RAQAMLI IQTISODIYOT TIZIMIDA AXBOROTLARNI HIMOYALASH USUL VA VOSITALARI TAHLILI

Tadjiyeva Malika Murotovna
Raqamli hukumat loyihalarini boshqarish markazi
Davlat muassasasi Lavozim: Yetakchi mutaxassis

Annotatsiya: Ushbu maqolada raqamli iqtisodiyot sharoitida axborot xavfsizligini ta’minlashning kompleks yondashuvi tahlil qilinadi. Kirish qismida raqamli platformalar, sun’iy intellekt va global internet infratuzilmasi kengayishi bilan bog‘liq risklar hamda ma’lumotlarning ishonchliligi, yaxlitligi va maxfiyligi iqtisodiy barqarorlik uchun hal qiluvchi omil ekani asoslanadi. Asosiy tahdidlar sifatida kiberhujumlar (DoS/DDoS, phishing, malware), ma’lumotlarning o‘g‘irlanishi, ichki xodimlar (insider) xavfi, kriptografik kalitlarni buzish va autentifikatsiyani chetlab o‘tish, shuningdek bulut va IoT muhitlaridagi konfiguratsion zaifliklar tizimli ravishda ko‘rib chiqiladi. Himoya blokida kriptografik usullar (AES, RSA/ECC, ChaCha20/Ascon, SHA-2/3), kuchaytirilgan autentifikatsiya (MFA), ruxsatlarni boshqarish modellari (RBAC/ABAC), tarmoq darajasida firewall va IDS/IPS, VPN hamda Zero Trust arxitekturasi integratsiyalangan holda baholanadi. Monitoring qatlamida ELK, SIEM yechimlari va mashinaviy o‘qitishga tayangan anomaliya aniqlash yondashuvlari erta ogohlantirish va tezkor javob choralarini ta’minlashi ko‘rsatiladi. Natijalarga ko‘ra, texnik (kriptografiya, tarmoq xavfsizligi), tashkiliy (siyosatlar, rollar/atributlar) va analitik (SIEM/AI) choralar uyg‘unligi asosida ko‘p bosqichli mudofaa modeli raqamli iqtisodiyot subyektlari uchun eng maqbul strategiya hisoblanadi.

Kalit so‘zlar: raqamli iqtisodiyot, axborot xavfsizligi, kriptografiya, MFA, RBAC/ABAC, Zero Trust, SIEM, ELK, IoT, bulut xavfsizligi.

Abstract: This article analyzes a comprehensive approach to ensuring information security in the context of the digital economy. The introduction substantiates that, with the expansion of digital platforms, artificial intelligence, and global internet infrastructure, risks increase, while the reliability, integrity, and confidentiality of data become decisive factors for economic stability. Major threats are systematically examined, including cyberattacks (DoS/DDoS, phishing, malware), data theft, insider risks, cryptographic key compromise and authentication bypass, as well as configuration vulnerabilities in cloud and IoT environments. In the protection block, cryptographic methods (AES, RSA/ECC, ChaCha20/Ascon, SHA-2/3), enhanced authentication (MFA), access control models (RBAC/ABAC), network-level defenses such as firewalls and IDS/IPS, VPN, and integrated Zero Trust architecture are evaluated. At the monitoring layer, ELK, SIEM solutions, and machine learning–

based anomaly detection approaches are highlighted as enablers of early warning and rapid incident response. According to the results, a multi-layered defense model that combines technical (cryptography, network security), organizational (policies, role/attribute-based access), and analytical (SIEM/AI) measures is identified as the most optimal strategy for digital economy entities.

Keywords: digital economy, information security, cryptography, MFA, RBAC/ABAC, Zero Trust, SIEM, ELK, IoT, cloud security.

Аннотация: В данной статье анализируется комплексный подход к обеспечению информационной безопасности в условиях цифровой экономики. Во введении обосновывается, что с расширением цифровых платформ, искусственного интеллекта и глобальной интернет-инфраструктуры возрастают риски, а надежность, целостность и конфиденциальность данных становятся решающими факторами экономической стабильности. Системно рассматриваются основные угрозы, включая кибератаки (DoS/DDoS, фишинг, вредоносное ПО), кражу данных, риски инсайдеров, компрометацию криптографических ключей и обход аутентификации, а также уязвимости конфигурации в облачных и IoT-средах. В блоке защиты оцениваются криптографические методы (AES, RSA/ECC, ChaCha20/Ascon, SHA-2/3), усиленная аутентификация (MFA), модели управления доступом (RBAC/ABAC), сетевой уровень защиты (межсетевые экраны, IDS/IPS, VPN) и интегрированная архитектура Zero Trust. На уровне мониторинга рассматриваются решения ELK, SIEM и подходы к обнаружению аномалий на основе машинного обучения, обеспечивающие раннее оповещение и оперативное реагирование. Согласно полученным результатам, многоуровневая модель защиты, сочетающая технические (криптография, сетевая безопасность), организационные (политики, ролевой/атрибутивный доступ) и аналитические (SIEM/ИИ) меры, является наиболее оптимальной стратегией для субъектов цифровой экономики.

Ключевые слова: цифровая экономика, информационная безопасность, криптография, MFA, RBAC/ABAC, Zero Trust, SIEM, ELK, IoT, облачная безопасность.

Raqamli iqtisodiyot bu axborot-kommunikatsiya texnologiyalari, global internet tarmog‘i, sun’iy intellekt va raqamli platformalar asosida ishlab chiqarish, taqsimlash, ayirboshlash hamda iste’mol jarayonlarini boshqarishning yangi paradigmasidir. Ushbu tizim iqtisodiyotning barcha bo‘g‘inlariga chuqur kirib borib, moliya, bank, sanoat, savdo, ta’lim va davlat boshqaruvi kabi sohalarda innovatsion yechimlarni joriy etmoqda. Raqamli iqtisodiyotning jadal rivojlanishi nafaqat samaradorlikni oshirmoqda, balki axborot xavfsizligini ta’minlash masalalarini ham keskin dolzarb qilmoqda.

Chunki raqamli muhitda faoliyat yurituvchi barcha subyektlar – davlat organlari, xususiy korxonalar va oddiy fuqarolar – katta hajmdagi axborot oqimi bilan bevosita ishlaydi. Ushbu ma’lumotlarning **ishonchliligi, yaxlitligi va maxfiyligi** iqtisodiy barqarorlikning asosiy kafolatlaridan biri hisoblanadi. Raqamli iqtisodiy tizimlarda ma’lumotlar oqimi moliyaviy tranzaksiyalar, onlayn savdo, elektron hujjat aylanishi, shaxsiy ma’lumotlarni qayta ishlash kabi jarayonlarni o‘z ichiga oladi. Shu sababli ushbu ma’lumotlarning noto‘g‘ri saqlanishi yoki ruxsatsiz qo‘llarga o‘tib qolishi davlat xavfsizligi, biznesning raqobatbardoshligi hamda fuqarolarning konstitutsiyaviy huquqlariga jiddiy xavf tug‘diradi.

Bugungi kunda kiberxavfsizlik bo‘yicha xalqaro statistikalar ham raqamli iqtisodiyotning rivojlanishi bilan bog‘liq tahdidlarning ortib borayotganini ko‘rsatmoqda. Masalan, **Juniper Research** tadqiqotlariga ko‘ra, 2023 yilga kelib dunyo miqyosida kiberjinoyatchilik oqibatida 33 milliarddan ortiq hujjat o‘g‘irlangan. Xuddi shu kabi, Symantec va Kaspersky laboratoriyalari hisobotlarida ta’kidlanishicha, so‘nggi yillarda zararli dasturiy vositalar hajmi keskin oshgan, mobil ilovalar va IoT qurilmalariga qilingan hujumlar soni esa yangi rekord darajaga yetgan [1,7].

Shu nuqtayi nazardan, raqamli iqtisodiyotda axborot xavfsizligini ta’minlash davlat siyosati, korporativ strategiya va shaxsiy foydalanuvchi darajasida kompleks yondashuvni talab etadi. Bu esa **kriptografik algoritmlar, ko‘p faktorli autentifikatsiya, tarmoq xavfsizlik vositalari, monitoring tizimlari** va **normativ-huquqiy hujjatlar** uyg‘unligida amalga oshirilishi lozim.

Asosiy tahdidlar. Raqamli iqtisodiyot tizimida axborot xavfsizligiga tahdid soluvchi omillar ko‘plab manbalardan kelib chiqadi. Ushbu xavf-xatarlar texnologik infratuzilma, inson omili va tashqi kiberjinoyatchilik faoliyati bilan chambarchas bog‘liqdir. Quyida asosiy tahdidlar batafsil tahlil qilinadi:

Kiberhujumlar. Raqamli iqtisodiyotning asosiy infratuzilmasi – bank tizimlari, elektron to‘lov platformalari, davlat axborot resurslari va onlayn xizmatlar – turli xil kiberhujumlarga duchor bo‘lmoqda. Jumladan, **DoS/DDoS hujumlari** xizmat ko‘rsatishni izdan chiqarish orqali moliyaviy yo‘qotishlarga olib keladi. **Fishing (phishing)** hujumlari orqali foydalanuvchilardan login-parol yoki moliyaviy ma’lumotlar noqonuniy ravishda qo‘lga kiritiladi. **Zararli dasturlar (malware)** esa tizimlarga yashirin kirib borib, ma’lumotlarni o‘g‘irlash, shifrlash yoki butunlay ishdan chiqarish imkonini beradi.

Ma’lumotlarning o‘g‘irlanishi. Tijorat sirlari, moliyaviy ma’lumotlar va shaxsiy identifikatsiya axborotlari (PII) raqamli iqtisodiyotning eng qimmat resurslaridan biridir. Ularning o‘g‘irlanishi korxonalarga katta moliyaviy zarar yetkazishi bilan birga, iste’molchilar ishonchini ham pasaytiradi. So‘nggi yillarda ma’lumotlar bazasiga noqonuniy kirish, zararli skriptlar orqali ma’lumotlarni eksport

qilish va tarmoq zaifliklaridan foydalanish keng tarqalgan usullardan hisoblanadi.

Ichki xodimlar tomonidan ruxsatsiz foydalanish. Ko‘plab kiberxavfsizlik hodisalari tashqi hujumchilardan emas, balki tashkilot ichida ishlovchi xodimlarning beparvoligi yoki ataylab qilgan zararli harakatlari natijasida yuzaga kelmoqda. Masalan, maxfiy ma’lumotlarni ruxsatsiz ko‘chirish, tijorat sirlarini raqobatchilarga sotish yoki tizimlarga zarar yetkazish hollari kuzatiladi. Shu sababli, “insider threat” raqamli iqtisodiyotdagi eng xavfli omillardan biri hisoblanadi.

Kriptografik kalitlarni buzish va autentifikatsiyani chetlab o‘tish. Axborotni himoya qilishning asosiy vositalaridan biri – kriptografiya. Ammo zaif kalitlarni buzish, xakerlik dasturlari yordamida **brute force** hujumlarini amalga oshirish yoki autentifikatsiya jarayonidagi kamchiliklardan foydalanish orqali kiberjinoyatchilar himoya qatlamini aylanib o‘tishi mumkin. Bu esa moliyaviy tranzaksiyalar, elektron imzolar va onlayn xizmatlarning ishonchliligini shubha ostiga qo‘yadi [3,5].

Tarmoqlararo zaifliklar. Bulutli texnologiyalar, Buyumlar Interneti (Internet of Things, (IoT)) qurilmalari va mobil ilovalar keng joriy qilinishi bilan yangi turdagi hujum ssenariylari paydo bo‘lmoqda. Masalan, zaif parollar bilan himoyalangan IoT qurilmalari botnetlarga qo‘shilib, keng ko‘lamli hujumlarni amalga oshirish uchun ishlatiladi. Bulutli xizmatlarda esa noto‘g‘ri konfiguratsiya va ma’lumotlarga ruxsatsiz kirish muammosi kuzatiladi. Bu turdagi zaifliklar raqamli iqtisodiyot infratuzilmasining butun tizimiga salbiy ta’sir ko‘rsatishi mumkin.

Axborotni himoya qilish usullari va vositalari. Raqamli iqtisodiyot tizimida axborot xavfsizligini ta’minlash ko‘p bosqichli va kompleks yondashuvni talab qiladi. Quyida amaliyotda keng qo‘llaniladigan asosiy usul va vositalar batafsil yoritiladi:

Kriptografik vositalar. Bu ma’lumotlarni maxfiy saqlash, yaxlitligini kafolatlash va foydalanuvchi autentifikatsiyasini ta’minlashning eng samarali yo‘llaridan biridir. Zamonaviy raqamli iqtisodiyotda turli xil kriptografik algoritmlar qo‘llaniladi:

- **Simmetrik shifrlash algoritmlari (AES, DES, GOST).** Simmetrik algoritmlar tezkorligi bilan ajralib turadi va katta hajmdagi ma’lumotlarni shifrlashda qo‘llaniladi. AES (Advanced Encryption Standard) bugungi kunda eng ishonchli standartlardan biri hisoblanadi.
- **Nosimmetrik shifrlash algoritmlari (RSA, ECC).** Ular ochiq va yopiq kalit juftligi asosida ishlaydi. ECC (Elliptic Curve Cryptography) qisqa kalit uzunligida yuqori xavfsizlik darajasini ta’minlashi sababli mobil qurilmalar va IoT tizimlarida keng qo‘llanilmoqda.
- **Oqimli shifrlash algoritmlari (ChaCha20, Salsa20, Ascon).** Bunday algoritmlar real vaqtda ma’lumot uzatishda samarali hisoblanadi. Ascon algoritmi esa NIST tomonidan “Lightweight Cryptography” tanlovida g‘olib bo‘lib, resurslari cheklangan qurilmalarda qo‘llash uchun tavsiya etilgan.

- **Xesh-funksiyalar (SHA-2, SHA-3).** Ma’lumotlarning yaxlitligini tekshirishda ishlatiladi. Masalan, elektron imzo va blokcheyn texnologiyalarida xesh algoritmlar asosiy xavfsizlik kafolati hisoblanadi.

Autentifikatsiya va ruxsat boshqaruvi. Axborot tizimlariga kirishda foydalanuvchini to‘g‘ri identifikatsiya qilish va ruxsatlarni boshqarish xavfsizlikning muhim elementi hisoblanadi [6,9]:

- **Bir faktorli autentifikatsiya.** Eng sodda usul bo‘lib, odatda foydalanuvchi nomi va paroldan foydalaniladi. Ammo bu usul mustaqil qo‘llanganda zaif hisoblanadi.
- **Ko‘p faktorli autentifikatsiya (MFA).** Parol bilan bir qatorda SMS kod, biometrik (barmoq izi, yuzni tanish) yoki maxsus tokenlardan foydalaniladi. Bu yondashuv foydalanuvchi hisoblarini himoya qilish samaradorligini sezilarli oshiradi.
- **Ruxsatlarni boshqarish modellari (RBAC va ABAC).** RBAC (Role-Based Access Control) foydalanuvchining roliga qarab huquqlarni belgilaydi, ABAC (Attribute-Based Access Control) esa yanada moslashuvchan bo‘lib, foydalanuvchi atributlari, vaqt, joylashuv kabi omillarga asoslanadi.

Tarmoq darajasidagi himoya. Tarmoq infratuzilmasi raqamli iqtisodiyotning yuragi hisoblanadi. Uni himoyalash uchun quyidagi texnologiyalar qo‘llaniladi:

- **Firewalls va IDS/IPS tizimlari.** Xavfsizlik devorlari (firewall) ruxsatsiz ulanishlarni bloklaydi. IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) tizimlari esa hujumlarni aniqlash va ularning oldini olishda muhim rol o‘ynaydi. Masalan, Snort va Suricata ochiq kodli mashhur tizimlar sirasiga kiradi.
- **VPN texnologiyalari.** Virtual xususiy tarmoqlar (VPN) ochiq internet orqali uzatiladigan ma’lumotlarni shifrlash orqali xavfsiz ulanishni ta’minlaydi. Bu ayniqsa masofadan ishlash va transchegaraviy hamkorlikda muhimdir.
- **Zero Trust Architecture.** Ushbu yondashuvda “ishonchli foydalanuvchi” tushunchasi mavjud emas. Har bir foydalanuvchi va qurilma doimiy ravishda autentifikatsiya va avtorizatsiyadan o‘tadi. Bu esa ichki tahdidlardan ham samarali himoya qilish imkonini beradi.

Monitoring va sun’iy intellekt vositalari. Zamonaviy kiberxavfsizlik faqat oldini olish bilan cheklanmaydi, balki tizimni doimiy kuzatib borishni ham talab qiladi:

- **ELK Stack (Elasticsearch, Logstash, Kibana).** Ushbu platforma loglarni yig‘ish, saqlash va vizual tahlil qilish imkonini beradi. Katta hajmdagi ma’lumotlar asosida hujum izlarini aniqlash samaradorligini oshiradi.
- **SIEM tizimlari (Splunk, IBM QRadar).** Security Information and Event Management (SIEM) tizimlari turli manbalardan olingan xavfsizlik ma’lumotlarini real vaqt rejimida birlashtirib, tahlil qiladi.
- **Mashinaviy o‘qitish asosidagi monitoring.** Sun’iy intellekt va mashinaviy o‘qitish algoritmlari orqali an’anaviy vositalar aniqlay olmaydigan anomal faoliyatni

kuzatish mumkin. Masalan, foydalanuvchining odatiy faoliyatidan chetga chiqqan xatti-harakatlar avtomatik tarzda xavf sifatida qayd etiladi.

1-jadval

Raqamli iqtisodiyot tizimidagi asosiy axborot xavfsizligi tahdidlari tahlili

№	Tahdid nomi	Mazmuni	Oqibatlari	Amaliy misollar
1	**Kiberhujumlar** (DoS/DDoS, phishing, malware)	Bank tizimlari, elektron to‘lovlar va davlat resurslariga tashqi hujumlar orqali xizmatlarni izdan chiqarish yoki foydalanuvchi ma’lumotlarini qo‘lga kiritish.	Moliyaviy yo‘qotishlar, xizmatlarning to‘xtashi, ma’lumotlarning buzilishi.	2021-yilda DDoS hujumlari oqibatida Yevropa banklari onlayn xizmatlari vaqtincha ishdan chiqqan.
2	**Ma’lumotlarning o‘g‘irlanishi**	Tijorat sirlari, moliyaviy va shaxsiy identifikatsiya axborotlarini noqonuniy qo‘lga kiritish.	Korxona obro‘siga putur yetishi, mijozlar ishonchini yo‘qotish, katta moliyaviy zarar.	Equifax (2017) hodisasi – 147 mln foydalanuvchining shaxsiy ma’lumotlari o‘g‘irlangan.
3	**Ichki xodimlar tomonidan ruxsatsiz foydalanish**	Xodimlarning beparvoligi yoki ataylab qilgan zararli harakati natijasida maxfiy axborotning tarqalishi.	Ichki ma’lumotlar oqishi, raqobatchilarga sirlarning sotilishi, huquqiy javobgarlik.	Snowden ishi (2013) – maxfiy davlat ma’lumotlarining oshkor qilinishi.
4	**Kriptografik kalitlarni buzish va autentifikatsiyani chetlab o‘tish**	Brute force, zaif kalitlardan foydalanish yoki autentifikatsiyadagi zaifliklarni ekspluatatsiya qilish.	Elektron imzo va tranzaksiyalarning ishonchliligini yo‘qotish, tizimni buzish.	2019-yilda Microsoft Exchange Server autentifikatsiya zaifligidan keng miqyosda foydalanilgan.
5	**Tarmoqlararo zaifliklar** (Cloud, IoT)	Bulutli texnologiyalar va IoT qurilmalaridagi noto‘g‘ri konfiguratsiya, zaif parollar yoki zaif protokollardan foydalanish.	Botnetlar orqali keng ko‘lamli hujumlar, ma’lumotlarning ruxsatsiz o‘qilishi yoki o‘chirib yuborilishi.	2016-yilda Mirai botneti zaif IoT qurilmalaridan foydalanib, global DDoS hujumlarni amalga oshirgan.

Sun’iy intellekt asosida kiberhujumlarni aniqlash mexanizmlariga tayanishi zarur. Chunki, axborotlarni ishonchli himoyalash raqamli iqtisodiyotning barqaror rivojlanishi va xalqaro maydondagi raqobatbardoshligini ta’minlashda hal qiluvchi ahamiyat kasb etadi.

2-jadval

Raqamli iqtisodiyotda axborotni himoya qilishning asosiy usullari va vositalari

№	Yo‘nalish	Usul/Vosita	Asosiy imkoniyatlar	Amaliy qo‘llanilishi
1	**Kriptografik vositalar**	**Simmetrik shifrlash (AES, DES, GOST)**	Katta hajmdagi ma’lumotlarni tezkor shifrlash, samarali ishlash.	Bank ma’lumotlar bazalari, elektron to‘lov tizimlari.
		Nosimmetrik shifrlash (RSA, ECC)	Ochiq va yopiq kalitlar orqali yuqori darajadagi xavfsizlik. ECC – qisqa kalit bilan kuchli himoya.	Elektron imzo, raqamli sertifikatlar, IoT qurilmalari.
		Oqimli shifrlash (ChaCha20, Salsa20, Ascon)	Real vaqt rejimida ma’lumot uzatishda samarali. Ascon – resurslari cheklangan qurilmalar uchun optimallashtirilgan.	IoT, mobil qurilmalar, onlayn messenjerdagi trafikni shifrlash.
		Xesh funksiyalar (SHA-2, SHA-3)	Ma’lumot yaxlitligini nazorat qilish, elektron imzo yaratish.	Blokcheyn, elektron hukumat hujjatlari, parol saqlash.
2	**Autentifikatsiya va ruxsat boshqaruvi**	**Bir faktorli autentifikatsiya (parol)**	Foydalanuvchini aniqlashning eng oddiy shakli.	Past darajali tizimlarda, kichik korxonalar.
		Ko‘p faktorli autentifikatsiya (MFA)	Parol + SMS, biometrika, token orqali ko‘p bosqichli himoya.	Internet-banking, davlat xizmatlari portallari.
		RBAC va ABAC modellari	RBAC – rol asosida huquqlar belgilash, ABAC – foydalanuvchi atributlariga qarab dinamik boshqaruv.	Korporativ tarmoqlar, bulutli xizmatlar.
3	**Tarmoq darajasidagi himoya**	**Firewalls va IDS/IPS (Snort, Suricata)**	Ruxsatsiz ulanishlarni to‘sish, hujumlarni aniqlash va oldini olish.	Davlat axborot tizimlari, yirik kompaniyalar tarmoqlari.
		VPN texnologiyalari	Internet orqali ma’lumotlarni shifrlash, xavfsiz ulanishni ta’minlash.	Masofaviy ish, transchegaraviy biznes jarayonlari.
		Zero Trust Architecture	“Ishonchli foydalanuvchi” tushunchasini yo‘q qiladi, doimiy tekshiruv asosida xavfsizlikni oshiradi.	Davlat muassasalari va korporativ tarmoqlarda qo‘llaniladi.
4	**Monitoring va sun’iy intellekt vositalari**	**ELK Stack (Elasticsearch, Logstash, Kibana)**	Loglarni yig‘ish, saqlash va vizual tahlil qilish.	Katta hajmdagi tizimlarda kiberhujumlarni tahlil qilish.
		SIEM tizimlari (Splunk, IBM QRadar)	Turli manbalardan xavfsizlik ma’lumotlarini real vaqt rejimida tahlil qilish.	Banklar, sug‘urta kompaniyalari, davlat idoralari.
		Mashinaviy o‘qitish asosidagi monitoring	Foydalanuvchi xatti-harakatlaridagi anomaliyalarni avtomatik aniqlash.	Fraud-detektsiya, onlayn savdo platformalarida firibgarlikni aniqlash.

Xulosa

Raqamli iqtisodiyotning jadal kengayishi ma’lumotlar hajmini keskin oshirib, axborot xavfsizligini iqtisodiy barqarorlikning ajralmas shartiga aylantirdi. Tahlil

shuni ko‘rsatadiki, kiberhujumlar, ma’lumotlarning o‘g‘irlanishi, ichki xodimlar xatari, kriptografik kalitlarni buzish va tarmoqlararo zaifliklar raqamli infratuzilmaning eng muhim zaif nuqtalaridir. Ushbu xatarlarni kamaytirish uchun kriptografik himoya (AES, ECC, Ascon, SHA-2/3), kuchaytirilgan autentifikatsiya (MFA), rollar va atributlarga tayanuvchi ruxsat boshqaruvi (RBAC/ABAC) hamda tarmoq darajasida firewall va IDS/IPS kombinatsiyasi kompleks qo‘llanilishi lozim. Zero Trust arxitekturasi doimiy tekshiruv va minimal imtiyoz tamoyili orqali ichki va tashqi tahdidlarga nisbatan chidamlilikni oshiradi. Monitoring qatlamida ELK, SIEM va mashinaviy o‘qitish asosidagi anomalya aniqlash yechimlari erta ogohlantirishni ta’minlab, insidentlarga javob berish vaqtini qisqartiradi. Bulut va IoT muhitlarida xavfsizlikni ta’minlash uchun to‘g‘ri konfiguratsiya, kalitlarni xavfsiz boshqarish va zaifliklarni muntazam skanerlash zarur. Korporativ darajada siyosatlar, xodimlar uchun uzluksiz kiberxavfsizlik treninglari va auditlar texnik choralarni institutsional darajada mustahkamlaydi. Natijada, texnik, tashkiliy va me’yoriy choralar uyg‘unligiga tayanadigan ko‘p bosqichli mudofaa modeli raqamli iqtisodiyot subyektlari uchun chidamli, ishonchli va raqobatbardosh axborot muhitini yaratadi.

Foydanilgan adabiyotlar ro‘yxati:

1. ENISA. (2024). ENISA Threat Landscape 2023/2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications
2. FireEye/Mandiant. (2024). M-Trends 2024: Insights into today’s threat landscape. Mandiant. https://www.mandiant.com/resources/m-trends
3. IBM Security, & Ponemon Institute. (2024). Cost of a data breach report 2024. IBM. https://www.ibm.com/reports/data-breach
4. International Organization for Standardization. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.
5. Kaspersky Lab. (2023). Kaspersky Security Bulletin 2023: Statistics & trends. Kaspersky. https://www.kaspersky.com
6. Microsoft. (2024). Digital Defense Report 2024. Microsoft. https://www.microsoft.com/digitaldefense
7. National Institute of Standards and Technology. (2020). Zero Trust architecture (SP 800-207). NIST. https://doi.org/10.6028/NIST.SP.800-207
8. National Institute of Standards and Technology. (2023). Lightweight cryptography: Announcement of selected algorithms (Ascon). NIST. https://csrc.nist.gov/projects/lightweight-cryptography
9. National Institute of Standards and Technology. (2024). Cybersecurity Framework (CSF) 2.0. NIST. https://www.nist.gov/cyberframework
10. Open Web Application Security Project. (2021). OWASP Top 10: 2021. OWASP Foundation. https://owasp.org
11. Open Web Application Security Project. (2023). OWASP API Security Top 10: 2023. OWASP Foundation. https://owasp.org