IOT QURILMALARIDA KIBERXAVFSIZLIK: ZAIFLIKLAR, XAVFLAR VA XAVFLARNI KAMAYTIRISH STRATEGIYALARI

Majidov Anvarxon Maxmudxon o‘g‘li
O‘zbekiston Milliy Unversiteti, Axborot xavfsizligi magistranti.
E-mail: *anvarxonmajidov2000@gmail.com*

Annotatsiya. Internet narsalar (IoT) kundalik hayotning ajralmas qismiga aylanib bormoqda, u aqlli uylar, sog‘liqni saqlash, sanoat va transport kabi sohalarni qamrab oladi. Biroq, IoT qurilmalari sonining oshishi ularning ishlatilishi bilan bog‘liq kiberxavf-xatarlarning ko‘payishiga olib kelmoqda. Ushbu maqolada IoT qurilmalarining asosiy zaifliklari tahlil qilinadi, ular bilan bog‘liq xavflar ko‘rib chiqiladi hamda ularni minimallashtirish strategiyalari taklif etiladi.
Kalit so‘zlar: Internet narsalar,qurilmalar, IoT, AKT, kiberxavfsizlik, zaiflik, kompyuter tizimi.
Аннотация. Интернет вещей (IoT) становится неотъемлемой частью повседневной жизни, охватывая такие секторы, как умные дома, здравоохранение, промышленность и транспорт. Однако рост числа устройств Интернета вещей приводит к росту киберрисков, связанных с их использованием. В статье анализируются основные уязвимости устройств Интернета вещей, изучаются связанные с ними риски и предлагаются стратегии по их минимизации.
Ключевые слова: Интернет вещей, устройства, IoT, ИКТ, кибербезопасность, уязвимость, компьютерная система.
Abstract. The Internet of Things (IoT) is becoming an integral part of everyday life, covering areas such as smart homes, healthcare, industry, and transportation. However, the increasing number of IoT devices is leading to an increase in cyber risks associated with their use. This article analyzes the main vulnerabilities of IoT devices, considers the risks associated with them, and proposes strategies to minimize them.
Keywords: Internet of Things, devices, IoT, ICT, cybersecurity, vulnerability, computer system.

Kirish

IoT ma’lumotlarni yig‘uvchi, qayta ishlaydigan va uzatuvchi o‘zaro bog‘langan qurilmalar tarmog‘ini o‘z ichiga oladi. IoT qurilmalari cheklangan hisoblash resurslariga ega, bu ko‘pincha ularni an’anaviy kompyuter tizimlariga qaraganda kamroq xavfsiz qiladi. Bu holat IoT qurilmalariga qaratilgan hujumlar sonining ko‘payishiga olib keldi, bu esa kiberxavfsizlikni sohadagi asosiy muammolardan biriga aylantirdi.

ISSN 3030-3907



1-rasm. IoT dasturiy ta’minotining ulangan qurilmalar bilan o‘zaro ta’siri.

IoT tizimlaridagi zaifliklar jiddiy, hatto halokatli oqibatlarga olib kelishi mumkin. Bu IoT virtual va jismoniy komponentlarni birlashtirgani bilan bog‘liq. Masalan, internetga ulangan aqlli mashinaga kirish huquqiga ega bo‘lgan tajovuzkorlar uning asosiy xavfsizlik funksiyalarini o‘chirib qo‘yishi mumkin. Sanoat IoT tizimlariga hujumlar butun korxonalarga ta’sir qiladigan halokatli natijalarga olib kelishi mumkin.

ADABIYOTLAR TAHLILI

Tibbiy IoT qurilmalari keng qo‘llaniladigan sog‘liqni saqlash sohasida ularning murosaga kelishi bemorning maxfiy ma’lumotlarining sizib chiqishiga olib kelishi va ularning sog‘lig‘ini xavf ostiga qo‘yishi mumkin. Aqlli uylarda xakerlar IoT qurilmalariga kirib, uyni boshqarish tizimini nazorat qilish va uning aholisi xavfsizligini buzishi mumkin.

ISSN 3030-3907

1-jadval.

IoT qurilmalarining zaifliklari.

Dasturiy ta’minot himoyasi yetarli emas	Ko‘pgina IoT qurilmalari eskirgan yoki yomon himoyalangan dasturiy ta’minot bilan chiqariladi. Ko‘pincha avtomatik yangilash mexanizmlari mavjud emas, zaifliklarni tuzatmagan holda qoldiradi.
Ma’lumotlarni shifrlashning yetishmasligi	IoT qurilmalari va serverlari o‘rtasida uzatiladigan ma’lumotlar ko‘pincha shifrlanmagan bo‘lib, “o‘rtadagi odam” (MITM) hujumlari uchun eshikni ochadi.
Zaif autentifikatsiya mexanizmlari	Oldindan o'rnatilgan parollar yoki zaif autentifikatsiya usullaridan foydalanish qurilmalarni buzib kirishni osonlashtiradi.
Kirish nazorati yetarli emas	Ko‘pgina IoT qurilmalari ruxsatsiz foydalanishga olib kelishi mumkin bo‘lgan qat'iy nazoratsiz o‘z funktsiyalariga cheksiz kirishni ta’minlaydi.
Aloqa protokollaridagi zaifliklar	IoT qurilmalari (masalan, MQTT, CoAP) o‘rtasidagi aloqa uchun foydalaniladigan protokollar tajovuzkorlar tomonidan ishlatilishi mumkin bo‘lgan ma’lum zaifliklarga ega.

2-jadval.

IoT dan foydalanish bilan bog‘liq xavflar.

Ma’lumotlar maxfiyligini buzish	IoT qurilmalari ko‘pincha katta hajmdagi shaxsiy ma’lumotlarni to‘playdi, agar ular sizib chiqsa, xavf tug‘diradi.

ISSN 3030-3907

Infratuzilmaga hujumlar	Zaif IoT qurilmalari butun tarmoqlarni falajlashi mumkin bo'lgan tarqatilgan xizmat ko'rsatishni rad etish (DDoS) hujumlarini boshlash uchun ishlatilishi mumkin.
Jismoniy tahdidlar	Aqlli qulflar yoki tibbiy qurilmalar kabi IoT qurilmalarini buzish jismoniy yoki mulkiy zararga olib kelishi mumkin.
Sanoat tizimlariga tahdidlar	Sanoat muhitida IoT qurilmalariga hujumlar ishlab chiqarish jarayonlariga ta’sir qilishi mumkin, bu esa katta moliyaviy yo'qotishlarga olib keladi.

TADQIQOT METODOLOGIYASI

IoT tizimlari kundalik hayotda, sanoat va davlat tuzilmalarida keng qo‘llaniladi. Biroq, ularning integratsiyasi maxfiylik, ma’lumotlar yaxlitligi, shuningdek, jismoniy va axborot xavfsizligiga tahdid solishi mumkin bo‘lgan bir qator xavflar bilan bog‘liq.

Asosiy tahdidlardan biri bu ma’lumotlar maxfiyligini buzishdir. IoT qurilmalari foydalanuvchilarning joylashuvi, salomatligi, afzalliklari va kundalik faoliyati haqidagi ma’lumotlarni o‘z ichiga olgan katta hajmdagi shaxsiy ma’lumotlarni to‘playdi. Ushbu qurilmalarning zaifligi ma’lumotlarning sizib chiqishiga jiddiy tahdid soladi. Masalan, fitnes-trekerlar va aqlli soatlar kabi taqiladigan qurilmalarni buzish ma’lumotlarning firibgarlik yoki shantaj uchun ishlatilishiga olib kelishi mumkin. Shunga o‘xshash xavflar aqlli uylarda paydo bo‘ladi, bu yerda kameralar yoki termostatlar kabi qurilmalarni buzish foydalanuvchilar hayotining shaxsiy ma’lumotlarini oshkor qilishi mumkin. Korporativ muhitda IoT qurilmalari tomonidan to‘plangan ma’lumotlarning sizib chiqishi raqobatchilar yoki tajovuzkorlarga maxfiy biznes ma’lumotlariga kirish imkonini berishi mumkin.

IoT qurilmalari ham kiberhujumlar uchun oson nishon hisoblanadi, ayniqsa ular ommaviy ravishda buzib kirilgan bo‘lsa. Bunday qurilmalar ko‘pincha botnetlarda xizmat ko‘rsatishni rad etish (DDoS) hujumlarini amalga oshirish uchun ishlatiladi. Ushbu hujumlar tarmoqlarni falaj qilishi, davlat xizmatlarini buzishi yoki milliy xavfsizlikka tahdid solishi mumkin. Masalan, transport yoki energiya tizimlari bilan bog‘liq infratuzilmalarni buzish muhim xizmatlar ko‘rsatishda jiddiy uzilishlarga olib kelishi mumkin.

ISSN 3030-3907

MUHOKAMA VA NATIJALAR

Jismoniy tahdidlar ham katta xavf tug‘diradi, chunki IoT qurilmalari bevosita jismoniy ob'ektlarga ulangan. Smart qulflarni buzish uylar yoki ofislarga ruxsatsiz kirishga olib kelishi mumkin, yurak stimulyatori yoki insulin nasoslari kabi tibbiy asboblarni buzish esa bemorlarning hayotini xavf ostiga qo‘yadi. Bundan tashqari, tarmoqqa ulangan transport vositalarini buzish tormoz ishdan chiqishi yoki marshrutni o‘zgartirish bilan bog‘liq favqulodda vaziyatlarga olib kelishi mumkin.

Sanoat muhitida ishlab chiqarish jarayonlarini boshqarish uchun IoT qurilmalaridan foydalanish qo‘shimcha xavflarni keltirib chiqaradi. Bunday tizimlarga hujum ishlab chiqarishning to‘xtab qolishiga, mahsulotning shikastlanishiga yoki xavfli moddalarning sizib chiqishi sababli ekologik ofatlarga olib kelishi mumkin. Ushbu xavflar ehtiyotkorlik bilan boshqarishni va mustahkam himoya mexanizmlarini joriy qilishni talab qiladi.

- Xatarlarni kamaytirish strategiyalari.
- Kuchli autentifikatsiyani ta’minlash.

Har bir qurilma uchun ikki faktorli autentifikatsiya va noyob parollardan foydalanish ruxsatsiz kirish xavfini kamaytirishga yordam beradi.

Ma’lumotlarni shifrlash.

O‘tkazilgan ma’lumotlarni himoya qilish uchun kuchli shifrlash usullarini (masalan, TLS/SSL) qo‘llash tutib qolish xavfini kamaytiradi.

Dasturiy ta’minotni muntazam yangilash Ishlab chiqaruvchilar muntazam xavfsizlik yangilanishlarini taqdim etishlari kerak va foydalanuvchilar ularni o‘z vaqtida o‘rnatishlari shart.

Tarmoq segmentatsiyasi.

IoT qurilmalari va muhim tizimlarni turli tarmoqlarga ajratish butun infratuzilmaning buzilishi ehtimolini kamaytiradi.

Monitoring va anomaliyalarni aniqlash.

IoT qurilmalarining shubhali xatti-harakatlarini aniqlash uchun monitoring tizimlaridan foydalanish tahdidlarga tezkor javob berishga imkon beradi.

Standartlar va sertifikatlash.

Xalqaro xavfsizlik standartlarini ishlab chiqish va joriy etish IoT qurilmalari ularning xavfsizligini yaxshilashga yordam beradi. Internet of Things xavfsizlik hodisalariga misollar.

So‘nggi yillarda IoT qurilmalari kiberjinoyatchilar tomonidan nishonga olingan ko‘plab holatlar mavjud. Mana ba’zi mashhur misollar:

2016 yil - Mirai botnet hujumi.

2016-yilda Mirai botneti buzilgan yuz minglab IoT qurilmalarini bog‘ladi.

ISSN 3030-3907

Zararli dasturlar bilan zararlangan qurilmalar tarmog‘i botnet internetda o‘z egalarini bilmagan holda avtomatlashtirilgan harakatlarni amalga oshirdi. Hujum Spotify, Netflix va PayPal kabi yirik onlayn xizmatlarning keng tarqalishiga olib keldi.

2018 yil - VPNFilter zararli dasturlarini tarqatish.

2018-yilda 50 mamlakatda yarim milliondan ortiq marshrutizator VPNFilter zararli dasturi qurboni bo‘ldi. Ushbu virus ma’lumotlarni to‘xtatadigan, trafikni bloklaydigan va foydalanuvchi hisob ma’lumotlarini o‘g‘irlaydigan qurilmalarga zararli dasturlarni o‘rnatishga imkon berdi.

2020 - Tesla Model X zaifligi.

2020-yilda kiberxavfsizlik bo‘yicha mutaxassis Bluetooth protokolidagi zaiflikdan foydalanib, Tesla Model X’ni bir necha daqiqada buzish usulini topdi. Shunga o‘xshash hujumlar kirish va ishga tushirish uchun simsiz kalitlardan foydalanadigan boshqa transport vositalariga ta’sir qildi.

2021 yil - Verkada kuzatuv kameralariga xakerlar hujumi. 2021-yilda xakerlar Verkadaga tegishli 150 000 ta kuzatuv kameralaridagi video tasmalarga kirish huquqiga ega bo‘ldi. Zarar ko‘rgan ob'ektlar orasida davlat va xususiy muassasalar: maktablar, kasalxonalar, qamoqxonalar va idoralar bor. Ushbu hodisalar maxfiylik va ma’lumotlarni himoya qilishning buzilishi bilan bog‘liq jiddiy xavflarni ko‘rsatdi.

XULOSA

IoT qurilmalaridagi kiberxavfsizlik ularni amalga oshirishning muhim jihati hisoblanadi. Zaiflik va xavflarni samarali boshqarish sotuvchilar, dasturiy ta’minot ishlab chiquvchilari, xavfsizlik tadqiqotchilari va oxirgi foydalanuvchilar o‘rtasida hamkorlikdagi sa’y-harakatlarni talab qiladi. Taklif etilayotgan strategiyalarni amalga oshirish IoT qurilmalarini himoya qilish darajasini sezilarli darajada oshirishi va potentsial tahdidlarni minimallashtirishi mumkin.

ADABIYOTLAR RO‘YHATI

1. Беляев А.В. Кибербезопасность в Интернете вещей: современные угрозы и подходы к защите // Информационные технологии и безопасность. – 2023. – №4(18). – С. 15–22.
2. Majidov A.M. IoT systems programming // Science Shine. International Scientific Journal. – 2025. – №3(38). – S. 8. – ISSN 3030-377X.
3. Козырев С.Н., Михеев И.В. Анализ уязвимостей IoT-устройств и методы их минимизации // Журнал прикладной информатики. – 2023. – Т. 19, №2. – С. 44–52.
4. Majidov A.M. IoT qurilmalariga qarshi DDoS hujumlarining tahlili // Aqlli texnologiyalar va tadqiqotlarda innovatsion yondashuv: raqamli kelajakni

ISSN 3030-3907

yaratish. Xalqaro ilmiy-amaliy konferensiya materiallari. – Adju universiteti, Toshkent, 2025. – 22 fevral. – S. 5.
5. Смирнов Д.В., Петрова Л.И. Риски и угрозы безопасности в Интернете вещей: российский контекст // Безопасность информационных технологий. – 2022. – №3. – С. 27–34.
6. Majidov A.M. IOT (Internet of Things) – narsalar interneti // Yosh ilmiy tadqiqotchi. Pedagogik ilmiy-amaliy anjumani materiallari. – Buxoro davlat universiteti. – Buxoro, 2025. – 15 mart. – S. 4.
7. Иванов А.А., Сергеев Н.В. Принципы обеспечения информационной безопасности в устройствах IoT // Вестник информационной безопасности. – 2024. – №1. – С. 10–18.
8. Majidov A.M. Aqlli texnologiyalar va kiberxavfsizlik: IoT va AI integratsiyasi // Sun’iy intellekt va o‘qitishning zamonaviy an’analari. Xalqaro ilmiy anjumani materiallari. – Samarqand viloyati pedagogik mahorat markazi. – Samarqand, 2025. – 18–19 aprel. – S. 5.
9. Сидоров В.И., Зотова М.В. Методы идентификации и устранения уязвимостей в системах Интернета вещей // Электронная техника. Сер. 10. – 2023. – №5. – С. 66–73.
10. Majidov A.M. Axborot hujumlari modellarini qurish usuli // Yoshlar ilm-fan jurnali. – 2025. – №1. – 22 may. – S. 6.
11. Шапошников К.С. Интернет вещей и киберугрозы: вызовы и пути их преодоления // Информационные системы и технологии. – 2023. – №4. – С. 40–46.
12. Majidov A.M. IoT tizimlarida axborot xavfsizligini ta’minlashning ahamiyati // Zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar. Respublika ilmiy-texnik anjumani materiallari. – O‘zbekiston Milliy universiteti Jizzax filiali. – Jizzax, 2025. – 16–17 may. – S. 5.
13. Захаров И.П. Обеспечение конфиденциальности и целостности данных в IoT-устройствах // Проблемы информационной безопасности. – 2022. – №2. – С. 22–29.
14. Фролов А.Е., Матвеева О.Н. Анализ подходов к разработке защищённых архитектур Интернета вещей // Защита информации. – 2023. – №6. – С. 35–41.
15. Majidov A.M. IoT tizimida ma’lumotlarni himoya qilishning zamonaviy muammolari // Axborot xavfsizligi sohasida raqamlashtirish muammolari va istiqbollari. Respublika ilmiy-amaliy konferensiyasi materiallari. – O‘zbekiston Xalqaro Islom Akademiyasi. – Toshkent, 2025. – 15 may. – S. 3.

ISSN 3030-3907

16. Мельников Р.А., Лебедев Г.В. Технологии шифрования и их роль в защите IoT-устройств // Криптография и безопасность. – 2022. – №3. – С. 14–21.
17. Чернов В.В. Эффективные стратегии снижения киберрисков в системах Интернета вещей // Информационные войны. – 2024. – №1. – С. 19–26.
18. Попов Е.С., Гришина А.В. Этические аспекты кибербезопасности в эпоху IoT // Этика и технологии. – 2023. – №2. – С. 8–14.

ISSN 3030-3907