IOTDA XAVFSIZLIK TIZIMLARI

Umarov Bekzod Azizovich
Farg‘ona davlat unversiteti o‘qituvchi
ubaumarov@mail.ru
Otaqo’ziyeva Muqaddam Shukurjon qizi
Farg’ona davlat unversiteti 3-kurs talalabasi
muqaddamotaqo’ziyeva@gmail.com

Annotatsiya. *Ushbu maqola xavfsizlik tizimlarining paydo bo’lishidan tortib bugungi kunda ularni qayta shakllantiruvchi ilg’or innovatsiyalargacha o’rganadi.*

IoT (Internet of Things) texnologiyalarining keng joriy etilishi bilan xavfsizlik masalalari jiddiy muammoga aylanmoqda. IoT qurilmalari turli sohalarda – uy-joy, sog‘liqni saqlash, transport, sanoat va boshqa ko‘plab sohalarda qo‘llanilmoqda. Bu qurilmalarning tarmoqqa ulanganligi va ma'lumotlarni almashishi ularni turli xil kiberhujumlarga nisbatan himoyasiz qiladi. IoT xavfsizligi bo‘yicha asosiy muammolar orasida autentifikatsiya va shifrlashning yetishmasligi, xavfsizlik standartlari va protokollarining yo‘qligi, va foydalanuvchilarning xabardorlik darajasi pastligi kiradi.

Kalit so’zlar. *IoT xavfsizligi, Autentifikatsiya, Shifrlash, Kiberhujumlar, Tarmoq himoyasi, Ma’lumotlar himoyasi, Xavfsizlik standartlari, Qurilma xavfsizligi, IoT protokollari, Kirish nazorati, Foydalanuvchi sozlamalari, Zaiflikni bartaraf etish, Xavfsizlik monitoringi.*

Annotation: *This article explores security systems from their origins to the breakthrough innovations that are reshaping them today.*

ISSN 3060-4567

With the widespread adoption of IoT (Internet of Things) technologies, security issues are becoming a serious problem. IoT devices are being used in a variety of industries - housing, healthcare, transportation, industry, and many more. The fact that these devices are networked and share data makes them vulnerable to various cyber attacks. Major IoT security challenges include lack of authentication and encryption, lack of security standards and protocols, and low user awareness. Research and development on this topic is focused on developing critical measures to protect IoT systems.

Keywords: *IoT security, Authentication, Encryption, Cyber attacks, Network protection, Data protection, Safety standards, device security, IoT protocls, Access control, User settings, Security monitoring.*

Аннотация: *В этой статье исследуются системы безопасности от их истоков до прорывных инноваций, которые меняют их сегодня.*

С широким распространением технологий IoT (Интернета вещей) вопросы безопасности становятся серьезной проблемой. Устройства Интернета вещей используются в различных отраслях: жилищном строительстве, здравоохранении, транспорте, промышленности и многих других. Тот факт, что эти устройства подключены к сети и обмениваются данными, делает их уязвимыми для различных кибератак. Основные проблемы безопасности Интернета вещей включают отсутствие аутентификации и шифрования, отсутствие стандартов и протоколов безопасности, а также низкую осведомленность пользователей. Исследования и разработки по этой теме сосредоточены на разработке критически важных мер по защите систем Интернета вещей.

Ключевые слова: *Безопасность Интернета вещей, Аутентификация, Шифрование, Кибератаки, Защита сети, Защита*

данных, Стандарты безопасности, Безопасность устройства, Протоколы Интернета вещей, Контроль доступа, Пользовательские настройки, Мониторинг безопасности.

IoT xavfsizligi (narsalar interneti xavfsizligi) - bu IoT-da ulangan qurilmalar va tarmoqlarni himoya qilishga qaratilgan texnologiya segmenti. IoT o'zaro bog'liq bo'lgan hisoblash qurilmalari, mexanik va raqamli mashinalar, ob'ektlar, hayvonlar va odamlar tizimiga internet ulanishini qo'shishni o'z ichiga oladi. Har bir narsaning o'ziga xos identifikatori va ma'lumotlarni tarmoq orqali avtomatik ravishda uzatish qobiliyati mavjud. Biroq, qurilmalarning internetga ulanishini yoqish, agar ular to'g'ri himoyalanmagan bo'lsa, ularni jiddiy zaifliklarga olib keladi.

IoT xavfsizligi IoT qurilmalari va ular ulanadigan zaif tarmoqlarni kiberhujumlardan himoya qilish uchun kiberxavfsizlik strategiyasiga asoslangan. IoT qurilmalarida o'rnatilgan xavfsizlik yo'q. IoT xavfsizligi ma’lumotlar buzilishining oldini olish uchun zarur, chunki IoT qurilmalari ma’lumotlarni internet orqali shifrlanmagan holda uzatadi va standart kiberxavfsizlik tizimlari tomonidan aniqlanmasdan ishlaydi. IoT xavfsizligi ma'nosi bilan bir qatorda, IoT xavfsizligi masalalarini hal qilishda korxonalar duch keladigan ko'plab muammolarni tushunish muhimdir. IoT qurilmalari xavfsizlikni hisobga olgan holda ishlab chiqilmagan. IoT qurilmalari va aloqa kanallarining doimiy tarqalishi va xilma-xilligi tashkilotingiz uchun kiber tahdidlarga duchor bo'lish potentsialini oshiradi. Afsuski, ko'pgina IoT qurilmalarida xavfsizlik dasturlarini o'rnatishning hech qanday usuli yo'q. IoT qurilmalari hatto ulanganda tarmoqqa zarar etkazadigan zararli dasturlarni ham yuborishi mumkin. Shu sababli tarmoq xavfsizligi IoT xavfsizligi uchun ustuvor ahamiyatga ega. IoT atamasi juda keng va bu texnologiya rivojlanishda davom etar ekan, atama yanada kengroq bo'ladi. Soatlardan termostatlargacha, video o'yin pristavkalarigacha deyarli har bir

texnologik qurilma ma'lum quvvatda internet yoki boshqa qurilmalar bilan o'zaro aloqada bo'lishi mumkin.

IoT xavfsizligi ayniqsa qiyin bo'lishi mumkin, chunki ko'pgina IoT qurilmalari kuchli xavfsizlik bilan ishlab chiqilmagan - odatda ishlab chiqaruvchilar qurilmalar tezda bozorga chiqishi uchun xavfsizlik emas, balki xususiyatlar va qulaylikka e'tibor qaratadi.

IoT qurilmalari tobora kundalik hayotning bir qismi bo'lib bormoqda va iste'molchilar ham, biznes ham IoT xavfsizligi muammolariga duch kelishi mumkin.

IoT xavfsizligi muammolari qurilmalarning bir-biriga ulanish usullari qanchalik ko'p bo'lsa, tahdid qiluvchilar uchun ularni ushlab qolish imkoniyati shunchalik ko'p bo'ladi. Gipermatnni uzatish protokoli va API-lar IoT qurilmalari xakerlar ushlashi mumkin bo'lgan ikkita kanaldir. IoT soyaboniga internetga asoslangan qurilmalar ham kirmaydi. Bluetooth texnologiyasidan foydalanadigan qurilmalar ham IoT qurilmalari hisoblanadi va shuning uchun IoT xavfsizligini talab qiladi.

IoT xavfsizligining quyidagi muammolari jismoniy shaxslar va tashkilotlarning moliyaviy xavfsizligiga tahdid solmoqda:

Masofaviy ta'sir qilish. Boshqa texnologiyalardan farqli o'laroq, IoT qurilmalari internetga ulanishi tufayli ayniqsa katta hujum maydoniga ega. Ushbu qulaylik juda qimmatli bo'lsa-da, u xakerlarga qurilmalar bilan masofadan turib muloqot qilish imkoniyatini ham beradi. Shuning uchun fishing kabi xakerlik kampaniyalari ayniqsa samarali. IoT xavfsizligi, shu jumladan bulut xavfsizligi, aktivlarni himoya qilish uchun ko'p sonli kirish nuqtalarini hisobga olishi kerak.

Sanoatni oldindan bilishning etishmasligi. Tashkilotlar raqamli transformatsiyalarni davom ettirar ekan, ayrim tarmoqlar va ularning mahsulotlari ham mavjud. Avtomobilsozlik va sog'liqni saqlash sanoati yanada samaraliroq va

tejamkor bo'lish uchun IoT qurilmalarini tanlashni kengaytirdi. Biroq, ushbu raqamli inqilob, shuningdek, har qachongidan ham ko'proq texnologik qaramlikka olib keldi. IoT xavfsizligi ayniqsa qiyin bo'lishi mumkin, chunki ko'pgina IoT qurilmalari kuchli xavfsizlik bilan ishlab chiqilmagan - odatda ishlab chiqaruvchilar qurilmalar tezda bozorga chiqishi uchun xavfsizlik emas, balki xususiyatlar va qulaylikka e'tibor qaratadi. IoT qurilmalari tobora kundalik hayotning bir qismi bo'lib bormoqda va iste'molchilar ham, biznes ham IoT xavfsizligi muammolariga duch kelishi mumkin. IoT va xavfsizlik talablarini faqat butun tarmoq infratuzilmasi bo'ylab ko'rish, segmentatsiya va himoyani ta'minlaydigan integratsiyalashgan yechim bilan bajarish mumkin, masalan, xavfsizlikning yaxlit yondashuvi. Sizning IoT xavfsizligingiz quyidagi asosiy qobiliyatlarni o'z ichiga olishi kerak:

Qurilmalaringiz foydalanadigan protokollarni tushunish xavfsizlik xavflarini kamaytirishga yordam beradi.

Shifrlash ma'lumotlarni himoya qilishning samarali usulidir, ammo kriptografik kalitlar ma'lumotlarning himoyalanganligini, lekin kerak bo'lganda foydalanish mumkin bo'lishini ta'minlash uchun ehtiyotkorlik bilan boshqarilishi kerak. IoT qurilmalari ko'pincha o'zlariga mo'ljallanmagan bo'lsa-da, o'rnatilgan xavfsizliksiz, ular ma'lumotlarning buzilishiga olib kelishi mumkin bo'lgan zararli dasturlarni tarqatish uchun jozibali kanal bo'lib xizmat qiladi.

Bulutli xavfsizlik - bu biznes xavfsizligiga tashqi va ichki tahdidlarni bartaraf etish uchun mo'ljallangan protseduralar va texnologiyalar to'plami. Tashkilotlar o'zlarining raqamli transformatsiya strategiyasiga o'tayotganda va bulutga asoslangan vositalar va xizmatlarni o'z infratuzilmasining bir qismi sifatida birlashtirganda bulut xavfsizligiga muhtoj.

Raqamli transformatsiya va bulutli migratsiya atamalari so'nggi yillarda korxona sozlamalarida muntazam ravishda qo'llanilmoqda. Ikkala ibora ham turli

tashkilotlar uchun har xil narsalarni anglatishi mumkin bo'lsa-da, ularning har biri umumiy maxrajga asoslangan: o'zgarish zarurati.

Bulutli hisoblash “Bulutli” yoki aniqrog'i, “bulutli hisoblash" Internet orqali va mahalliy apparat cheklovlari doirasidan tashqarida resurslar, dasturiy ta'minot va ma'lumotlar bazalariga kirish jarayonini anglatadi. Ushbu texnologiya tashkilotlarga infratuzilma boshqaruvining bir qismini yoki ko'p qismini uchinchi tomon hosting provayderlariga yuklash orqali o'z operatsiyalarini kengaytirishda moslashuvchanlikni beradi.Eng keng tarqalgan va keng tarqalgan bulutli hisoblash xizmatlari quyidagilardir:

IaaS (Xizmat sifatidagi infratuzilma): Gibrid yondashuvni taklif qiladi, bu tashkilotlarga o'zlarining ba'zi ma'lumotlari va ilovalarini joyida boshqarish imkonini beradi. Shu bilan birga, u serverlar, apparat, tarmoq, virtualizatsiya va saqlash ehtiyojlarini boshqarish uchun bulutli provayderlarga tayanadi.

NATIJA:

Ushbu maqolada IOTda xavfsizlik tizimlarini, IOT qurilmalari orasida uy jihozlari, sanoat avtomatlashgan tizimlari, sog’liqni saqlash texnologiyalari va transport vositalari kabi turli sohalar uchun keng ko’lamli ekanligini ko’rdik.

IoT (Internet of Things) xavfsizligi sohasida natijalar qismi odatda ushbu texnologiyalarning xavfsizlik darajasini yaxshilash va himoya choralarini kuchaytirish bo'yicha muhim xulosalarni o'z ichiga oladi. Quyida IoT xavfsizligidagi natija qismining umumiy ko'rinishi keltirilgan. Kuchli autentifikatsiya va shifrlash zarurati. IoT qurilmalarining himoyasini kuchaytirish uchun autentifikatsiya va shifrlash usullarini qo'llash muhimdir. Bu ma'lumotlar uzatilishi va saqlanishi paytida ularga ruxsatsiz kirishlarning oldini olishga yordam beradi. Yaxshi xavfsizlik standartlari va me'yorlari: IoT tizimlari uchun belgilangan xavfsizlik standartlari va me'yorlarni rivojlantirish va ularga rioya qilish zarur. Bu qurilmalarni ishlab chiqaruvchilar va foydalanuvchilar uchun

qo'llanma sifatida xizmat qiladi. Yangilanishlar va zaifliklarni yamoqlash: IoT qurilmalarida xavfsizlik zaifliklarini bartaraf etish uchun doimiy yangilanishlar va xavfsizlik yamoqlarini ta'minlash kerak. Bu qurilmalar yangicha tahdidlarga qarshi himoyalanishiga yordam beradi.

XULOSA.

IOT(Internet of Things) xavfsizlik mavzusida juda va keng qamrovli. IoT qurilmalari hayotimizning turli sohalarida keng qo'llanilmoqda. Uydagi aqlli moslamalardan tortib, sanoat tizimlari va transport vositalarigacha. Biroq ushbu qurilmalar sonining o'sishi bilan birga xavfsizlik xatarlarining ko'payishi ham kutilmoqda.IoT xavfsizligi zamonaviy texnologiyalar rivojlanayotgan sayin dolzarblashib bormoqda. IoT tizimlarini himoya qilish uchun xavfsizlik strategiyalari, shifrlash, kirish nazorati va monitoring kabi usullarni qo'llash zarur. Xavfsizlik choralarining to'g'ri bajarilishi IoT qurilmalari va foydalanuvchi ma'lumotlarini himoya qilishda katta ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR.

1. Qosimov S.S ―Axborot texnologiyalari‖ texnik oliy o'quv yurtlari uchun uslubiy qo'lanma. Toshkent.: ―Aloqachi‖ 2006

2. Signalling in Telecommunication networks., 2007 Publishing by John Wiley&Sons Inc., Hoboken New Jersey, USA.

3. D.A. Davronbekov, U. T. Aliyev, X. X. Madaminov, J. D. Isroilov (2021) "Simsiz tarmoqlar".

4. TCP/IP protocol suite, Behrouz A. Forouzan, New York, International edition, 2010y.

5. Principles voice and data communication, The MC Graw-Hill Company, International edition, 2007y. USA

6. A Tool for Formal Modeling and Analysis of Systems Which Exhibit Random or Probabilistic. Behavior//www.prismmodelchecker.org.

7. Security and Privacy in Internet of Things.