DOI: 10.65322/j.srd.05192026.62

KIBERXAVFSIZLIK VA RAQAMLI MUHITDA AXBOROTNI HIMOYALASH MASALALARI

Shermatova X.M., *dotsent,*
Axborot texnologiyalari kafedrasi,
E-mail: shermatovahilola1978@gmail.com
Yunusova D.A., *, III-kurs talabasi,*
Axborot - tizimlari va texnologiyalari yo'nalishi,
E-mail: yunusovadilrabo0613@gmail.com
Farg'ona davlat universiteti

Annotatsiya. *Mazkur maqolada raqamli muhitda axborotni himoyalash va kiberxavfsizlikni ta'minlashning zamonaviy masalalari tahlil qilingan. Raqamli texnologiyalar, internet xizmatlari va axborot tizimlarining jadal rivojlanishi natijasida yuzaga kelayotgan phishing, zararli dasturlar, ransomware, DDoS hujumlari, akkauntlarni buzish hamda ijtimoiy muhandislik kabi kiberxavflarning xususiyatlari yoritilgan. Shuningdek, axborotni himoyalashda kuchli parollar, ko'p bosqichli autentifikatsiya, ma'lumotlarni shifrlash, antivirus va firewall vositalari, zaxira nusxalash hamda dasturiy ta'minotni muntazam yangilashning ahamiyati tahlil qilingan.*

Аннотация. *В данной статье анализируются актуальные вопросы защиты информации и кибербезопасности в цифровой среде. Рассматриваются характерные черты таких киберугроз, как фишинг, вредоносное ПО, программы-вымогатели, DDoS-атаки, компрометация учетных записей и социальная инженерия, возникших вследствие стремительного развития цифровых технологий, интернет-сервисов и информационных систем. Кроме того, в статье анализируется значимость таких мер обеспечения информационной безопасности, как использование надежных паролей, многофакторная аутентификация, шифрование данных, применение антивирусного программного обеспечения и межсетевых экранов, резервное копирование данных, а также регулярное обновление программного обеспечения.*

Kalit so'zlar: *kiberxavfsizlik, axborot xavfsizligi, raqamli muhit, raqamli texnologiyalar, kiberhujum, phishing, malware, ransomware, DDoS, kriptografiya, autentifikatsiya.*

Ключевые слова: *кибербезопасность, информационная безопасность, цифровая среда, цифровые технологии, кибератака, фишинг, вредоносное ПО, программы-вымогатели, DDoS, криптография, аутентификация.*

Kirish. Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi jamiyat hayotining deyarli barcha sohalarida tub o'zgarishlarni yuzaga keltirmoqda. Iqtisodiyot, ta'lim, tibbiyot, bank-moliya tizimi, davlat boshqaruvi, sanoat va xizmat ko'rsatish sohalarida raqamli platformalar, axborot tizimlari va internet xizmatlaridan foydalanish ko'lami tobora kengayib bormoqda [1-3]. Raqamlashtirish jarayonining tezlashishi natijasida katta hajmdagi ma'lumotlarni elektron shaklda yaratish, saqlash, qayta ishlash va uzatish imkoniyatlari sezilarli darajada oshdi. Bu jarayon ish samaradorligini yaxshilash, xizmatlarni tezkor ko'rsatish va boshqaruv jarayonlarini avtomatlashtirish uchun katta imkoniyatlar yaratmoqda. Internet tarmog'ining keng tarqalishi esa axborot almashinuvi jarayonlarini yanada tezlashtirdi. Hozirgi vaqtda foydalanuvchilar turli axborot resurslari, elektron xizmatlar, ijtimoiy tarmoqlar, bulutli platformalar va onlayn tizimlardan kundalik faoliyatida muntazam foydalanmoqda. Tashkilotlar faoliyatida ham turli axborot tizimlarining o'zaro bog'lanishi va yagona raqamli muhitda ishlashi kuzatilmoqda [4-8]. Bunday integratsiya ma'lumotlardan tezkor foydalanish imkonini bersa-da, axborot tizimlarining turli kiberxavflarga duch kelish ehtimolini ham oshirmoqda.

DOI: 10.65322/j.srd.05192026.62

Raqamli muhitda axborot nafaqat oddiy ma’lumotlar yig‘indisi, balki tashkilotlar, korxonalar va davlat uchun muhim strategik resurs sifatida namoyon bo‘lmoqda. Moliyaviy ma’lumotlar, shaxsiy ma’lumotlar, tijorat sirlari, ilmiy tadqiqot natijalari va davlat axborot resurslarining yo‘qolishi yoki ruxsatsiz tarqalishi jiddiy iqtisodiy va tashkiliy oqibatlarga olib kelishi mumkin. Shu sababli axborotning maxfiyligi, yaxlitligi va mavjudligini ta’minlash raqamli tizimlardan foydalanishning eng muhim shartlaridan biriga aylanmoqda. Shu bilan birga, raqamli texnologiyalarning rivojlanishi bilan kiberjinoyatchilik va kiberhujumlarning shakllari ham takomillashib bormoqda. Foydalanuvchilarning login va parollarini qo‘lga kiritishga qaratilgan fishing hujumlari, zararli dasturlar, ransomware, DDoS hujumlari, ijtimoiy muhandislik va boshqa tahdidlar axborot tizimlari xavfsizligiga jiddiy xavf tug‘dirmoqda. Ayniqsa, inson omili bilan bog‘liq xatolar kiberxavfsizlikdagi zaif nuqtalardan biri bo‘lib qolmoqda. Foydalanuvchining shubhali havolani ochishi, noma’lum faylni yuklab olishi yoki maxfiy ma’lumotlarni begona shaxslarga berishi butun tizim xavfsizligiga salbiy ta’sir ko‘rsatishi mumkin.

Kiberxavfsizlik tushunchasi va uning asosiy vazifalari. Kiberxavfsizlik - raqamli texnologiyalar, axborot tizimlari, kompyuter tarmoqlari, dasturiy ta’minot hamda ularda saqlanadigan ma’lumotlarni turli xil kiberxavflardan himoya qilishga qaratilgan texnik, tashkiliy va huquqiy choralar majmuasidir. Raqamli muhitning kengayishi natijasida insonlar va tashkilotlarning faoliyati tobora ko‘proq axborot tizimlariga bog‘lanib borayotganligi sababli kiberxavfsizlik zamonaviy axborot jamiyatining muhim tarkibiy qismiga aylandi. Uning asosiy maqsadi axborot resurslaridan qonuniy va xavfsiz foydalanishni ta’minlash, ruxsatsiz kirishlarning oldini olish hamda kiberhodisalar yuzaga kelganda ularning salbiy oqibatlarini imkon qadar kamaytirishdan iborat. Kiberxavfsizlik tushunchasi faqat kompyuter yoki serverlarni viruslardan himoya qilish bilan cheklanmaydi. U butun raqamli infratuzilmaning xavfsizligini ta’minlashni nazarda tutadi. Bunga kompyuterlar, mobil qurilmalar, serverlar, ma’lumotlar bazalari, bulutli xizmatlar, telekommunikatsiya tarmoqlari, veb-saytlar va turli axborot tizimlarining himoyasi kiradi. Shuningdek, foydalanuvchilarning raqamli xavfsizlik qoidalariga rioya qilishi ham ushbu jarayonning muhim qismi hisoblanadi.

Kiberxavfsizlikning muhim tamoyillaridan biri axborotning maxfiyligini ta’minlash hisoblanadi. Maxfiylik ma’lumotlardan faqat tegishli huquqqa ega bo‘lgan shaxslar foydalanishini anglatadi. Masalan, bank hisob raqamlari, shaxsiy ma’lumotlar, korxonaning tijorat sirlari yoki davlatga oid ma’lumotlar begona shaxslar tomonidan qo‘lga kiritilmasligi kerak. Buning uchun autentifikatsiya, avtorizatsiya, ma’lumotlarni shifrlash va kirish huquqlarini boshqarish kabi mexanizmlardan foydalaniladi. Kiberxavfsizlikning yana bir muhim jihati axborot va xizmatlarning mavjudligini ta’minlashdir. Foydalanuvchilar kerakli vaqtda axborot tizimlari va raqamli xizmatlardan foydalana olishi lozim. Tizimning ishdan chiqishi, serverlarning bloklanishi yoki DDoS kabi hujumlar natijasida xizmatlarning vaqtincha ishlamasligi tashkilotga moddiy va tashkiliy zarar yetkazishi mumkin. Shu sababli tizimlarning uzluksiz ishlashini ta’minlash, zaxira infratuzilmasidan foydalanish va favqulodda holatlarga tayyorgarlik ko‘rish kiberxavfsizlikning muhim vazifalaridan biridir. Kiberxavfsizlikning vazifalari orasida kiberhujumlarni oldini olish, aniqlash, ularga javob qaytarish va zararni tiklash jarayonlari alohida o‘rin tutadi. Zamonaviy xavfsizlik tizimlari tarmoqdagi shubhali faoliyatni doimiy kuzatib boradi va xavfli harakatlarni aniqlashga yordam beradi. Hujum sodir bo‘lgan taqdirda esa uning manbasini aniqlash, zararlangan tizimlarni ajratish, xavfni bartaraf etish va normal faoliyatni qayta tiklash talab etiladi.

Raqamli muhitdagi asosiy kiberxavfsizlik tahdidlari. Raqamli texnologiyalarning keng qo‘llanilishi bilan bir qatorda axborot tizimlariga nisbatan turli xil kiberxavflar ham ortib bormoqda. Kiberjinoyatchilar foydalanuvchilarning shaxsiy ma’lumotlari, moliyaviy resurslari, korxonalarning axborot bazalari va boshqa muhim raqamli aktivlarini qo‘lga kiritish uchun turli texnik va psixologik usullardan foydalanmoqda. Bunday tahdidlar nafaqat yirik tashkilotlar, balki oddiy internet foydalanuvchilari uchun ham jiddiy xavf tug‘diradi. Shu sababli zamonaviy raqamli

DOI: 10.65322/j.srd.05192026.62

muhitda mavjud kiberxavflarni tushunish va ulardan himoyalanish usullarini bilish muhim ahamiyatga ega. Keng tarqalgan kiberxavflardan biri phishing bo‘lib, bunda tajovuzkorlar foydalanuvchini aldash orqali maxfiy ma’lumotlarni qo‘lga kiritishga harakat qiladi. Odatda bunday hujumlar elektron pochta, messenjerlar, ijtimoiy tarmoqlar yoki soxta veb-saytlar orqali amalga oshiriladi. Foydalanuvchiga bank, tashkilot yoki boshqa ishonchli manbadan yuborilgandek ko‘rinadigan xabar kelishi va undan login, parol, bank karta ma’lumotlari yoki tasdiqlash kodini kiritish talab qilinishi mumkin. Phishing hujumlarining xavfliligi shundaki, ular ko‘pincha murakkab texnik vositalardan ko‘ra insonning ishonuvchanligi va e’tiborsizligidan foydalanadi.

Keng tarqalgan kiberxavflardan biri phishing bo‘lib, bunda tajovuzkorlar foydalanuvchini aldash orqali maxfiy ma’lumotlarni qo‘lga kiritishga harakat qiladi. Odatda bunday hujumlar elektron pochta, messenjerlar, ijtimoiy tarmoqlar yoki soxta veb-saytlar orqali amalga oshiriladi. Foydalanuvchiga bank, tashkilot yoki boshqa ishonchli manbadan yuborilgandek ko‘rinadigan xabar kelishi va undan login, parol, bank karta ma’lumotlari yoki tasdiqlash kodini kiritish talab qilinishi mumkin. Phishing hujumlarining xavfliligi shundaki, ular ko‘pincha murakkab texnik vositalardan ko‘ra insonning ishonuvchanligi va e’tiborsizligidan foydalanadi. Tarmoq xizmatlarining ishlashiga qaratilgan tahdidlar orasida DDoS hujumlar ham alohida o‘rin egallaydi. Bunday hujumlarda server yoki internet xizmatiga juda katta miqdorda so‘rovlar yuborilib, uning normal ishlashiga xalaqit beriladi. Natijada veb-sayt yoki onlayn xizmat foydalanuvchilar uchun sekinlashishi yoki vaqtincha ishlamay qolishi mumkin. DDoS hujumlari ayniqsa elektron tijorat, bank xizmatlari va doimiy onlayn faoliyatga bog‘liq tashkilotlar uchun sezilarli xavf tug‘diradi. Kiberxavfsizlikdagi muhim tahdidlardan yana biri ijtimoiy muhandislik hisoblanadi. Bu usulda texnik zaiflikdan ko‘ra insonning psixologik xususiyatlaridan foydalanishga e’tibor qaratiladi. Tajovuzkor o‘zini tashkilot xodimi, bank vakili, tanish inson yoki boshqa ishonchli shaxs sifatida ko‘rsatib, foydalanuvchini ma’lum bir harakatni bajarishga undashi mumkin. Masalan, maxfiy ma’lumotni aytish, havolaga kirish yoki tasdiqlash kodini yuborish so‘ralishi mumkin. Shu sababli foydalanuvchilarning kiberxavfsizlik bo‘yicha bilim va hushyorligini oshirish texnik himoya vositalari kabi muhimdir.

Axborotni himoyalashning zamonaviy usullari. Raqamli muhitda axborotni himoyalash birgina texnik vositadan foydalanish bilan cheklanmaydi. Samarali himoya tizimi foydalanuvchi, dasturiy ta’minot, tarmoq va ma’lumotlar darajasidagi xavfsizlik choralarining o‘zaro uyg‘unligiga asoslanadi. Ayniqsa, kiberhujumlarning tobora murakkablashib borayotgani sababli “bitta vosita - bitta himoya” tamoyili o‘zini oqlamaydi. Masalan, kuchli antivirus dasturi mavjud bo‘lsa ham, foydalanuvchi akkaunti oddiy parol bilan himoyalangan bo‘lsa, tajovuzkor aynan shu zaif nuqtadan foydalanishi mumkin. Demak, axborot xavfsizligida himoya qatlamlarini bir-birini to‘ldiradigan tarzda tashkil etish muhimdir.

Foydalanuvchi akkauntlarini himoyalashning eng oddiy, biroq samarali vositalaridan biri kuchli va noyob parollardan foydalanishdir. Parolning murakkabligi uning uzunligi, turli belgilar kombinatsiyasi va boshqa xizmatlarda takrorlanmasligi bilan belgilanadi. Ayniqsa, bitta paroldan elektron pochta, ijtimoiy tarmoq, bank ilovasi va boshqa xizmatlarda birgalikda foydalanish xavfsizlik nuqtayi nazaridan katta muammo tug‘diradi. Bitta xizmatdagi ma’lumotlar sizib chiqishi natijasida boshqa akkauntlar ham xavf ostida qolishi mumkin. Shu sababli har bir muhim raqamli xizmat uchun alohida paroldan foydalanish va ularni xavfsiz parol menejerlari yordamida boshqarish maqsadga muvofiqdir. Biroq faqat parolga tayanish zamonaviy raqamli muhit uchun yetarli emas. Shu nuqtada ikki bosqichli yoki ko‘p omilli autentifikatsiya qo‘shimcha himoya qatlamini hosil qiladi. Ushbu yondashuvda foydalanuvchini aniqlash faqat parol orqali emas, balki qo‘shimcha tasdiqlash vositasi yordamida amalga oshiriladi. Masalan, parol kiritilgandan keyin mobil qurilmaga yuborilgan kodni tasdiqlash yoki maxsus autentifikatsiya ilovasidan foydalanish talab qilinishi mumkin. Natijada tajovuzkor foydalanuvchining parolini bilgan taqdirda ham

DOI: 10.65322/j.srd.05192026.62

akkauntga kirishda qo‘shimcha to‘siqqa duch keladi. Shu jihatdan ko‘p omilli autentifikatsiya ayniqsa elektron pochta, moliyaviy xizmatlar va muhim axborot tizimlarida qo‘llash uchun muhim vositalardan biridir

Axborot tizimlarining xavfsizligi ko‘p jihatdan dasturiy ta’minotning yangilangan holatda bo‘lishiga ham bog‘liq. Dasturlarda aniqlangan zaifliklar kiberjinoyatchilar tomonidan tizimga kirish uchun foydalanilishi mumkin. Ishlab chiquvchilar bunday zaifliklarni bartaraf etish maqsadida xavfsizlik yangilanishlarini taqdim etadilar. Agar foydalanuvchi yoki tashkilot ushbu yangilanishlarni uzoq vaqt davomida o‘rnatmasa, mavjud zaifliklardan foydalanish ehtimoli ortadi. Shu sababli operatsion tizim, brauzer, antivirus va boshqa muhim dasturlarni muntazam yangilab borish kiberxavfsizlikning oddiy, ammo samarali choralaridan biri hisoblanadi.

Quyidagi model axborotni himoyalashning kompleks yondashuvini ifodalashi mumkin:

Kuchli parol → Ko‘p omilli autentifikatsiya → Shifrlash → Tarmoq va qurilma himoyasi → Zaxira nusxa → Muntazam yangilash

Bu vositalarning har biri alohida xavfsizlik qatlamini hosil qiladi. Bir qatlam buzilgan taqdirda, keyingi qatlamlar axborotni himoyalashni davom ettiradi. Masalan, foydalanuvchi phishing hujumi sababli parolini oshkor qilgan taqdirda, ko‘p omilli autentifikatsiya akkauntga kirishni cheklashi mumkin. Agar zararli dastur tizimga kirib, fayllarni shifrlasa, oldindan yaratilgan zaxira nusxasi ma’lumotlarni qayta tiklash imkonini beradi. Shu sababli zamonaviy kiberxavfsizlikda asosiy e’tibor alohida himoya vositasiga emas, balki bir nechta xavfsizlik mexanizmlarining o‘zaro bog‘langan tizimiga qaratilishi lozim.

1-jadval

Zamonaviy kiberxavfsizlikda himoya

Himoya usuli	Asosiy maqsadi	Himoyalaydigan xavf
Kuchli parol	Akkauntga kirishni cheklash	Parolni buzish
Ko‘p omilli autentifikatsiya	Qo‘shimcha tekshiruv	Akkauntni o‘g‘irlash
Shifrlash	Ma’lumot mazmunini yashirish	Ma’lumot sizib chiqishi
Antivirus	Zararli dasturlarni aniqlash	Malware
Firewall	Tarmoq ulanishlarini nazorat qilish	Ruxsatsiz kirish
Zaxira nusxa	Ma’lumotni tiklash	Ransomware, texnik nosozlik
Yangilash	Zaifliklarni bartaraf etish	Dasturiy hujumlar

O‘zbekistonda kiberxavfsizlikni rivojlantirish istiqbollari. O‘zbekistonda so‘nggi yillarda raqamli texnologiyalarning jadal rivojlanishi davlat boshqaruvi, bank-moliya, ta’lim, tibbiyot, savdo va boshqa ko‘plab sohalarda elektron xizmatlardan foydalanish imkoniyatlarini kengaytirmoqda. Davlat va xususiy tashkilotlarning raqamli platformalarga o‘tishi fuqarolar uchun xizmatlardan masofadan foydalanish, hujjatlarni elektron shaklda almashish va turli jarayonlarni avtomatlashtirish imkonini bermoqda. Biroq raqamli xizmatlar sonining ortishi bilan ular orqali qayta ishlanadigan ma’lumotlarning hajmi ham oshadi. Natijada ushbu ma’lumotlarni ruxsatsiz foydalanish, o‘g‘irlash, o‘zgartirish yoki yo‘q qilishdan himoyalash masalasi yanada dolzarb ahamiyat kasb etmoqda. Raqamli xizmatlarning kengayishi sharoitida axborot tizimlarining ishonchli ishlashi mamlakat raqamli infratuzilmasining muhim ko‘rsatkichlaridan biri hisoblanadi. Davlat idoralari, banklar, ta’lim muassasalari va yirik tashkilotlarda katta hajmdagi ma’lumotlar elektron tizimlarda saqlanayotgani sababli ularning xavfsizligini ta’minlash kompleks yondashuvni talab qiladi. Bunda axborot tizimlarini muntazam auditdan o‘tkazish, mavjud zaifliklarni aniqlash, dasturiy ta’minotni yangilash, foydalanuvchilarning kirish huquqlarini nazorat qilish va ma’lumotlarning zaxira nusxalarini yaratish muhim ahamiyatga ega.

DOI: 10.65322/j.srd.05192026.62

O‘zbekistonda kiberxavfsizlikni rivojlantirish istiqbolini “texnologiya + mutaxassis + foydalanuvchi” uchligi orqali ko‘rib chiqish mumkin. Zamonaviy texnologiyalar xavflarni aniqlash va oldini olish uchun zarur bo‘lsa, malakali mutaxassislar ushbu tizimlarni boshqaradi va takomillashtiradi. Raqamli savodxon foydalanuvchilar esa kiberhujumlarning inson omili bilan bog‘liq qismini kamaytirishga xizmat qiladi. Ushbu uch yo‘nalishning birgalikdagi rivojlanishi mamlakatning raqamli infratuzilmasini yanada barqaror va xavfsiz qilishga yordam beradi. Bundan tashqari, kelajakda sun’iy intellekt, mashinaviy o‘qitish va avtomatlashtirilgan monitoring tizimlaridan kiberxavfsizlikda foydalanish imkoniyatlari kengayishi kutiladi. Bunday texnologiyalar katta hajmdagi ma’lumotlarni tezkor tahlil qilish, noodatiy faoliyatni aniqlash va potensial xavflar haqida oldindan signal berish imkonini yaratadi. Shu bilan birga, sun’iy intellektning o‘zi ham yangi kiberxavflar manbai bo‘lishi mumkinligi sababli ushbu texnologiyalarni xavfsiz va mas’uliyatli qo‘llash masalasiga ham alohida e’tibor qaratish lozim.

Natijalar va muhokama. Maqolada kiberxavfsizlik va raqamli muhitda axborotni himoyalash bilan bog‘liq masalalarni tahlil qilish natijasida axborot xavfsizligining samaradorligi bir nechta o‘zaro bog‘liq omillarga bevosita bog‘liqligi aniqlandi. Raqamli texnologiyalardan foydalanish ko‘lami kengaygani sari kiberxavflarning shakllari ham murakkablashib bormoqda. Shu sababli faqat bitta himoya vositasidan foydalanish zamonaviy tahdidlarni to‘liq bartaraf etish imkonini bermaydi. Samarali kiberxavfsizlik tizimi doimiy monitoring, xavflarni baholash, dasturiy va texnik himoya vositalaridan foydalanish, foydalanuvchilarni o‘qitish hamda xavfsizlik siyosatini muntazam takomillashtirishga asoslanishi lozim.

Tahlillar shuni ko‘rsatadiki, texnik va tashkiliy himoya choralarini birgalikda qo‘llash axborot xavfsizligini ta’minlashda muhim natija beradi. Texnik vositalar zararli dasturlarni aniqlash, tarmoqdagi shubhali faoliyatni nazorat qilish, ma’lumotlarni shifrlash va ruxsatsiz ulanishlarni cheklash imkonini beradi. Biroq texnik himoyaning o‘zi yetarli emas. Tashkilotda axborot xavfsizligi siyosatining mavjudligi, xodimlarning vazifalari va javobgarligini aniq belgilash, ma’lumotlardan foydalanish huquqlarini nazorat qilish hamda favqulodda vaziyatlarda harakat qilish tartibining ishlab chiqilishi zarur. Buni quyidagi oddiy bog‘liqlik orqali ifodalash mumkin:

Texnik himoya + Tashkiliy choralar + Inson omili = Kompleks kiberxavfsizlik

Sun’iy intellekt asosidagi tizimlarning yana bir muhim jihati - tezkor tahlil va avtomatlashtirish imkoniyatidir. Katta tashkilotlarda tarmoqdagi millionlab hodisalarni inson tomonidan doimiy ravishda tekshirish amaliy jihatdan qiyin. AI texnologiyalari esa katta hajmdagi loglar, tarmoq trafigi va boshqa xavfsizlik ma’lumotlarini qisqa vaqt ichida tahlil qilib, mutaxassis e’tiborini talab qiladigan hodisalarni ajratib ko‘rsatishi mumkin. Natijada xavfsizlik guruhlarining ish samaradorligi oshadi va kiberhodisalarga javob berish vaqti qisqaradi. Umumiy natijalar shuni ko‘rsatadiki, raqamli muhitda axborotni samarali himoyalash uchun ko‘p qatlamli xavfsizlik modeli eng maqbul yondashuvlardan biridir. Bunda texnik vositalar, tashkiliy choralar, xodimlarning bilim va ko‘nikmalari hamda sun’iy intellekt asosidagi zamonaviy texnologiyalar yagona tizim sifatida faoliyat yuritishi kerak. Aynan mana shunday kompleks yondashuv kiberhujumlarni oldindan aniqlash, ularning oqibatlarini kamaytirish va axborot tizimlarining barqarorligini ta’minlash imkonini beradi.

2-jadval

Kiberhujumlarga kompleks yondashuv

Omil	Kutiladigan natija	Ahamiyati
Texnik himoya	Kiberhujumlarni aniqlash va cheklash	Yuqori
Tashkiliy himoya	Xavfsizlik jarayonlarini tizimlashtirish	Yuqori
Xodimlarni o‘qitish	Inson xatosi xavfini kamaytirish	Yuqori
Ko‘p bosqichli autentifikatsiya	Akkauntlarni qo‘shimcha himoyalash	Yuqori
Zaxira nusxalash	Yo‘qolgan ma’lumotlarni tiklash	Yuqori

DOI: 10.65322/j.srd.05192026.62

AI texnologiyalari	Tahdidlarni tezkor aniqlash va tahlil qilish	Istiqbolli
Doimiy monitoring	Xavflarni erta aniqlash	Yuqori

Xulosa. Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi axborot almashinuvi, ma'lumotlarni qayta ishlash va elektron xizmatlardan foydalanish imkoniyatlarini sezilarli darajada kengaytirmoqda. Shu bilan birga, raqamli muhitning kengayishi axborot tizimlari oldida yangi kiberxavfsizlik muammolarini ham yuzaga keltirmoqda. Tadqiqot davomida kiberxavfsizlik nafaqat texnik masala, balki texnologik, tashkiliy va inson omillarini o'zida mujassamlashtiruvchi kompleks jarayon ekanligi aniqlandi. Phishing, zararli dasturlar, ransomware, DDoS hujumlari, akkauntlarni buzish va ijtimoiy muhandislik kabi tahdidlar axborotning maxfiyligi, yaxlitligi va mavjudligiga salbiy ta'sir ko'rsatishi mumkin. Tadqiqot natijalaridan kelib chiqib, axborotni kompleks himoyalash zamonaviy raqamli muhitning asosiy talablaridan biri ekanligini ta'kidlash mumkin. Bunda texnik vositalar bilan bir qatorda tashkilotning ichki xavfsizlik siyosati, xodimlarning mas'uliyati, ma'lumotlardan foydalanish huquqlarini nazorat qilish va favqulodda vaziyatlarda harakat qilish mexanizmlari ham muhim ahamiyatga ega. Ayniqsa, inson omili kiberxavfsizlik tizimining eng muhim qismlaridan biri bo'lib, foydalanuvchilarning raqamli savodxonligini oshirish ko'plab kiberhujumlarning oldini olishga xizmat qiladi.

Tadqiqot natijalaridan kelib chiqib, axborotni kompleks himoyalash zamonaviy raqamli muhitning asosiy talablaridan biri ekanligini ta'kidlash mumkin. Bunda texnik vositalar bilan bir qatorda tashkilotning ichki xavfsizlik siyosati, xodimlarning mas'uliyati, ma'lumotlardan foydalanish huquqlarini nazorat qilish va favqulodda vaziyatlarda harakat qilish mexanizmlari ham muhim ahamiyatga ega. Ayniqsa, inson omili kiberxavfsizlik tizimining eng muhim qismlaridan biri bo'lib, foydalanuvchilarning raqamli savodxonligini oshirish ko'plab kiberhujumlarning oldini olishga xizmat qiladi.

Foydalanilgan adabiyotlar

1. Stallings W. *Cryptography and Network Security: Principles and Practice*. - Pearson, 2020.
2. Anderson R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. - 3rd ed. Wiley, 2020.
3. Bishop M. *Computer Security: Art and Science*. - 2nd ed. Addison-Wesley Professional, 2018.
4. Whitman M. E., Mattord H. J. *Principles of Information Security*. - Cengage Learning, 2021.
5. Kurose J. F., Ross K. W. *Computer Networking: A Top-Down Approach*. - Pearson, 2021.
6. National Institute of Standards and Technology. *Cybersecurity Framework (CSF) 2.0*. - NIST, 2024.
7. O'zbekiston Respublikasi. **"**Kiberxavfsizlik to'g'risida"gi Qonun, O'RQ-764-son, 15.04.2022.
8. O'zbekiston Respublikasi. "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun, O'RQ-547-son, 02.07.2019.