KIBER XAVFSIZLIKNI TA’MINLASHDA INSON OMILINING O‘RNI

Rahmatullaeva Lobarxon

Pace University, Lubin Biznes Maktabi

Biznes Boshqaruvi Magistraturasi (MBA)

Biznes Analitika yo‘nalishi bitiruvchisi New-York

Annotatsiya: Maqolada kiber xavfsizlikni ta’minlashda inson omilining roli va uni boshqarish mexanizmlari o‘rganiladi. Tadqiqotlar shuni ko‘rsatdiki, xodimlarning xulq-atvori va bilim darajasi xavfsizlik tizimlarining samaradorligini oshirishi yoki zaiflashtirishi mumkin. Ilmiy izlanishlarga tayangan holda, inson omilini boshqarishning amaliy yo‘llari: xodimlarni muntazam o‘qitish, ichki nazorat tizimini takomillashtirish va kiber xavfsizlik madaniyatini rivojlantirish orqali tizimni barqarorlashtirish zarur ekanligi mazkur maqolada o‘z aksini topgan.

Аннотация: В статье исследуется роль человеческого фактора в обеспечении кибербезопасности и механизмы его контроля. Исследования показали, что поведение и уровень знаний сотрудников могут повысить или ослабить эффективность систем безопасности. Опираясь на научные исследования, в данной статье отражена необходимость стабилизации системы посредством практических путей управления человеческим фактором: регулярного обучения персонала, совершенствования системы внутреннего контроля и развития культуры кибербезопасности.

Abstract: This article explores the role of the human factor in cybersecurity and the mechanisms for managing it. Research has shown that the behavior and knowledge

of employees can either enhance or weaken the effectiveness of security systems. Based on scientific research, this article highlights the need to stabilize the system through practical approaches to managing the human factor, such as regular staff training, improving internal control systems, and fostering a culture of cybersecurity.

Kalit so‘zlar: Kiber xavfsizlik, kiber madaniyat, kiber muhit, inson omili, boshqaruv, axborot, axborot xavfsizligi, axborot xavfsizligi madaniyati, raqamli muhit, raqamlashtirish

Ключевые слова: кибербезопасность, киберкультура, кибер-среда, человеческий фактор, менеджмент, информация, информационная безопасность, культура информационной безопасности, цифровая среда, оцифровка

Keywords: cybersecurity, cyberculture, cyber environment, human factor, management, information, information security, information security culture, digital environment, digitization

Raqamli texnologiyalarning jadal rivojlanishi va boshqaruv jarayonlarining raqamlashtirilishi sharoitida kiber xavfsizlik masalasi zamonaviy jamiyatning ustuvor muammolaridan biriga aylandi. Davlat boshqaruvi, moliyaviy tizimlar, ta’lim va sog‘liqni saqlash kabi muhim sohalarda axborot tizimlaridan keng foydalanilishi kiber tahdidlarning ko‘lami va murakkabligini oshirmoqda. Mazkur jarayonda texnik himoya vositalari bilan bir qatorda inson omili kiber xavfsizlikni ta’minlashda hal qiluvchi omil sifatida namoyon bo‘lmoqda. Amaliyotlar shuni ko‘rsatadiki, kiber hodisalarning sezilarli qismi foydalanuvchilarning ehtiyotsizligi, axborot xavfsizligi qoidalariga rioya etmasligi, yetarli bilim va ko‘nikmalarga ega emasligi bilan bog‘liq. Xodimlarning kiber xavfsizlik madaniyati pastligi, boshqaruv qarorlarida inson omilining yetarlicha hisobga olinmasligi tashkilotlarning axborot xavfsizligiga jiddiy tahdid tug‘diradi. Shu bois kiber xavfsizlikni faqat texnologik muammo sifatida emas,

balki murakkab tashkiliy-boshqaruv jarayoni sifatida ko‘rib chiqish zarurati yuzaga kelmoqda.

Kiber xavfsizlikni ta’minlashda inson omilini boshqarish masalasi xodimlarni tayyorlash, ularning mas’uliyatini oshirish, xavfsizlikka yo‘naltirilgan xulq-atvorni shakllantirish hamda boshqaruv mexanizmlarini takomillashtirish bilan chambarchas bog‘liqdir. Ayniqsa, raqamli transformatsiya sharoitida sun’iy intellekt va avtomatlashtirilgan tizimlardan foydalanish kengayib borayotgan bir paytda, inson va texnologiya o‘rtasidagi o‘zaro aloqani samarali boshqarish muhim ahamiyat kasb etadi.

Ilmiy tadqiqotlar shuni ko‘rsatadiki, “....inson omili kiber xavfsizlik tizimida ikki qarama-qarshi rolni bajaradi: bir tomondan, xodimlarning mas’uliyatli xulq-atvori va yuqori darajadagi xabardorligi mavjud xavfsizlik choralarining samaradorligini oshirsa, ikkinchi tomondan, insoniy xatoliklar, beparvolik va axborot xavfsizligi qoidalariga rioya etmaslik tizimning eng zaif bo‘g‘iniga aylanishi mumkin” [1] ligini, yoki “....xodimlarning texnologik siyosatlarga amal qilmasligi, parollar bilan bog‘liq sustkashlik yoki fishing hujumlariga nisbatan yetarli bilimga ega emasligi kiber hujumlar uchun qulay sharoit yaratadi”[2] deb ta’kidlaganlar.

O‘zbekiston kontekstida kiberxavfsizlik masalalari ko‘plab tadqiqotlarda xavfsizlik madaniyati va inson omilini nazorat qilish orqali yoritilgan. Masalan, Sitora Mahmatmurodova tomonidan chop etilgan maqolada kiberxavfsizlikning zamonaviy jamiyatda o‘rni, xodimlar xatti-harakatlari va xavfsizlik madaniyati ahamiyati ta’kidlanadi. Xususan, inson omilining axborot tizimlarida kiber tahdidlarga qarshi turishda muhim rol o‘ynashi qayd etilgan. Ular, “Inson omili va xavfsizlik madaniyati raqamli jamiyatda barqaror rivojlanish va ishonchli kelajakni ta’minlash uchun muhim omil hisoblanadi.”[3] kabi fikrlarlarga to‘xtalgan.

O‘zbekiston va qo‘shni hududlarda olib borilgan tadqiqotlar ham inson omilining kiberxavfsizlikdagi ahamiyatini tasdiqlaydi. Misol uchun, Jo‘rabek Suyumov va

[1] Alghamdi, A. (2025). Human factors in cybersecurity: an interdisciplinary review. International Journal of Information Security. DOI: 10.1007/s10207-025-01032-0.2025
[2] Zangana, H. M. et al. The Human Factor in Cybersecurity: Addressing the Risks of Insider Threats.2025
[3] Mahmatmurodova S.U. Kiberxavfsizlik va uning zamonaviy jamiyatdagi o‘rni. Universal Science Perspectives International Scientific Practical Journal, 2025.

boshqalar maqolasida **inson omili va ijtimoiy muhandislik** asosiy xavf omillari sifatida ajratiladi. Mualliflar kiber tahdidlarga qarshi samarali himoya tizimi texnologik yechimlar bilan bir qatorda xodimlarning doimiy ta’limi va qat’iy tashkiliy siyosatni birlashtirishi kerakligini ta’kidlaydi.jumladan, “Axborot xavfsizligida yuqori risklar asosan inson omili (ijtimoiy muhandislik) va bulutli konfiguratsiya xatolari bilan bog‘liq”[4]ligi haqida o‘z qarashlarida izohlaganlar.

Bizning fikrimizcha, zamonaviy kiber xavfsizlik tizimlarining barqaror ishlashi nafaqat texnik va dasturiy vositalarga, balki inson omilining samarali boshqarilishiga ham bevosita bog‘liqdir. Tadqiqot jarayonida tahlil qilingan ilmiy manbalar shuni ko‘rsatadiki, axborot tizimlarida yuzaga kelayotgan kiber hodisalarning sezilarli qismi insoniy xatoliklar, beparvolik va axborot xavfsizligi qoidalariga rioya etmaslik bilan izohlanadi. Shu sababli, inson omilini kiber xavfsizlikning ikkinchi darajali elementi sifatida emas, balki strategik resurs sifatida ko‘rib chiqish zarur, deb hisoblaymiz.

Izlanishlarimiz natijalariga ko‘ra, kiber tahdidlarning muhim qismi ijtimoiy muhandislik, fishing hujumlari hamda xodimlarning ichki xatolari bilan bog‘liq. Bizning fikrimizcha, bu holat boshqaruv tizimlarida inson omiliga alohida e’tibor qaratish zarurligini ko‘rsatadi. Axborot xavfsizligi siyosati mavjud bo‘lgan taqdirda ham, agar u xodimlar tomonidan to‘liq anglanmasa va amalda qo‘llanilmasa, kutilgan natijaga erishib bo‘lmaydi.

Shu nuqtai nazardan, inson omili bilan bog‘liq kiber xavflarni aniqlash va baholash boshqaruv faoliyatining ajralmas qismi bo‘lishi lozim, deb hisoblaymiz. Bunda rahbarlarning kiber xavfsizlik masalalariga bo‘lgan munosabati va qaror qabul qilish jarayonida ushbu omilni inobatga olishi muhim ahamiyat kasb etadi.

Kiber xavfsizlikni ta’minlashda inson omilini boshqarish tashkiliy va boshqaruv mexanizmlarini tizimli ravishda joriy etishni talab etadi. Tadqiqotimiz davomida aniqlanishicha, xodimlarni muntazam o‘qitish, axborot xavfsizligi bo‘yicha treninglar

[4] Suyumov J.Y., Xolmatova J.I., Adhamova M.B. Elektron axborot resurslarining xavfsizligi va himoyasi. Modern Education and Development, 2025.

tashkil etish hamda ichki nazorat mexanizmlarini kuchaytirish inson omili bilan bog‘liq xavflarni sezilarli darajada kamaytiradi.

Shuningdek, biz kiber xavfsizlik masalalarini tashkilot strategiyasining muhim tarkibiy qismi sifatida qarash lozim, degan xulosaga keldik. Rahbarlarning shaxsiy mas’uliyati, xodimlarning faoliyatini baholash tizimi va rag‘batlantirish mexanizmlari inson omilining ijobiy rolini kuchaytirishga xizmat qiladi.

Kiber xavfsizlik madaniyatini shakllantirish inson omilini boshqarishning asosiy yo‘nalishlaridan biri sifatida qaraldi. Shunday ekan, kiber xavfsizlik madaniyati shakllangan muassasalarda xodimlar kiber tahdidlarga nisbatan ongli va mas’uliyatli munosabat bildirishga qodir bo‘ladi.

Kiber xavfsizlik madaniyatini shakllantirish bo‘yicha quyidagilarni tavsiya etamiz:

1. ***Xodimlarning kiber xavfsizlik bo‘yicha doimiy xabardorligini oshirish***; kiber xavfsizlik madaniyatini shakllantirishda xodimlarning bilim darajasini muntazam yangilab borish muhim ahamiyatga ega. Shu sababli, treninglar, seminarlar va qisqa amaliy mashg‘ulotlarni tizimli ravishda tashkil etish zarur.

2. ***Axborot xavfsizligi qoidalarini institutsional darajada mustahkamlash***; kiber xavfsizlikka oid ichki me’yoriy hujjatlar, yo‘riqnomalar va siyosatlarni ishlab chiqish hamda ularning barcha xodimlar tomonidan majburiy bajarilishini ta’minlash madaniyatni shakllantirishning muhim sharti hisoblanadi.

3.***Rahbarlarning shaxsiy namunasini kuchaytirish;*** rahbarlarning kiber xavfsizlikka mas’uliyatli munosabati va shaxsiy namunasi xodimlarda xavfsizlikka nisbatan ongli yondashuvni shakllantiradi. Rahbarlar ushbu jarayonda yetakchi rolni bajarishi lozim.

4.***Inson omiliga asoslangan kiber risklarni muntazam baholash;*** tashkilotlarda inson omili bilan bog‘liq kiber xavflarni aniqlash va baholash mexanizmlarini joriy etish kiber xavfsizlik madaniyatini tizimli rivojlantirishga xizmat qiladi.

5. ***Ijtimoiy muhandislik va fishing hujumlariga qarshi amaliy mashg‘ulotlar o‘tkazish***; xodimlarning real tahdidlarga nisbatan tayyorgarligini oshirish maqsadida fishing simulyatsiyalari va amaliy treninglarni o‘tkazish samarali natija beradi.

6. ***Xodimlarning mas’uliyatini va shaxsiy javobgarligini kuchaytirish***; kiber xavfsizlik qoidalariga rioya etish har bir xodimning shaxsiy mas’uliyati sifatida belgilanishi, bu borada rag‘batlantirish va intizomiy choralar tizimi ishlab chiqilishi lozim.

7. ***Kiber xavfsizlik madaniyatini baholash va monitoring qilish tizimini joriy etish;*** odimlarning bilim darajasi, xulq-atvori va xavfsizlik qoidalariga amal qilish holatini muntazam monitoring qilish orqali madaniyatning rivojlanish darajasini baholab borish mumkin.

8. ***Ta’lim va boshqaruv jarayonlariga kiber xavfsizlikni integratsiya qilish***; kiber xavfsizlik madaniyati alohida tadbir sifatida emas, balki ta’lim, boshqaruv va kundalik faoliyatning ajralmas qismi sifatida qaralishi lozim.

Natijada, inson omili kiber xavfsizlik tizimining zaif bo‘g‘ini emas, balki uning barqarorligi va ishonchliligini ta’minlovchi muhim omilga aylanishi mumkin, degan xulosaga kelamiz.

Xulosalar shuni ko‘rsatdiki, kiber xavfsizlikni ta’minlashda inson omili strategik ahamiyatga ega bo‘lib, u tizimning samaradorligini oshiruvchi yoki zaiflashtiruvchi omil sifatida namoyon bo‘ladi. Xodimlarning bilim darajasi, xulq-atvori va axborot xavfsizligiga mas’uliyati kiber tahdidlarga qarshi kurashishning samaradorligini belgilaydi. Shu sababli, inson omilini boshqarish jarayoni kiber xavfsizlikning ajralmas qismi sifatida qaralishi lozim.

Maqolada keltirilgan tahlillar va tavsiyalar asosida samarali boshqaruv mexanizmlari quyidagilarni o‘z ichiga oladi: xodimlarni muntazam o‘qitish, ichki nazorat tizimini takomillashtirish, rahbarlarning mas’uliyatini oshirish hamda kiber xavfsizlik madaniyatini rivojlantirish. Ushbu yondashuv inson omilini tizimning zaif

bo‘g‘ini emas, balki barqarorligini ta’minlovchi asosiy resursga aylantirish imkonini beradi.

Foydalanilgan adabiyotlar ro‘yxati

1. Alghamdi, A. (2025). Human factors in cybersecurity: an interdisciplinary review. International Journal of Information Security. DOI: 10.1007/s10207-025-01032-0.2025
2. Zangana, H. M. et al. The Human Factor in Cybersecurity: Addressing the Risks of Insider Threats.2025
3. Mahmatmurodova S.U. Kiberxavfsizlik va uning zamonaviy jamiyatdagi o‘rni. Universal Science Perspectives International Scientific Practical Journal, 2025.
4. Suyumov J.Y., Xolmatova J.I., Adhamova M.B. Elektron axborot resurslarining xavfsizligi va himoyasi. Modern Education and Development, 2025.
5. Jafarli, M. The Role of Human Factors and Awareness in Cybersecurity. Global Spectrum of Research and Humanities. 2025
6. Rustandi, A. M. Role of Human Factors in Cyber Security Awareness: A Systematic Literature Review. Quanta Research Journal.-2025