IOT QURILMALARIGA QARATILGAN DDOS HUJUMLARIGA UMUMIY SHARH

O'rinov Nodirbek Toxirjonovich[1], Mamadaliyev Sarvar Saloxiddin o'g'li[1], Akbarova Madina Shavkatbek qizi[1]

[1]Zahiriddin Muhammad Bobur nomidagi Andijon davlat universiteti Axborot texnologiyalari kafedrasi
Email: nodirbekurinov1@gmail.com

KEYWORDS

DDoS, IoT, botnet, xizmatdan voz kechish, Mirai.

ABSTRACT

Tarqatilgan "xizmatdan voz kechish" (DDoS) hujumlari Internet tarmog'idagi eng global tahdidlardan biriga aylanmoqda. Internet narsalari (IoT) qurilmalari sonining ortib borishi DDoS hujumlarini amalga oshirish usullarining ko'payishiga sabab bo'lmoqda. Ushbu maqolada IoT qurilmalariga qaratilgan DDoS hujumlariga umumiy sharh berilgan va IoT qurilmalariga ega IT infratuzilmalari xavfsizligini ta'minlash bo'yicha asosiy tavsiyalar keltirilgan.

Kirish

DDoS-hujumlar (Distributed Denial of Service – tarqatilgan "xizmatdan voz kechish" hujumlari) – bu hisoblash tizimlariga (tarmoq resurslari yoki aloqa kanallariga) qaratilgan hujum bo'lib, ularning qonuniy foydalanuvchilar uchun foydalanish imkoniyatini cheklashni maqsad qiladi. DDoS hujumlari bir yoki bir nechta Internetga ulangan kompyuterlardan ma'lum bir resursga bir vaqtning o'zida ko'p miqdorda so'rovlar yuborishni o'z ichiga oladi. Agar minglab, o'n minglab yoki millionlab kompyuterlar bir vaqtning o'zida ma'lum bir server (yoki tarmoq xizmatiga) so'rovlar yuborishni boshlasa, bu serverni ishlamay qolishiga yoki aloqa kanalining o'tkazuvchanligi yetarli bo'lmasligiga olib keladi. Har ikkala holatda ham Internet foydalanuvchilari hujum qilingan server yoki hatto bloklangan aloqa kanaliga ulangan barcha server va resurslarga kira olmaydilar [8].

Boshqacha qilib aytganda, DDoS hujumi – bu serverlar, tarmoq infratuzilmasini sekinlashtirish yoki ishdan chiqarish hamda ilovalar trafiki ustiga turli resurslardan "bomba" kabi so'rovlar yuborishga qaratilgan hujumdir. Natijada, DDoS-hujumlar tufayli veb-saytlar va ilovalar ishlashda uzilishlar yoki to'liq ishlamay qolish holatiga duch keladi. Bugungi kunda ilovalar va serverlarning ishlamay qolishining 30% dan ortig'i DDoS hujumlari bilan bog'liq [1].

Dunyo miqyosida har kuni ikki mingga yaqin DDoS hujumi qayd etiladi. Bir DDoS hujumi yirik kompaniyaga o'rtacha soatiga 250 AQSh dollari miqdorida zarar keltiradi [2].

Adabiyotlar tahlili va metodologiyasi. Xozirgi vaqtga kelib IoT texnologiyalari va DDoS hujumlarini o'rganib taxlil qilish bo'yicha Sh.R.G'ulomov, A.A.G'aniyev, A.V.Kobulov, S.S.To'xtayev, Горев A.B. va boshqalar ilmiy ishlar olib bormqda.

DDoS hujumlarida Botnetlardan foydalanish

DDoS hujumlarini amalga oshirishning eng xavfli va keng tarqalgan usullaridan biri bu botnetlardan foydalanishdir. Botnet – bu zararli dasturiy ta'minot bilan yuqtirilgan va hujumchi tomonidan masofadan boshqariladigan qurilmalar tarmog'idir. Ushbu tarmoq kiberjinoyatchilarga spam va zararli dasturlarni tarqatish, shuningdek, DDoS hujumlarini tashkil etish imkonini beradi. Eng xavflisi shundaki, qurilma egasi bundan bexabar bo'lishi mumkin.

IoT qurilmalari tobora keng tarqalib borayotganligi sababli, ushbu texnologiya botnetlar uchun jiddiy xavf tug‘diradi [1].IoT botneti – bu zararli dastur bilan yuqtirilgan IoT qurilmalarining tarmog‘i bo‘lib, ular hujumchilar tomonidan boshqariladi. Botlar odatda zaif himoyalangan tizimlarga hujum qilish orqali yoki foydalanuvchilarni aldamchi dasturlarni o‘rnatishga majburlash yo‘li bilan tarqaladi. Ushbu tarqatish usullari muntazam ravishda takomillashtirilib, yanada murakkablashib bormoqda.

Agar botnet yetarli darajada yirik bo‘lsa – minglab yoki hatto yuz minglab qurilmalardan iborat bo‘lsa – u ma’lum bir server yoki tarmoq xizmatiga ko‘plab so‘rovlar yuborishi mumkin. Natijada, xizmat yoki serverning resurslari tugaydi yoki tarmoq kanali haddan tashqari yuklanadi. Natijada, ushbu xizmat oddiy foydalanuvchilar uchun foydalanib bo‘lmaydigan holatga keladi. Agar har bir infeksiya qilingan qurilma soniyada o‘nlab yoki yuzlab so‘rovlar yuborsa, hujumning intensivligi bir necha barobar ortib, hatto eng mustahkam serverlarni ham ishdan chiqarishi mumkin. [8].

Shu sababli, botnetlarga qarshi samarali xavfsizlik choralarini ko‘rish muhim bo‘lib, ayniqsa, IoT qurilmalarining himoyasini mustahkamlash dolzarb masalaga aylangan.

IoT qurilmalariga qaratilgan DDoS hujumlari

2016-2023 yillarda DDoS hujumlarining soni va ta’sir doirasi sezilarli darajada oshdi, bu holat asosan Internet narsalari (IoT) texnologiyasining keng joriy etilishi bilan bog‘liqdir [1]. IoT – bu turli xil qurilmalarni Internetga ulash orqali ma’lumot almashish va avtomatlashtirilgan boshqaruv imkoniyatlarini kengaytiruvchi zamonaviy texnologiya. Ushbu qurilmalar o‘zaro hamkorlik qilib, veb-xizmatlar va ilovalar bilan ma’lumot almashishi mumkin. IoT texnologiyasi turli sohalarda qo‘llanilib, aqlli uylarni avtomatlashtirish, chiqindilarni samarali boshqarish va real vaqt rejimida biometrik ma’lumotlarni yig‘ish kabi qulayliklar yaratmoqda.

Biroq, IoT qurilmalarining keng tarqalishi kiberxavfsizlik bilan bog‘liq muammolarni ham keltirib chiqarmoqda. Ularning aksariyati yetarlicha himoyalanmagan bo‘lib, bu esa kiberjinoyatchilar uchun yangi hujum nishonlarini yaratadi. Masalan, botnetlar IoT qurilmalaridagi zaifliklardan foydalanib, yuz minglab qurilmalarni o‘z nazoratiga olishi va ularni katta miqyosdagi DDoS hujumlarini uyushtirish uchun ishlatishi mumkin [3].

Bugungi kunda IoT konsepsiyasi quyidagi ikki asosiy texnologiyaga asoslanadi:

1. **Radiochastota identifikatsiyasi (RFID)** – obyektlarni aniqlash texnologiyasi bo‘lib, radioto‘lqinlar yordamida ma’lumotlarni yozish va o‘qish imkonini beradi.
2. **Simsiz sensorli tarmoqlar (WSN)** – ko‘plab sensorlar va bajaruvchi qurilmalar radioto‘lqinlar orqali birlashtirilgan bo‘lib, ularning qamrov doirasi bir necha metrdan bir necha kilometrgacha yetishi mumkin.

IoT arxitekturasi bir necha qatlamlardan tashkil topgan bo‘lib, ular sensor tarmog‘i, shlyuz, boshqaruv va ilova darajalaridan iborat. IoT xizmatlari ko‘pincha katta hajmdagi tugunlardan olingan ma’lumotlarni qayta ishlashga tayanadi, bu esa an’anaviy tarmoq arxitekturalaridan tubdan farq qiladi. Shu sababli, IoT qurilmalarining bir-biri va yuqori darajadagi tizimlar bilan o‘zaro aloqa qilishini ta’minlash uchun maxsus protokollar talab etiladi.

Internet tarmog‘ida, jumladan, IoT tizimlarida axborot xavfsizligining asosiy zaif jihatlaridan biri bu TCP/IP protokollar to‘plamining himoyasizligidir. Ushbu protokollar global tarmoq kommunikatsiyalarining asosini tashkil qilgani sababli, ularning zaif tomonlaridan foydalanib, IoT qurilmalariga qaratilgan turli hujumlar, jumladan, DDoS xurujlarini amalga oshirish mumkin. Shu bois, IoT ekotizimini himoya qilish uchun ilg‘or xavfsizlik choralarini ishlab chiqish va qo‘llash muhim ahamiyatga ega.

IoT uchun botnetlar

IoT uchun botnetlar Windows asosidagi botnetlardan farqlanadi. Ular buzilgan IoT qurilmalaridan tashkil topgan bo‘lib, IoTning keng tarmoqlaridan foydalanib, juda ko‘p qurilmalarga tarqalishi mumkin. Bundan tashqari, oddiy botnetlardan farqli o‘laroq, asosan spam yuborishga xizmat qiladigan botnetlar IoT qurilmalari bilan ishlaganda yanada katta zarar yetkazishi mumkin, chunki ular IoT qurilmalari foydalanadigan jismoniy muhitga ta’sir o‘tkazadi.

Masalan, IoT botnetlarining svetoforlarga qilgan hujumi shaharda tartibsizlik keltirib chiqarishi va aqlli shahar infratuzilmasini buzishi mumkin. Xuddi shunday, xakerlar aqlli uylardagi haroratni oshirib, sun’iy ravishda neft yoki gazga bo‘lgan talabni kuchaytirishi mumkin.

Shaxsiy kompyuterlar va serverlardan farqli o‘laroq, ular odatda fayervol va zararli dasturlarni aniqlovchi funksiyalar bilan himoyalangan bo‘lsa, IoT qurilmalari bu kabi xavfsizlik vositalariga ega emas. Shu sababli, botnetlar uchun IoT qurilmalari jozibali nishonga aylanadi.

IoT botsetlarining tarqalishi bilan bog‘liq kiberxavfsizlik tahdidi 2016-yilda bashorat qilingan edi. Ammo internet xavfsizligi bo‘yicha mutaxassislar ushbu muammoga yetarlicha e’tibor bermadilar. O‘sha paytda ushbu tahdid unchalik jiddiy ko‘rinmagan. Biroq, tez orada IoT qurilmalardagi himoyalanmagan zaifliklardan foydalanishga imkon beruvchi vositalar paydo bo‘ldi. 2016-yil oktabr oyida Mirai botnet hujumi IoT rivojlanishidagi asosiy burilish nuqtasiga aylandi.

Xakerlarni IoT qurilmalari “qurbon” sifatida qiziqtirmaydi. Ularning maqsadi qurilmani egallab olib, uni DDoS hujumlarini amalga oshiradigan botnetga qo‘shishdir.

IoT xavfsizligi ko‘pincha odatiy foydalanuvchilar va hatto kompaniyalar tomonidan ham e’tiborsiz qoldiriladi yoki yetarlicha baholanmaydi. IoT qurilmalarining zaifligi va ularning soni ortib borayotgani sababli bu soha xakerlar uchun qiziqarli bo‘lib qolmoqda [1].

Yiliga IoT qurilmalari sonining ko‘payishi bilan birga, ushbu qurilmalarning ichki dasturiy ta’minotidagi zaifliklar soni ham oshib bormoqda. Zaifliklarni aniqlash tezligi ularni bartaraf etuvchi yamalar (patch) chiqish tezligiga ta’sir qiladi. Shu sababli, IoT qurilmalaridagi ichki dasturiy ta’minot zaifliklarini aniqlash jarayonining samaradorligini oshirish zarur [5].

IoT qurilmalari qamrovi

Internet narsalari turli qurilmalarda mavjud: smartfonlar, aqlli kiyimlar, kiyiladigan texnologiyalar (masalan, bilakuzuklar, virtual haqiqat ko‘zoynaklari va boshqalar), maishiy texnikalar, aqlli televizorlar, o‘yin konsollari, transport tizimlari, binolar (masalan, kuzatuv kameralari), konditsionerlar, kirishni nazorat qilish tizimlari va boshqalar. Shuningdek, IoT jamoat infratuzilmasi (ko‘priklar, yo‘llar, parklar va boshqalar), jamoat xizmatlari, sanoat komponentlari (masalan, SCADA tizimlari) va transport tizimlarida ham mavjud.

Turli qurilmalardan ma’lumot yig‘ish va tahlil qilish miqdori oshgani sayin, nafaqat sanoat va xizmat ko‘rsatish sektorlarida, balki butun jamiyatning asosiy texnologik infratuzilmasi xavf ostida qoladi. Bu xavfsizlik tahdidlarini oshiradi, chunki ma’lumotlar hajmi tobora tezroq o‘sib, bir necha eksabaytga yetadi.

Tashkilotlangan jinoyatchilikning sanoat, harbiy, moliyaviy, tibbiy va boshqa infratuzilmalar bilan bog‘liq bashorat qilish tizimlariga ruxsatsiz kirishi juda xavfli bo‘lib, bu deyarli tuzatib bo‘lmaydigan oqibatlarga olib kelishi mumkin [6].

Hozirgi uylardagi xavfsizlik tizimlarining zaifligi

Hozirgi zamonaviy uylardagi har bir kompyuter tizimida zararli dasturlarni aniqlovchi skaner mavjud emas. Misol uchun, uydagi Linux, ARM yoki MIPS protsessorlariga asoslangan o‘nlab qurilmalarni uchratish mumkin: aqlli tizimlar boshqaruvidagi televizorlar, tarmoq qurilmalari

(masalan, tarmoq nuqtalari yoki Powerline adapterlari), internet-radio va Raspberry Pi kabi qurilmalar.

Linux operatsion tizimida xavfsizlikka oid dasturlar va xavfsizlik choralari kamligi ushbu qurilmalarni xakerlar uchun jozibador qiladi. Zararli dasturlar odatda ishga tushiriladi va o‘chiriladi, ya’ni qurilma qayta yuklangandan so‘ng yo‘q bo‘lib ketadi. Shu sababli, operatsion tizim nusxalarini tahlil qilish yoki mavjud fayllarni tekshirish foydasiz bo‘lib qoladi.

Mirai – IoT uchun eng xavfli botnetlardan biri

Mirai — bu zararli dastur bo‘lib, ARC protsessorida ishlaydigan aqlli qurilmalarni infeksiyalaydi va ularni masofadan boshqariladigan botlar yoki "zombi" tarmog‘iga aylantiradi. Ushbu botlar tarmog‘i ko‘pincha DDoS hujumlarini amalga oshirish uchun ishlatiladi.

Mirai internetni skaner qilib, ARC protsessorida ishlaydigan IoT qurilmalarni qidiradi. Ushbu protsessor odatda Linuxning qisqartirilgan versiyasida ishlaydi. Agar qurilmaning foydalanuvchi nomi va paroli o‘zgartirilmagan bo‘lsa, Mirai qurilmaga kirib, uni infeksiyalashi mumkin.

Vaqt o‘tishi bilan Mirai evolyutsiyalashdi. Xakerlar internetda qolgan Mirai dasturining ochiq kodidan foydalanib, boshqa botnetlar yaratdilar va yaratishda davom etmoqdalar, masalan, Okiru, Satori, Masuta va PureMasuta.

Mirai o‘z mutatsiyalarini deyarli har kuni namoyon qilmoqda. Ularning zarar yetkazish va ko‘payish qobiliyatini saqlab qolgani IoT qurilmalar ishlab chiqaruvchilarining xavfsizlik choralariga loqayd munosabatini ko‘rsatadi. Ajablanarlisi, bunday botnetlar va ularning qurilmalariga keltiradigan tahdidlariga qaramasdan, ular yetarlicha o‘rganilmagan. Shu bilan birga, murakkab hujumlar orqali internet infratuzilmasiga katta zarar yetkazish ehtimoli mavjud [7].

Mirai skanerlash xususiyatlari

Mirai botnetining qurilmalarni skanerlashdagi asosiy xususiyati uning qurilmaga ulanishga harakat qilganda foydalanadigan login va parollar lug‘atidadir. Mirai dasturining asl muallifi dastlabki skanerlash jarayoniga nisbatan kichikroq login va parollar ro‘yxatini kiritgan edi. Ammo hozirgi vaqtda ushbu ro‘yxat turli IoT qurilmalar uchun “standart” login va parollar hisobiga kengaytirilib, botning modifikatsiyalari paydo bo‘lganini ko‘rsatadi.

IoTrooper va Reaper botnetlari

Yaqinda IoTrooper va Reaper nomlari bilan tanilgan yangi va kuchli botnet aniqlangan. U IoT qurilmalarini Mirai’dan ko‘ra tezroq buzishga qodir. Reaper ko‘proq ishlab chiqaruvchilar qurilmalarini nishonga ola oladi va o‘z botlari ustidan ancha katta nazoratga ega [7].

DDoS hujumlarni aniqlashning an’anaviy strategiyalari

1. **Imzo asosidagi aniqlash** DDoS hujumlarini aniqlashda keng qo‘llaniladigan ikki yondashuv mavjud: imzo asosidagi va anomaliyaga asoslangan aniqlash. Imzo asosidagi aniqlash odatda mavjud ma'lumotlarni hujumning ma’lum namunalariga moslashtirishga harakat qiladi. Bunga misol sifatida Captcha tizimlari keltirilishi mumkin. Captcha — inson uchun oson hal qilinadigan, lekin zamonaviy kompyuter dasturlari uchun murakkab bo‘lgan vazifani o‘z ichiga oladi. Ushbu yondashuvning afzalligi — soddaligi. Yangi hujum aniqlanganda, uning faoliyatiga xos bo‘lgan noyob xususiyatlarni aniqlash va ularni imzolar bazasiga qo‘shish mumkin.

Masalan, **Mirai botneti** skanerlash va infeksiya jarayonida o‘ziga xos tarmoq trafik imzolarini namoyon qiladi, bu esa uni imzo asosida aniqlash uchun kuchli nomzod qiladi.

2. **Anomaliyaga asoslangan aniqlash** Anomaliyaga asoslangan aniqlash hujumlarni me’yordan chetga chiqish asosida aniqlaydi. Ushbu strategiyaning odatiy amalga oshirilishi shundan iboratki, aniqlash mexanizmi tizimning normal

holatini kuzatib, uzoq vaqt davomida uni o‘rganadi. Noodatiy faoliyat aniqlanganda, tizim xavotir signalini chiqaradi. Anomaliyalarni aniqlashning keng tarqalgan strategiyasi tizim ishini statistik modellashtirishdir. Bu usul tizimning nima sababdan normal va nima sababdan g‘ayritabiiy ekanligini matematik asosda aniqlashga imkon beradi. Ushbu usul aniqlash uchun tor doiradagi imzolarni ishlatmasligi sababli, u nol-kun hujumlarini ham aniqlashga qodir. Bu yangi hujum paydo bo‘lganda tizimda kuzatilgan g‘ayritabiiy faoliyatni aniqlaydi.

Afsuski, anomaliyalarni aniqlash ham kamchiliklardan holi emas. Garchi tizim juda noodatiy holat bilan duch kelsa-da, bu uning hujumga uchraganligini anglatmaydi. Anomaliyalarni aniqlash tizimlari o‘z tabiatiga ko‘ra, faollikni hujum deb belgilashda ortiqcha harakat qilishga moyildir, bu esa yuqori darajadagi yolg‘on ogohlantirishlarga olib keladi [3].

Bot-netlarning tahdidini to‘liq yo‘q qilish imkonsiz bo‘lsa-da, bu hujumlarning ta’sirini va miqyosini cheklashning hali ham usullari mavjud, agar oldindan choralar ko‘rilsa. Ulardan biri – Internet narsalari qurilmalarini tashqi trafikdan himoyalangan segmentatsiyalangan tarmoqda joylashtirish. Shuningdek, tizimlarni monitoring qilishni boshlash va zararli kirishlarni aniqlash jarayonlarini ishlab chiqishga sarmoya kiritish juda muhim, chunki bu foydalanuvchiga tizimning buzilganligi haqida ogohlantirish berish uchun katta ahamiyatga ega bo‘ladi.

Tarmoqni segmentatsiya qilish va test qilishdan tashqari, dasturni yangilash va apparat ta'minotini yangilash kabi asosiy xavfsizlik choralarini unutmaslik kerak, shuningdek, ma'lum bir qurilmaga kimlarning kirish huquqiga ega ekanligini nazorat qilish imkoniyati ham juda muhimdir [9].

IoT davrida IT-infrastrukturalarni himoya qilish bo‘yicha asosiy tavsiyalar

DDoS va boshqa turdagi kiberhujumlardan himoyalanish zamonaviy xavfsizlik tahdidlarining murakkabligini tushunishdan boshlanadi. "Narsalar interneti" (IoT) bog‘liq qurilmalarni o‘z IT-infrastrukturalarining bir qismiga aylantirayotgan korxonalar, shuningdek, korporativ veb-saytlar, CRM-tizimlar va sozlanadigan ijtimoiy tarmoq yechimlarini boshqaradigan kompaniyalar uchun yangi xavfsizlik muammolarini keltirib chiqardi.

Quyidagi umumiy, ammo samarali maslahatlarga amal qilib, IoT bilan bog‘liq xavfsizlik xatarlarini sezilarli darajada kamaytirishingiz va IT-infrastrukturalaringizni himoya qilishingiz mumkin:

- **Standart parollarni o‘zgartirishni va dasturiy ta’minotni yangilashni unutmang.** IoT qurilmalarining standart parollari kiberhujumlarning asosiy sabablaridan biridir. Masalan, Mirai botneti hujumining sodir bo‘lishiga aynan shu omil sabab bo‘lgan. IT-bo‘limlarning 47 foizi yangi qurilmalarni tarmoqga ulashdan oldin ishlab chiqaruvchi tomonidan belgilangan standart parollarni o‘zgartirmagan. Agar boshqaruv interfeysiga kirib, standart parollarni o‘zgartirishning imkoni yo‘qligini aniqlasangiz, bunday qurilmalarni tarmoqdan chiqarib tashlang yoki ularni umuman xarid qilmang. Shu bilan birga, dasturiy ta’minotni yangilash jarayoni avtomatik bo‘lishi yoki kamida IT-jamoasi tomonidan nazorat qilinishi kerak.

- **Qurilmalarni to‘g‘ridan-to‘g‘ri internetga ulamang.** Katta hajmdagi ma’lumotlarni qayta ishlaydigan va yuqori tarmoqli kenglik talab qiladigan IoT qurilmalari, masalan, kuzatuv kameralarini har doim xavfsizlik devori (firewall) bilan himoya qilish kerak. Bundan tashqari, BullGuard kabi trafikni skanerlash va ochiq portlarni aniqlash imkonini beruvchi uchinchi tomon vositalaridan foydalanish orqali IP-manzil ochiqligini tekshirishingiz mumkin.

- **Ishonchli IoT yetkazib beruvchilar bilan ishlash.** IoT qurilmalarning eng ko‘p uchraydigan zaifliklari, jumladan, autentifikatsiya va avtorizatsiya mexanizmlarining noto‘g‘ri ishlatilishi, transport darajasidagi shifrlashning yo‘qligi va dasturiy ta’minotni yangilashdagi muammolar IoT dasturiy ta’minotini ishlab chiqish jarayonida qabul qilingan noto‘g‘ri qarorlar natijasidir. Agar siz

uchinchi tomon yoki sozlanadigan IoT yechimini ish joyida joriy etishni rejalashtirayotgan bo‘lsangiz, IoT yechimlarini ishlab chiqishda o‘zini isbotlagan kompaniyalarga murojaat qiling.

• **Veb-ilovalarning xavfsizligini kuchaytiring.** IoT hujumlari tufayli yuzaga keladigan xavflar haqida eng yomon xabar shundaki, IoT yechimlaridan foydalanayotgan yoki foydalanmayotgan har qanday kompaniya yoki shaxs bu hujumlarga osongina duch kelishi mumkin. Veb-ilovalaringizni IoT botnetlardan himoya qilish uchun bir nechta usul mavjud:

- Veb-trafikingizni maskalash uchun VPN yechimlarini joriy qiling.
- Xavfsizlik zaifliklariga ega bo‘lmagan tayyor CMS plaginlari va ochiq kodli dasturiy komponentlardan foydalaning.
- Hech qachon sifatni ta’minlash bo‘yicha murosaga bormang.

Ushbu choralar IT-infrastrukturalarni IoT bilan bog‘liq kiberxavflardan himoya qilishda muhim ro‘l o‘ynaydi [10].

1. **Foydalanilmaydigan funksiyalarni o‘chiring.**
2. **Ish faoliyatini kuzatib boring.** Masalan, siz uyda bo‘lmagan paytda issiqlik regulyatori qanday ishlaganini tekshiring.
3. **Aqlli uy uchun maxsus ishlab chiqilgan antivirus dasturlaridan foydalaning.** Ushbu dasturlar qurilmalarni botnet hujumlaridan himoya qiladi.
4. **Ovozni boshqarish funksiyasidan foydalansangiz, faollashtirish uchun ishlatiladigan iboralarni vaqti-vaqti bilan o‘zgartiring.**
5. **UPnP (Universal Plug & Play) protokolini o‘chiring.** UPnP o‘xshash qurilmalarni aniqlab, ularga ulanadi. Biroq, bu protokoldagi zaifliklar zararli dastur tomonidan buzilishiga olib kelishi mumkin. Ya’ni, agar aqlli uy qurilmasi boshqa qurilmalar bilan ulanib tursa, ular ham zarar ko‘rishi mumkin.

Xulosa

Narsalar interneti (IoT) texnologiyasi kengayishi bilan kompyuter tarmoqlari tez sur’atlarda o‘sib bormoqda. IoT qurilmalari hayotning ko‘plab jihatlarida foyda keltirayotgan bo‘lsa-da, ular xavfsizlik zaifliklari shaklida xavf-xatarlarni ham keltirib chiqaradi va xakerlar uchun milliardlab yangi nishonlarni yaratadi. Shu sababli, IoT qurilmalarini himoya qilish faqat dasturiy ta’minot ishlab chiquvchilar tomonidan emas, balki avvalo foydalanuvchilar tomonidan ta’minlanishi lozim. Umumiy, ammo samarali qoidalarga rioya qilgan holda, foydalanuvchilar IoT bilan bog‘liq xavfsizlik xatarlarini sezilarli darajada kamaytirishlari va alohida qurilmalar hamda butun IT-infrastrukturaning xavfsizligini ta’minlashlari mumkin.

Foydalanilgan adabiyotlar:

1. Баженов А.С. Обзор DDoS атак на IoT устройства // Наука настоящего и будущего. 2019. Т. 1. С. 122-125.
2. Горев А.В. Интеллектуальный анализ DDoS-атак ботнета на IoT устройства при помощи Sap Analytics Cloud // Безопасность информационного пространства. Сборник трудов XIX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Екатеринбург, 2021. С. 10-14.
3. Оралбаев Е.А. Обнаружения DDoS-атак ботнетов в сетях доступа IoT // Актуальные вопросы современной науки и образования. Монография. Пенза, 2021. С. 190-200.
4. Савченко Е.В., Ниссенбаум О.В. Ботнет-атаки на устройства интернета вещей // Математическое и информационное моделирование. сборник научных трудов, электронный ресурс. Тюмень, 2018. С. 347-356.
5. Тавасиев Д.А., Команов П.А., Ревазов Х.Ю., Семиков В.С. Анализ методов выявления уязвимостей во встроенном программном обеспечении IoT устройств // Междуна родный научно-

исследовательский журнал. 2020. № 1-1 (91). С. 34-37.
6. Díaz J. Internet of Things and Distributed Denial of Service as Risk Factors in Information Security: [Электронный ресурс]. URL: https://www.intechopen.com/chapters/73910. (Дата обращения: 25.10.2021).
7. What is the Mirai botnet?: [Электронный ресурс] // Cloudaflare. URL: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/. (Дата обращения: 20.11.2021).
8. DDoS-атаки и как от них защищаться. Систематизация мирового и российского опыта: [Электронный ресурс] // Nag. URL: https://nag.ru/material/16862. (Дата обращения: 10.11.2021).
9. IoT Botnets and DDoS Attacks: Architecting Against Disaster: [Электронный ресурс] // IoT for all. URL: https://www.iotforall.com/iot-botnets-ddos-attack-architecture. (Дата обращения: 15.11.2021).
10. Взгляд внутрь инициированных IoT DDoS-атак и защита ИТ-инфраструктур: [Электронный ресурс] // SecurityLab. URL: https://www.securitylab.ru/blog/personal/bezmaly/ 344271.php. (Дата обращения: 11.11.2021).