

Date: 25th September-2026**AQLLI UY QURILMALARIDA KIBERXAVFSIZLIK MUAMMOLARI:
ARXITEKTURA, ZAIFLIKAR VA ULARNI BARTARAF ETISH YO‘LLARI****Habibjonova G.M.***Muxammad al-Xorazmiy nomidagi TATU, Kiberxavfsizlik va kriminalistika kafedrası
assistenti*

Annotatsiya. Ushbu ishda aqlli uy (Smart Home) qurilmalarining texnik arxitekturası va ular bilan bog‘liq kiberxavfsizlik muammolari kompleks tarzda tahlil qilinadi. Dastlab aqlli uy tizimining uch qatlamli modeli — qurilma qatlami, tarmoq/ma‘lumot uzatish qatlami va ilova qatlami — hamda ushbu ekotizimdagi to‘rt guruh ishtirokchi (foydalanuvchi, ishlab chiqaruvchi, tarmoq provayderi, ilova xizmati provayderi) ko‘rib chiqiladi. Aqlli termostat, aqlli qulf va aqlli bolalar monitori misolida funksionallik ortishi bilan xavfsizlik xavfining o‘shishi o‘rtasidagi bog‘liqlik ochib beriladi. Kiberxavfsizlikning nazariy asosi sifatida CIA (Confidentiality, Integrity, Availability) triadasi va "zaiflik → tahdid → insident → zarar" jarayoni tavsiflanadi. OWASP tashkilotining IoT qurilmalaridagi eng muhim kamchiliklar ro‘yxatiga tayanib, dasturiy/firmware zaifliklari, autentifikatsiya va avtorizatsiyaning yetarli emasligi hamda ma‘lumot uzatishda shifrlashning yo‘qligi statistik ma‘lumotlar (xususan, Hewlett Packard Enterprise, 2015) va real hodisalar (Mirai botneti, aqlli qulf va bolalar monitorlarining buzib kirilishi) misolida batafsil yoritiladi. Shuningdek, yetkazilgan zararni qoplash (kompensatsion) va uning oldini olish (preventiv) choralari nuqtai nazaridan huquqiy yondashuvlar tahlil qilinadi. Tadqiqot natijalariga ko‘ra, aqlli uy qurilmalarida kiberxavfsizlikning yetishmasligi texnik (resurs cheklovlari), iqtisodiy (bozor rag‘batining yo‘qligi) va inson omili (foydalanuvchi va ishlab chiqaruvchi bilimining yetarli emasligi) kabi uch darajali muammolar majmuidan kelib chiqadi va uni faqat kompleks — texnik, tashkiliy hamda huquqiy choralari uyg‘unligi orqaligina bartaraf etish mumkin.

Kalit so‘zlar: aqlli uy, IoT, kiberxavfsizlik, CIA triadasi, autentifikatsiya, shifrlash, OWASP, dasturiy zaifliklar, mahsulot javobgarligi, kiberxavfsizlik iqtisodiyoti.

So‘nggi yillarda aqlli uy (Smart Home) qurilmalari bozori jadal sur‘atlarda o‘shib bormoqda: 2017-yilda uning global qiymati 33,5 mlrd. AQSh dollarini tashkil etgan bo‘lsa, yillik 27,5 foizlik o‘shish sur‘ati bilan 2022-yilga borib 113 mlrd. dollarga yetishi kutilgan edi. Qiyoslash uchun, 2015-yilda bu ko‘rsatkich atigi 9,8 mlrd. dollarni tashkil etgan. Yevropa Komissiyasi 2016-yildayoq aqlli uyni IoT bozorining eng istiqbolli beshta yo‘nalishidan biri sifatida belgilagan edi. Samsung (SmartThings), Apple (HomeKit) va Amazon (Echo) kabi yirik texnologik kompaniyalar o‘zlarining to‘liq aqlli uy platformalarini taqdim etib, ushbu bozorda yetakchilikka intilmoqda.

Biroq bunday jadal o‘shish bilan bir qatorda foydalanuvchilarning xavfsizlik va shaxsiy hayotga aralashuv borasidagi tashvishlari ham kuchaymoqda. So‘rovlar shuni ko‘rsatadiki, foydalanuvchilarning qariyb 40 foizi aqlli uy qurilmalari o‘z shaxsiy hayotlari haqida haddan tashqari ko‘p ma‘lumot oshkor qilishidan xavotirda, yana shuncha qismi esa ularning harakatlari kuzatilishidan cho‘chidi. Bu tashvishlar behuda emas: aqlli uy qurilmalari inson



Date: 25th September-2026



turar joyi — huquqiy nuqtai nazardan eng himoyalangan makonlardan biriga — joylashtirilgan holda, doimiy ravishda shaxsiy ma'lumotlarni yig'adi, saqlaydi va uzatadi. Shu sababli, ushbu tezisning maqsadi aqlli uy qurilmalarining texnik ishlash tamoyillarini, ularda uchraydigan asosiy kiberxavfsizlik zaifliklarini hamda ushbu zaifliklarning oldini olish va ularning oqibatlarini bartaraf etishga qaratilgan choralarni ilmiy jihatdan tizimlashtirishdan iborat.

Aqlli uy tizimining texnik arxitekturası

Aqlli uy — bu "aholi turar joyini masofadan boshqarish, nazorat qilish va monitoring qilish imkonini beruvchi sensorlar, tizimlar va qurilmalar majmuasini o'z ichiga olgan turar joy" sifatida ta'riflanadi. U kengroq tushuncha — Buyumlar interneti (Internet of Things, IoT) ning bir bo'lagi hisoblanadi. Iqtisodiy Hamkorlik va Taraqqiyot Tashkiloti (OECD) IoT'ni "jismoniy dunyoni his qiladigan va u bilan aloqa qiladigan qurilmalardan yig'ilgan ma'lumotlar asosida ishlaydigan ilovalar va xizmatlar ekotizimi" sifatida ta'riflaydi. Har qanday aqlli qurilmaning ishlashi to'rtta bosqichdan iborat: (1) sensorlar atrof-muhitdan ma'lumot yig'adi; (2) ma'lumot internet orqali odatda bulutli serverga uzatiladi; (3) ma'lumot tahlil qilinib, qaror qabul qilinadi (inson yoki mashina tomonidan); (4) aktuatorlar ushbu qarorni jismoniy harakatga aylantiradi.

Ma'lumotlarning ushbu to'rt bosqich bo'ylab harakatini tushunish uchun IoT tizimini uch qatlamli model orqali ko'rib chiqish maqsadga muvofiqdir:

Qurilma qatlami (device layer) — ma'lumotni yig'uvchi va yuqori qatlamlardan buyruq qabul qiluvchi aqlli qurilmaning o'zi (sensorlar, protsessor, aktuatorlar);

Tarmoq va ma'lumot uzatish qatlami (network and data communications layer) — ma'lumotni uzatish, ulanish va bulutli saqlash kabi tarmoq xizmatlarini ta'minlaydi;

Ilova qatlami (application layer) — ma'lumotni tahlil qilib, foydalanuvchiga vizual taqdim etadigan yuqori darajadagi dasturiy ta'minot (mobil ilovalar va boshqaruv paneli).

Ushbu uch qatlamli arxitektura kamida tfrtta turdagi ishtirokchi qatnashadi: (a) yakuniy foydalanuvchi; (b) qurilma ishlab chiqaruvchisi (shu jumladan apparat va dasturiy ta'minot komponentlarining uchinchi tomon yetkazib beruvchilari); (v) tarmoq va aloqa xizmati provayderlari (internet-provayderlar, hosting xizmatlari); (g) ilova xizmati provayderlari, ular ko'pincha qurilma ishlab chiqaruvchisi bilan bir xil bo'lishi mumkin (vertikal integratsiya). Har bir ishtirokchining kiberxavfsizlik borasidagi mas'uliyati turlicha bo'lib, bu masalaning huquqiy tahlilini murakkablashtiradi. Ushbu tezisda, xususan, qurilma ishlab chiqaruvchisining mas'uliyatiga alohida e'tibor qaratiladi, chunki aksariyat xavfsizlik zaifliklari aynan qurilma qatlamida (dasturiy ta'minot va firmware darajasida) yuzaga keladi.

Funksionallik va xavfsizlik nisbati: uchta aqlli qurilma misolida

Aqlli qurilmalarning an'anaviy ("offlayn") hamkasblaridan farqi va ular keltirib chiqaradigan qo'shimcha xavfsizlik xavflarini tushunish uchun uchta keng tarqalgan aqlli uy qurilmasi — termostat, qulf va bolalar monitori — misolida qiyosiy tahlil o'tkaziladi.

Aqlli termostat

An'anaviy termostat foydalanuvchi tomonidan qo'lda yoki oldindan belgilangan jadval asosida boshqariladi. Aqlli termostat esa foydalanuvchi odatlarini "o'rganish" orqali harorat

Date: 25th September-2026

sozlamalarini avtomatik tarzda moslashtiradi va mobil ilova orqali masofadan boshqarishga imkon beradi. Zamonaviy aqlli termostatlar 10 tagacha harorat sensori, shuningdek namlik, harakat va yorug'lik sensorlariga ega bo'lishi mumkin. Ma'lumotlar bulutli serverga uzatilib, u yerda tahlil qilinadi va foydalanuvchi ilovasida vizual tarzda taqdim etiladi. Bu qurilmani nafaqat mahsulot, balki xizmat ko'rsatuvchi vosita sifatida ham ko'rish imkonini beradi. Internetga ulanish termostatni uchinchi shaxs tomonidan masofadan boshqarib olinishi xavfiga duchor qiladi, shuningdek foydalanuvchining uyda bor-yo'qligi haqidagi ma'lumot — shaxsiy hayotga tegishli nozik ma'lumot — to'planadi, bu esa an'anaviy termostatda mavjud bo'lmagan yangi xavfsizlik va maxfiylik muammosini keltirib chiqaradi.

Aqlli qulf

An'anaviy qulf ikkita jismoniy elementdan — qulf va kalitdan iborat bo'lib, uning ishonchliligi kalitni tiklash infratuzilmasiga (mahalliy chilangar xizmatlariga) bog'liq. Aqlli qulfdan esa jismoniy qulf smartfon yoki boshqa token yordamida boshqariladi, mobil ilova esa kirish huquqlarini boshqarish va "kalitni tiklash" vazifasini bajaradi. Aqlli qulflarni ishlash masofasiga ko'ra ikki turga bo'lish mumkin: qisqa masofali texnologiyalar (masalan, Bluetooth) asosidagi qulflar, ularda hujum qilish uchun tajovuzkor jismoniy yaqinlikda bo'lishi kerak, va internetga ulangan qulflar, ularda hujumni istalgan masofadan amalga oshirish mumkin. Ikkinchi holatda kirish huquqlarini boshqaruvchi infratuzilmaning zaifligi uchinchi shaxslarga o'ziga ruxsat berish va uyga kirish imkonini berishi mumkin, bundan tashqari, ichki dasturiy nosozliklar qulfni yopiq holatda "qotib qolishi"ga va hatto uy egasini o'z uyidan mahrum qilishga olib kelishi mumkin.

Aqlli bolalar monitori

An'anaviy bolalar monitorlari radio texnologiyasi asosida ishlaydi, aqlli bolalar monitorlari esa mahalliy Wi-Fi tarmog'i orqali internetga ulanadi. Ularda mikrofon va kamera bo'lib, audio-video oqim internet orqali smartfonga uzatiladi, kamerani masofadan boshqarish (aylantirish, kattalashtirish), dinamik orqali bolaga gapirish, shuningdek harorat, namlik va shovqin sensorlari kabi qo'shimcha funksiyalar mavjud bo'lishi mumkin. Ushbu qo'shimcha funktsionallik, agar kiberxavfsizlik yetarli darajada ta'minlanmasa, jiddiy xavf tug'diradi: video/audio oqim ruxsatsiz shaxslar tomonidan ushlab qolinishi yoki qurilmaning o'zi masofadan boshqarib olinishi mumkin. Termostat va qulfdan farqli o'laroq, bolalar monitori uyga doimiy o'rnatilmagan bo'lib, faqat Wi-Fi ulanishiga tayanadi, biroq undagi buzilish oqibatlarini hissiy jihatdan eng og'ir kechadigan holatlar qatoriga kiradi.

Uchala misoldan ko'rinib turibdiki, qurilmaga qo'shilgan har bir yangi "aqlli" funktsiya (masofadan boshqarish, ma'lumot yig'ish, bulutga ulanish) bir vaqtning o'zida foydalanuvchiga qulaylik va tajovuzkorga qo'shimcha imkoniyat yaratadi. Funktsionallik va xavfsizlik o'rtasidagi ushbu muros (trade-off) aqlli uy qurilmalarini loyihalashning markaziy muammosidir.

Kiberxavfsizlik tushunchasi va nazariy asosi

Kiberxavfsizlik atamasi keng va noaniq tushuncha bo'lib, uni ikki nuqtai nazardan ko'rib chiqish mumkin: "texnik kompyuter xavfsizligi" (individual foydalanuvchi va uning mulkini himoya qilishga qaratilgan) hamda "kiber-xavfsizlik" (jamiyat miqyosida, milliy

Date: 25th September-2026

xavfsizlik nuqtai nazaridan qaraladigan, masalan, Mirai botnetining kritik infratuzilmaga hujumlari kabi holatlar). Ushbu tezisda birinchi — texnik kompyuter xavfsizligi nuqtai nazari qo'llaniladi, chunki maqsad aynan iste'molchiga yetkaziladigan shaxsiy zarar bilan bog'liq muammolarni tahlil qilishdir.

Kiberxavfsizlikning umumiy qabul qilingan nazariy asosi — bu CIA triadasi bo'lib, u uchta asosiy xususiyatni birlashtiradi:

— *Confidentiality (maxfiylik)* — ma'lumot va tizim resurslarining ruxsatsiz shaxslar tomonidan oshkor qilinishidan himoyalanganligi;

— *Integrity (yaxlitlik)* — ma'lumot va tizimlarning ruxsatsiz o'zgartirish yoki buzishdan himoyalanganligi;

— *Availability (mavjudlik)* — tizim va ma'lumotlardan foydalanish huquqiga ega shaxslar uchun ularning har doim ishlab turishi.

Ushbu uchta xususiyatning har qandayidagi kamchilik "zaiflik" (vulnerability) deb ataladigan holatni keltirib chiqaradi. Zaiflik — tizimdagi kamchilik yoki xato bo'lib, ruxsatsiz shaxsga masofadan yoki mahalliy tarzda buyruq berish, ma'lumotni o'zgartirish yoki tizim ishini buzish imkonini beradi. Zaiflikdan foydalanish imkoniyati "tahdid" (threat) deb ataladi, tahdid amalga oshganda esa "xavfsizlik insidenti" yuzaga keladi, natijada foydalanuvchiga moddiy yoki nomoddiy zarar yetkazilishi mumkin. Muhim jihati shundaki, xavfsizlik insidenti nafaqat qasddan qilingan hujum (masalan, xakerlik), balki tizimdagi tasodifiy nuqson yoki e'tiborsizlik (masalan, yangilanish mexanizmining yo'qligi) natijasida ham yuzaga kelishi mumkin.

Asosiy kiberxavfsizlik zaifliklari

OWASP (Open Web Application Security Project) tashkiloti IoT qurilmalaridagi eng muhim xavfsizlik kamchiliklari ro'yxatini ishlab chiqqan. Ushbu ro'yxat barcha IoT qurilmalariga (jumladan, aqlli uy qurilmalariga) tegishli bo'lib, aksariyat holatlarda qurilma ishlab chiqaruvchisining javobgarligiga bog'liq. Ushbu tezisda shu ro'yxatga asoslanib, aqlli uy qurilmalarida eng ko'p uchraydigan uchta dasturiy zaiflik ko'rib chiqiladi. E'tiborli jihati shundaki, apparat (hardware) darajasidagi jismoniy xavfsizlik muammolari (masalan, USB portlar orqali hujum) tahlildan chetda qoldirildi, chunki aqlli uy qurilmalari, jamoat joylaridagi IoT qurilmalaridan farqli o'laroq, uy ichida joylashgani sababli jismoniy hujumlar uchun qiyinroq nishondir.

Dasturiy/firmware zaifliklari

100% xavfsiz dastur yaratib bo'lmazligi umumiy tan olingan haqiqatdir — har qanday dasturiy ta'minot da ma'lum yoki hali kashf etilmagan zaifliklar ("bug"lar) mavjud bo'lishi mumkin. Xavfsiz dasturiy ta'minot ga ega bo'lish qurilma ishlab chiqarilgan kundan boshlab uning butun hayotiy sikli davomida davom etadigan jarayondir: birinchidan, qurilma zavoddan chiqqan paytdayoq eng so'nggi dasturiy versiyaga ega bo'lishi kerak; ikkinchidan, xavfsiz yangilanish mexanizmi mavjud bo'lishi shart. Bunday mexanizm nafaqat yangilanish yuklab olinadigan aloqa kanalini, balki yangilanish faylining o'zini ham shifrlashni, shuningdek yangilanish serverining xavfsizligini va faylning avtorizatsiyadan o'tishini talab qiladi.



Date: 25th September-2026

Amaliyotda IoT qurilmalari ko‘pincha ushbu talablarning barchasiga javob bermaydi. Hewlett Packard Enterprise kompaniyasining 2015-yildagi tadqiqotiga ko‘ra, tekshirilgan IoT qurilmalarining 60 foizi yangilanishlarni yuklab olishda xavfsiz ulanishdan foydalanmagan yoki yangilanish fayllarini shifrlamagan. Bunday zaiflik ikki turdagi tahdidga olib kelishi mumkin: ichki tahdid (masalan, dasturiy xato natijasida qurilmaning o‘zi buzilishi, ya’ni aqlli termostatning batareyasi tugab, qurilma to‘liq o‘chib qolishi) va tashqi tahdid (uchinchi shaxs tomonidan zaiflikdan foydalanish, masalan, o‘g‘ri tomonidan aqlli qulfni buzib kirish). Umuman olganda, xavfsiz bo‘lmagan dasturiy ta’minot ma’lumotga ruxsatsiz kirish, qurilmani ruxsatsiz boshqarib olish yoki uni boshqa tizimlarga hujum qilish uchun ishlatish (masalan, DDoS hujumlarida) kabi oqibatlariga olib kelishi mumkin.

Autentifikatsiya va avtorizatsiyaning yetarli emasligi

Autentifikatsiya — foydalanuvchi yoki jarayon shaxsini tasdiqlash jarayoni bo‘lib, odatda foydalanuvchi nomi va parol orqali amalga oshiriladi. Avtorizatsiya esa tasdiqlangan shaxsga tizimdan foydalanish huquqini berish jarayonidir. Amaliyotda muhim va oson erishsa bo‘ladigan xavfsizlik yechimi — bu ishonchli parol boshqaruvi bo‘lib, unga kuchli parollarni talab qilish, standart holatda noyob login-parol o‘rnatish, orqa eshik (backdoor) akkauntlarining yo‘qligi, xavfsiz parolni tiklash mexanizmi va imkon qadar ikki bosqichli autentifikatsiya (2FA) kiradi.

IoT qurilmalari, jumladan aqlli uy qurilmalari, “1234” yoki “password” kabi zaif standart parollar bilan mashhur. HP kompaniyasining 2015-yilgi tadqiqotiga ko‘ra, tekshirilgan qurilmalarning (bulutli va mobil ilova komponentlari bilan birga) 80 foizi yetarli murakkablikdagi va uzunlikdagi parolni talab qilmagan. Bunga eng yorqin misol — Mirai botneti bo‘lib, u atigi 61 ta keng tarqalgan login-parol kombinatsiyasi (masalan, admin-admin yoki admin-1234) yordamida taxminan 400 000 ta IoT qurilmasini egallab, Twitter, Spotify va PayPal kabi yirik xizmatlarga qarshi taqsimlangan xizmat rad etish (DDoS) hujumlarini uyushtirgan edi. Boshqa hujjatlashtirilgan hodisalar orasida bolalar monitorlarining video-oqimi ochiq internetda paydo bo‘lishi yoki notanish shaxslarning dinamik orqali bolaga qichqirishi kabi holatlar mavjud. OWASPning ta’kidlashicha, autentifikatsiya va avtorizatsiyaning yetarli emasligi ma’lumotning yo‘qolishi yoki buzilishi, javobgarlikning yo‘qligi yoki qurilma va foydalanuvchi akkauntining to‘liq egallab olinishiga olib kelishi mumkin.

Ma’lumot uzatishda shifrlashning yo‘qligi

Shifrlash — ma’lumotni tushunarli (plaintext) shakldan tushunarsiz (ciphertext) shaklga aylantirish jarayoni bo‘lib, uni faqat ishonchli tomonlar o‘rtasida almashilgan shifrlash kaliti yordamida qayta ochish mumkin. IoT qurilmasi shifrlanmagan ma’lumotni uzatganda, u mahalliy tarmoq yoki internet orqali ochiq matn holida ushlab qolinishi mumkin, bu esa, ayniqsa, login va parol kabi nozik ma’lumotlar uchun jiddiy xavf tug‘diradi. OWASPga ko‘ra, IoT qurilmalarida mahalliy tarmoqqa ma’lumot uzatishda shifrlashning yo‘qligi keng tarqalgan muammo hisoblanadi. HP kompaniyasining 2015-yilgi tadqiqotida qurilmalarning 70 foizi mahalliy tarmoqqa yoki internetga uzatiladigan ma’lumotlarni shifrlamaganligi aniqlangan.

Date: 25th September-2026

Muammoni murakkablashtiruvchi omillardan biri shundaki, ko'pgina aqlli uy qurilmalari resurs jihatidan cheklangan bo'lib, cheklangan protsessor quvvati va xotiraga ega, bu esa ba'zi murakkab kriptografik yechimlarni qo'llashni imkonsiz qiladi. Shu sababli, resurslari cheklangan qurilmalar uchun yengil kriptografiya (Lightweight Cryptography, LWC) usullari alohida ahamiyat kasb etadi. Xususan, BITAG tashkiloti ishlab chiqaruvchilarni ma'lumot uzatishda TLS (Transport Layer Security) yoki LWCdan foydalanishga chaqiradi. Shifrlashning yo'qligi ma'lumotning "o'rtadagi odam" (man-in-the-middle) hujumi orqali ushlab qolinishiga va, agar login-parol kabi muhim ma'lumotlar oshkor bo'lsa, butun qurilma yoki akkauntning kompromentatsiyaga uchrashiga olib kelishi mumkin.

Kiberxavfsizlik yetishmasligining sabablari

Aqlli uy qurilmalarida asosiy kiberxavfsizlik amaliyotlariga ham rioya qilinmasligining sababi nima? Ushbu savolga to'liq javob berish ushbu tezisning maqsadi bo'lmasa-da, uchta asosiy sabab guruhini ajratib ko'rsatish mumkin. Birinchidan, ba'zi aqlli qurilmalar hajm, vazn, quvvat sarfi, xotira va narx o'rtasidagi murosalar asosida loyihalanadi, natijada ular cheklangan protsessor quvvati va xotiraga ega bo'lib, bu murakkab xavfsizlik yechimlarini (masalan, kuchli shifrlashni) qo'llashga to'sqinlik qiladi — masalan, ba'zi aqlli qulflar shifrlash mexanizmini qo'llash uchun yetarli hisoblash quvvatiga ega emas. Ikkinchidan, iste'molchi tomonida texnik bilim va kiberxavfsizlikka qiziqishning yetishmasligi muammosi mavjud: foydalanuvchilar ko'pincha xavfsizlik xavflaridan bexabar bo'ladi yoki bexabar bo'lmasa ham standart parolni almashtirish yoki dasturiy yangilanishni o'rnatish kabi oddiy vazifalarni bajarmaydi. Uchinchidan, ishlab chiqaruvchi tomonida ham texnik bilim va rag'batning yetishmasligi kuzatiladi: ko'plab an'anaviy mahsulot ishlab chiqaruvchilari mavjud mahsulotlariga dasturiy ta'minot va ulanish qo'shishda kiberxavfsizlikka yetarlicha e'tibor bermaydi, chunki ularning bu sohada tajribasi kam. Bundan tashqari, kiberxavfsizlik iqtisodiyoti nuqtai nazaridan, bozor odatda xavfsizlikdan ko'ra funksiyalar va past narxni ustuvor qo'yadi — bu axborot assimetriyasi, salbiy eksternalliklar va axloqiy xavf kabi bozor nomukammalliklarining namoyon bo'lishi bo'lib, natijada ishlab chiqaruvchilar xarajatlarni kamaytirish va mahsulotni tezroq bozorga chiqarish uchun rag'batlantiriladi, xavfsizlikka esa yetarlicha mablag' ajratmaydi.

1-jadval

Aqlli uy qurilmalaridagi asosiy kiberxavfsizlik zaifliklarining qiyosiy tahlili

T/r	Zaiflik turi	Asosiy sababi	Xavf/Oqibati	Texnik yechim
1	Dasturiy/firmware zaifligi	Xatoli yoki eskirgan dastur, xavfsiz yangilanish mexanizmining yo'qligi	Qurilmaning ishdan chiqishi, masofadan boshqarib olinishi, DDoS hujumlariga jalb qilinishi	Xavfsiz yetkazib berish, shifrlangan avtomatik yangilanish, secure boot
2	Autentifikatsiya/avtorizatsiya yetishmasligi	Zaif yoki standart parollar, backdoor akkauntlar	Qurilma yoki akkauntning to'liq egallab olinishi (mas., Mirai botneti)	Kuchli standart parollar, ikki bosqichli



Date: 25th September-2026

T/r	Zaiflik turi	Asosiy sababi	Xavf/Oqibati	Texnik yechim
				autentifikatsiya (2FA)
3	Ma'lumot uzatishda shifrlash yo'qligi	Resurs cheklovlari, shifrlashning e'tiborga olinmasligi	Ma'lumotning ushlab qolinishi (man-in-the-middle), login/parolning oshkor bo'lishi	TLS, yengil kriptografiya (LWC)

Real xavfsizlik insidentlari: qiyosiy tahlil

Yuqorida keltirilgan zaifliklarning amaliyotdagi ta'siri quyidagi uchta hodisada yaqqol namoyon bo'ladi. Ushbu holatlar tasodifiy emas — ular haqiqatda qayd etilgan xavfsizlik insidentlariga asoslangan bo'lib, har biri turli zaiflik turining alohida yoki bir nechtasining birgalikdagi ta'sirini ko'rsatadi.

2-jadval.

Aqlli uy qurilmalari bilan bog'liq real xavfsizlik insidentlari tahlili

Qurilma	Bog'liq zaiflik	Insident tavsifi	Yetkazilgan zarar
Aqlli termostat	Dasturiy/firmware zaifligi	Dasturiy xato natijasida batareya tugab, qurilma to'liq o'chib qoladi; ishlab chiqaruvchi yangilanishni kechiktiradi	Qishda uy sovib, egalari uzoq muddat uydan chiqib turgach, suv quvurlari muzlab yorilib, uyga suv zarari yetkazadi
Aqlli qulf	Shifrlash yo'qligi + autentifikatsiya zaifligi	Arzon qulf shifrlashsiz ishlab chiqarilgan; o'g'ri Shodan qidiruv tizimi orqali qurilmani topib, login ma'lumotlarini ushlab qoladi	Uy bo'sh vaqtda unga kirib, qimmatbaho buyumlar o'g'irlanadi; sug'urta kompaniyasi bostirib kirish isboti yo'qligi sababli zararni qoplamaydi
Aqlli bolalar monitori	Zaif standart parol	Video-oqim ochiq internetda mavjud bo'lib qoladi; notanish shaxs dinamik orqali bolaga qichqiradi	Ota-onada kuchli tashvish va stress, bolaning xavfsizligiga real tahdid

Ushbu uchta holat kiberxavfsizlik zaifliklarining nafaqat texnik, balki jiddiy moddiy (mulkiy zarar) va psixologik (tashvish, stress) oqibatlariga olib kelishi mumkinligini ko'rsatadi. Shu bilan birga, aqlli qulf misolida ko'rinib turibdiki, an'anaviy huquqiy vositalar (masalan, sug'urta) kiberxavfsizlik insidentlari natijasida yetkazilgan zararni to'liq qoplashga har doim ham qodir emas, chunki raqamli hujumning isbotlanishi jismoniy bostirib kirishga qaraganda ancha murakkabdir.

Zararni qoplash va oldini olish: huquqiy yondashuvlar

Date: 25th September-2026

Kiberxavfsizlik insidentlari natijasida yetkazilgan zararni bartaraf etishga qaratilgan huquqiy vositalarni ikki katta guruhga bo'lish mumkin: kompensatsion (compensatory) va preventiv (preventive) choralar.

—*Kompensatsion choralar* — insident natijasida yetkazilgan zararni qoplashga qaratilgan bo'lib, jismoniy shikastlanish, shaxsiy mulkka yetkazilgan zarar, boshqa mulkka yetkazilgan zarar va nomoddiy zarar (masalan, tashvish va stress) kabi turlarga ajratiladi;

—*Preventiv choralar* — xavfsizlik insidentining yuzaga kelishini yoki tahdidning ro'yobga chiqish xavfini kamaytirishga qaratilgan bo'lib, ishlab chiqaruvchini xavfsizlik yangilanishlarini taqdim etishga, qurilmani ta'mirlash yoki almashtirishga, sotuv vaqtida yoki xavfsizlik zaifligi aniqlangan paytda tegishli ma'lumot berishga majburlovchi sud buyrug'i (injunction) shaklida bo'lishi mumkin.

Yevropa Ittifoqining Mahsulot javobgarligi to'g'risidagi Direktivasi (Product Liability Directive) misolida ko'rsatilganidek, mavjud fuqarolik-huquqiy vositalar asosan jismoniy shikastlanish va shaxsiy mulkka yetkazilgan zararni qoplashga qaratilgan bo'lib, nomoddiy zarar (masalan, aqlli bolalar monitori misolidagi tashvish va stress) odatda ushbu vositalar doirasidan tashqarida qoladi. Bundan tashqari, xavfsizlik yangilanishini taqdim etish yoki qurilmani ta'mirlash kabi preventiv choralar ko'proq shartnoma huquqi doirasiga kirsa-da, amaliyotda ularni tovar javobgarligi tizimi orqali ham qo'llash imkoniyati muhokama qilinmoqda. Bu shuni ko'rsatadiki, faqat texnik yechimlarga tayanish yetarli emas — kiberxavfsizlik muammosini samarali hal etish uchun texnik, tashkiliy va huquqiy choralarning uyg'unlashtirilgan yondashuvi zarur.

Xulosa

Ushbu tezisdagi aqlli uy qurilmalarining texnik arxitekturasini (uch qatlamli IoT modeli), funktsionallik va xavfsizlik o'rtasidagi murosa (termostat, qulf va bolalar monitori misolida), kiberxavfsizlikning nazariy asosi (CIA triadasi va "zaiflik → tahdid → insident" jarayoni), uchta asosiy dasturiy zaiflik (dasturiy/firmware kamchiliklari, autentifikatsiya yetishmasligi, shifrlash yo'qligi) hamda ularning real hodisalardagi namoyon bo'lishi kompleks tarzda tahlil qilindi.

Tadqiqot natijalari shuni ko'rsatadiki, aqlli uy qurilmalarida kiberxavfsizlikning yetishmasligi uch darajali muammolar majmuidan kelib chiqadi: texnik daraja (qurilmalarning cheklangan apparat resurslari), inson omili darajasi (iste'molchi va qisman ishlab chiqaruvchining texnik bilimi yetarli emasligi) va iqtisodiy daraja (bozorning xavfsizlikdan ko'ra past narx va tezkor ishlab chiqarishni ustuvor qo'yishi). Shu sababli, muammoni faqat bitta yo'nalish — masalan, sof texnik yechimlar — orqali hal etib bo'lmaydi.

Kelajakda aqlli uy tizimlarining xavfsizligini oshirish uchun quyidagi kompleks yondashuv tavsiya etiladi: (1) texnik jihatdan — "loyihalash bosqichidayoq xavfsizlik" (security by design) tamoyiliga rioya qilish, kuchli standart parollar va ikki bosqichli autentifikatsiyani joriy etish, avtomatik va shifrlangan dasturiy yangilanish mexanizmlarini ta'minlash hamda resurslari cheklangan qurilmalar uchun yengil kriptografiya usullaridan foydalanish; (2) tashkiliy jihatdan — ishlab chiqaruvchilarni xavfsizlik standartlariga rioya qilishga undovchi sertifikatlash va monitoring tizimlarini joriy etish; (3) huquqiy jihatdan



Date: 25th September-2026

— mahsulot javobgarligi tizimini zamonaviy dasturiy va kiberxavfsizlik xavflarini hisobga oladigan tarzda takomillashtirish, shu jumladan nomoddiy zararni qoplash va preventiv choralarni (masalan, majburiy xavfsizlik yangilanishlari) kengaytirish. Faqat ushbu uch yoʻnalishning uygʻun qoʻllanilishi aqlli uy tizimlarining ishonchliligi, xavfsizligi va isteʼmolchilar ishonchini taʼminlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR:

1. Van den Heuvel K. Securing the Smart Home: A study on cybersecurity problems in smart home devices and European product liability law: Information Law Research Master Thesis. – Amsterdam: University of Amsterdam, 2018. – 129 b.
2. Bugeja J. va boshq. On Privacy and Security in Smart Connected Homes // 2016 European Intelligence and Security Informatics Conference (EISIC), Uppsala. – 2016. – B. 1–14.
3. OECD Working Party on Communication Infrastructures and Services Policy. The Internet of Things: Seizing the Benefits and Addressing the Challenges. – Paris: OECD Publishing, 2015. – B. 9.
4. Poudel S. Internet of Things: Underlying Technologies, Interoperability and Threats to Privacy and Security // Berkeley Technology Law Journal. – 2016. – T. 31. – B. 997–1022.
5. Nissenbaum H. Where Computer Security Meets National Security // Ethics and Information Technology. – 2005. – T. 7. – B. 61–73.
6. Arnbak A. Securing Private Communications: doktorlik dissertatsiyasi. – Amsterdam: University of Amsterdam, 2015. – B. 155–171.
7. Samaila M.G. va boshq. Security Challenges of the Internet of Things // Beyond the Internet of Things: Everything Interconnected. – Cham: Springer International Publishing AG, 2017. – B. 54–71.
8. OWASP. Top IoT Vulnerabilities [Elektron resurs]. – URL: <https://www.owasp.org> (murojaat sanasi: ...).
9. Hewlett Packard Enterprise. Internet of Things Research Study: texnik hisobot. – Palo Alto: HPE, 2015. – B. 5.
10. BITAG. Internet of Things (IoT) Security and Privacy Recommendations: texnik hisobot. – Denver: Broadband Internet Technical Advisory Group, 2016. – B. 1–20.
11. ENISA. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures: texnik hisobot. – Heraklion: European Union Agency for Network and Information Security, 2017. – B. 18–32.
12. Ragan S. Here are the 61 passwords that powered the Mirai IoT botnet // CSO Online. – 2016.
13. Symantec. Internet Security Threat Report. – Mountain View: Symantec Corporation, 2017. – B. 66.
14. Dean B.C. An Exploration of Strict Products Liability and the Internet of Things: texnik hisobot. – Washington, D.C.: Center for Democracy & Technology, 2018. – B. 1–9.



Date: 25th September-2026

15. Yevropa Ittifoqi. 85/374/EEC-son Kengash Direktivasi — nuqsonli mahsulotlar uchun javobgarlikka oid a'zo davlatlarning qonun, qoida va ma'muriy qoidalarini yaqinlashtirish to'g'risida (Mahsulot uchun javobgarlik direktivasi). – 1985.

