini joylashtirish kabi kiberxavfsizlik choralari zararli dastur, fishing va xakerlik kabi kiber tahdidlarga qarshi muhim himoya hisoblanadi. Raqamli savodxonlik va ta'limni targ'ib qilish juda muhimdir, chunki u foydalanuvchilarga kiberxavfsizlikning eng yaxshi amaliyotlarini tushunishga va qabul qilishga yordam beradi, mas'uliyatli onlayn xatti-harakatlar madaniyatini rivojlantiradi. Va nihoyat, raqamli vositalar va platformalarning kengroq ijtimoiy ta'sirini hisobga olgan holda va ulardan jamiyat uchun mas'uliyatli va foydali usullarda foydalanishga intilib, texnologiyadan axloqiy foydalanishga ustuvor ahamiyat berishimiz kerak. Ushbu keng qamrovli strategiya zamonaviy axborot almashinuvi uchun xavfsiz, ishonchli va axloqiy raqamli muhitni ta'minlaydi. Zamonaviy axborot almashinuvida raqamli muhitni himoya qilish bugungi o'zaro bog'liq dunyoda xavfsizlik, maxfiylik va ma'lumotlardan axloqiy foydalanishni ta'minlash uchun juda muhimdir. Raqamli aloqa tobora keng tarqalgan bo'lib, bu muhitni muhofaza qilish bir nechta o'zaro bog'liq strategiyalarni o'z ichiga oladi.

Zamonaviy axborot almashinuvi texnologiyalarining rivojlanishi bilan raqamli muhitda axborot almashinuvi osonlashdi va kengaydi. Internet, mobil qurilmalar, bulutli texnologiyalar va ijtimoiy tarmoqlar axborot almashinuvi jarayonlarini tez, qulay va samarali qildi. Bu rivojlanish nafaqat shaxsiy, balki biznes va davlat darajasida ham katta ahamiyatga ega.

Axborot almashinuvi vositalari va texnologiyalari

- Internet: Eng asosiy va keng qo‘llaniladigan axborot almashinuvi vositasi.

Veb-saytlar, elektron pochta, ijtimoiy tarmoqlar va boshqa ko‘plab xizmatlar orqali ma’lumotlar tezkorlik bilan yetkaziladi.

- Mobil qurilmalar: Smartfonlar va planshetlar orqali foydalanuvchilar har qanday vaqtda va har qanday joyda axborotga kirishlari va uni almashishlari mumkin.

- Bulutli texnologiyalar: Ma'lumotlarni bulutda saqlash va ulashish imkoniyati. Bu texnologiyalar axborotni har qanday qurilmadan va joydan foydalanish imkonini beradi.

- Ijtimoiy tarmoqlar: Facebook, Twitter, Instagram kabi platformalar foydalanuvchilarga shaxsiy va professional ma’lumotlarni tez va keng auditoriyaga yetkazish imkonini beradi.

Axborot almashinuvi afzalliklari

- Ma’lumotlarni tez va oson yetkazish va olish imkoniyati.
- Axborot bir zumda butun dunyoga tarqalishi mumkin.
- Foydalanuvchilar o'zaro munosabatda bo'lishlari, fikr almashishlari va hamkorlik qilishlari mumkin.

Axborot almashinuvidagi muammolar va xavflar

- Maxfiylik va xavfsizlik: Axborotning ruxsatsiz kirish va zararli faoliyatlardan himoya qilinishi zarur.

- Ma’lumotlarning ishonchliligi: Noto‘g‘ri yoki yolg‘on axborot tarqalishi mumkin.

- Kiberxavfsizlik tahdidlari: Xakerlar va zararli dasturlar orqali hujumlar amalga oshirilishi mumkin.

Himoya choralari

- Kiberxavfsizlik: Firewall, antivirus dasturlari, shifrlash texnologiyalari va boshqa xavfsizlik choralari.

- Shaxsiy ma'lumotlarni himoya qilish: Malumotlarni yig‘ish, saqlash va ulashish qoidalariga rioya qilish.

- Foydalanuvchilar uchun eng yaxshi amaliyotlar: Kuchli parollar, ikki bosqichli autentifikatsiya va muntazam xavfsizlik yangilanishlari.

Zamonaviy axborot almashinuvi raqamli dunyoning ajralmas qismiga aylandi. Ma'lumotlarning tezkor, qulay va keng tarqalishi orqali ko'plab yangi

imkoniyatlar ochildi, lekin shu bilan birga, ma'lumotlarni himoya qilish zarurati ham oshdi. Raqamli xavfsizlikni ta'minlash uchun zamonaviy texnologiyalar va amaliyotlardan foydalanish muhimdir.

Birinchidan, ma’lumotlar maxfiyligi va xavfsizligi asosiy hisoblanadi. Bunga ma'lumotlarni uzatish paytida himoya qilish uchun shifrlashdan foydalanish, xavfsiz aloqa protokollaridan foydalanish va foydalanuvchi identifikatorlarini tekshirish uchun ishonchli autentifikatsiya usullarini qo'llash kiradi. Ushbu chora-tadbirlar ruxsatsiz kirishni oldini oladi va maxfiy ma'lumotlarni buzilishlardan himoya qiladi. Kiberxavfsizlik choralari teng darajada muhimdir. Dasturiy ta'minotni muntazam yangilab turish, xavfsizlik devorlaridan foydalanish va antivirus dasturlarini tarqatish zararli dastur, fishing va xakerlik kabi turli xil kiber tahdidlarga qarshi muhim himoya hisoblanadi. Ushbu faol qadamlar raqamli tizimlar va ma'lumotlarning yaxlitligi va mavjudligini saqlashga yordam beradi. Tashkilotlar barcha qonuniy talablar to'g'risida xabardor bo'lishlari va ularni qondirish uchun zarur kafolatlar berilishini ta'minlashlari, shu bilan foydalanuvchi ma'lumotlarini himoya qilishlari va ishonchni saqlashlari kerak. Raqamli savodxonlik va ta'limni targ'ib qilish bu harakat uchun juda muhimdir. Foydalanuvchilarga kiberxavfsizlikning eng yaxshi amaliyotlari, potentsial tahdidlar va xavfsiz onlayn xatti-harakatlar haqida ma'lumot berish xavfsizroq raqamli muhitni yaratishga yordam beradi. Bunga tashkilotlarda xodimlarni o'qitish va kiberxavfsizlikning ahamiyati to'g'risida jamoatchilik xabardorligini oshirish kiradi. Texnologiyadan axloqiy foydalanish ustuvor vazifa bo'lishi kerak. Bunga raqamli vositalar va platformalarning ijtimoiy ta'sirini hisobga olish, ulardan mas'uliyat bilan va jamoaga foyda keltiradigan usullarda foydalanishni ta'minlash kiradi. Axloqiy fikrlarga foydalanuvchi maxfiyligini hurmat qilish, ma'lumotlarni noto'g'ri ishlatishdan qochish va axborotni boshqarish va ishlatishda shaffoflikni targ'ib qilish zarur hisoblanadi. Xulosa qilib aytganda, zamonaviy axborot almashinuvida raqamli muhitni himoya qilish ma'lumotlar maxfiyligi, kiberxavfsizlik, tartibga rioya qilish, raqamli savodxonlik va texnologiyalardan axloqiy foydalanishni o'z ichiga olgan kompleks

yondashuvni talab qiladi. Ushbu elementlar xavfsiz, ishonchli va axloqiy raqamli landshaftni yaratish uchun birgalikda ishlaydi.

Antivirus dasturlari zararli dasturlarni, shu jumladan viruslar, qurtlar, troyanlar va to'lov dasturlarini aniqlash, oldini olish va olib tashlash uchun mo'ljallangan. Ular shubhali xatti-harakatlarni tahlil qilish orqali yangi, noma'lum zararli dasturlarni aniqlash uchun ma'lum tahdidlarni va evristik asoslangan aniqlashni aniqlash uchun imzoga asoslangan aniqlashdan foydalanadilar. Zararli dasturlarning tobora ko'payib borishi bilan antivirus dasturi shaxsiy kompyuterlar va tashkiliy tarmoqlarni ma'lumotlarning buzilishi, moliyaviy yo'qotish va tizimning shikastlanishidan himoya qilish uchun juda muhimdir. Xavfsizlik devorlari ishonchli ichki tarmoq va ishonchsiz tashqi tarmoqlar o'rtasida to'siq bo'lib xizmat qiladi. Ular oldindan belgilangan xavfsizlik qoidalari asosida kiruvchi va chiquvchi tarmoq trafigini kuzatib boradi va nazorat qiladi, qonuniy aloqaga ruxsat berishda zararli trafikni bloklaydi. Xavfsizlik devorlari tarmoq resurslariga ruxsatsiz kirishni oldini olish, tarmoqqa asoslangan hujumlardan himoya qilish va xavfsiz aloqa kanallarini ta'minlash uchun juda muhimdir. Internet xavfsizligi. Xavfsizlik buzilishlari to‘g‘risida ogohlantiradi. Ushbu tizimlar real vaqt rejimida potentsial tahdidlarni aniqlash va ularga javob berish, muvaffaqiyatli kiberhujumlar xavfini kamaytirish orqali qo'shimcha himoya qatlamini ta'minlaydi.. Shifrlash dasturi: shifrlash dasturi ma'lumotlarni o'qib bo'lmaydigan kodga aylantirish orqali himoya qiladi, uni faqat vakolatli tomonlar to'g'ri kalit bilan shifrlashi mumkin. Bu maxfiy ma'lumotlar, hatto ushlangan bo'lsa ham, maxfiy va xavfsiz bo'lib qolishini ta'minlaydi. Shifrlash moliyaviy ma'lumotlar, shaxsiy ma'lumotlar va intellektual mulk kabi nozik ma'lumotlarni himoya qilish uchun juda muhimdir, ayniqsa ishonchsiz tarmoqlar orqali uzatishda. Parol menejerlari shifrlangan ma'lumotlar bazasida foydalanuvchilar parollarini saqlaydi va boshqaradi. Ular har bir hisob uchun kuchli, noyob parollarni yaratadilar va kirish ma'lumotlarini avtomatik to'ldiradilar, bu esa parol bilan bog'liq buzilishlar xavfini kamaytiradi. Onlayn hisoblar sonining ko‘payishi bilan parol menejerlari foydalanuvchilarga bir nechta murakkab parollarni eslab qolmasdan kuchli

xavfsizlik amaliyotlarini saqlashga yordam beradi. Xavfsizlik ma'lumotlari va tadbirlarni boshqarish. Tizimlari tashkilotning xavfsizlik holatini har tomonlama ko‘rish uchun turli xil xavfsizlik manbalaridan ma’lumotlarni to‘playdi va tahlil qiladi. Ular real vaqtda monitoring va tarixiy tahlil orqali potentsial xavfsizlik hodisalarini aniqlaydilar va ularga javob berishadi. Yechimlari tashkilotlarga xavfsizlik intsidentlarini yanada samarali aniqlash, tekshirish va ularga javob berishga imkon beradi, tahdidlarni o'z vaqtida kamaytirishni ta'minlaydi. So'nggi nuqta qurilmalarini (kompyuterlar, mobil qurilmalar, serverlar) turli xil tahdidlardan, shu jumladan zararli dasturlardan, to'lov dasturlaridan va fishing hujumlaridan himoya qiladi. Ular antivirus, xavfsizlik devori va boshqa xavfsizlik xususiyatlarini bitta echimga birlashtiradi. Tashkilotlarda so'nggi nuqta qurilmalarining ko‘payishi bilan tarmoqqa ulangan barcha qurilmalarning xavfsizligini ta'minlab, keng ko'lamli tahdidlardan har tomonlama himoya qiladi. Internet orqali xavfsiz, shifrlangan ulanishlarni yaratadi, bu foydalanuvchilarga shaxsiy tarmoqlarga kirish va ma'lumotlarni xavfsiz almashish imkonini beradi. Ular Foydalanuvchining IP-manzilini niqoblaydi, maxfiylikni ta'minlaydi va ma'lumotlarni ushlashdan himoya qiladi. VPN-lar korporativ tarmoqlarga xavfsiz masofadan kirish, onlayn maxfiylikni himoya qilish va maxfiy ma'lumotlarning jamoat tarmoqlari orqali xavfsiz uzatilishini ta'minlash uchun juda muhimdir.

Zamonaviy axborot almashinuvida raqamli muhitni himoya qilish kompleks yondashuvni talab qiladigan ko'p qirrali harakatdir. Raqamli aloqa ko'lami va ahamiyati jihatidan o'sishda davom etar ekan, axborotning yaxlitligi, maxfiyligi va xavfsizligini himoya qilish birinchi o'ringa chiqadi. Ushbu himoya bir nechta asosiy komponentlarni o'z ichiga oladi. Ma'lumotlar maxfiyligi va xavfsizligi ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlash juda muhimdir. Bunga ruxsatsiz kirish va ma'lumotlar buzilishining oldini olish uchun ilg'or shifrlash texnikasi, xavfsiz aloqa protokollari va ishonchli autentifikatsiya usullaridan foydalanish kiradi. Tashkilotlar ishonchni saqlash va qonuniy talablarga rioya qilish uchun shaxsiy va maxfiy ma'lumotlarni himoya qilishni birinchi o'ringa qo'yishlari kerak. Kiberxavfsizlik choralari: kuchli kiberxavfsizlik

himoyasini amalga oshirish zararli dastur, fishing va xakerlik kabi ko'plab tahdidlardan himoya qilish uchun juda muhimdir. Dasturiy ta'minotni muntazam yangilab turish, xavfsizlik devorlari va antivirus dasturlari bu harakatning muhim vositasidir. Bundan tashqari, proaktiv monitoring va javob berish strategiyalari potentsial tahdidlarni sezilarli zarar etkazishdan oldin aniqlash va yumshatishga yordam beradi. Raqamli savodxonlik va ta'lim foydalanuvchilar orasida raqamli xavfsizlik amaliyotlari to'g'risida xabardorlik va tushunishni rivojlantirish juda muhimdir. Bu shaxslarni xavfsiz onlayn xatti-harakatlar haqida o'rgatish, potentsial tahdidlarni tan olish va kiberxavfsizlik choralarining ahamiyatini tushunishni o'z ichiga oladi. Bilimga ega bo'lgan foydalanuvchilar o'zlarini yaxshiroq himoya qilishlari va xavfsizroq raqamli muhitga hissa qo'shishlari mumkin. Texnologiyadan axloqiy foydalanish ishonchli raqamli muhitni saqlashda texnologiyadan axloqiy foydalanish muhim ahamiyatga ega. Bunga foydalanuvchi maxfiyligini hurmat qilish, ma'lumotlarni noto'g'ri ishlatishdan qochish va ma'lumotlarni yig'ish va foydalanish amaliyoti to'g'risida shaffof bo'lish kiradi. Axloqiy mulohazalar, shuningdek, raqamli vositalarning kengroq ijtimoiy ta'sirini baholash va ularning jamiyatga foyda keltiradigan usullarda ishlatilishini ta'minlashni o'z ichiga oladi. Zamonaviy axborot almashinuvida raqamli muhitni himoya qilish hukumatlar, tashkilotlar va shaxslar o'rtasida hamkorlikni talab qiladigan doimiy mas'uliyatdir. Ma'lumotlarning maxfiyligi va xavfsizligiga ustuvor ahamiyat berish, kiberxavfsizlik bo'yicha mustahkam choralarni amalga oshirish, tartibga muvofiqlikni ta'minlash, raqamli savodxonlikni targ'ib qilish va axloqiy amaliyotlarga rioya qilish orqali biz xavfsiz, ishonchli va ishonchli raqamli landshaftni yaratishimiz mumkin. Ushbu yaxlit yondashuv nafaqat ma'lumotni himoya qiladi, balki barqaror raqamli kelajak uchun asos yaratadi.

Foydalanilgan adabiyotlar

1. *Axborot xavfsizligi*. Ganiyev, S. K.. 2017.
2. Axborot xavfsizligi qoidalari Daminov Husniddin Gulmat o‘g‘li

3. “Axborot-kommunikatsiya texnologiyalarini yanada rivojlantirishga oid qo‘shimcha chora-tadbirlar to‘g‘risida” O‘zbekiston Respublikasi Prezidentining 2005 yil 8 iyuldagi-117-son qarori.

4. Kadrlarni tayyorlash milliy dasturi // Xalq ta’limi. 1998 №1. S.5-41.

5. A.Parpiyev, A.Maraximov, R.Hamdamov, U.Begimqulov, M.Bekmuradov, N.Taylokov. Yangi axborot texnologiyalari. Oliy muassasalari uchun. O‘zME davlat ilmiy nashriyoti.-T.: 2008, 118 b.

6. Abduqodirov A. A. Теория и практика интенсификации подготовки учителей физико-математических дисциплин. Аспект использования компьютерных средств в учебно-воспитательном Автореф...докт.пед.наук.

7. Abduqodirov A. A. va boshq. Axborot texnologiyasi fani bo‘yicha kasb-hunar kollejlari uchun o‘quv dasturi. - Toshkent: 2000.- 8 bet.

8. “Axborot-kommunikatsiya texnologiyalarini yanada rivojlantirishga oid qo‘shimcha chora-tadbirlar to‘g‘risida” O‘zbekiston Respublikasi Prezidentining 2005 yil 8 iyuldagi-117-son qarori.

9. Kiber xavfsizlik asoslari : S.K.Ganiyev A.A.Ganiyev. Z.T.Xudoykulov

10. Axborot texnologiyalari (A.Abduqodirov, A.Hayitov, R.Shodiyev)

11. Axborot texnologiyalari (M.Aripov, B.Begalov va b.)

12. Axborot tizimlari va texnologiyalari (S.G'ulomov, R.Alimov va b.)