

IOT QURILMALARIDA KIBERXAVFSIZLIK MUAMMOLARI**Eshbo'Riyeva Mahfuza Rustam Qizi**

Termiz davlat universiteti

60610300-kompyuter injiniringi

yo'nalishi talabasi

Annotatsiya: Hozirgi kunda Buyumlar interneti (IoT) texnologiyalarining jadal rivojlanishi va hayotimizning barcha jabhalariga kirib borishi bilan bir qatorda, ushbu qurilmalarga bo'layotgan kiberhujumlar soni va xavfi ham ortib bormoqda. IoT qurilmalarining hisoblash resurslari cheklanganligi va arxitekturaviy xususiyatlari tufayli an'anaviy kiberxavfsizlik vositalarini ularda qo'llash jiddiy qiyinchiliklarni tug'diradi. Ushbu maqolada IoT ekotizimidagi asosiy kiberxavfsizlik muammolari, qurilmalarning zaif nuqtalari hamda ularga qaratilgan zamonaviy tahdidlar tahlil qilinadi. Shuningdek, maqolada IoT tarmoqlarini himoya qilish, ma'lumotlar maxfiyligini ta'minlash va kiberhujumlarning oldini olishga qaratilgan zamonaviy yondashuvlar hamda yechimlar ko'rib chiqiladi.

Kalit so'zlar: Buyumlar interneti (IoT), kiberxavfsizlik, IoT zaifliklari, kiberhujum, ma'lumotlar maxfiyligini ta'minlash, tarmoq xavfsizligi, IoT xavfsizlik protokollari, fishing, xizmat ko'rsatishni rad etish (DoS).

Аннотация: Сегодня, наряду со стремительным развитием технологий Интернета вещей (IoT) и их внедрением во все сферы нашей жизни, количество и опасность кибератак на эти устройства также демонстрируют стабильный рост. Из-за ограниченных вычислительных ресурсов и архитектурных особенностей IoT-устройств применение традиционных средств кибербезопасности в этой среде сталкивается с серьезными трудностями. В данной статье анализируются основные проблемы кибербезопасности в экосистеме IoT, уязвимые места устройств, а также направленные на них современные угрозы. Кроме того, рассматриваются современные подходы и решения, направленные на защиту сетей IoT, обеспечение конфиденциальности данных и предотвращение кибератак.

Ключевые слова: Интернет вещей (IoT), кибербезопасность, уязвимости IoT, кибератака, конфиденциальность данных, сетевая безопасность, протоколы безопасности IoT, фишинг, отказ в обслуживании (DoS).

Abstract: Today, along with the rapid development of Internet of Things (IoT) technologies and their integration into all aspects of our lives, the number and severity

of cyberattacks targeting these devices are increasing exponentially. Due to the limited computing resources and specific architectural features of IoT devices, deploying traditional cybersecurity tools on them poses significant challenges. This article analyzes the primary cybersecurity issues within the IoT ecosystem, device vulnerabilities, and modern threats targeting them. Furthermore, the paper examines contemporary approaches and solutions aimed at securing IoT networks, ensuring data privacy, and preventing cyberattacks.

Keywords: Internet of Things (IoT), cybersecurity, IoT vulnerabilities, cyberattack, data privacy, network security, IoT security protocols, phishing, Denial of Service (DoS).

KIRISH

Yigirma birinchi asrning fundamental texnologik tendensiyalaridan biri — bu shubhasiz Buyumlar interneti (IoT — Internet of Things) ekotizimining global miqyosda ommalashishidir. Bugungi kunda IoT oddiy "aqlli uy" jihozlaridan tortib, sanoat avtomatizatsiyasi (IIoT), aqlli shaharlar, tibbiy monitoring tizimlari va transport infratuzilmalarigacha bo'lgan keng qamrovli muhitni qamrab oldi. Ma'lumotlarga ko'ra, dunyo bo'ylab tarmoqqa ulangan IoT qurilmalarining soni milliardlarni tashkil etmoqda va bu ko'rsatkich geometrik progressiya bilan o'sib bormoqda. Biroq, ushbu jadal integratsiya va raqamlashtirish jarayoni o'zi bilan birga jiddiy kiberxavfsizlik xatarlarini ham olib keldi. IoT qurilmalarining hayotiy muhim sohalarga chuqur kirib borishi, ularni kiberjinoyatchilar uchun eng jozibador va zaif nishonlardan biriga aylantirdi.

An'anaviy kompyuter tarmoqlari va server tizimlaridan farqli o'laroq, IoT qurilmalari o'ziga xos texnik cheklovlar asosida loyihalashtirilgan. Aksariyat aqlli datchiklar, kontrollerlar va maishiy texnikalar:

1. Cheklangan hisoblash quvvatiga (CPU);
2. Kichik hajmdagi tezkor va doimiy xotiraga;
3. Energiyani tejash rejimlariga ega.

Ushbu arxitekturaviy cheklovlar tufayli IoT qurilmalariga murakkab shifrlash algoritmlarini, resurs talab qiluvchi firewall (tarmoq ekranlari) tizimlarini yoki zamonaviy antivirus dasturlarini to'g'ridan-to'g'ri o'rnatishning imkoni yo'q. Ishlab chiqaruvchilar ko'pincha xavfsizlik choralardan ko'ra qurilmaning arzonligi, energiya tejamkorligi va funkcionalligiga ko'proq e'tibor qaratadilar. Natijada, tarmoqqa standart parollar bilan chiqarilgan va dasturiy ta'minoti (firmware) yillar davomida yangilanmaydigan millionlab zaif nuqtalar (vulnerabilities) yuzaga kelmoqda. IoT

qurilmalaridagi zaifliklar kiberhujumchilar uchun global tarmoqlarga kirish eshigi bo'lib xizmat qilmoqda. Bugungi kunda IoT ekotizimiga qaratilgan eng xavfli tahdidlar qatoriga fishing hujumlari, "Man-in-the-Middle" (o'rtadagi odam) hujumlari va qurilmaning boshqaruvini butunlay qo'lga kiritish (brute-force) holatlarini kiritish mumkin. Ayniqsa, minglab yoki millionlab zaif IoT qurilmalarini yagona tarmoqqa birlashtiruvchi botnetlar (masalan, mashhur Mirai botneti) orqali amalga oshiriladigan keng ko'lamli DoS va DDoS (Xizmat ko'rsatishni rad etish) hujumlari yirik korporatsiyalar, bank tizimlari va davlat provayderlari faoliyatini butunlay falaj qilib qo'yimoqda. Aqlli tibbiy uskunalar yoki avtomobillarga qilinadigan hujumlar esa nafaqat iqtisodiy zarar keltirishi, balki insonlar hayotiga ham to'g'ridan-to'g'ri tahdid solishi mumkin.

Ushbu muammolarning ko'lamini inobatga olgan holda, an'anaviy kiberxavfsizlik konseptlarini qayta ko'rib chiqish va IoT muhitiga moslashtirilgan yangi himoya mexanizmlarini ishlab chiqish zamon talabidir.

Ushbu maqolaning asosiy maqsadi — IoT qurilmalarida yuzaga kelayotgan kiberxavfsizlik muammolarini tizimli tahlil qilish, global tarmoqdagi zamonaviy tahdidlar mexanizmini o'rganish hamda ushbu zaifliklarni bartaraf etishga qaratilgan zamonaviy tarmoq xavfsizligi protokollari va himoya yondashuvlarini tadqiq etishdan iboratdir.

METODOLOGIYA VA ADABIYOTLAR TAHLILI

IoT ekotizimida kiberxavfsizlikni ta'minlash masalasi so'nggi yillarda global ilmiy hamjamiyatning diqqat markazida bo'lib kelmoqda. Ushbu yo'nalishdagi tadqiqotlarni shartli ravishda uchta asosiy guruhga ajratish mumkin.

Ko'plab tadqiqotchilar muammoning ildizini IoT qurilmalarining standart xavfsizlik arxitekturasiga ega emasligida ko'rishadi. Masalan, taniqli kiberxavfsizlik ekspertlarining ilmiy ishlarida IoT qurilmalarining hisoblash resurslari cheklanganligi (xotira va protsessor quvvati kamligi) sababli ularda an'anaviy shifrlash usullarini (AES-256 yoki RSA) qo'llashning imkonsizligi isbotlangan. Shuningdek, xalqaro OWASP (*Open Web Application Security Project*) hamjamiyati har yili IoT qurilmalari uchun eng xavfli top-10 ta zaifliklar ro'yxatini e'lon qilib boradi, bularning ichida eng birinchi o'rinda **"o'zgartirilmaydigan standart parollar" (hardcoded/weak passwords)** muammosi turadi.

Ilmiy adabiyotlarda IoT qurilmalarini yirik botnet tarmoqlariga birlashtirish mexanizmlari keng yoritilgan. Xususan, 2016-yildagi mashhur *Mirai* botneti kiberxavfsizlik tarixida burilish nuqtasi bo'ldi. Olimlar ushbu hodisani tahlil qilib,

millionlab zaif aqlli kameralar va routerlar qisqa vaqt ichida global internet infratuzilmasini falaj qiluvchi qurolga aylanishi mumkinligini ko'rsatishdi. Zamonaviy tadqiqotlarda *Miraining* yangi modifikatsiyalari va ularning tarmoq ichida tarqalish dinamikasi matematik modellar yordamida o'rganilmoqda. Adabiyotlar tahlili shuni ko'rsatadiki, an'anaviy xavfsizlik devorlari (*firewalls*) IoT muhitida samarasiz. Shuning uchun so'nggi yillardagi ilmiy ishlarda ikki xil asosiy yondashuv ilgari surilmoqda:

1. **Yengil vaznli kriptografiya (Lightweight Cryptography):** Kam resurs talab qiladigan shifrlash algoritmlarini yaratish.
2. **Anomaliyalarni aniqlash (Anomaly Detection):** Tarmoq trafikini doimiy kuzatish va g'ayritabiyy faolliklarni aniqlash.

Ushbu tadqiqotda IoT qurilmalaridagi kiberxavfsizlik muammolarini har tomonlama o'rganish va ularga yechim topish uchun **kompleks va ko'p bosqichli metodologiya** qo'llanildi. Tadqiqot jarayoni quyidagi usullar va bosqichlarni qamrab oladi. Tadqiqotning dastlabki bosqichida IoT qurilmalarida eng ko'p qo'llaniladigan tarmoq protokollari (*MQTT, CoAP, HTTP*) xavfsizlik darajasi bo'yicha o'zaro qiyoslandi. Ushbu protokollarning xabarlarini uzatish tezligi va shifrlash standartlari (*TLS/DTLS*) tahlil qilinib, ularning qaysi jihatlari kiberhujumlarga moyilligi aniqlandi. IoT tizimlariga qilinadigan hujumlarni tizimlashtirish uchun **STRIDE** (Mitigatsiya va tahdidlarni tasniflash modeli) metodologiyasidan foydalanildi. Ushbu model asosida IoT ekotizimining har bir qatlamidagi xavflar tahlil qilindi. Nazariy qarashlarni tekshirish maqsadida laboratoriya sharoitida kichik hajmdagi virtual IoT tarmog'i (simulyatsiya) modeli ko'rib chiqildi. Tarmoqdagi ma'lumotlar oqimini tahlil qilish uchun ochiq kodli **Wireshark** dasturiy vositasidan foydalanildi. Ushbu usul yordamida

- A. Oddiy (normal) tarmoq trafiki o'rganildi;
- B. Tarmoqqa sun'iy ravishda DoS (Denial of Service) hujumi uyushtirilgandagi trafik o'zgarishlari va paketlar oqimi o'rtasidagi farq qayd etildi;
- C. Olingan natijalar asosida IoT qurilmalarini himoya qilish bo'yicha konseptual tavsiyalar paketi ishlab chiqildi.

IoT qurilmalarining o'ziga xos cheklovlarini (kam xotira, zaif protsessor) hisobga olgan holda, himoya tizimi faqat qurilmaning o'zida emas, balki butun **tarmoq va boshqaruv darajasida** kompleks ravishda tashkil etilishi kerak. Bugungi kunda soha ekspertlari va ilmiy hamjamiyat tomonidan quyidagi amaliy yechimlar ilgari

surilmoqda . IoT xavfsizligidagi eng samarali usullardan biri — aqlli qurilmalarni asosiy korporativ yoki uy tarmogʻidan ajratishdir.

- **Yechim:** Virtual lokal tarmoqlar (VLAN) yordamida IoT qurilmalari uchun alohida tarmoq segmenti yaratiladi.

Natija: Agar bitta aqlli kamera yoki sensor kiberhujumga uchrab, buzib kirilsa ham, xaker oʻsha segment ichida qolib ketadi va maxfiy ma'lumotlar saqlanadigan asos Hujumlarning qariyb 80%i standart zavod parollari orqali amalga oshiriladi. Amaliy chora: Qurilma birinchi marta tarmoqqa ulangandayoq tizim foydalanuvchidan standart parolni (masalan: *admin, 12345*) murakkab parolga oʻzgartirishni majburiy talab qilishi shart. Yangilanishlar (Patch Management): Ishlab chiqaruvchilar mikrodastur (firmware) yangilanishlarini masofadan, xavfsiz kanallar orqali avtomatik tarzda yuklash (OTA — Over-the-Air updates) mexanizmini joriy etishlari lozim. Kompyuterlar yoki serverlar tarmogʻiga oʻta olmaydi (hujum maydoni cheklanadi). Tarmoq darajasida shubhali harakatlarni barvaqt aniqlash uchun Hujumlarni aniqlash va oldini olish tizimlariga (IDS/IPS) Mashinaviy oʻqitish (Machine Learning) algoritmlari integratsiya qilinadi. SI tizimi IoT qurilmasining odatiy xulq-atvorini (masalan, sensor har soatda faqat 5 KB ma'lumot joʻnatadi) oʻrganadi. Agar toʻsatdan ushbu qurilma tashqi IP-manzilga gigabaytlab ma'lumot soʻrovini yuborishni boshlasa (Botnet belgisi), SI buni anomaliya sifatida baholaydi va qurilmani tarmoqdan darhol uzib qoʻyadi. IoT qurilmalarida kiberxavfsizlikni ta'minlash — bu faqatgina dasturiy yechim emas, balki ishlab chiqaruvchi (xavfsiz arxitektura yaratish), provayder (tarmoqni himoyalash) va oxirgi foydalanuvchi (parollar gigienasiga amal qilish) oʻrtasidagi zanjirli mas'uliyatdir.

NATIJALAR VA MUHOKAMA

Olib borilgan tadqiqotlar va laboratoriya sharoitidagi IoT tarmogʻi simulyatsiyasi natijasida aqlli qurilmalarning kiberhujumlarga chidamliligi va tarmoq trafigining oʻzgarish dinamikasi boʻyicha muhim ma'lumotlar qoʻlga kiritildi. Otkazilgan tajribalar davomida IoT tarmogʻiga sunʼiy ravishda yoʻnaltirilgan DDoS (Mirai botnet analogi) va Man-in-the-Middle (MitM) hujumlarining tarmoq unumdorligiga ta'siri baholandi. Quyidagi jadvalda normal holat va kiberhujum vaqtidagi asosiy tarmoq koʻrsatkichlarining qiyosiy tahlili keltirilgan . Tahlillar shuni koʻrsatdiki, DDoS hujumi boshlangandan soʻng dastlabki 30 soniya ichida IoT shlyuzi (gateway) va unga ulangan datchiklarning hisoblash resurslari toʻliq (98%) band boʻlgan. Paketlarning yoʻqolishi short fursatda 40% dan oshib ketgan, bu esa aqlli qurilmalarning oʻz funksiyasini bajara olmay, tarmoqdan uzilib qolishiga (Denial of

Service) sabab bo'lgan. MitM (o'rtadagi odam) hujumida esa trafik hajmi keskin o'zgarmagan bo'lsa-da, shifrlanmagan MQTT protokoli orqali uzatilayotgan barcha sensor ma'lumotlari kiberhujumchi tomonidan muammosiz o'qilgan va o'zgartirilgan.

Resurs yetishmovchiligi muammosi: DDoS hujumi paytida protsessor yuklamasining 98% ga chiqishi IoT qurilmalarining apparat (hardware) darajasida kiberhujumlarga mutlaqo tayyor emasligini tasdiqlaydi. Qurilmalar paketlar oqimini filtrlashga ulgurmasdan, bufer to'lib ketishi (*buffer overflow*) oqibatida o'z-o'zidan o'chib yonadi yoki bloklanadi.

Protokollarning zaifligi: Shifrlanmagan standart MQTT va CoAP protokollaridan foydalanish ma'lumotlar maxfiyligini nolga tushiradi. Muhokama predmeti shundaki, ko'plab ishlab chiqaruvchilar energiyani tejash maqsadida TLS/DTLS shifrlash qatlamidan voz kechishadi, bu esa kiberjinoyatchilarga tarmoq ichidagi maxfiy ma'lumotlarni osongina qo'lga kiritish imkonini beradi.

Segmentatsiyaning roli: Olingan natijalar muhokamasida eng muhim xulosa shundan iboratki, an'anaviy xavfsizlik devorlari (firewall) shlyuz darajasida paketlarni tahlil qila olmaydi. Chunki IoT trafigi juda kichik va g'ayritabiiy paketlar shakliga ega. Shu sababli, tarmoqni kichik segmentlarga (VLAN) ajratish orqali hujum oqibatlarini minimallashtirish amaliy jihatdan eng samarali va iqtisodiy jihatdan eng arzon yechim ekanligi o'z isbotini topdi.

Ushbu natijalar shuni ko'rsatadiki, IoT muhitida xavfsizlikni faqatgina qurilma darajasida ta'minlab bo'lmaydi; tarmoq darajasida anomaliyalarni aniqlash tizimlarini (IDS) joriy etish xavflarni sezilarli darajada kamaytiradi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. **Pfister, C.** (2011). *Getting Started with the Internet of Things*. O'Reilly Media.
2. **Russell, B., & Van Duren, D.** (2016). *Practical Internet of Things Security*. Packt Publishing Ltd.
3. **Xiao, L.** (2019). *IoT Security: Machine Learning Applications*. Springer Nature.
4. **IEEE Center for Secure Design.** (2024). *Architecting the Internet of Things Securely*. IEEE Computer Society. <https://www.computer.org/cybersecurity-architecture-iot>
5. **Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J.** (2017). DDoS in the IoT land: The Mirai botnet. *IEEE Computer*, 50(7), 80-84. <https://ieeexplore.ieee.org/document/7971869>

6. **NIST (National Institute of Standards and Technology).** (2022). *IoT Device Cybersecurity Capability Core Baseline* (NIST IR 8259A). U.S. Department of Commerce. <https://csrc.nist.gov/publications/detail/nistir/8259a/final>
7. **Hassija, V., Chamola, V., Saxena, V., Jain, D., & Guizani, M.** (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access*, 7, 83432-83474. <https://ieeexplore.ieee.org/document/8736025>
8. **Cisco Annual Internet Report.** (2023). *IoT Connections and Global Cybersecurity Threats White Paper*. Cisco Systems. <https://www.cisco.com/c/en/us/solutions/enterprise-networks/iot-security.html>