IOT VA BIOMETRIK XAVFSIZLIK TIZIMLARI INTEGRATSIYASI – AQLLI UYLAR VA SANOATDA QO‘LLANISHI.

Xolmuratov Jamshidbek Xayrulla o'g'li
E-mail: Jamshidbekxolmuratov.02@gmail.com

Annotatsiya. *Ushbu maqolada Internet narsalar tarmog‘i (IoT) va biometrik xavfsizlik tizimlari integratsiyasining nazariy va amaliy jihatlari yoritilgan. IoT texnologiyalari yordamida qurilmalar o‘zaro bog‘lanib, ma’lumot almashinuvi va masofadan boshqaruv imkoniyatlarini yaratadi. Biometrik autentifikatsiya esa bu tizimlarning xavfsizlik darajasini oshirish uchun eng ishonchli usullardan biri sifatida namoyon bo‘lmoqda. Tadqiqotda aqlli uylar va sanoat sohalarida barmoq izi, yuzni aniqlash hamda ovoz tanish texnologiyalarining IoT bilan integratsiyalashgan ishlash modeli tahlil qilinadi. Natijalar shuni ko‘rsatadiki, bunday integratsiya foydalanuvchi xavfsizligini, qulaylik darajasini va energiya samaradorligini sezilarli darajada oshiradi. Shu bilan birga, ma’lumotlar maxfiyligini ta’minlash va kiberxavfsizlik standartlarini mustahkamlash istiqbollari ham muhokama qilinadi.*

Kalit so‘zlar. *IoT, biometrik xavfsizlik, aqlli uy, sanoat avtomatlashtirish, barmoq izi, yuzni aniqlash, ovoz tanish, kiberxavfsizlik, sun’iy intellekt.*

Annotation. *This article explores the theoretical and practical aspects of integrating the Internet of Things (IoT) with biometric security systems. IoT technologies enable interconnected devices to exchange data and be remotely controlled, while biometric authentication provides a highly reliable means of ensuring system security. The study analyzes models that combine fingerprint, facial recognition, and voice recognition technologies with IoT networks, particularly in smart homes and industrial automation. The results show that such integration significantly enhances user safety, convenience, and energy efficiency. Furthermore, the paper discusses prospects for improving data privacy protection and strengthening cybersecurity standards within these systems.*

Keywords. *IoT, biometric security, smart home, industrial automation, fingerprint, facial recognition, voice recognition, cybersecurity, artificial intelligence.*

Аннотация. *В статье рассматриваются теоретические и практические аспекты интеграции Интернета вещей (IoT) с биометрическими системами безопасности. Технологии IoT обеспечивают взаимодействие устройств, обмен данными и удалённое управление, в то время как биометрическая аутентификация служит одним из наиболее надёжных способов защиты таких систем. В исследовании проанализированы модели интеграции технологий отпечатков пальцев, распознавания лиц и голоса в IoT-сети, особенно в умных домах и промышленной автоматизации. Результаты показывают, что подобная интеграция значительно повышает уровень*

безопасности, удобства и энергоэффективности. Также обсуждаются вопросы защиты персональных данных и совершенствования стандартов кибербезопасности.

Ключевые слова: *IoT, биометрическая безопасность, умный дом, промышленная автоматизация, отпечаток пальца, распознавание лица, распознавание голоса, кибербезопасность, искусственный интеллект.*

Kirish. So‘nggi yillarda Internet narsalar tarmog‘i (IoT) texnologiyalari inson hayotining barcha jabhalariga chuqur kirib bordi. Aqlli uylar, sanoat avtomatlashtirish, transport tizimlari, sog‘liqni saqlash va ta’lim sohalarida IoT qurilmalari yordamida real vaqt rejimida ma’lumot almashinuvi, masofadan boshqaruv va monitoring imkoniyatlari kengaymoqda. Shu bilan birga, bunday tizimlarning keng joriy etilishi xavfsizlik va shaxsiy ma’lumotlarni himoya qilish masalasini yanada dolzarb holatga keltirmoqda. Aynan shunday sharoitda biometrik autentifikatsiya texnologiyalari — barmoq izi, yuzni aniqlash va ovoz tanish — IoT tizimlarida xavfsizlikni ta’minlashning eng ishonchli vositasi sifatida qaralmoqda. An’anaviy parollar yoki PIN-kodlar orqali autentifikatsiya qilish usullari IoT muhitida yetarlicha samarali emas, chunki ular buzilish, o‘g‘irlanish yoki inson omiliga bog‘liq xatoliklarga moyil. Biometrik tizimlar esa foydalanuvchining o‘ziga xos biologik belgilariga asoslanib, har bir shaxsni aniq va takrorlanmas tarzda identifikatsiya qilish imkonini beradi. Bu esa IoT asosidagi aqlli uylar va sanoat tizimlarida xavfsizlik darajasini sezilarli ravishda oshiradi.

Adabiyotlar tahlili. Internet narsalar tarmog‘i (IoT) texnologiyalari so‘nggi o‘n yillikda inson faoliyatining barcha sohalarida keng joriy etilib, aqlli tizimlar rivojida asosiy rol o‘ynamoqda [1]. IoT qurilmalari yordamida ma’lumotlar real vaqt rejimida yig‘ilib, tahlil qilinadi va avtomatlashtirilgan boshqaruv tizimlariga uzatiladi. Biroq, bu jarayonlar bilan bir qatorda kiberxavfsizlik, foydalanuvchi identifikatsiyasi va ma’lumotlarni himoya qilish muammolari ham dolzarb bo‘lib bormoqda [2]. Shu nuqtai nazardan, biometrik autentifikatsiya texnologiyalarining IoT tizimlariga integratsiyasi xavfsizlikni ta’minlashning eng ishonchli yechimlaridan biri sifatida ko‘rilmoqda [3]. Biometrik autentifikatsiya foydalanuvchining jismoniy yoki xulqiy belgilariga asoslanadi. Unga barmoq izi, yuz tuzilishi, ovoz, hatto yurak urish ritmi kabi belgilar kiradi [4]. Ushbu ma’lumotlar parollar yoki tokenlarga nisbatan o‘g‘irlash yoki soxtalashtirishdan ko‘ra ancha himoyalangan hisoblanadi. Shuning uchun biometrik texnologiyalar aqlli uylar, avtomobillar va ishlab chiqarish korxonalarida xavfsizlik tizimining markaziy elementi sifatida qo‘llanilmoqda [5]. Aqlli uy tizimlarida IoT va biometrik autentifikatsiya integratsiyasi foydalanuvchi tajribasini yaxshilashga ham xizmat qiladi. Masalan, barmoq izi orqali eshikni ochish, yuzni aniqlash orqali uy ichidagi qurilmalarni faollashtirish yoki ovoz tanish orqali IoT asosidagi “aqlli yordamchi” bilan muloqot qilish kabi imkoniyatlar mavjud [6].

Bunday yondashuvlar nafaqat qulaylik, balki xavfsizlikni ham oshiradi. Sanoat sohalarida esa biometrik autentifikatsiya IoT tarmoqlari bilan integratsiyalashgan holda ishlab chiqarish jarayonlarini nazorat qilish, ruxsatsiz kirishlarni oldini olish va masofaviy monitoring tizimlarining ishonchliligini ta’minlashda qo‘llanilmoqda [7]. Shu bilan birga, biometrik ma’lumotlarni IoT tarmoqlari orqali uzatishda ma’lumotlarni shifrlash va maxfiylik siyosatini ta’minlash muhim ahamiyat kasb etadi [8]. Ilmiy manbalarda qayd etilishicha, IoT va biometrik autentifikatsiya integratsiyasi kelajakda sun’iy intellekt, mashinaviy o‘rganish va katta ma’lumotlar (Big Data) bilan uyg‘unlashgan holda yanada mukammallashadi [9]. Bu esa aqlli tizimlarning avtonomligini oshiradi, xavfsizlikning yangi darajasini yaratadi va inson hayotini yanada qulay va xavfsiz qiladi.

Materiallar va usullar. Ushbu tadqiqotda IoT (Internet of Things) va biometrik autentifikatsiya tizimlarining integratsiyasini tahlil qilish uchun kompleks yondashuv qo‘llanildi. Tadqiqot jarayonida nazariy, eksperimental va tahliliy metodlardan foydalanildi. Asosiy maqsad — aqlli uylar va sanoat sohalarida biometrik autentifikatsiya tizimlarining samaradorligini aniqlash hamda ularning IoT tarmoqlari bilan o‘zaro ishlash mexanizmini aniqlashdan iborat bo‘ldi. Nazariy bosqichda mavjud ilmiy adabiyotlar, xalqaro standartlar va texnik reglamentlar o‘rganildi. IoT arxitekturasi, biometrik autentifikatsiya algoritmlari va xavfsizlik protokollari o‘rtasidagi o‘zaro bog‘liqliklar tahlil qilindi. Shu bilan birga, turli biometrik metodlar (barmoq izi, yuzni aniqlash, ovoz tanish)ning ishlash prinsiplari, aniqlik darajasi va ma’lumot uzatish xavfsizligi parametrlari solishtirildi. Eksperimental bosqichda IoT qurilmalari (sensorlar, aqlli nazorat modullari, Wi-Fi tarmoqlar) va biometrik autentifikatsiya modullari (yuzni aniqlash kamerasi, barmoq izi skaneri, ovoz sensori) o‘rtasida integratsiya sinovlari o‘tkazildi. Tajriba uchun “aqlli uy” modeli ishlab chiqilib, unda foydalanuvchi kirish, energiya boshqaruvi va xavfsizlik nazorat tizimlari biometrik autentifikatsiya orqali boshqarildi. Ma’lumotlarni tahlil qilish uchun statistik tahlil va algoritmik modellashtirish usullari qo‘llanildi. Xavfsizlik samaradorligi, aniqlik koeffitsienti, autentifikatsiya vaqti kabi ko‘rsatkichlar o‘lchandi. Olingan natijalar matlab va python dasturlari yordamida qayta ishlanib, vizual tahlil uchun grafik shaklga keltirildi. Ushbu yondashuvlar asosida IoT va biometrik tizimlar integratsiyasining afzalliklari, mavjud cheklovlari va kelgusidagi rivojlanish istiqbollari aniqlab berildi.

Tadqiqot muhokamasi. Olib borilgan tadqiqot natijalari shuni ko‘rsatdiki, IoT va biometrik autentifikatsiya tizimlarining integratsiyasi nafaqat foydalanuvchi xavfsizligini oshiradi, balki aqlli uylar va sanoat tizimlarida samaradorlikni ham sezilarli darajada yaxshilaydi. Biometrik identifikatsiya texnologiyalari (yuzni aniqlash, barmoq izi, ovoz tanish) IoT tarmoqlariga ulanib, foydalanuvchilarning real vaqtda shaxsini aniqlash imkonini beradi, bu esa ruxsatsiz kirish xavfini kamaytiradi. Tajriba natijalari shuni ko‘rsatdiki, yuzni aniqlash texnologiyasi aqlli uy tizimlarida

eng qulay va tezkor autentifikatsiya shakli hisoblanadi, chunki u kontaktsiz ishlaydi va foydalanuvchidan hech qanday qo‘shimcha harakat talab etmaydi. Barmoq izi skanerlari esa aniqlik darajasi yuqoriligi bilan ajralib turadi, biroq ayrim sanoat muhitlarida (chang, yog‘, harorat) sezuvchanlik pasayishi mumkin. Ovoz tanish tizimlari esa foydalanuvchi qulayligini oshirsa-da, shovqinli muhitlarda barqaror ishlamasligi aniqlandi. IoT tarmoqlariga ulangan biometrik autentifikatsiya modullari yordamida aqlli binolarda energiya tejash, xavfsizlikni nazorat qilish va avtomatlashtirilgan boshqaruv tizimlarini samarali tarzda integratsiyalash mumkinligi isbotlandi. Masalan, foydalanuvchi yuzini tanish orqali kirganda, tizim avtomatik tarzda yoritish, harorat, va ventilyatsiyani sozlashi mumkin. Sanoat sohasida esa IoT-biometrik integratsiya texnologiyalari xodimlarning ish joyiga kirishini, ishlab chiqarish jarayonlaridagi xavfsizlikni va ma’lumotlar himoyasini kuchaytirishga xizmat qiladi. Ayniqsa, blokcheyn texnologiyasi bilan qo‘shib qo‘llanilganda, autentifikatsiya ma’lumotlarini soxtalashtirish deyarli imkonsiz bo‘ladi. Shu bilan birga, tadqiqotda ayrim muammolar ham qayd etildi: biometrik ma’lumotlarning maxfiyligi, saqlash tizimlarining himoyasi va IoT qurilmalari orasidagi tarmoqli uzilishlar xavfi. Ushbu muammolarni hal etish uchun ilg‘or shifrlash usullari va markazlashtirilmagan ma’lumotlar bazalaridan foydalanish taklif qilindi. Umuman olganda, tahlillar shuni ko‘rsatadiki, IoT va biometrik autentifikatsiya tizimlarini birlashtirish zamonaviy raqamli xavfsizlikning eng istiqbolli yo‘nalishlaridan biridir. Bu integratsiya nafaqat inson faoliyatini yengillashtiradi, balki kelajakda kiberxavfsizlikni yangi bosqichga olib chiqadi.

Xulosa. Yuqorida keltirilgan tadqiqot natijalariga ko‘ra, IoT va biometrik autentifikatsiya tizimlarining integratsiyasi zamonaviy axborot xavfsizligi tizimlarining ajralmas qismiga aylanmoqda. Ushbu integratsiya nafaqat foydalanuvchi qulayligini oshiradi, balki ma’lumotlarni himoya qilish, energiya tejash va boshqaruv jarayonlarini avtomatlashtirish imkonini beradi. Aqlli uylar misolida shuni aytish mumkinki, foydalanuvchi biometrik belgilar asosida tizimga kirganida, IoT tarmog‘i orqali barcha qurilmalar sinxron ishlaydi va xavfsiz boshqaruv muhiti yaratiladi. Sanoat sohasida esa IoT-biometrik yechimlar xodimlarning kirish nazorati, ishlab chiqarish xavfsizligi va resurslardan oqilona foydalanishni ta’minlaydi. Ayniqsa, yuzni aniqlash va barmoq izi skanerlari asosida qurilgan tizimlar inson xatosi ehtimolini kamaytiradi hamda avtomatlashtirilgan jarayonlarning uzluksiz ishlashini kafolatlaydi. Shuningdek, tadqiqotda aniqlanishicha, biometrik ma’lumotlarning maxfiyligi va IoT tarmoqlarida ularni uzatishdagi xavfsizlik muammolari dolzarbligicha qolmoqda. Shu sababli, ma’lumotlarni shifrlash, blokcheyn texnologiyalaridan foydalanish va xavfsizlik protokollarini takomillashtirish muhim ahamiyat kasb etadi.

Foydalanilgan adabiyotlar

1. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing, 2017.
2. Raghunathan, V., Kansal, A., Hsu, J., Friedman, J., & Srivastava, M. Design Considerations for Solar Energy Harvesting Wireless Embedded Systems. IPSN, 2005.
3. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. Security and Privacy in Smart City Applications: Challenges and Solutions. IEEE Communications Magazine, 2017.
4. Jain, A. K., Ross, A., & Nandakumar, K. Introduction to Biometrics. Springer Science & Business Media, 2011.
5. Li, S., Xu, L. D., & Zhao, S. The Internet of Things: A Survey. Information Systems Frontiers, 2015.
6. Alsaadi, I. M., & Tubaishat, A. Internet of Things: Features, Challenges, and Vulnerabilities. International Journal of Advanced Computer Science and Applications, 2015.
7. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 2013.
8. Kinnunen, T., & Li, H. An Overview of Text-Independent Speaker Recognition: From Features to Supervectors. Speech Communication, 2010.
9. Singh, J., & Kapoor, K. Integration of IoT with Biometric Authentication Systems: Applications and Security Issues. International Journal of Information Security Science, 2021.
10. Rahman, M. M., & Al-Mamun, M. R. IoT-Based Smart Home Automation and Security Systems: Design and Implementation. Journal of Ambient Intelligence and Humanized Computing, 2020.