MULTIDISCIPLINARY JOURNAL: FUNDAMENTAL RESEARCH SCIENTIFIC JOURNAL
VOLUME 02. ISSUE 07. JULY 2026.
ResearchBib Impact Faktor: 13.943 ISSN: 3060-513X

UDK 004.056

RAQAMLI ASRDA KIBERXAVFSIZLIK: TAHDIDLAR, HIMOYA MEXANIZMLARI VA YANGI TENDENSIYALAR

Malikov Abdurashidxon Jasurxon o'g'li
Muhammad Al-Xorazmiy nomidagi ixtisoslashtirilgan maktab o'quvchisi, O'zbekiston Respublikasi

ANNOTATSIYA

Iqtisodiy, davlat boshqaruvi va ijtimoiy jarayonlarning tezkor raqamlashtirilishi kiberxavfsizlikni XXI asrning eng dolzarb muammolaridan biriga aylantirdi. Ushbu maqolada zamonaviy kiberxavfsizlik tahdidlarining asosiy turlari, ularga qarshi qo'llaniladigan texnik va tashkiliy mexanizmlar, shuningdek axborotni himoya qilishni tartibga soluvchi xalqaro va milliy standartlar ko'rib chiqiladi. So'nggi sanoat hisobotlari va me'yoriy hujjatlarga asoslangan qiyosiy-tahliliy yondashuv yordamida o'tkazilgan tadqiqot shuni ko'rsatadiki, fishing va login-parollarning noto'g'ri ishlatilishi kabi inson omili bilan bog'liq holatlar hujumchilar uchun asosiy kirish nuqtasi bo'lib qolmoqda, shu bilan birga ma'lumotlar buzilishining o'rtacha global qiymati o'sishda davom etmoqda. Maqolada asosiy kiberhujum turlari va yetakchi xalqaro kiberxavfsizlik freymvorklari ikkita jadvalda taqqoslanadi hamda samarali himoya texnik, tashkiliy va huquqiy strategiyalarning uyg'unlashuvini, jumladan xodimlarni muntazam o'qitish, zaifliklarni o'z vaqtida bartaraf etish va NIST Kiberxavfsizlik Freymvorki, ISO/IEC 27001 kabi tan olingan standartlarga rioya qilishni talab qilishi haqida xulosa qilinadi.

KALIT SO'ZLAR: kiberxavfsizlik; axborot xavfsizligi; kiberhujum; fishing; ransomware; ma'lumotlar buzilishi; NIST Kiberxavfsizlik Freymvorki; ISO/IEC 27001; xavflarni boshqarish; muhim axborot infratuzilmasi.

KIRISH

So'nggi o'n yillikda axborot-kommunikatsiya texnologiyalari bank tizimi, sog'liqni saqlash, ta'lim, davlat boshqaruvi va sanoat ishlab chiqarishining asosiy tayanchiga aylandi. Raqamli infratuzilmaga bunday qaramlik, o'z navbatida, zararli niyatli shaxslar uchun mavjud bo'lgan "hujum maydoni"ni kengaytirdi va kiberxavfsizlikni davlatlar, tashkilotlar hamda alohida foydalanuvchilar uchun strategik ustuvorlikka aylantirdi. Kiberxavfsizlik deganda tarmoqlar, qurilmalar,

dasturlar va ma'lumotlarni ruxsatsiz kirish, zarar yetkazish yoki buzishdan himoya qilishga qaratilgan texnologiyalar, jarayonlar va amaliyotlar majmuasi tushuniladi.

Mavzuning dolzarbligi xalqaro statistik ma'lumotlar bilan ham tasdiqlanadi: Ponemon instituti tomonidan tayyorlangan va IBM homiyligidagi 2024-yilgi "Ma'lumotlar buzilishi xarajatlari" hisobotiga ko'ra, ma'lumotlar buzilishining o'rtacha global qiymati 4,88 million AQSh dollariga yetdi — bu o'tgan yilga nisbatan 10 foizga o'sish bo'lib, pandemiyadan keyingi eng katta yillik sakrashdir. Shu bilan birga, 94 ta davlatda 30 mingdan ortiq xavfsizlik insidentini tahlil qilgan Verizon kompaniyasining 2024-yilgi "Ma'lumotlar buzilishini tekshirish" hisobotida ko'rsatilishicha, buzilishlarning aksariyati hamon xodimning ijtimoiy muhandislik hujumiga uchrashi yoki xatoga yo'l qo'yishi kabi zararli bo'lmagan inson omili bilan bog'liq bo'lib qolmoqda.

O'zbekiston Respublikasida bu masala qonunchilik darajasida "Kiberxavfsizlik to'g'risida"gi Qonun hamda bir qator Prezident farmon va qarorlari orqali tartibga solinadi, jumladan 2020-yilda axborot tizimlari va resurslarini himoya qilish davlat tizimini joriy etish hamda kiberxavfsizlikni ta'minlash tizimini yanada takomillashtirish bo'yicha qabul qilingan chora-tadbirlar, shuningdek axborotni himoya qilishni barqaror raqamli rivojlanishning zaruriy sharti sifatida belgilaydigan "Raqamli O'zbekiston – 2030" strategiyasi. Ushbu maqolaning maqsadi kiberxavfsizlik tahdidlarining asosiy turlarini tizimlashtirish, yetakchi himoya mexanizmlari va xalqaro standartlarni tavsiflash hamda shular asosida tashkiliy darajada kiberxavfsizlikni mustahkamlash bo'yicha amaliy tavsiyalar ishlab chiqishdan iborat.

MATERIAL VA METODLAR

Tadqiqot ochiq sanoat hisobotlari (IBM "Ma'lumotlar buzilishi xarajatlari" hisoboti, 2024; Verizon "Ma'lumotlar buzilishini tekshirish" hisoboti, 2024; ENISA "Tahdidlar landshafti", 2024), xalqaro standartlar va freymvorklar (NIST Kiberxavfsizlik Freymvorki 2.0, ISO/IEC 27001:2022, EI 2016/679-sonli Reglamenti), kriptografiya va xavfsizlik muhandisligi bo'yicha ixtisoslashtirilgan ilmiy adabiyot, shuningdek O'zbekiston Respublikasining axborot va kiberxavfsizlikni tartibga soluvchi qonunchilik hujjatlari tahliliga asoslanadi. Tadqiqotda qiyosiy-tahliliy metod qo'llanildi: hujum turlari, ularning chastotasi va qiymati bo'yicha to'plangan ma'lumotlar tasniflash jadvaliga tizimlashtirildi, ko'rib chiqilgan standart va

freymvorklar esa ularni ishlab chiquvchi tashkilot va asosiy yo'nalishi bo'yicha ikkinchi jadvalda taqqoslandi. Hisobotlardan olingan miqdoriy ko'rsatkichlarni izohlash va ularni ilmiy adabiyotda tavsiya etilgan himoya mexanizmlari bilan bog'lash uchun qo'shimcha ravishda tavsifiy metoddan foydalanildi.

Material uch mezon asosida tanlandi: dolzarblik (so'nggi ikki-uch yil ichida chop etilgan ma'lumotlar), manbaning ishonchliligi (xalqaro tashkilotlar, standartlashtirish organlari, retsenziyadan o'tgan darsliklar va rasmiy huquqiy hujjatlar) hamda tor texnik yo'nalishdan ko'ra umumiy, tarmoqlararo kiberxavfsizlik konteksti uchun tatbiq etilishi. Bu statistik dalillarni me'yoriy va nazariy material bilan yagona izchil tahliliy doirada birlashtirish imkonini berdi.

NATIJA VA MUHOKAMA

Zamonaviy tahdid ma'lumotlarini tahlil qilish kiberhujumlarning asosiy turlarini ularning ta'sir mexanizmi va xarakterli oqibatlariga ko'ra tasniflash imkonini beradi (1-jadval).

1-jadval. Kiberhujumlarning asosiy turlari va ularning tavsifi

Hujum turi	Mexanizmi	Xarakterli oqibati / misoli
Fishing (phishing)	Foydalanuvchini ishonchli tashkilot nomidan yuborilgan soxta xat, xabar yoki veb-sahifa orqali aldab, login va parollarni yoki zararli dasturni o'rnatishga majbur qilish	So'nggi o'n yil ichida buzilishlarning taxminan uchdan bir qismida ishtirok etgan yetakchi kirish vektori
Dasturlar to'lov talab qilishi (ransomware)	Qurbonning ma'lumotlarini shifrlab, uni ochish uchun to'lov talab qiladigan zararli dastur	Barcha buzilishlarning taxminan uchdan bir qismi to'lov undirishga qaratilgan usullarni, jumladan ransomware'ni o'z ichiga oladi
DDoS-hujum (xizmatni rad etish)	Server yoki tarmoqni bir vaqtning o'zida ko'plab manbalardan yuborilgan ortiqcha trafik bilan to'ldirib,	Xizmat ko'rsatishning to'xtab qolishi, obro'ga putur yetishi, onlayn platformalar uchun daromad yo'qotilishi

	uni ishlamay qolishga majbur qilish	
SQL-in'yeksiya	Tekshirilmagan kiritish maydonlari orqali ma'lumotlar bazasini boshqarish uchun zararli SQL buyruqlarini kiritish	Ma'lumotlar bazasidagi yozuvlarning ruxsatsiz oshkor bo'lishi, o'zgartirilishi yoki o'chirilishi
Zaifliklardan foydalanish (shu jumladan zero-day)	Dasturiy ta'minotdagi yamalanmagan, jumladan hali ma'lum bo'lmagan (zero-day) zaifliklardan foydalanib, ruxsatsiz kirish huquqiga ega bo'lish	2023–2024 yillarda dastlabki kirish vektori sifatida deyarli 3 barobar (180%) o'sish kuzatildi
Ijtimoiy muhandislik	Shaxsni maxfiy ma'lumotni oshkor qilishga yoki xavfsiz bo'lmagan harakatni amalga oshirishga undash uchun psixologik manipulyatsiya qilish	Buzilishlarning aksariyati inson omili bilan bog'liq bo'lganligi sababli, ko'pchilik hujum turlarining asosida yotadi

1-jadvalda ko'rsatilganidek, zamonaviy hujum usullarining aksariyati, oxir-oqibat, texnik zaiflikdan yoki inson xatosidan foydalanadi. Bu xulosa Verizon kompaniyasining topilmalari bilan mos keladi: dastlabki kirish vektori sifatida zaifliklardan foydalanish deyarli 3 barobar (180%) oshdi, bu asosan ransomware hujumchilari tomonidan zero-day zaifliklarning ommaviy ravishda ishlatilishi bilan bog'liq, shuningdek so'nggi o'n yil ichida o'g'irlangan yoki noto'g'ri ishlatilgan login-parollar buzilishlarning taxminan uchdan bir qismida uchragan.

Ushbu hujumlarning moliyaviy o'lchami ham katta ahamiyatga ega. 2024-yilgi IBM hisobotiga ko'ra, o'g'irlangan yoki buzilgan login-parollar bilan bog'liq buzilishlarni aniqlash va nazorat ostiga olish o'rtacha 292 kunni tashkil etdi — bu o'rganilgan boshqa har qanday hujum vektoriga nisbatan uzoqroq muddat bo'lib, ichki zararli niyatli xodimlar tomonidan amalga oshirilgan buzilishlar esa har biri deyarli

besh million AQSh dollarini tashkil etib, eng qimmat turgan. Xavfsizlik operatsiyalarida sun'iy intellekt va avtomatlashtirishdan keng foydalangan tashkilotlar insidentlarni taxminan yuz kun tezroq aniqlab, nazorat ostiga olgan va ulardan foydalanmagan tashkilotlarga nisbatan sezilarli darajada pastroq o'rtacha xarajatlarni qayd etgan, bu esa avtomatlashtirilgan aniqlashning buzilish oqibatlarini cheklashda hal qiluvchi omilga aylanib borayotganini ko'rsatadi.

Ushbu tahdidlarga qarshi kurashish uchun tashkilotlar texnik nazorat vositalari (fayervollar, hujumni aniqlash va oldini olish tizimlari, shifrlash, ko'p bosqichli autentifikatsiya, terminal himoyasi), tashkiliy chora-tadbirlar (xavfsizlik bo'yicha ogohlantirish treninglari, insidentlarga javob berish rejasi, muntazam auditlar) va tan olingan boshqaruv standartlariga rioya qilishning uyg'unlashuvidan foydalanadi. 2-jadvalda ushbu uyg'un yondashuvni tashkil etuvchi eng keng qo'llaniladigan xalqaro va milliy freymvorklarning ba'zilari taqqoslangan.

2-jadval. Yetakchi xalqaro va milliy kiberxavfsizlik standartlari va freymvorklarining qiyosiy tahlili

Standart / freymvork	Ishlab chiquvchi tashkilot	Asosiy yo'nalishi
NIST Kiberxavfsizlik Freymvorki (CSF) 2.0	AQSh Milliy standartlar va texnologiyalar instituti (NIST)	Boshqarish, aniqlash, himoya qilish, aniqlab olish, javob berish va tiklash funksiyalari asosida qurilgan xavf-asosli yondashuv
ISO/IEC 27001:2022	Xalqaro standartlashtirish tashkiloti (ISO)	Axborot xavfsizligini boshqarish tizimini joriy etish, amalga oshirish va uzluksiz takomillashtirish talablari
GDPR (EI 2016/679-sonli Reglamenti)	Yevropa Parlamenti va Kengashi	Shaxsiy ma'lumotlar va maxfiylikni himoya qilish, buzilish yuz berganda majburiy xabar berish talablari

O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni	O'zbekiston Respublikasi Oliy Majlisi	Milliy kiberxavfsizlik tizimi, muhim axborot infratuzilmasini himoya qilish va insidentlarga javob berishning huquqiy asosi

2-jadvaldagi taqqoslash zamonaviy kiberxavfsizlikni boshqarish bir-birini to'ldiruvchi bir necha qatlamga asoslanishini ko'rsatadi: NIST Kiberxavfsizlik Freymvorki kabi texnik xavflarni boshqarish bo'yicha ko'rsatmalar, ISO/IEC 27001 kabi sertifikatlanadigan boshqaruv tizimi talablari, GDPR misolida ko'rsatilgan ma'lumotlarni himoya qilish bo'yicha reglament, hamda muhim axborot infratuzilmasini mamlakat ichida himoya qilishning huquqiy asosini belgilaydigan O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni kabi milliy qonunchilik. O'zbekiston va Markaziy Osiyoning kengroq mintaqasida faoliyat yurituvchi tashkilotlar uchun amaliy xulosa shundan iboratki, bitta standartga rioya qilishning o'zi yetarli emas; samarali himoya ichki texnik nazorat vositalarini xalqaro yaxshi amaliyot bilan ham, milliy qonunchilikning aniq talablari bilan ham muvofiqlashtirishni talab qiladi.

Muhokama, shuningdek, muhim uslubiy jihatni ham ko'rsatadi: buzilishlarning aksariyati sof texnik hujumdan emas, balki inson omili bilan bog'liq nosozlikdan boshlanganligi sababli, texnologiyaga faqat sarmoya kiritish xodimlarni muntazam o'qitish va insidentlarga javob berishning aniq belgilangan madaniyatining o'rnini bosa olmaydi. Bu xulosa xavfsizlikni yagona nazorat vositasining emas, balki butun ijtimoiy-texnik tizimning xususiyati sifatida ko'rib chiqadigan xavfsizlik muhandisligi bo'yicha ilmiy adabiyotga ham mos keladi.

XULOSA

O'tkazilgan tahlil kiberxavfsizlik barqaror raqamli rivojlanishning ajralmas tarkibiy qismiga aylanganini tasdiqlaydi. Hujum turlarini tizimlashtirish shuni ko'rsatadiki, fishing, ransomware, yamalanmagan zaifliklardan foydalanish va ijtimoiy muhandislik hamon ustun tahdidlar bo'lib qolmoqda, shuningdek buzilishlarning aksariyati sof texnik nosozlikdan ko'ra inson omili bilan bog'liq. Xalqaro

freymvorklarni taqqoslash shuni ko'rsatadiki, yagona standartning o'zi yetarli emas: samarali himoya NIST Kiberxavfsizlik Freymvorki kabi xavf-asosli freymvorklar, ISO/IEC 27001 kabi sertifikatlanadigan boshqaruv tizimlari, ma'lumotlarni himoya qilish bo'yicha reglamentlar hamda O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni kabi milliy huquqiy vositalarning birgalikda qo'llanilishini talab qiladi. Shular asosida tashkilotlarga texnik nazorat vositalariga, xodimlarni muntazam o'qitishga, zaifliklarni o'z vaqtida bartaraf etishga va tan olingan standartlarga rasmiy muvofiqlikka bir vaqtning o'zida sarmoya kiritish tavsiya etiladi, chunki bunday uyg'un yondashuv kiber insidentlarning ham ehtimolini, ham moliyaviy oqibatlarini kamaytirishning eng ishonchli yo'lidir. Kelgusi tadqiqotlar ushbu freymvorklarni O'zbekiston va boshqa Markaziy Osiyo davlatlarining raqamli iqtisodiyoti doirasida tarmoq bo'yicha tatbiq etishga qaratilishi maqsadga muvofiqdir.

FOYDALANILGAN ADABIYOTLAR

1. IBM Security. Cost of a Data Breach Report 2024. Armonk, NY: IBM Corporation, Ponemon Institute, 2024.

2. Verizon Business. 2024 Data Breach Investigations Report. New York: Verizon Communications Inc., 2024.

3. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: U.S. Department of Commerce, 2024.

4. International Organization for Standardization. ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO/IEC, 2022.

5. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. Athens: ENISA, 2024.

6. European Parliament and Council of the European Union. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union, 2016.

7. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Boston: Pearson, 2023.

8. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis: Wiley, 2020.

9. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni.

10. O'zbekiston Respublikasi Prezidentining 2020-yil 15-iyundagi "O'zbekiston Respublikasining axborot tizimlari va resurslarini himoya qilish davlat tizimini joriy etish chora-tadbirlari to'g'risida"gi PF-6007-son Farmoni.

11. O'zbekiston Respublikasi Prezidentining 2020-yil 15-iyundagi "O'zbekiston Respublikasida kiberxavfsizlikni ta'minlash tizimini yanada takomillashtirishga doir qo'shimcha chora-tadbirlar to'g'risida"gi PQ-4751-son Qarori.

12. O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi "Raqamli O'zbekiston – 2030" strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to'g'risida"gi PF-6079-son Farmoni.