RAQAMLI IQTISODIYOT TIZIMIGA BO‘LADIGAN HUJUMLAR TAHLILI

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

Annotatsiya: Ushbu maqolada raqamli iqtisodiyot infratuzilmasiga nisbatan keng tarqalgan kiberhujumlar - DDoS, phishing, ransomware, credential stuffing, API suiste’moli va bulut konfiguratsiyasi xatolari - ning mohiyati, ta’sir doirasi va evolyutsiyasi tizimli tahlil qilinadi. ENISA (2024), Verizon DBIR (2024), IBM (2024) va boshqa manbalar asosida bank/to‘lov tizimlari, davlat resurslari hamda e-commerce sektorlarida xatarlar profilining farqlari ko‘rsatiladi. Shuningdek, ko‘p bosqichli mudofaa modeli doirasida texnik (AES, ECC, Ascon; MFA/FIDO2; WAF, IDS/IPS; DDoS mitigatsiya), tashkiliy (siyosatlar, treninglar, ta’minot zanjiri auditi) va analitik (SIEM, ELK, AI-asosli monitoring) choralarining integratsiyalashgan qo‘llanishi samaradorligi asoslanadi. Natijalar shuni ko‘rsatadiki, sektorga xos xavf profiliga moslashtirilgan va me’yoriy talablar bilan uyg‘unlashgan kompleks yondashuv barqarorlik, uzluksizlik va foydalanuvchi ishonchini ta’minlashda hal qiluvchi ahamiyat kasb etadi.

Kalit so‘zlar:raqamli iqtisodiyot; kiberxavfsizlik; DDoS; phishing; ransomware; credential stuffing; API xavfsizligi; bulut konfiguratsiyasi xatolari; IAM; Zero Trust; MFA/FIDO2; SIEM; ELK; IoT botnetlar.

Abstract: This article provides a systematic analysis of widespread cyberattacks targeting digital economy infrastructures, including DDoS, phishing, ransomware, credential stuffing, API exploitation, and cloud misconfigurations. Based on ENISA (2024), Verizon DBIR (2024), IBM (2024), and other sources, the study highlights differences in risk profiles across banking/payment systems, government resources, and e-commerce sectors. Furthermore, the paper evaluates the effectiveness of a multi-layered defense model that integrates technical measures (AES, ECC, Ascon; MFA/FIDO2; WAF, IDS/IPS; DDoS mitigation), organizational measures (policies, training, supply chain audits), and analytical measures (SIEM, ELK, AI-based monitoring). The findings demonstrate that adopting a comprehensive approach tailored to sector-specific risk profiles and aligned with regulatory requirements is essential for ensuring stability, service continuity, and user trust.

Keywords: digital economy; cybersecurity; DDoS; phishing; ransomware; credential stuffing; API security; cloud misconfigurations; IAM; Zero Trust; MFA/FIDO2; SIEM; ELK; IoT botnets.

Аннотация: В данной статье представлен системный анализ наиболее распространённых кибератак, нацеленных на инфраструктуру цифровой экономики, включая DDoS, фишинг, программ-вымогатели (ransomware), credential stuffing, эксплуатацию API и ошибки конфигурации облачных сервисов. На основе данных ENISA (2024), Verizon DBIR (2024), IBM (2024) и других источников рассматриваются различия в профиле рисков для банковско-платёжных систем, государственных ресурсов и сектора электронной коммерции. Кроме того, оценивается эффективность многоуровневой модели защиты, включающей технические меры (AES, ECC, Ascon; MFA/FIDO2; WAF, IDS/IPS; DDoS-смягчение), организационные меры (политики, обучение, аудит цепочки поставок) и аналитические меры (SIEM, ELK, мониторинг на основе ИИ). Полученные результаты показывают, что комплексный подход, адаптированный к отраслевым профилям рисков и согласованный с нормативными требованиями, является ключевым условием обеспечения устойчивости, непрерывности сервисов и доверия пользователей.

Ключевые слова: цифровая экономика; кибербезопасность; DDoS; фишинг; ransomware; credential stuffing; безопасность API; ошибки конфигурации облака; IAM; Zero Trust; MFA/FIDO2; SIEM; ELK; IoT-ботнеты.

Raqamli iqtisodiyot – bu axborot-kommunikatsiya texnologiyalari, global internet tarmog‘i, bulutli hisoblash va sun’iy intellekt imkoniyatlariga asoslangan yangi iqtisodiy faoliyat modeli bo‘lib, u jamiyatning barcha sohalarida innovatsion yechimlarni joriy etmoqda. Moliya, bank, ta’lim, davlat boshqaruvi, sog‘liqni saqlash va elektron savdo kabi tarmoqlarda raqamli infratuzilmaning kengayishi samaradorlikni oshirayotgani bilan birga, yangi turdagi xavf-xatarlarni ham yuzaga chiqarmoqda.

So‘nggi yillarda raqamli iqtisodiyot nafaqat iqtisodiy o‘sishning, balki milliy xavfsizlikning ham muhim tarkibiy qismiga aylandi. Ma’lumotlar oqimi moliyaviy tranzaksiyalar, shaxsiy identifikatsiya ma’lumotlari (PII), intellektual mulk, davlat resurslari va IoT qurilmalari orqali real vaqt rejimida shakllanmoqda. Shu sababli ushbu axborotlarning ishonchliligi, yaxlitligi va maxfiyligi davlat va biznes barqarorligining asosiy kafolatlaridan biri sifatida ko‘rilmoqda.

Xalqaro statistik ma’lumotlar raqamli iqtisodiyotning kengayishi bilan kiberjinoyatchilik faoliyati hajmi va murakkabligi keskin ortayotganini ko‘rsatadi. ENISA (2024) “Threat Landscape” hisobotida ta’kidlanishicha, so‘nggi ikki yil ichida Yevropa Ittifoqi hududida eng ko‘p uchrayotgan hujumlar qatoriga ma’lumotlarni o‘g‘irlash, xizmat ko‘rsatishni ishdan chiqaruvchi (DoS/DDoS) hujumlar va fishing kiradi. Xuddi shuningdek, Verizon’ning 2024-yilgi “Data Breach Investigations Report” hisobotida global miqyosdagi kiberhodisalarning 60% dan ortig‘i to‘g‘ridan-

to‘g‘ri moliyaviy foyda olishga qaratilgani, ularning katta qismi esa firibgarlik va maxfiy ma’lumotlar oqishi bilan bog‘liq ekani qayd etilgan.

Bundan tashqari, Microsoft (2024) “Digital Defense Report” ma’lumotlariga ko‘ra, bulutli infratuzilma va mobil ilovalarga qilingan hujumlar rekord darajaga yetgan, xususan, API xavfsizligi zaifliklari va credential stuffing kabi hujum turlari tez sur’atlar bilan ko‘paymoqda. Bu esa shuni ko‘rsatadiki, raqamli iqtisodiyot subyektlari uchun kiberxavfsizlik masalalari endilikda faqat texnik jihat emas, balki strategik boshqaruv va milliy iqtisodiy siyosat darajasida ham dolzarb muammo hisoblanadi [2,5].

Shu nuqtayi nazardan, raqamli iqtisodiyot tizimiga bo‘ladigan hujumlarni tizimli tahlil qilish, ularning oqibatlarini baholash va samarali himoya choralarini ishlab chiqish ilmiy hamda amaliy jihatdan dolzarb ahamiyat kasb etadi.

Raqamli iqtisodiyotga hujumlarning asosiy turlari. Xizmat ko‘rsatishdan voz kechishga undovchi hujumlar (Denial of Service — DoS va Distributed Denial of Service — DDoS) raqamli iqtisodiyot infratuzilmasiga eng katta tahdid soluvchi kiberhujum turlaridan biri hisoblanadi. Bu turdagi hujumlarda hujumchi ma’lum bir server, tarmoq yoki onlayn xizmatga juda katta hajmdagi soxta trafikni yo‘naltiradi. Natijada tizimning resurslari (protsessor, xotira, tarmoq o‘tkazuvchanligi) haddan tashqari band bo‘lib qoladi va qonuniy foydalanuvchilar uchun xizmat ko‘rsatish imkoni keskin pasayadi yoki butunlay to‘xtaydi.

DDoS hujumlari ayniqsa moliyaviy muassasalar, davlat xizmatlari portallari, elektron savdo tizimlari va bulut xizmatlari uchun xavfli, chunki ularning uzluksiz ishlashi iqtisodiy barqarorlik va mijozlar ishonchi uchun hal qiluvchi ahamiyatga ega. Masalan, ENISA (2024) ma’lumotlariga ko‘ra, 2023-yilda Yevropa banklaridan bir nechtasi kuchli DDoS hujumlari oqibatida bir necha soat davomida mijozlarga xizmat ko‘rsata olmagan. Bu nafaqat moliyaviy yo‘qotishlarga, balki reputatsion zararlarga ham sabab bo‘lgan.

So‘nggi yillarda DDoS hujumlarining texnik imkoniyatlari yanada murakkablashdi. Ular ko‘pincha **botnetlar** (masalan, Mirai yoki IoT qurilmalaridan tashkil topgan tarmoqlar) yordamida amalga oshiriladi. Internetga ulangan zaif qurilmalar hujumchilarning nazoratiga o‘tib, ulardan bir vaqtning o‘zida millionlab so‘rov yuborish uchun foydalaniladi. Bu esa hujumlarning hajmi va samaradorligini oshiradi. Cloudflare (2024) hisobotida qayd etilishicha, ayrim DDoS hujumlari soniyasiga **70 milliondan ortiq HTTP so‘rovini** qayd etgan, bu esa tarixiy rekord darajani tashkil etadi.

DDoS hujumlarining iqtisodiy ta’siri ham e’tiborga molik. IBM Security (2024) hisobotiga ko‘ra, yirik kompaniyalar bitta DDoS hodisasi oqibatida o‘rtacha 1,5–2 million AQSh dollari miqdorida zarar ko‘rishi mumkin. Bundan tashqari, xizmat

uzilishi elektron to‘lovlarning kechikishi, onlayn savdo operatsiyalarining to‘xtashi va foydalanuvchilarning boshqa raqobatchi xizmatlarga o‘tib ketishiga olib keladi.

Shuningdek, zamonaviy DDoS hujumlari ko‘pincha boshqa hujumlar bilan uyg‘unlashtiriladi. Masalan, hujumchilar DDoS orqali xizmatlarni vaqtinchalik falaj qilib, shu jarayonda ma’lumotlar bazasiga kirish yoki ransomware tarqatish kabi qo‘shimcha zararli faoliyatni amalga oshirishi mumkin. Bu jarayon “distraction attack” (chalg‘itish hujumi) deb ataladi.

DDoS hujumlariga qarshi samarali himoya ko‘p qatlamli choralarni talab qiladi. Eng keng qo‘llaniladigan yondashuvlar qatoriga:

- **Trafikni filtrlash va tahlil qilish** (IDS/IPS, WAF);
- **DDoS mitigatsiya xizmatlari** (Cloudflare, Akamai, Radware kabi provayderlar);
- **Tarmoq resurslarini geografik taqsimlash** (Content Delivery Network – CDN orqali);
- **Anomaliya asosida tahlil** (AI va ML yordamida hujum signallarini erta aniqlash).

Umuman olganda, DDoS hujumlari raqamli iqtisodiyotning eng jiddiy tahdidlaridan biri bo‘lib qolmoqda. Ularning tezligi, miqyosi va murakkabligi ortib borayotgani sababli, tashkilotlar ushbu xatarga qarshi texnik, tashkiliy va iqtisodiy choralarni kompleks ravishda qo‘llashlari lozim [5,8].

Ransomware. Bu zararli dasturiy ta’minotning bir turi bo‘lib, uning asosiy vazifasi qurbonning ma’lumotlarini shifrlash va ularni tiklash evaziga to‘lov (odatda kriptovalyuta ko‘rinishida) talab qilishdir. Ushbu hujum turi 2010-yillardan buyon mavjud bo‘lsa-da, so‘nggi besh yil ichida u global miqyosdagi eng xavfli va iqtisodiy zararli kiberjinoyatlardan biriga aylandi.

Ransomware hujumlarining muvaffaqiyatli bo‘lishi bir necha omillar bilan bog‘liq:

- tashkilotlarda zaxira nusxalarning muntazam yaratilmasligi;
- xodimlarning phishing orqali yuborilgan zararli fayllarni ochib yuborishi;
- operatsion tizim va ilovalardagi zaifliklarning o‘z vaqtida yopiqlanmasligi;
- ta’minot zanjiri orqali tarqaluvchi hujumlarning ko‘payishi.

Statistik tahlil. Mandiant’ning “M-Trends 2024” hisobotiga ko‘ra, ransomware hujumlari eng ko‘p zarar yetkazgan segmentlar sifatida davlat muassasalari, sog‘liqni saqlash tizimlari va moliya sektori qayd etilgan. IBM Security (2024) hisobotida esa ransomware hodisasining o‘rtacha iqtisodiy zarari 4,45 million AQSh dollarini tashkil qilgani ko‘rsatilgan. ENISA (2024) ma’lumotlariga ko‘ra, ransomware 2023-yilda Yevropa kiberxavfsizlik landshaftida eng ko‘p qayd etilgan uch tahdiddan biri bo‘lib qolmoqda.

Mashhur hujumlar. 2021-yilda **Colonial Pipeline** kompaniyasiga qilingan ransomware hujumi AQShning yirik energiya infratuzilmasini vaqtinchalik ishdan chiqardi va millionlab dollar to‘lov evaziga tizimlar tiklandi.

2023-yilda Yevropadagi bir nechta shifoxonalar LockBit va Conti kabi ransomware guruhlari hujumiga uchrab, bemorlar ma’lumotlari vaqtincha ishdan chiqqan.

Evolyutsiya. Ransomware dastlab faqat ma’lumotlarni shifrlash bilan cheklangan bo‘lsa, bugungi kunda hujumchilar “double extortion” (ikki tomonlama majburlash) usulidan foydalanadi: ya’ni ma’lumotlar nafaqat shifrlanadi, balki hujumchilar ularni o‘g‘irlab, agar to‘lov amalga oshirilmasa, internetda oshkor qilish bilan tahdid qilishadi. Bu usul tashkilotlar uchun qo‘shimcha bosim omilini yuzaga keltiradi.

Himoya choralari. Ransomware hujumlariga qarshi samarali kurashish quyidagi choralarni talab qiladi:

- **Zaxira nusxalar (backup)** – Ma’lumotlarni muntazam ravishda offline yoki bulutli muhitda zaxiralash.
- **Patch management** – Operatsion tizim va ilovalardagi zaifliklarni o‘z vaqtida yopish.
- **Xodimlarni o‘qitish** – Phishing orqali ransomware tarqatilishining oldini olish uchun treninglar.
- **Zero Trust arxitekturasi** – Har bir foydalanuvchi va qurilma uchun qat’iy autentifikatsiya va avtorizatsiya.
- **SIEM va SOAR tizimlari** – Hujum signallarini erta aniqlash va avtomatlashtirilgan javob choralarini amalga oshirish.

API (Application Programming Interface) hujumlari — zamonaviy raqamli iqtisodiyotda eng tez o‘sib borayotgan tahdid turlaridan biridir. API interfeyslari turli xizmatlar, mobil ilovalar, IoT qurilmalari va bulut platformalari o‘rtasida ma’lumot almashishning asosiy vositasi bo‘lgani sababli, ular kiberjinoyatchilar uchun jozibali hujum nuqtasiga aylanmoqda [1,9].

API hujumlari odatda **noto‘g‘ri autentifikatsiya va avtorizatsiya mexanizmlari**, **zaif seans boshqaruvi**, **haddan tashqari ekspozitsiya qilingan ma’lumotlar** yoki **xavfsiz bo‘lmagan so‘rovlarni qayta ishlash** kabi zaifliklardan foydalanish orqali amalga oshiriladi. Masalan, foydalanuvchi identifikatorlari va tokenlar noto‘g‘ri boshqarilganda, hujumchilar boshqa foydalanuvchi resurslariga ruxsatsiz kirishi mumkin.

Statistik ma’lumotlar. OWASP (2023) “API Security Top 10” ro‘yxatiga ko‘ra, API suiste’moli global miqyosda eng tez o‘sib borayotgan hujum turiga aylangan. Gartner’ning prognoziga ko‘ra, 2025-yilga kelib barcha web-ilova hujumlarining qariyb 90% API interfeyslari orqali amalga oshiriladi. Bu esa API

xavfsizligini endilikda faqat texnik masala emas, balki biznes xavfsizligi va strategik ustuvor yo‘nalish sifatida ko‘rish zarurligini ko‘rsatadi.

Amaliy misollar. 2021-yilda Facebookning APIdagi zaiflik natijasida 533 milliondan ortiq foydalanuvchining shaxsiy ma’lumotlari internetda oshkor bo‘ldi.

2022-yilda bir nechta fintech startaplari APIdagi noto‘g‘ri autentifikatsiya mexanizmlari sababli mijozlarning moliyaviy ma’lumotlari sizib chiqdi.

Verizon DBIR (2024) ma’lumotlariga ko‘ra, so‘nggi yillarda API hujumlarining katta qismi credential stuffing va avtomatlashtirilgan bot-hujumlar orqali amalga oshirilgan.

API hujumlarining asosiy turlari:

- **Broken Object Level Authorization (BOLA):** foydalanuvchi boshqa foydalanuvchi resurslariga ruxsatsiz kirishi.
- **Broken Authentication:** tokenlar va sessiya boshqaruvi zaifliklaridan foydalanish.
- **Excessive Data Exposure:** API foydalanuvchiga ortiqcha ma’lumot qaytarib berishi natijasida maxfiy ma’lumotlarning oqib chiqishi.
- **Rate Limiting zaifliklari:** hujumchilar cheksiz so‘rov yuborib, credential stuffing yoki brute-force hujumlarini amalga oshirishi.
- **Himoya choralari.** API hujumlariga qarshi samarali mudofaa quyidagi choralarni o‘z ichiga oladi:
- **Kuchli autentifikatsiya va avtorizatsiya** (OAuth 2.0, OpenID Connect).
- **Tokenlarni xavfsiz boshqarish** va ularning amal qilish muddatini cheklash.
- **Rate limiting va throttling** mexanizmlarini joriy etish.
- **Ma’lumotlarni minimal qaytarish tamoyili** (Principle of Least Privilege).
- **Web Application Firewall (WAF) va API Gateway** yechimlaridan foydalanish.
- **Loglarni monitoring qilish va SIEM tizimlari** orqali anomaliyalarni erta aniqlash.

API hujumlari raqamli iqtisodiyotning asosiy xavf manbalaridan biri bo‘lib qolmoqda. Ularning murakkablashib borayotgani sababli, tashkilotlar API xavfsizligini dasturiy ta’minot ishlab chiqish siklining barcha bosqichiga integratsiya qilishi, “Security by Design” tamoyilini amalda qo‘llashi zarur.

Bulutli texnologiyalar raqamli iqtisodiyotning markaziy infratuzilmasiga aylanib bormoqda. Ular tezkorlik, masshtablilik va xarajatlarni optimallashtirish imkoniyatlarini taqdim etadi. Shu bilan birga, noto‘g‘ri konfiguratsiya qilingan bulut muhitlari tashkilotlar uchun eng jiddiy xavfsizlik muammolaridan biri sifatida ko‘rilmoqda. ENISA (2024) va IBM Security (2024) hisobotlariga ko‘ra, bulut xizmatlaridagi ma’lumotlar oqishining 70% dan ortig‘i konfiguratsiya xatolaridan kelib chiqadi.

Asosiy xatoliklar quyidagilarni o‘z ichiga oladi:

Ochiq “bucket”lar (misol: Amazon S3) – autentifikatsiyasiz umumiy foydalanish imkoniyati berilganda, maxfiy ma’lumotlar butun internetga oshkor bo‘lib qolishi mumkin.

Zaif IAM (Identity and Access Management) sozlamalari – foydalanuvchilarga ortiqcha imtiyoz berilishi yoki rollar noto‘g‘ri belgilanganda, hujumchilar bitta akkauntni egallab, butun infratuzilmaga kirib olish imkoniyatiga ega bo‘lishadi.

Noto‘g‘ri tarmoq segmentatsiyasi – xavfsiz bo‘lishi kerak bo‘lgan xizmatlar va ma’lumotlar umumiy tarmoq orqali ochiq qolishi oqibatida lateral harakat (lateral movement) hujumlarini yengillashtiradi.

Shifrlashning yo‘qligi yoki noto‘g‘ri qo‘llanishi – tranzit yoki dam olish (at rest) holatidagi ma’lumotlar himoyasiz qoladi.

Amaliy misollar.

2021-yilda misol tariqasida, bir nechta sog‘liqni saqlash tashkilotlarining S3 bucketlari noto‘g‘ri sozlanganligi sababli millionlab bemorlarning tibbiy yozuvlari internetda oshkor bo‘lgan.

2022-yilda Gartner ma’lumotlariga ko‘ra, bulutdagi noto‘g‘ri IAM siyosatlari sababli yuz bergan hujumlar umumiy bulut hodisalarining qariyb 45% ini tashkil qilgan.

Verizon DBIR (2024) ma’lumotida bulutdagi ma’lumot oqishlari kompaniyalar uchun o‘rtacha 4,1 million AQSh dollari zarar keltirgani qayd etilgan.

Xavf darajasi. Bulut konfiguratsiyasi xatolari nafaqat ma’lumotlarning noqonuniy oqib chiqishiga, balki GDPR, HIPAA yoki mahalliy axborot xavfsizligi standartlari kabi me’yoriy hujjatlar talablarining buzilishiga ham olib keladi. Bu esa jarimalar, sud jarayonlari va mijozlar ishonchining keskin pasayishiga sabab bo‘ladi.

Himoya choralariga quyidagilar kiradi:

- **Security by Design** tamoyiliga asoslangan holda bulut xizmatlarini loyihalash;
- **IAM siyosatlarini minimal imtiyoz tamoyiliga (PoLP) asoslash;**
- **Bulut xavfsizlik monitoring vositalari (CSPM — Cloud Security Posture Management)** yordamida noto‘g‘ri sozlamalarni avtomatik aniqlash;
- **Regulyar audit va pentestlar** orqali konfiguratsiya xatolarini aniqlash va bartaraf etish;
- **Shifrlash va loglash** mexanizmlarini majburiy qo‘llash.

Sektorlar bo‘yicha xatar profili. Raqamli iqtisodiyotning turli segmentlari o‘z faoliyat xususiyatlariga ko‘ra turlicha kiberxatarlar bilan yuzma-yuz keladi. ENISA (2024), IBM Security (2024) va Verizon DBIR (2024) hisobotlari tahliliga ko‘ra, har bir sektor uchun ustuvor tahdidlar farq qiladi. Quyida asosiy sohalar bo‘yicha xatar profili ko‘rib chiqiladi.

1-jadval

Sektorlar bo‘yicha kiberxatar profili

Sektor	Asosiy tahdidlar	Tahliliy izoh va amaliy misollar
Bank va to‘lov tizimlari	- Credential stuffing - Phishing - API hujumlari	**Credential stuffing** – boshqa tizimlardan o‘g‘irlangan login-parollar avtomatlashtirilgan tarzda sinovdan o‘tkazilib, onlayn banking tizimlariga kirish amalga oshiriladi. Bu holat ko‘p hollarda mijoz hisoblarini buzilishiga olib keladi. **Phishing** – bank mijozlari yoki xodimlarini aldash orqali maxfiy ma’lumotlarni qo‘lga kiritish. Verizon DBIR (2024) ma’lumotiga ko‘ra, moliya sohasidagi buzilishlarning 25% ga yaqini phishingga to‘g‘ri keladi. **API hujumlari** – mobil banking va to‘lov tizimlarida noto‘g‘ri autentifikatsiya/avtorizatsiya mexanizmlaridan foydalanib, tranzaksiyalarni manipulyatsiya qilish.
Davlat resurslari	- DDoS hujumlari - Ransomware - Bulut konfiguratsiyasi xatolari	**DDoS hujumlari** – davlat portallari va e-hukumat xizmatlarini vaqtinchalik ishdan chiqarib, fuqarolarning muhim xizmatlardan foydalanishini cheklaydi. ENISA (2024) hisobotida bir nechta Yevropa davlat resurslariga qilingan massiv DDoS hujumlari qayd etilgan. **Ransomware** – davlat idoralari bazalaridagi maxfiy ma’lumotlarni shifrlash va tiklash uchun to‘lov talab qilish. Mandiant (2024) ma’lumotiga ko‘ra, davlat sektori ransomware hujumlaridan eng ko‘p zarar ko‘rgan sohalardan biridir. **Bulut konfiguratsiyasi xatolari** – IAM sozlamalaridagi xatoliklar yoki ochiq bucket’lar natijasida fuqarolarning sezgir ma’lumotlari oqib chiqishi ehtimoli yuqori.

Elektron tijorat (E-commerce)	- Bot hujumlari - Phishing - Ma’lumot o‘g‘irlanishi	**Bot hujumlari** – avtomatlashtirilgan dasturlar orqali chegirmalarni suiiste’mol qilish, narx manipulyatsiyasi yoki soxta buyurtmalar berish. Bu biznesning moliyaviy yo‘qotishiga va xizmat sifatining pasayishiga olib keladi. **Phishing** – soxta onlayn savdo sahifalari orqali mijozlarning kredit karta ma’lumotlari o‘g‘irlanadi. **Ma’lumot o‘g‘irlanishi** – PII (shaxsiy identifikatsiya ma’lumotlari) va to‘lov kartasi ma’lumotlari noqonuniy ravishda qo‘lga olinadi. IBM (2024) ma’lumotiga ko‘ra, e-commerce sohasidagi ma’lumot oqishining o‘rtacha zarari 3,9 mln AQSh dollarini tashkil etadi.

Bank va moliya sektorida iqtisodiy manfaatga qaratilgan credential stuffing va API hujumlari ustun bo‘lsa, davlat resurslarida xizmatni falaj qiluvchi DDoS va ransomware tahdidlari yetakchi o‘rinda turadi. E-commerce platformalari esa bot hujumlari va mijozlar ma’lumotlarining o‘g‘irlanishi xavfi bilan ko‘proq to‘qnash keladi. Shu sababli, har bir sektor uchun xos himoya strategiyasini ishlab chiqish raqamli iqtisodiyot barqarorligini ta’minlashda muhim ahamiyat kasb etadi.

2-jadval

Qarshi choralar va yechimlar

Daraja	Asosiy vositalar / choralar	Amaliy misollar va qo‘llanishi
Texnik	- Kriptografik algoritmlar (AES, ECC, Ascon) - Kuchaytirilgan autentifikatsiya (MFA, FIDO2) - Tarmoq xavfsizlik vositalari (WAF, IDS/IPS) - DDoS mitigatsiya xizmatlari	- IoT va mobil qurilmalarda ECC va Ascon - Internet-bankingda MFA va FIDO2 - Davlat portallarida WAF va IDS/IPS - Cloudflare, Akamai orqali DDoS himoyasi
Tashkiliy	- Xavfsizlik siyosatlari (RBAC, ABAC) - Xodimlarni muntazam kiberxavfsizlik treninglari - Uchinchi tomon xizmatlari uchun xavf baholash	- Korporativ tarmoqlarda rollarga asoslangan ruxsat - Phishing simulyatsiyalari orqali trening - Ta’minot zanjiri xavfini audit qilish

Analitik	- SIEM tizimlari - ELK Stack (Elasticsearch, Logstash, Kibana) - Sun'iy intellekt asosida monitoring	- Splunk, IBM QRadar orqali real vaqt monitoring - ELK orqali loglarni vizual tahlil - AI yordamida anomal faoliyatni aniqlash (fraud-detektsiya, credential stuffing)

Xulosa

Raqamli iqtisodiyotning jadal rivojlanishi bilan bir qatorda kiberxavfsizlik tahdidlari ham tobora murakkablashib, ko‘lam va intensivligi ortib bormoqda. Hozirgi davrda kuzatilayotgan hujumlar orasida **DDoS, phishing, ransomware, credential stuffing, API suiste'moli hamda IoT botnetlar** eng xavfli toifalardan hisoblanadi. Ushbu hujumlar moliya sektori, davlat resurslari va elektron tijorat tizimlariga sezilarli darajada zarar yetkazib, ularning **ishonchliligi, xizmat ko‘rsatish barqarorligi va foydalanuvchilar ishonchi**ga tahdid solmoqda.

Xalqaro hisobotlar (ENISA, 2024; IBM, 2024; Verizon DBIR, 2024) keltirganidek, kiberjinoyatchilikning asosiy motivatsiyasi iqtisodiy manfaat bilan bog‘liq bo‘lsa-da, davlat resurslariga qilingan hujumlar siyosiy va ijtimoiy barqarorlikka ham xavf tug‘dirishi mumkin. Ayniqsa, ransomware va bulut konfiguratsiyasi xatolari kabi tahdidlar shaxsiy ma'lumotlar va maxfiy hujjatlarning katta hajmda oqib chiqishiga sabab bo‘lmoqda.

Mazkur sharoitda **ko‘p bosqichli mudofaa model**ini joriy etish raqamli iqtisodiyot subyektlari uchun eng maqbul strategiya sifatida e'tirof etilmoqda. Bu model quyidagilarni o‘z ichiga oladi:

- **Texnik choralar** – ilg‘or kriptografik algoritmlar (AES, ECC, Ascon), ko‘p faktorli autentifikatsiya (MFA, FIDO2), WAF va IDS/IPS, DDoS mitigatsiya xizmatlari yordamida tizimlarni bevosita himoya qilish.
- **Tashkiliy choralar** – xavfsizlik siyosatlarini ishlab chiqish, xodimlarni muntazam kiberxavfsizlik treninglaridan o‘tkazish hamda uchinchi tomon xizmatlarini qat'iy audit qilish orqali inson omili va ta'minot zanjiri xatarlarini kamaytirish.
- **Analitik choralar** – SIEM, ELK Stack va sun'iy intellekt asosida anomal faoliyatni aniqlash tizimlari yordamida erta ogohlantirish va tezkor insidentlarga javob berish.

Demak, texnik, tashkiliy va analitik choralar uyg‘unligiga asoslangan yondashuv nafaqat mavjud tahdidlarni kamaytiradi, balki kelajakdagi yangi xavflarga nisbatan ham tizimlarning chidamliligini oshiradi. Natijada, bunday mudofaa modeli raqamli iqtisodiyotning **barqarorligi, xavfsizligi va xalqaro raqobatbardoshligini** ta'minlashda hal qiluvchi omil bo‘lib xizmat qiladi.

Foydalanilgan adabiyotlar

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