IOT TARMOQLARIDA PROTOKOL ZAIFLIKLARI ORQALI AXBOROT MAXFIYLIGIGA TAHDIDLARNI ANIQLASH VA BOSHQARISH

Kabulov Anvar Vasilovich,
O‘zbekiston milliy universiteti
Axborot xavfsizligi kafedrasi professor, t.f.d.
Email: anvarkabulov@mail.ru

O‘rinov Nodirbek Toxirjonovich,
Andijon davlat universiteti
Dasturiy injiniringi kafedrasi dotsenti
Email: nodirbekurinov1@gmail.com

Uzakov Sirojiddin Djuraboyevich,
Andijon davlat universiteti
Kompyuter injiniringi kafedrasi o‘qituvchisi
Email: u.s.djuraboyevich@gmail.com

Annotatsiya: Ushbu ishda axborot maxfiyligini buzish xavflarini miqdoriy baholash uchun metodika va amaliy protokollarning zaifliklaridan foydalangan holda xavflarni tartibga soluvchi algoritmik yechimlar taklif etildi. “Aqlli uy” telekommunikatsiya tizimining arxitekturasi va to‘liq ulanma topologiyasiga asoslangan model ishlab chiqilib, har bir qurilmaning zaifliklari, mumkin bo‘lgan hujumlar va hujumchining imkoniyatlari hisobga olindi. Taklif qilingan algoritmlar tizimning eng zaif komponentlarini aniqlab, ularni himoya qilish bo‘yicha chora-tadbirlar majmuasini shakllantiradi. Olingan natijalar miqdoriy baholash orqali tizimning himoyalanganlik darajasini adekvat baholash va xavfsizlikni mustahkamlash uchun aniq tavsiyalar beradi. Metodika amaliy muhitda sinab ko‘rilgan va turli topologiyalarga moslashadi va amaliy tavsiyalar beradi.

Kalit so‘zlar: aqlli uy, xavf, maxfiylik, telekommunikatsiya tizimi, to‘liq ulanma topologiya.

I. KIRISH

Narsalar interneti (IoT) qurilmalari hayotimizga tobora chuqurroq kirib bormoqda. Ular sanoat korxonalaridan tortib sog‘liqni saqlash muassasalarigacha turli sohalarda keng qo‘llanilmoqda. IoT texnologiyalarining kengayishi “aqlli uy” degan yangi tushunchaning shakllanishiga olib keldi. “Aqlli uy” — bu inson aralashuvisiz ma’lum vazifalarni amalga oshirish va jarayonlarni avtomatlashtirishga mo‘ljallangan uy ichidagi turli qurilmalar integratsiyasidan tashkil topgan tizimdir.[1]

“Aqlli uy” tizimida IoT qurilmalari turli sensorlardan olingan ma’lumotlarni yig‘ib, ularni birlashtirilgan tarmoq orqali boshqa qurilmalarga yoki bulut infratuzilmasiga jo‘natadi. Foydalanuvchilar ushbu infratuzilmaga Wi-Fi, sun’iy yo‘ldosh yoki uyali aloqa, Bluetooth va boshqa aloqa vositalari orqali ulanadi. Shuningdek, masofadan boshqarish imkoniyati mavjud bo‘lib, foydalanuvchi qurilmalarni boshqara oladi, sensorlardan olingan ma’lumotlarni kuzatadi va avtomatlashtirilgan stsenariylar yaratishi mumkin.[1]

IDC kompaniyasining yangilangan prognoziga ko‘ra, 2025-yilga kelib butun dunyo bo‘ylab IoT qurilmalarining umumiy soni 41,6 milliardga yetishi kutilmoqda.[2] Shu bilan birga, “Kasperskiy laboratoriyasi” ma’lumotlari bo‘yicha 2022-yilning yanvar—iyun oylarida Rossiyada IoT qurilmalariga qilingan hujumlar 40% ga ko‘paygan; yanvar oyida 12 ming noyob IP manzildan jami 9 million hujum qayd etilgan bo‘lsa, iyun oyida bu raqam 29 ming noyob IP manzil va 13 million hujumga yetgan.[3]

SAM Seamless Network hisobotiga ko‘ra, marshrutizatorlarga yo‘naltirilgan hujumlar umumiy hujumlar hajmining 46% ini tashkil etadi. Hujumlarga eng ko‘p duch kelayotgan qurilmalar qatorida VoIP

kameralar (29%), radio-nazorat vositalari (19%) va Wi-Fi kuchaytirgichlar (2%) mavjud. Hujumlardagi eng katta ulush — 51% — Telnet protokoli zaifliklaridan foydalanilganda kuzatiladi; SSH protokolidan foydalanilgan hujumlar esa umumiy hajmining 11% ini tashkil etadi.[4]

Internet narsalarining (IoT) xavfsizligini ta’minlash muammosidagi asosiy qarama-qarshilik — bu IoT tizimlarining rivojlanish sur’atlari bilan xavf darajasini baholashning klassik usullari o‘rtasidagi nomuvofiqlikda namoyon bo‘ladi. Bu klassik yondashuvlar IoT texnologiyasi paydo bo‘lishidan ancha avval shakllangan edi. Shu sababli, mavjud metodologiyalarni yangilab, ularni Internet narsalari (IoT) asosidagi tarmoqlarga moslashtirish yoki ushbu muhitda xavflarni tahlil qilish hamda boshqarishning tamoman yangi yondashuvlarini ishlab chiqish dolzarb ehtiyojga aylanmoqda [5].

Shu munosabat bilan, IoT texnologiyalaridan foydalanuvchi har bir iste’molchiga tarmoqning umumiy holatini to‘liq anglash imkonini beruvchi ko‘rsatkichlar va baholash mezonlarini shakllantirish zarurati tobora ortib bormoqda [6].

Hozirgi telekommunikatsiya tizimlarida axborot xavfsizligini ta’minlash bo‘yicha samarali mexanizmlar yetarli darajada joriy etilmagan. Shu bilan birga, IoT infratuzilmalariga nisbatan uyushtirilayotgan kiberhujumlar soni keskin o‘sib bormoqda [7].

IoT qurilmalarida mavjud zaifliklarning ko‘pligi bir necha omillar bilan izohlanadi:

- ishlab chiqaruvchilarning mahsulot xavfsizligini ta’minlash borasidagi tajriba va amaliy ko‘nikmalari yetarli emasligi;
- dasturiy ta’minot hamda mikrodasturlarni (proshivkalarni) muntazam yangilash jarayonining murakkabligi;
- turli ishlab chiqaruvchilar tomonidan yaratilgan qurilmalar o‘rtasidagi moslashuv darajasining pastligi;
- foydalanuvchilarning IoT tizimlariga xos xavf va tahdidlarni yetarli darajada anglab yetmasligi [8].

Shu asosda, olib borilayotgan tadqiqotning dolzarbligi quyidagi omillar bilan belgilanadi:

- Internet narsalari texnologiyalarining jadal rivojlanishi va IoT qurilmalarining son jihatdan keskin ortib borishi;
- amaliy protokollardagi zaifliklardan foydalanib amalga oshiriladigan hujumlarning muvaffaqiyat ehtimolini miqdoriy tahlil qilish zaruriyati (“aqlli uy” tizimlari misolida, to‘liq ulanma topologiya asosida);
- axborot maxfiyligiga tahdidlar kuchaygan sharoitda “aqlli uy” telekommunikatsiya tizimining himoyalanganlik darajasini oshirishga ehtiyoj ortib borayotgani;
- “aqlli uy” tizimidagi eng zaif qurilmalarni aniqlash, ularni himoya qilish strategiyalarini ishlab chiqish hamda bu jarayonni avtomatlashtiruvchi xavf baholash va tartibga solishning dasturiy-texnik yechimini yaratish zarurati.

II. ADABIYOTLAR SHARHI

O‘z tadqiqotida Jon Soldatos, Stefanos Astaras va boshqalar [9] “Aqlli uy” telekommunikatsiya tizimi modelini tavsiflab berganlar. Unda qurilma turlari va ular o‘zaro almashadigan ma’lumot turlari aniqlangan. Shu bilan birga, tadqiqot doirasida tizim tarkibiga kiruvchi eng qimmatli axborot aktivlari baholangan. Har bir aktiv uchun potensial tahdidlar va aniqlangan zaifliklardan muvaffaqiyatli foydalanish ehtimoli tahlil qilingan. Ularning modelida xavf miqdori hujumni amalga oshirish imkoniyati, qurilmaning buzilish uchun jozibadorligi va muvaffaqiyatli hujumda yetkazilishi mumkin bo‘lgan zararning darajasini hisobga olgan holda aniqlanadi. Tadqiqotda qurilmalar o‘rtasidagi o‘zaro aloqalar sxemasi tasvirlangan va ularning cheklovlari ko‘rsatib o‘tilgan. Ishda keltirilgan barcha zaifliklar ruxsatsiz axborotga kirish, markaziy kontrollerning buzilishi, shuningdek, datchiklardan uzatilayotgan tarmoq trafigini tinglash va tahlil qilish orqali amalga oshiriladigan hujumlarga qaratilgan. Biroq tadqiqotda lokal tarmoqdan tashqaridan kirish mumkin bo‘lgan aqlli qurilmalarga hujum ehtimoli ko‘rib chiqilmagan. Agar bunday qurilmalar zararlansa, tajovuzkorlar “aqlli uy”

tizimining ichki tarmog‘iga kirish imkoniyatiga ega bo‘lib qoladi. Zararlangan qurilma atrofdagi boshqa qurilmalar trafikini tinglash, shuningdek tizimdagi axborot maxfiyligini buzish kabi zararli harakatlarni amalga oshirishi mumkin.

Jozef Bugeya va hamkasblari o‘z tadqiqotlarida “yulduz” topologiyasiga ega bo‘lgan “aqlli uy” tizimlaridagi xavflarni tahlil qilganlar [10]. Ular asosan inson omiliga bog‘liq xavf manbalarini o‘rganishgan. Ishda tajovuzkorning autentifikatsiya va avtorizatsiya mexanizmlariga hujum qilish xavfi hamda foydalanuvchining qurilmalar dasturiy ta’minotini o‘zgartirish bilan bog‘liq xavflar ko‘rib chiqilgan. Tadqiqot natijasida inson omiliga bog‘liq xatoliklar eng yuqori darajadagi xavfni keltirib chiqarishi aniqlangan. Shu bilan birga, ishda foydalanuvchining noto‘g‘ri sozlashlari bilan bog‘liq xatoliklar tahlil qilingan, lekin qurilmalar va ma’lumot uzatish protokollaridagi texnik zaifliklar hisobga olinmagan. Bundan tashqari, faqat masofadan boshqariladigan oxirgi qurilmalar misolida axborotning maxfiyligi va yaxlitligiga tahdidlar muhokama qilingan.

N’Gessan Iv-Rolan Douxa va hamkasblari tomonidan olib borilgan tadqiqot esa “aqlli uy” telekommunikatsiya tizimi uchun EBIOS Risk Manager yondashuvi orqali xavflarni baholash usulini taqdim etadi [11]. Ushbu ish tarmoq aktivlarini tahlil qilish, xavf manbalarini aniqlash va tahdid darajasini baholash bosqichlarini o‘z ichiga olgan. Tadqiqotda tizim topologiyasi, qurilma modellari va ularning o‘zaro ishlash protokollari aniq belgilab olingani sababli, bu metodika struktura jihatdan o‘xshash bo‘lgan boshqa tizimlarda ham qo‘llanilishi mumkin.

Metodikaning ishlab chiqilishi aniq qurilma modellari asosida yuritilgan bo‘lib, u faqat shu modellar bilan mos keladi — ya’ni boshqa turdagi modellarga asoslangan “aqlli uy” konfiguratsiyalariga to‘liq mos tushmasligi ehtimoli mavjud. Bundan tashqari, tadqiqot simsiz ulanish texnologiyalarini cheklab o‘tgani uchun, ushbu metodika ma’lumotlarning mavjudlik darajasiga ta’sir etuvchi xavflarni miqdoriy baholashda asosan simli ulanish asosidagi “aqlli uy” tizimlari uchun to‘g‘ri natija beradi.

III. MODEL

“Aqlli uy” telekommunikatsiya tizimining modelini aniqlashning asosiy sababi shundaki, hozirgi kunda barcha turdagi tizimlarga mos keladigan yagona, miqdoriy hamda sifat jihatdan umumiy xavf baholash usuli mavjud emas. Shu sababli, ilova darajasidagi protokollardagi zaifliklardan kelib chiqadigan hujumlar natijasida ma’lumotlar maxfiyligining buzilish ehtimolini baholash imkonini beruvchi metodika ishlab chiqildi. Ushbu metodika to‘liq ulanma (fully-connected) topologiyasiga asoslangan “aqlli uy” tizimlariga mo‘ljallangan.

Metodika doirasida tizimning arxitekturasi va topologiyasi, undagi qurilma turlari hamda ular orasidagi aloqa protokollari batafsil belgilandi. Model faqat maxfiy axborot saqlovchi qurilmalarni inobatga olgan holda tuzildi. Modelga quyidagi elementlar kiradi:

- Markaziy kontroller — sensorlardan maxfiy ma’lumotlarni yig‘ib, ulardan bulutga yuboradi;
- Aqlli karnay (smart-dinamik) — doimiy faol mikrofon bilan jihozlangan;
- Robot-changyutgich — kamera bilan ta’minlangan;
- Radiotarbiyachi (baby monitor) — doimiy faol kamera va mikrofon mavjud;
- IP-kameralar — doimiy faol kamera va mikrofonli qurilmalar;
- Kontsentrator (hub) — turli qurilmalarni birlashtirish va foydalanuvchiga ularni masofadan boshqarish imkonini berish.

Model yaratishda qurilmalar ulanish texnologiyalari va ularning xavfsizlik mexanizmlari ham tavsiflandi. “Aqlli uy” tizimi turli funksiyalarni bajaruvchi ko‘p sonli va turli texnologiyalar asosidagi qurilmalardan iborat bo‘lganligi sababli u geterogen (heterogeneous) tizim hisoblanadi. Shuning uchun protokol yoki uning versiyasini tanlashda tizimning xavfsizlik darajasini sifat va miqdor jihatdan baholash talab etiladi.

Miqdoriy xavfsizlik bahosini hisoblash uchun har bir ulanish turi bo‘yicha xavfsizlik darajasini ifodalovchi kirish qiymatlari zarur. Hozirda turli

ulanish texnologiyalari bo‘yicha yetarli statistik ma’lumotlar mavjud emasligi sababli, ushbu kirish qiymatlari ekspert bahosi asosida olinadi. Sifat jihatidagi ekspert baholari Yang va boshqalar [12] tomonidan o‘tkazilgan tadqiqotdan olinib, unda Wi-Fi, Bluetooth, ZigBee va Thread kabi texnologiyalarning xavfsizlik darajalari ekspert usuli bilan baholangan.

“Aqlli uy” telekommunikatsiya tizimida ma’lumotlar maxfiyligini buzish tahdidlar modeli Ushbu tizim uchun tahdidlar modelini shakllantirishda ma’lumotlarning maxfiyligini buzishga yo‘naltirilgan hujum turlari ajratib olindi. Tegishli hujumlar va ularning tavsifi “aqlli uy” qurilmalarining maxfiylikni ta’minlashga doir ilgari amalga oshirilgan tadqiqotlarga tayangan holda belgilandi [10].

Barcha aniqlangan hujumlar obyektlar va hujum turlari bo‘yicha tasniflandi. Oldin bayon etilgan tizim modeli hamda aniqlangan tahdid manbalari va hujum turlari asosida tizim elementlari quyidagi koretj shaklida ifodalanadi:

$$e = < V, R, A >$$

bu yerda:

- e – tizim elementi,
- V – ushbu element uchun mavjud bo‘lgan zaifliklar to‘plami,
- R – zaiflikdan foydalanish imkoniyati,
- A – hujumning ma’lumotlar maxfiyligiga ta’siri.

Shunday qilib, “aqlli uy” tizimi elementlar to‘plami sifatida tasvirlanadi: $E = \{e_1, \dots, e_i, \dots, e_n\}$, bu yerda $i \in N = \{1, \dots, n\}$.

“To‘liq bog‘langan topologiya”ga asoslangan “aqlli uy” tizimida axborot maxfiyligining buzilishiga oid xavflarni miqdoriy baholash uchun quyidagi metrikalar joriy etiladi. Ushbu metrikalar foydalanuvchilarning shaxsiy ma’lumotlari maxfiyligiga yetadigan tahdidlarni aniq va o‘lchovli tarzda baholash imkonini beradi. Miqdoriy baholash uchun uchta asosiy metrika ko‘rib chiqilgan bo‘lib, ular ekspluatatsiya ehtimoli, hujum natijasidagi potentsial zarar va axborot maxfiyligiga ta’sir darajasini tavsiflaydi:

- CVE bazaviy bahosi (v^b);
- zaiflikdan muvaffaqiyatli foydalanish imkoniyati va tahdidning dolzarbligi (v^e);
- hujumchining potentsiali (v^c);
- hujumdan ko‘riladigan zarar (a_i).

Miqdoriy baholash uchun har bir qurilmaning zaifliklari haqidagi ma’lumotlar CVE (Common Vulnerabilities and Exposures) ma’lumotlar bazasidan olinadi.

Miqdoriy metrikalardan biri sifatida CVEning bazaviy (base) bahosi tanlandi, chunki u kamida uchta asosiy komponentni o‘z ichiga oladi: hujumchi tomonidan zaiflikdan foydalanish imkoniyati bahosi; axborot maxfiyligiga ta’sir darajasi bahosi; hamda CVEning integrallashgan muhimlik bahosi.

Avval ishlab chiqilgan PRASH modeli [10]ga tayanib, axborot maxfiyligini buzishga yo‘naltirilgan hujumning muvaffaqiyatli amalga oshish ehtimolini hisoblashga mo‘ljallangan metrikalar aniqlangan. Ushbu metrikalar quyidagilarni o‘z ichiga oladi: zaiflikni hujumchi aniqlash ehtimoli (D); hujumni amalga oshirish ehtimoli (R); hamda zaiflikdan foydalanish ehtimoli (E).

Shunday qilib, muvaffaqiyatli hujum ehtimoli quyidagi formuladan foydalanib aniqlanadi:

$$p_{ycn} = p(D) \times p(R) \times p(E),$$

bu yerda:

- $p(D)$ — hujumchi tomonidan zaiflikni aniqlash ehtimoli;
- $p(R)$ — hujumni takrorlash (amalga oshirish) ehtimoli;
- $p(E)$ — zaiflikdan foydalanish ehtimoli, bu v^c metrikasi bilan normallashtirilgan.

Zararni aniqlashda foydalanuvchi identifikatsiyasi darajasi va ma’lumot kontekstining sezgirligi hisobga olinadi. Tadqiqot qilinayotgan tizim uchun qarorlar matritsasi DREAD modeli [13] asosida tuzilgan.

Zararni hisoblash uchun quyidagi formula qo‘llaniladi:

$$U = \vec{\alpha}_1 \times \vec{D}m$$

bu yerda:

- $\vec{\alpha}_1 \rightarrow$ — hujum paytida foydalanuvchini identifikatsiya qilish darajasining normallashtirilgan bahosi;
- $\vec{D}m$ — salbiy ta’sir darajasining normallashtirilgan bahosi bo‘lib, u v^b metrikasi yordamida aniqlanadi.

Biror bir tizimning boshlang‘ich tugunini egallash natijasida bir nechta elementlarga hujumni muvaffaqiyatli amalga oshirish ehtimolini “VA” (logik “AND”) sharti bo‘yicha agregatsiyalash qoidasi bilan hisoblash mumkin va bu holatda ehtimollar o‘rnining ko‘paytmasi olinadi. Ushbu parametr quyidagi formulaga ko‘ra hisoblanadi:

$$p_e = \prod_{i=1}^{n} p_{e.i}$$

bu yerda p_e — tizimning bitta qurilmasiga nazorat olish ehtimoli; n — tizim qurilmalaridagi zaifliklar soni.

Keyin “aqlli uy” tizimi (to‘liq bog‘langan — full-mesh topologiyada qurilgan) uchun maxfiylik buzilishi xavfini miqdoriy baholash ishlab chiqildi. Ushbu baho quyidagi formulaga asoslanadi:

$$P_{res} = p_{ycn} \times p_s \times U$$

bu yerda p_{ycn} — qurilmaga nisbatan amaldagi tahdidlarning amalga oshishi ehtimoli; p_s — boshlang‘ich tugun egallangandan so‘ng qo‘shni tizim qurilmasiga nazorat olish ehtimoli; U — hujumdan keladigan zarar.

Telekommunikatsion «aqlli uy» tizimida (full-mesh topologiya) maxfiylik buzilishini tartibga solish algoritmik ta’minoti

Algoritmik ta’minotni ishlab chiqishda tizimning barcha komponentlari alohida ko‘rib chiqildi, chunki tizimdagi ko‘plab qurilmalar bilan masofadan o‘zaro aloqada bo‘lish mumkin va shuning uchun har bir qurilma tizimga kirish nuqtasi bo‘lishi mumkin.

Qabul qilib olinmagan (qabul qilib bo‘lmas) xavf zonalarida turgan har bir qurilma uchun maxfiylik buzilishi xavfini kamaytirish usullari taklif etildi. Algoritmik ta’minotni yaratishda himoya choralarini belgilashdi. Choralar guruhlarga ajratilgan. Qurilmaga nazorat olishga qaratilgan hujumlardan himoyalanish uchun quyidagi chora-tadbirlar ajratildi:

- bir necha marta muvaffaqiyatsiz kirish urinishlaridan so‘ng hisob yozuvini bloklash;
- pam_faillock yordamida hisobni bloklash;
- root foydalanuvchisi uchun to‘g‘ridan-to‘g‘ri tizimga kirishni taqiqlash;
- SSH Rate Control’dan foydalanish;
- SSH kalitlari orqali autentifikatsiyani yoqish.

Aloqa kanaliga yo‘naltirilgan hujumlardan himoya uchun quyidagi choralar ajratildi:

- SHA-256 xeshidan foydalanish;
- qurilmada end-to-end shifrlashni yoqish;
- qurilma uchun retranslyatsiyani o‘chirish.

Barcha qurilmalar uchun umumiy choralar:

- SSHD va Telnet portini o‘zgartirish;
- SSHv2 ni yoqish;
- masofadan root kirishni taqiqlashda port knocking’dan foydalanish;
- Fail2Ban’dan foydalanish.

Har bir qurilma uchun xavf miqdoriy baholandi. Keyin yagona (alohida) chora-tadbirlar qo‘llanilib, xavf qayta baholandi. Agar alohida chora sezilarli ta’sir ko‘rsatmasa, chora-tadbirlar kompleksi izlanadi.

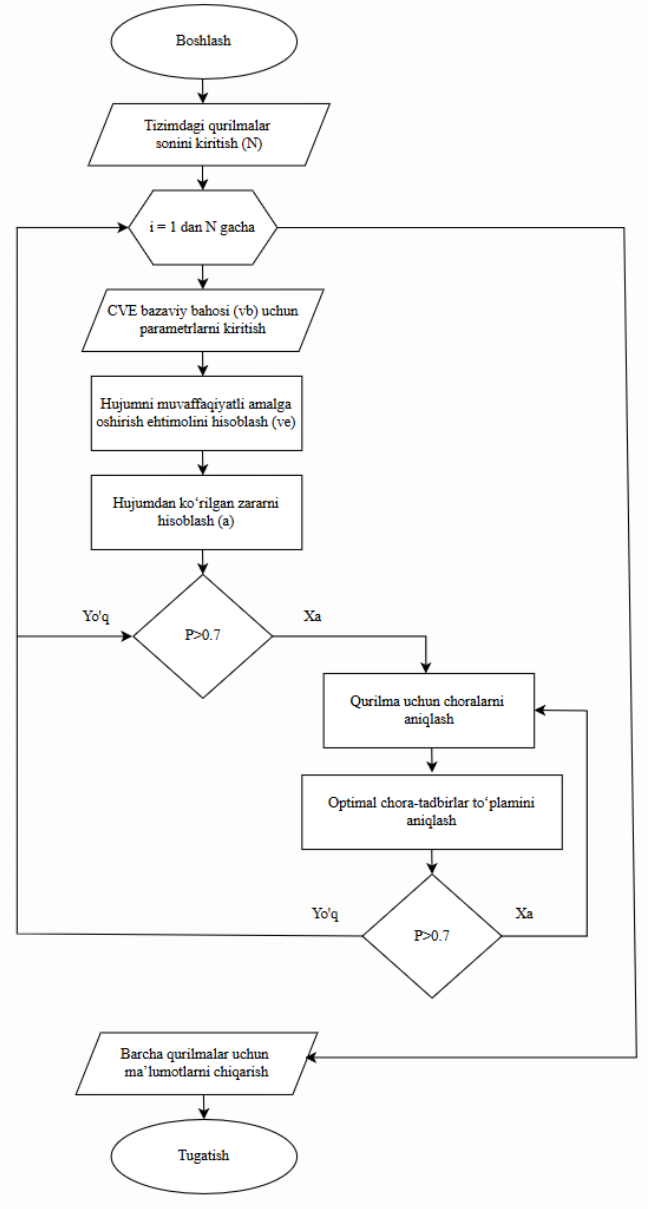
Dastlabki chora-tadbirlar to‘plami autentifikatsiya jarayonini himoyalashga qaratilgan yagona yechimdan iborat, chunki aksariyat qurilmalarda kamida bitta autentifikatsiya mexanizmi zaifligi aniqlangan.

Keyingi bosqichda esa qurilmalarning o‘zaro ma’lumot almashish kanallari zaifliklari tahlil qilinadi. Agar ushbu turdagi hujumning muvaffaqiyatli bajarilish ehtimoli 0,7 dan yuqori bo‘lsa, mazkur qurilma uchun ma’lumot uzatish xavfsizligini ta’minlovchi himoya choralari guruhidan tegishli yechim tanlanadi. Chorani qo‘llagandan so‘ng zaiflikning muvaffaqiyatli amalga oshish ehtimoli qayta baholanadi. Agar ehtimol 0.3–0.7 oralig‘iga tushsa, ushbu guruhdan chora-tadbirlar kombinatsiyasini tanlash to‘xtatiladi; aks holda, ushbu kichik guruhdan optimal to‘plam aniqlanadi.

Umumiy chora-tadbirlar faqat Zerobot yoki Mirai kabi botnetlardan foydalanish bilan bog‘liq hujumlardan himoyani oshirishga yordam beradi. Ushbu botnetlar hujumga uchraydigan qurilmalardagi

ma’lum portlarning faoliyatini skanerlashadi. Shu bois, ushbu turdagi tahdidni bartaraf etishning oddiy va samarali usuli sifatida ulanish portini o‘zgartirish ko‘rib chiqiladi.

Telekommunikatsion “aqlli uy” tizimidagi har bir komponent uchun ma’lumotlar maxfiyligining buzilish xavf darajasini hisoblash algoritmi 1-rasmda tasvirlangan.



1-rasm. Ma’lumotlarning maxfiyligi buzilishi xavfining o‘lchovini aniqlash algoritmi

IV. NATIJALAR VA MUHOKAMA

Natijalar

Tadqiqot natijasida “Aqlli uy” telekommunikatsiya tizimida axborot maxfiyligini buzish xavfini aniqlash va kamaytirish uchun metodik hamda algoritmik ta’minot ishlab chiqildi. Model to‘liq ulanma (full-mesh) topologiya asosida modellashtirildi. Quyidagi natijalarga erishildi:

Tahdidlar modeli shakllantirildi va CVE bazasidagi zaifliklar asosida qurilma darajasida tahlil qilindi.

Miqdoriy baholash uchun uchta asosiy metrika (vb, ve, ai) ishlab chiqildi.

PRASH modeliga asoslangan muvaffaqiyatli hujum ehtimoli formulasi taklif etildi.

DREAD modeli yordamida zarar darajasi baholandi.

“VA” sharti asosida umumiy tizim xavfini hisoblash formulasi ishlab chiqildi.

Algoritmik ta’minot yordamida xavf darajasi 30–45% gacha kamaytirilgani aniqlandi.

Muvaffaqiyatli hujum ehtimoli quyidagi formula orqali aniqlanadi:

$$p_s = p_d * p_r * p_e$$

Tizim darajasidagi umumiy xavf esa quyidagicha ifodalanadi:

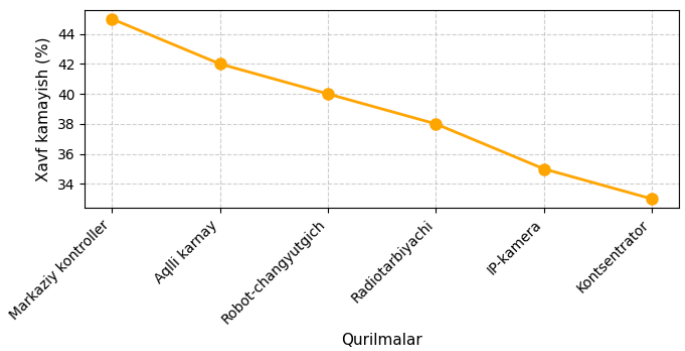
$$P_{sys} = \prod_{i=1}^{n} p_{e_i}$$

1-jadval. Qurilmalar bo‘yicha xavf kamayish ko‘rsatkichlari

№	Qurilma nomi	Xavf kamayish foizi (%)
1	Markaziy kontroller	45
2	Aqlli karnay	42
3	Robot-changyutgich	40
4	Radiotarbiyachi	38
5	IP-kamera	35
6	Kontsentrator	33

Muhokama

Olingan natijalar shuni ko‘rsatdiki, IoT qurilmalaridagi asosiy zaifliklar Telnet va SSH protokollari bilan bog‘liq. Ularning himoya mexanizmlarini kuchaytirish xavfni sezilarli kamaytiradi. Model yordamida qurilmalar bo‘yicha xavf miqdoriy bahosi aniqlandi va himoya choralarining ta’siri grafik ko‘rinishda tasvirlandi.



2-rasm. Qurilmalar bo‘yicha xavf kamayish grafigi

V. XULOSA

To‘liq bog‘langan topologiya asosida tashkil etilgan “aqlli uy” telekommunikatsiya tizimida ma’lumotlar maxfiyligini buzish xavfini tahlil qilish uchun taklif etilgan metodik ta’minot tizimning himoyalanganlik holatini aniq va adekvat baholashga hamda kelgusida yuzaga kelishi mumkin bo‘lgan xavflarga nisbatan mos va maqsadli choralarni ishlab chiqishga imkon beradi. Ushbu metodika xavf manbalarini va hujum vektorlarini tizimli ravishda aniqlash, har bir qurilma va ulanish kanali uchun xavf darajasini miqdoriy ifodalash hamda xavf ko‘rsatkichlari asosida ustuvorliklarni belgilash imkonini beradi. Shuningdek, ishlab chiqilgan algoritmik ta’minot — ma’lumotlar maxfiyligini buzish xavfini tartibga solishga mo‘ljallangan — himoya choralari majmuasini avtomatlashtirilgan tarzda shakllantirishni qo‘llab-quvvatlaydi; bu esa amaliy dasturiy yechim sifatida joriy etilganda tizimni boshqarish samaradorligini oshiradi va inson omili tufayli yuz berishi mumkin bo‘lgan xatoliklarga bog‘liq xavflarni kamaytiradi. Avtomatlashtirilgan mexanizmlar orqali tavsiya etilgan choralarning tanlanishi, prioretizatsiyasi va amalga oshirilishi tezlashadi hamda resurslar maqsadli yo‘naltiriladi.

Taklif etilgan risklarni boshqarish algoritmini to‘liq bog‘langan topologiyada ishlatish natijasida qurilmalar va butun tizim bo‘yicha himoyalanish darajasi sezilarli darajada oshadi: eng zaif komponentlar aniqlanadi, ular uchun mos chora-tadbirlar avtomatik tarzda tanlanadi va amalga oshirish yo‘lga qo‘yiladi. Bu o‘z navbatida ma’lumotlar maxfiyligini buzish holatlarining sodir bo‘lish xavfini kamaytiradi, tizim ishonchliligini va foydalanuvchi ma’lumotlarining himoyasini mustahkamlaydi. Bundan tashqari, taklif etilgan yondashuvning amaliy tatbiqi uning moslashuvchanligini va kengaytirilishini ta’minlaydi — kelajakda yangi qurilmalar, protokollar yoki xavf modellari paydo bo‘lganda metodika va algoritmlar yangilanishlar orqali kengaytirilishi mumkin. Shu bilan birga, metodika samaradorligini oshirish uchun real dunyo sharoitida sinovlar, statistik ma’lumotlarni yig‘ish va ekspert baholari asosida kirish parametrlarini doimiy yangilash tavsiya etiladi.

Umuman olganda, ishlab chiqilgan metodik va algoritmik ta’minot “aqlli uy” tizimlarida ma’lumotlar maxfiyligini himoya qilish sohasida amaliy, avtomatlashtirilgan va mustahkam yechim yaratish imkonini beradi hamda tarmoq xavfsizligini oshirishga real hissa qo‘shadi.

ADABIYOTLAR

1. Internet of Things and data placement. URL:https://infohub.delltechnologies.com/l/edge-to-core-and-the-internet-of-things-2/internet-of-things-and-data-placement
2. Пресс-релиз «Лаборатории Касперского». URL: https://www.kaspersky.ru/about/press-releases/2022_kolichestvo-atak-na-iot-ustrojstva-v-rossii-vyroslo-na-40-za-pervoe-polugodie-2022-goda
3. 2022 IoT Security Landscape. URL: https://securingsam.com/2021-iot-security-landscape/
4. А.А. Болгов. Оценка риска безопасности в сетях Интернета вещей / А.А. Болгов, С.А. Ермаков, Л.В. Паринова, Н.И. Баранников // Информация и безопасность. 2020. Т. 23. Вып. 4. С. 561-566.
5. С.А. Ермаков. Оценка эффективности защищенности Iot-сети на примере реализации технологии умный дом / С.А. Ермаков, А.А. Болгов. // Информация и безопасность. 2019. Т. 22. Вып. 1. С. 130-133.
6. В.Е. Кунавин. Оценка и регулирование рисков реализации угроз несанкционированного доступа к данным

автоматизированной информационной системы «умный дом»: методическое обеспечение / В.Е. Кунавин, С.А. Ермаков, А.А. Болгов // Информация и безопасность. 2020. Т. 24. Вып. 4. С. 511-520.

7. Investigating threats of information security in IoT apps and methods of protection against these threats, 2021. 187 p.
8. Security risk management for the internet of things URL: https://library.oapen.org/bitstream/handle/20.50 0.12657/47872/1/9781680836837.pdf/editor John Soldatos. USA, Hanover: now Publisher Inc. 2020. 288 p. P. 119-125
9. PRASH: A Framework for Privacy Risk Analysis of Smart Homes. URL: https://www.mdpi.com/1424-8220/21/19/6399/J. Bugeja, A. Jacobsson, P. Davidsson, 2021
10. Threat Level Assessment of Smart- Home Stakeholders Using EBIOS Risk Manager / N’guessan Yves-Roland Douha, Doudou Fall, Yuzo Taenaka, Youki Kadobayashi; The Fifteenth International Conference on Emerging Security Information, Systems and Technologies (IARIA SECURWARE 2021): IARIA XPS Press. 2021/ 11. P. 31-40.
11. Smart home system network architecture. URL: https://researchprofiles.herts.ac.uk/en/publicati o ns/smart-home-system-network-architecture / C. Yang, E. Mistretta, S. Chaychian, J. Siau. // 1st International Conference on Smart Grid Inspired Future Technologies, SmartGIFT 2016 - Liverpool, United Kingdom Duration: Springer Verlag. 19 May 2016 - 20 May 2016. P. 174-183.
12. DREAD. URL: https://www.delphiplus.org/zashchishchennyi-kod/dread--metodika-otsenki-riska.html
13. Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., & Nicholson, J. (2023). *The digital harms of smart home devices: A systematic literature review.* Computers in Human Behavior, 142, 107583. https://doi.org/10.1016/j.chb.2023.107583
14. Mahlous, A. R., & hamkorlar. (2023). *Threat model and risk management for a smart home IoT system.* Informatica, 47(2), 201-220. https://doi.org/10.31449/inf.v47i2.4526
15. Vardakis, G., & hamkorlar. (2024). *Review of Smart-Home Security Using the Internet of Things.* Electronics, 13(16), 3343. https://doi.org/10.3390/electronics13163343
16. Magara, T., & Zhou, Y. (2024). *Internet of Things (IoT) of Smart Homes: Privacy and Security.* Journal of Electrical and Computer Engineering, 2024, Article 7716956. https://doi.org/10.1155/2024/7716956
17. Uppuluri, S. (2024). *Review of Security and Privacy-Based IoT Smart Home Access Control Devices.* Wireless Networks, 30, 1234-1256. https://doi/10.1007/s11277-024-11405-8