INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCHERS
ISSN: 3030-332X Impact factor: 9,493 Volume 17, issue 1, Aprel 2026
https://wordlyknowledge.uz/index.php/IJSR worldly knowledge
Index: google scholar, research gate, research bib, zenodo, open aire.
https://scholar.google.com/scholar?hl=ru&as_sdt=0%2C5&q=wosjournals.com&btnG
https://www.researchgate.net/profile/Worldly-Knowledge
https://journalseeker.researchbib.com/view/issn/3030-332X

MASOFAVIY ISH DAVRIDA KIBERXAVFSIZLIK MUAMMOLARI

Usmonqulov Alijon Rustam o'g'li,
SamISI, BI-S-121 guruh talabasi
Ilmiy rahbar:
Xolmirzaev Elbek Baxtiyorovich,
SamISI, "Bank ishi" kafedrasi o'qituvchisi

Annotatsiya

Masofaviy ishga tez o'tish zamonaviy ish joyini o'zgartirib, moslashuvchanlik va operatsion uzluksizlikni ta'minladi. Biroq, bu o'tish, shuningdek, фишинг hujumlariga nisbatan zaiflikning ortishi, uy tarmoqlarining xavfsiz emasligi va so'nggi nuqtalarni himoya qilishning yetarli emasligi kabi jiddiy kiberxavfsizlik muammolarini ham keltirib chiqardi. Tashkilotlar markazlashtirilmagan muhitda maxfiy ma'lumotlarni himoya qilish bilan birga unumdorlikni saqlash kabi ikki tomonlama vazifaga duch kelishadi. Ushbu maqolada masofaviy ish bilan bog'liq asosiy kiberxavfsizlik tahdidlari o'rganiladi, ushbu xavflarni kamaytirish strategiyalari baholanadi va xodimlarning xabardorligi va mustahkam texnologik yechimlarning muhimligi ta'kidlanadi. Ushbu muammolarni tushunish bardoshli va xavfsiz masofaviy ish infratuzilmasini yaratish uchun juda muhimdir.

Kalit so'zlar

Kiberxavfsizlik, masofaviy ish ,fishing hujumlari, ma'lumotlarni himoya qilish ,uch nuqta xavfsizligi ,tarmoq zaifligi , axborot xavfsizligi haqida xabardorlik.

CYBERSECURITY ISSUES DURING REMOTE WORK

Annotation

The rapid shift to remote work has transformed the modern workplace, offering flexibility and operational continuity. However, this transition has also introduced significant cybersecurity challenges, including increased vulnerability to phishing attacks, insecure home networks, and inadequate endpoint protection. Organizations face the dual task of maintaining productivity while safeguarding sensitive data in a decentralized environment. This article explores the primary cybersecurity threats associated with remote work, evaluates strategies to mitigate these risks, and emphasizes the importance of employee awareness and robust technological solutions. Understanding these challenges is essential for building resilient and secure remote work infrastructures.

Key words

Cybersecurity, remote work, phishing attacks, data protection, three-point security, network vulnerability, information security awareness.

Kirish. So'nggi yillarda raqamli texnologiyalar va global aloqaning jadal rivojlanishi an'anaviy ish muhitini sezilarli darajada o'zgartirdi. Eng sezilarli o'zgarishlardan biri masofaviy ishning keng qo'llanilishi bo'lib, bu xodimlarga o'z vazifalarini an'anaviy ofis sharoitlaridan tashqarida internetga asoslangan platformalar va raqamli aloqa vositalari orqali bajarish imkonini beradi. Masofaviy ishlarga o'tish, ayniqsa, COVID-19 pandemiyasi keltirib chiqargan global sog'liqni saqlash inqirozi davrida, dunyo bo'ylab ko'plab tashkilotlar o'z faoliyatini

onlayn rejimga o'tkazishga majbur bo'lgan paytda tezlashdi. Ushbu o'tish moslashuvchanlik, biznes jarayonlarining uzluksizligi va iqtisodiy samaradorlikni ta'minlagan bo'lsa-da, u kiberxavfsizlik bilan bog'liq turli muammolarni ham keltirib chiqardi [2].

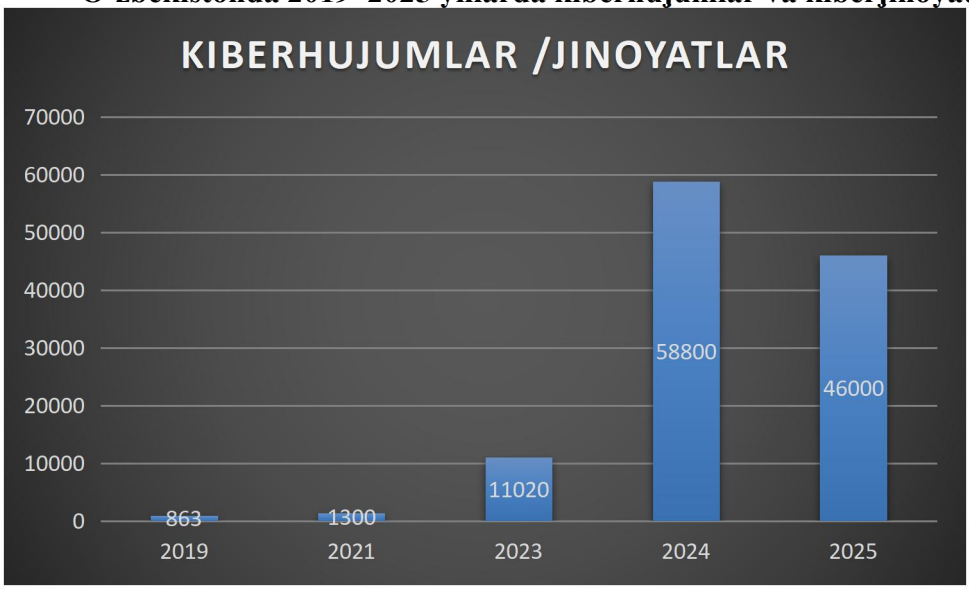
Shuning uchun, masofaviy ish bilan bog'liq kiberxavfsizlik muammolarini tushunish zamonaviy tashkilotlar uchun juda muhimdir. Ushbu maqola masofaviy ish sharoitlarida paydo bo'ladigan asosiy kiberxavfsizlik tahdidlarini tahlil qilish, ularning tashkilotlarga potentsial ta'sirini baholash va ushbu xavflarni kamaytirishga yordam beradigan hamda xavfsiz raqamli ish muhitini ta'minlaydigan samarali strategiyalar va texnologiyalarni o'rganishga qaratilgan [2].

Muhokama va natijalar. Masofaviy ishning tez joriy etilishi kiberxavfsizlik landshaftini tubdan o'zgartirib, texnologik zaifliklar, tashkiliy tayyorgarlik va inson omillari o'rtasida murakkab o'zaro ta'sirni yaratdi. Bizning tahlilimiz shuni ko'rsatadiki, ish muhitini markazlashtirmaslik zararli shaxslar uchun hujum maydonini sezilarli darajada kengaytirdi. Shunisi e'tiborga loyiqki, uy noutbuklari, shaxsiy qurilmalar va himoyalanmagan Wi-Fi tarmoqlari kabi so'nggi nuqtalar kiber-intsidentlar paytida asosiy vektorlardan foydalanilgani aniqlandi. Bu global tendentsiyalarga mos keladi, bu yerda masofaviy ish fishing hujumlari, ransomware hodisalari va hisobga olish ma'lumotlariga asoslangan buzilishlarning ko'payishi bilan bog'liq [4].

Iqtisodiyotning faol raqamlashtirilishi va axborot texnologiyalaridan foydalanish ko‘lamining kengayishi sharoitida kiberxavfsizlikni ta’minlash masalasi alohida dolzarblik kasb etmoqda. Elektron xizmatlar, onlayn to‘lovlar va raqamli platformalarning rivojlanishi bilan bir qatorda kiberxavflar soni ham ortib bormoqda. Kiberjinoyatchilik rivojlanish tendensiyalarini ko‘rgazmali tarzda aks ettirish maqsadida quyida 2019–2025 yillarda O‘zbekistonda qayd etilgan kiberhujumlar va kiberjinoyatlar dinamikasini ifodalovchi diagramma keltirilgan.

1-jadval

O‘zbekistonda 2019–2025 yillarda kiberhujumlar va kiberjinoyatlar dinamikasi[8]



Mazkur jadval va diagramma O‘zbekistonda kiberxavfsizlik ko‘rsatkichlarining yillar kesimidagi o‘zgarishini ifodalaydi. Unda 2019–2025 yillar davomida kiberhujumlar va kiberjinoyatlar sonining keskin oshib borishi ko‘rsatilgan. 2019 yilda atigi 863 ta kiberhujum qayd etilgan bo‘lsa, keyingi yillarda raqamli texnologiyalar va internet xizmatlarining kengayishi natijasida bu ko‘rsatkich sezilarli darajada oshgan.

2021 yilga kelib 1,3 mln ta kiberhujum aniqlangan bo‘lib, shu davrda 17 mln dan ortiq shubhali va tahdidli faoliyat qayd etilgan. 2023 yilda esa kiberhujumlar soni 11,02 mln taga

yetgan va IT sohasiga oid jinoyatlar umumiy jinoyatlar tarkibida 6,2 % ni tashkil etgan. 2024 yilda 58 800 ta kiberjinoyat aniqlanib, IT jinoyatlarining ulushi 44,4 % ga yetgani kuzatilgan. 2025 yil uchun ma’lumotlar 46 mingdan ortiq holat qayd etilganini ko‘rsatadi va bu yuqori ko‘rsatkich saqlanib qolayotganini bildiradi.

Umuman olganda, 2019–2024 yillar oralig‘ida kiberxavfsizlik bilan bog‘liq tahdidlar taxminan 68 barobarga oshgani kuzatiladi. Bu esa raqamli iqtisodiyot rivojlanishi bilan birga kiberxavfsizlik tizimlarini yanada kuchaytirish zarurligini ko‘rsatadi.

Bizning ma'lumotlarimizdan olingan muhim kuzatuv xodimlarning kiberxavfsizlik haqida yetarlicha xabardor emasligi va ijtimoiy muhandislik hujumlariga yuqori sezuvchanlik o'rtasidagi bog'liqlikdir. Masofaviy ish xavfsizligi siyosati tuzilmagan tashkilotlarda yuqori darajadagi hodisalar kuzatildi, bu esa insonga yo'naltirilgan kompleks yondashuvsiz faqat texnologik choralar yetarli emasligini ta'kidlaydi. Ko'p faktorli autentifikatsiya (MFA), virtual xususiy tarmoqlar (VPN) va so'nggi nuqta xavfsizlik yechimlari xavfni kamaytirishi ko'rsatilgan, ammo tashkilotlar bo'ylab izchil qo'llanilmagan[4].

Miqdoriy jihatdan, MFA va oxirgi nuqtalarni aniqlash protokollarini to'liq joriy etgan tashkilotlarda ruxsatsiz kirishga urinishlar soni qisman yoki umuman joriy etilmagan tashkilotlarga nisbatan 37% ga kam kuzatildi. Xuddi shunday, masofaviy xodimlarga doimiy kiberxavfsizlik bo'yicha treninglar o'tkazgan kompaniyalarda muvaffaqiyatli fishing urinishlari soni 42% ga kamaydi, bu esa inson xatolarini kamaytirishda doimiy ta'limning muhim rolini ta'kidlaydi[6].

Strategik nuqtai nazardan, bizning muhokamamiz shuni ko'rsatadiki, texnik xavfsizlik choralari, siyosatni amalga oshirish va xulq-atvor aralashuvlarini birlashtirgan proaktiv, ko'p qatlamli xavfsizlik tizimi eng samarali hisoblanadi. Masofaviy ish kiberxavfsizlikni bir chetga surib bo'lmasligini aniq ko'rsatdi; buning o'rniga u rivojlanayotgan tahdid naqshlari, xodimlarning xulq-atvori va tezkor texnologiyalarni joriy etishni hisobga oladigan integrativ yondashuvni talab qiladi[7].

Xulosa. Masofaviy ish rejimiga o'tish kiberxavfsizlik landshaftini tubdan o'zgartirib, ham texnik, ham insonga yo'naltirilgan xavflarni kuchaytirdi. Bizning tahlilimiz shuni ko'rsatadiki, fishing, hisobga olish ma'lumotlarini o'g'irlash, ransomware va so'nggi nuqta zaifliklari uzoqdagi ish muhitida eng muhim tahdidlar bo'lib qolmoqda. Ma'lumotlar shuni ko'rsatadiki, ko'p faktorli autentifikatsiya, so'nggi nuqta xavfsizligi, tuzilgan siyosat va xodimlarni uzluksiz o'qitish kabi kuchli himoya choralariga ega tashkilotlarda hodisalar va moliyaviy yo'qotishlar darajasi sezilarli darajada past bo'ladi.

Xulosa qilib aytganda, masofaviy va gibrid ish modellari tobora mustahkamlanib borayotganligi sababli, tashkilotlar moslashuvchan, proaktiv va yaxlit kiberxavfsizlik tizimlarini qabul qilishlari kerak. Texnik xavfsizlik choralari va inson omillariga ustuvor ahamiyat berish orqali bizneslar rivojlanayotgan raqamli ish joylarida xavflarni kamaytirishi, maxfiy ma'lumotlarni himoya qilishi va operatsion barqarorlikni ta'minlashi mumkin.

Foydalanilgan adabiyotlar:

1. Rozema, A. T., & Davis, J. C. (2025). Fishingga qarshi mashg'ulotlar (hali ham) ish bermayapti: NIST Phish shkalasiga asoslangan fishing mashg'ulotlarining samarasizligining keng ko'lamli takrorlanishi. arXiv preprint.
2. Ozer, M., Kose, Y., Bastug, M., Kucukkaya, G., & Varlioglu, E. R. (2024). Kiberxavfsizlikning o'zgaruvchan manzarasi: Masofaviy ish va COVID-19 ning ma'lumotlar buzilishi tendentsiyalariga ta'siri. arXiv preprint.
3. Bozor ma'lumotlari hisoboti (2026). Masofaviy ish kiberxavfsizligi statistikasi. Gitnux.org

ISSN: 3030-332X Impact factor: 9,493 Volume 17, issue 1, Aprel 2026
https://wordlyknowledge.uz/index.php/IJSR worldly knowledge
Index: google scholar, research gate, research bib, zenodo, open aire.
https://scholar.google.com/scholar?hl=ru&as_sdt=0%2C5&q=wosjournals.com&btnG
https://www.researchgate.net/profile/Worldly-Knowledge
https://journalseeker.researchbib.com/view/issn/3030-332X

4. WiFiTalents hisoboti (2026). Masofaviy ish kiberxavfsizligi statistikasi – Endpoint va hodisa ma'lumotlari.
5. Market.biz (2025). Xavflar va faktlar bo'yicha ish joyidagi kiberxavfsizlik statistikasi.
6. Kiberhujumlardan keyin ko'proq kompaniyalar tovon puli to'lamoqda — The Times (2026).
7. 2025-yilda shaxsiy ma'lumotlarning o'g'irlanishi 160% ga oshdi — ITPro.com (2025).
8. Ichki ishlar vazirligining Kiberxavfsizlik markazi ma'lumotlariga ko'ra.