WIRELESS SECURITY PROTOCOLS

Po’latov Doston Normurod o’g’li
Yoqubova Madinabonu Abdushukur qizi
Torebaeva Naziyra
Shonazarov Sarvarbek Maqsud o‘g‘li

Annotatsiya: *Simsiz tarmoqlar xavfsizligi protokollari, simsiz tarmoqlarda muloqotlarni shifrlash, autentifikatsiya qilish, ma'lumotlarni himoya qilish va hujumlarga qarshi himoya ta'minlash uchun ishlatiladigan protokollar jamlanmasidir. Bu protokollar, foydalanuvchilar va serverlar o'rtasidagi muloqotlarni shifrlaydi, ma'lumotlarni himoya qiladi va xavfsizlikni ta'minlayadi. Ular orqali, tarmoq operatorlari va foydalanuvchilar tarmoq muloqotlarini xavfsiz va himoyalangan qilishlari mumkin. Ularning kamchiliklari tarmoq tuzilishiga, xavfsizlik sozlashlari va qurilmalar orasidagi uyumsizliklarga bog'liq bo'lishi mumkin. Foydalanish uchun, protokollar to'g'ri va to'liq o'rnatilishi kerak va tarmoq administratorlarining va xavfsizlik mutaxassislarining yangilanishlarga e'tibor berishlari talab qilinadi.*

Kalit so’zlar: *Simsiz tarmoqlar xavfsizligi protokollari bilan bog'liq kalit so'zlar: Xavfsizlik, Shifrlash, Autentifikatsiya, Himoya, Hujum, Protokol, TLS (Transport Layer Security), VPN (Virtual Private Network), IPsec (Internet Protocol Security), HTTPS (HTTP Secure), OpenVPN.*

Abstract: *Wireless network security protocols are a set of protocols used to encrypt communications, authenticate, protect data, and protect against attacks in wireless networks. These protocols encrypt communications between users and servers, protecting data and ensuring security. Through them, network operators and users can make network communications safe and secure. Their disadvantages may depend on network structure, security settings and incompatibilities between devices. In order to be used, the protocols must be properly and fully installed, and network administrators and security professionals are required to pay attention to updates.*

Keywords*: Wireless Security Protocols Keywords: Security, Encryption, Authentication, Protection, Attack, Protocol, TLS (Transport Layer Security), VPN (Virtual Private Network), IPsec (Internet Protocol Security) , HTTPS (HTTP Secure), OpenVPN.*

KIRISH

Simsiz xavfsizlik protokollari Internet xavfsizligi va himoyasini ta'minlash uchun ishlatiladigan protokollardir. Ushbu protokollar ma'lumotlarni shifrlash, autentifikatsiya qilish, aloqa tarmog'ini ajratish va boshqa asosiy xavfsizlik tushunchalarini amalga oshirish uchun mo'ljallangan.

Quyida simsiz tarmoq xavfsizligining eng mashhur protokollari keltirilgan:

1. Transport Layer Security (TLS): Ushbu protokol internetdagi muayyan ulanishni himoya qilish uchun ishlatiladi. TLS mijoz va server o'rtasidagi shifrlash, autentifikatsiya va xavfsiz aloqalarni o'rnatish uchun bir nechta xavfsizlik qatlamlarini o'z ichiga oladi. Ushbu protokoldan https:// bilan boshlanadigan saytlar foydalanadi.

2. Secure Shell (SSH): SSH - bu tarmoq orqali xavfsiz aloqa o'rnatish uchun ishlatiladigan protokol. Ushbu protokol serverlarga masofaviy kirish va masofadan boshqarish jarayonlari uchun ishlatiladi. SSH aloqalarni shifrlash, autentifikatsiya qilish va aloqa xavfsizligini ta'minlash uchun qo'shimcha xavfsizlik tushunchalarini amalga oshiradi.

3. Internet Protocol Security (IPsec): IPsec IP tarmoqlari orqali ma'lum ulanishlarni himoya qilish uchun ishlatiladi. U protokol, shifrlash, autentifikatsiya va boshqa xavfsizlik tushunchalarini qo'llaydi. IPsec virtual xususiy tarmoqni (VPN) yaratish va joylashtirishda keng qo'llaniladi.

4. Simsiz himoyalangan kirish (WPA/WPA2/WPA3): Bu protokollar Wi-Fi tarmoqlari uchun ishlatiladigan xavfsizlik standartlaridir. Ular Wi-Fi ulanishlarini shifrlash, autentifikatsiya qilish va himoyalash uchun amalga oshiriladi. Ushbu protokollarda qisqa muddatli kalitlar va simmetrik kalitlar qo'llaniladi.

Ushbu protokollar Internet tarmog'ining xavfsizligini ta'minlashning asosiy vazifalarini bajarish uchun mo'ljallangan. Ulardan foydalanish shartlari va ishlash usullari protokoldan protokolga farq qilishi mumkin.

Simsiz tarmoq xavfsizligi protokollarining xavfsizligi va kamchiliklari quyidagilarni o'z ichiga olishi mumkin:

1. Shifrlash protokollari kamchiliklari: Shifrlash protokollari ma'lumotlarni shifrlash uchun ishlatiladi, lekin ularning kamchiliklari bo'lishi mumkin. Ba'zi protokollar eski yoki zayl sifatida shifrlash algoritmalari va protokollarini qo'llaydigan versiyalarda kamchiliklarga uchrayishi mumkin. Bu, saldırganlarni shifrlashni buzish, ma'lumotlarni o'qish va falsifikatsiya qilish imkoniyatini oshirishi mumkin.

2. Protokol kamchiliklari: Protokollar o'rtasidagi kamchiliklar talqinlash imkonini beradi. Bunday kamchiliklar tarmoq tuzilishlarida yoki protokollar o'rtasidagi muammo va nuqtai nazarlar tufayli yuzaga kelishi mumkin. Bu kamchiliklar, saldırganlarga protokolni foydalanishni buzish, muloqotlarni yo'q qilish yoki ma'lumotlar ustida hakimiyat qilish imkonini beradi.

3. Autentifikatsiya kamchiliklari: Protokollar autentifikatsiya jarayonlarida kamchiliklarga uchrayishi mumkin. Bu, yolg'on autentifikatsiya, identifikatsiya uchun kamchiliklar, autentifikatsiya ma'lumotlarining o'zgarishi va boshqalar kabi muammo va kamchiliklarni o'z ichiga oladi. Bu, saldırganlarni o'zgarish mumkin bo'lgan ma'lumotlarni ishlatish va autentifikatsiya jarayonlarini buzishga imkon berishi mumkin.

4. DoS hamjixatani ta'minlash kamchiliklari: Protokollar, DoS (xizmatni yo'qotish) va DDoS (tarqalib tuzish bilan xizmatni yo'qotish) hamjixatlarini ta'minlash uchun kamchiliklarga uchrayishi mumkin. Bu hamjixatlar saldırganlar tomonidan tarmoq tuzilishlarini buzish, resurslarni zaxiralash va ishga to'xtatish uchun ishlatiladi.

5. Tizim konfiguratsiyasi va tizim boshqarish kamchiliklari: Protokollar haqida noto'g'ri konfiguratsiya va xatoliklar tizimning xavfsizligiga ta'sir qilishi mumkin. Bu kamchiliklar, konfiguratsiya xatoliklari, yolg'on parametrlar, xavfsizlik sozlashlari va boshqalar kabi asosiy kamchiliklarga olib kelishi mumkin.

6. Protokolning tashqi tashqi bog'lovchilar bilan ishlash kamchiliklari: Protokollar o'rtasida ma'lumotlarni almashish uchun ishlatilgan bog'lovchilar (gateway, serverlar, routers, switches) bilan ishlashda kamchiliklar yuzaga kelishi mumkin. Bunday bog'lovchilar tarmoqni uzaytirish, ma'lumotlarni ko'chirish va to'plam ma'lumotlarini qayta ishlash jarayonlarida hamjihatlik kamchiliklari o'rnatish imkonini beradi.

7. Xavfsizlikning zidga yoki noaniq qismiga erishilishi: Protokollar bajarilishi lozim bo'lgan amaliyotlarni va tekshiruv jarayonlarini uyg'unlashtirishning muhim qismi bo'lib, ularning to'liq va qayd etilgan ishlatilishi talab etiladi. Agar protokolning muayyan bir qismi yoki to'liq amal qilishi to'g'ri amalga oshmagan bo'lsa, bu protokolda xavfsizlikni ta'minlashning kamchiliklari bo'lishi mumkin.

8. Protokollar va qurilmalar orasidagi uyumsizliklar: Protokollar va ulardagi xavfsizlik tushunchalari bir necha muhitlarda ishlatiladi. Xavfsizlik protokollari va qurilmalar orasidagi to'liq va to'g'ri integratsiya yo'li ko'rsatilmagan bo'lsa, bu protokolning xavfsizlik kamchiliklari bo'lishi mumkin. Uyumsizliklar ma'lumotlarni o'zgartirish, ishlatishni va muomalani xavfsizligini ta'minlashni to'xtatish imkonini beradi.

Simsiz tarmoqlar xavfsizligi protokollarining kamchiliklari tarmoq tuzilishining turiga, protokollar orasidagi aloqalarga, xavfsizlik sozlashlari va tizim boshqarish qobiliyatiga, ma'lumotlarni shifrlash algoritmalari va xavfsizlik standartlariga qarab o'zgarishi mumkin. Xavfsizlikni ta'minlashda bir nechta muhim omillar hisobga olinishi kerak va tarmoq administratorlarining va xavfsizlik mutaxassislarining protokollar va tarmoq xavfsizligi bo'yicha yangilanishlarga dikkat qaratishlari talab etiladi.

Quyidagi misollar, simsiz tarmoqlar xavfsizligi protokollariga misollar beradi:

1. HTTPS (HTTP Secure): Bu protokol, TLS (Transport Layer Security) va SSL (Secure Sockets Layer) protokollari orqali muloqotlarni shifrlash va xavfsizlikni ta'minlash uchun foydalaniladi. HTTPS, veb saytlarda ma'lumotlar almashishini shifrlaydi, foydalanuvchilar va serverlar o'rtasidagi muloqotlarni himoya qiladi.

2. OpenVPN: OpenVPN, VPN (Virtual Private Network) yaratishda foydalaniladigan xavfsizlik protokolining nomidir. Bu protokol, shifrlash, autentifikatsiya va muloqotni himoya qilishni ta'minlaydi. OpenVPN, maxsus kliyent dasturlar orqali foydalanuvchilar uchun xavfsiz va shifrlangan ulanish tuzishga imkon beradi.

3. IPsec (Internet Protocol Security): IPsec, IP tarmoqlari uchun ishlatiluvchi xavfsizlik protokolining nomidir. Ushbu protokol, IP paketlari orqali muloqotlarni shifrlash va autentifikatsiya qilish imkonini beradi. IPsec, VPN ulanishlari va tarmoqlar orasidagi birlashmalarni xavfsizlik bilan himoya qilishda keng qo'llaniladi.

4. WPA2/WPA3 (Wi-Fi Protected Access 2/3): Bu Wi-Fi tarmoqlari uchun ishlatiluvchi xavfsizlik standartlari hisoblanadi. WPA2 va undan keyingi versiyalari, Wi-Fi ulanishlarni

shifrlash va autentifikatsiya qilish imkonini beradi. Ushbu protokollar, Wi-Fi tarmoqlarida yuzaga kelishi mumkin bo'lgan hacks va hujumlar bilan kurashish uchun ishlatiladi.

5. SSH (Secure Shell): SSH, tarmoq ustida uzaktan kirish va uzaktan boshqarish jarayonlarini xavfsiz qilish uchun ishlatiluvchi protokoldir. SSH, muloqotlarni shifrlaydi va autentifikatsiya qilish imkonini beradi. Bu protokol, serverlar bilan ishlashda, uzaktan boshqarishda va fayllarni o'zgartirishda xavfsizlikni ta'minlash uchun keng qo'llaniladi.

6. TLS/DTLS (Transport Layer Security/Datagram Transport Layer Security): TLS va DTLS, muloqotlarni shifrlash va xavfsizlikni ta'minlash uchun ishlatiladigan protokollar hisoblanadi. TLS, istemolchi va server orasidagi muloqotlarni shifrlash va autentifikatsiya qilish uchun foydalaniladi.

7. SFTP (Secure File Transfer Protocol): SFTP, fayllarni xavfsiz tarzda o'zgartirish va uzatish uchun ishlatiluvchi protokoldir. Ushbu protokol, SSH protokolidan foydalanadi va muloqotlarni shifrlaydi, autentifikatsiya qiladi va fayllarni himoya qiladi.

8. SRTP (Secure Real-Time Transport Protocol): SRTP, yashirin qo'llaniladigan multimedia ma'lumotlarni uzatish uchun ishlatiluvchi protokoldir. SRTP, audio va video ma'lumotlarini shifrlaydi va autentifikatsiya qiladi, shuningdek qo'llab-quvvatlanayotgan xorijiy kodlashni ta'minlaydi.

9. DNSSEC (Domain Name System Security Extensions): DNSSEC, DNS (Domain Name System) protocolida xavfsizlikni ta'minlash uchun foydalaniladi. Bu protokol, DNS ma'lumotlarini shifrlaydi, imzolaydi va autentifikatsiya qiladi, shuningdek DNS mavzularini zahiralashni ta'minlaydi.

10. IKEv2 (Internet Key Exchange version 2): IKEv2, IPsec uchun autentifikatsiya va sessiyalarni boshqarish uchun ishlatiladigan bir protokoldir. Ushbu protokol, muloqotlarni shifrlaydi, autentifikatsiya qiladi va xavfsiz sessiyalarni o'rnatish uchun xavfsiz bir ishlab chiqish protokolining (ISAKMP) qo'llanilishini ta'minlaydi.

Bu misollar, simsiz tarmoqlar xavfsizligi protokollarining faqat bir necha namunalaridir. Bu protokollar va boshqa xavfsizlik tizimlari foydalanuvchilarga muloqotlarini himoya qilish, ma'lumotlarni shifrlash, autentifikatsiya qilish va hujumlarga qarshi himoya qilish imkonini beradi.

SIMSIZ QURILMALARNI QO'LLANISH SOHASI

Simsiz qurilmalar (IoT) bir qator sohalarda keng qo'llaniladi. Bu sohalardan ba'zilari quyidagilardir:

1. Uy va buyurtma tizimlari: Uy va buyurtma tizimlarida simsiz qurilmalar, uyotish mashinalari, termostatlar, amalga oshirish to'plamlari va boshqalar kabi vositalar orqali uy va ofis tizimlarini avtomatlashtirish uchun qo'llaniladi. Misol uchun, o'tkazma buyurtmalarni avtomatik ravishda qabul qilish, havoni tekshirish, yo'l-yo'riq ma'lumotlarini taqdim etish va boshqalar.

2. Transport va logistika: Transport va logistika sohasida IoT qurilmalari, transport vositalarini, konteynerlarini, transport xizmatlari monitoringini va boshqalarini birlashtirish uchun ishlatiladi. Bu qurilmalar orqali transport vositalarining joylashuvi va holati,

yuklarning yurishini monitoring qilish, tezkor yo'l-yo'riq ma'lumotlari, xavfsizlikni nazorat qilish, oqimlarni optimallashtirish va boshqalar amalga oshiriladi.

3. Soha va bog'liqlik: Simsiqlik sohasida IoT qurilmalari, binolar, mahalliy tarmoqlar, havo muhitini boshqarish tizimlari va boshqalar kabi vositalar orqali ishlatiladi. Bu qurilmalar orqali binolardagi energiya iste'moli, uyg'unlik, xavfsizlik, tarmoqlardagi suv, energiya va gaz iste'moli, joriyati va qurilmalar monitoringini ta'minlash mumkin.

4. Sog'lomlik va kasb-hunar sohasi: Sog'lomlik va kasb-hunar sohasida IoT qurilmalari, shaxsiy qurilmalar, barqarorlik monitorlari, kasb-hunar ta'lim tizimlari, telemedicine vositalari va boshqalar kabi vositalar orqali foydalaniladi. Bu qurilmalar orqali shaxsiy sog'lomlik monitoringi, sport mashg'ulotlari monitoringi, kasb-hunar uskunalari bilan ishlash va boshqalar amalga oshiriladi.

5. Ishlab chiqarish sohasi: Ishlab chiqarish sohasida IoT qurilmalari, mahsulotni takomillashtirish, avtomatik ishlab chiqarish jarayonlarini monitoring qilish, iste'molchilar talablari va holatini nazorat qilish, eskiyuvchi va qurilmalarni texnik ta'minotini o'rganish uchun foydalaniladi. Bu qurilmalar orqali ishlab chiqarish.

6. Energia boshqaruv: Simsiz qurilmalar energiya boshqaruv sohasida ham keng qo'llaniladi. Bu sohada, energetika sohasidagi IoT qurilmalari, energiya iste'moli monitoringi, energiya samaradorligi, tarmoqning tarqatish va tarqatishini ta'minlash, energetika tizimlarini avtomatlashtirish va boshqalar kabi vazifalarda foydalaniladi.

7. Agro-sanoat sohasi: Agro-sanoat sohasida IoT qurilmalari, fermerlik, korxonalar, suv resurslari boshqarish tizimlari, avtomatik irrigatsiya tizimlari va boshqalar kabi vositalar orqali foydalaniladi. Bu qurilmalar orqali ekinlar va hosilalar monitoringi, suv resurslarini samarali ishlatish, to'liq uvuqqa ega xaridorlar uchun xizmat taqdim etish va boshqalar amalga oshiriladi.

8. Smart City: Simsiz qurilmalar smart city (axborot-kommunikatsiya texnologiyalari yordamida aqlli shahar) loyihalarida ham keng qo'llaniladi. Bu loyihalar shahar tarkibidagi muhim sohalar, masalan, transport, ayrim qurilmalarning ish vaqti, energetika, qurilish boshqarish, xavfsizlik va surveillance, suv resurslari boshqarish, yoritish tizimlari va boshqalar uchun simsiz qurilmalardan foydalanishni o'z ichiga oladi.

9. Smart Home: Smart home (axborot-kommunikatsiya texnologiyalari yordamida aqlli uy) tizimlari ham simsiz qurilmalar orqali ishlatiladi. Uy tarkibidagi mashinalar, elektronika, energiya boshqarish tizimlari, isharoatlar, ko'ra ko'p ishlatiladigan qurilmalar (smart TV, smart maishiy texnika, smart osimliklar va boshqalar) va boshqalar orqali uyotish jarayonini avtomatlashtirish, xavfsizlikni ta'minlash va iste'molchilarning mug'oya talablari va talablari bilan moslashish uchun foydalaniladi.

10. Kuzatuv va hujjat boshqarish: Kuzatuv va hujjat boshqarish sohasida ham simsiz qurilmalardan foydalaniladi. Bu qurilmalar, xaridorlar, logistik tizimlar, ma'lumotlarni kuzatuv va analitikasi, ma'lumotlar almashinuvini, xavfsizlik va hujjatlar boshqarishini avtomatlashtirish uchun ishlatiladi.

11. Xavfsizlik va himoya: Simsiz qurilmalar qo'llanish sohasida xavfsizlik va himoya muhim o'rin tutadi. Qurilmalar o'rtasidagi ma'lumot almashinuvining xavfsizligini ta'minlash, foydalanuvchilarning shaxsiy ma'lumotlarini himoya qilish, xavfsizlik ta'qiqlanishlarini aniqlash, kimni yo'qotishga urish jarayonlarini nazorat qilish va boshqalar kabi vazifalarda simsiz qurilmalardan foydalaniladi.

12. Ma'lumotlar analitikasi: Simsiz qurilmalar orqali to'plangan ma'lumotlar analitikasi va ma'lumotlar tahlili amaliyotlari olib boriladi. Qurilmalar ma'lumotlarini tahlil qilish, ma'lumotlardan ma'lumot olish, ma'lumotlarni birlashtirish, ma'lumotlarni vizualizatsiya qilish, ma'lumotlar ustida prognostika qilish va boshqalar kabi amaliyotlar maqsadida foydalaniladi.

13. Internetga ulanish va kommunikatsiya: Simsiz qurilmalar, internetga ulanish va kommunikatsiya sohasida ham o'rnatiladi. Bu qurilmalar orqali qurilmalar o'rtasidagi ma'lumot almashinuvi, boshqa tizimlar bilan o'zaro kommunikatsiya, internetga ulanish va boshqalar amalga oshiriladi.

14. Mashina o'qish va yoritish: Simsiz qurilmalar, mashina o'qish va yoritish sohasida ham keng qo'llaniladi. Bu qurilmalar avtomobillarda o'qish va yoritish tizimlarini avtomatlashtirish, mashinalar o'rtasidagi kommunikatsiyani ta'minlash, avtomobil davomida xavfsizlikni nazorat qilish va boshqalar uchun ishlatiladi.

15. Ijtimoiy sohalar: Simsiz qurilmalar ijtimoiy sohalar, masalan, festival va tadbirlarda, turizm sohasida, yashash qo'ng'iroqlarida, sport tadbirlarida va boshqalar kabi tashqi tadbirlarda ham foydalaniladi. Bu qurilmalar orqali tadbirlarni avtomatlashtirish, yashash tajribasini yaxshilash, xaridorlarni yoqish va qiziqtirish, xavfsizlikni ta'minlash va boshqalar amalga oshiriladi.

Simsiz qurilmalar qo'llanish sohasi juda keng bo'lib, yuqorida keltirilganlar faqat ba'zi asosiy sohalardan iborat. Bu sohalar uchun simsiz qurilmalardan foydalanish sohasidagi yutuqlar yana ham rivojlantirilmoqda. Yangi innovatsiyalar va ilg'or texnologiyalar jamiyatning turli sohalarida yutuq berishga imkoniyat yaratayotgan bo'lsa-da, keyinroqda paydo bo'lgan yutuqlar quyidagilardan iborat bo'lishi mumkin:

16. Moliyaviy tizimlar: Simsiz qurilmalar, moliyaviy sohada ham qo'llaniladi. Moliyaviy institutlarda, banklarda, kassalarda, hisob-kitoblarda va boshqa moliyaviy tizimlarda tahlillash va boshqarish amalga oshirish uchun foydalaniladi. Bu qurilmalar orqali moliyaviy operatsiyalar, hisob-kitob va audit jarayonlari, to'lov va pul mablag'larini monitoring qilish, xavfsizlikni ta'minlash va boshqalar amalga oshiriladi.

17. Huquqiy soha: IoT, huquqiy sohada ham rivojlanmoqda. Avtomatlashtirilgan yuridik xizmatlar, elektronik imzolar, huquqiy asbob-uskunalar, sertifikatlash va autentifikatsiya tizimlari, ma'lumotlar yig'ilishi va arxivlashning xavfsizligi, huquqiy analitika va boshqalar kabi vositalar IoT asosida ishlab chiqariladi.

18. Ma'suliyat boshqarish: Simsiqlik va ma'lumotlar almashinuvi asosida qurilgan simsiz qurilmalar, ma'suliyat boshqarish sohasida ham qo'llaniladi. Bu qurilmalar, ma'suliyat boshqarish tizimlarini avtomatlashtirish, ma'suliyat hisobotlarini tayyorlash,

ma'lumotlarni tahlil qilish, ma'suliyat bo'yicha risklarini nazorat qilish va boshqalar amalga oshirish uchun foydalaniladi.

19. O'zaro ma'lumot almashinuvi: IoT qurilmalari o'zaro ma'lumot almashinuvi sohasida ham yutuq beradi. O'zaro bog'liqlik tizimlari, ma'lumot almashinuvi tizimlari, tarmoq tizimlari va boshqalar orqali ma'lumot almashinuvi jarayonlari olib boriladi. Bu qurilmalar orqali ma'lumot almashinuvi protokollari, ma'lumot almashinuvi tahlillari, ma'lumot almashinuvi analitikasi va boshqalar kabi xizmatlar amalga oshiriladi.

20. O'z-o'zini boshqaruv: Simsiz qurilmalar, o'z-o'zini boshqarish sohasida ham yutuq beradi. Bu, avtomatlashtirilgan tizimlar va algoritmlar orqali qurilmalar o'z-o'zini boshqarishini ta'minlashga imkon beradi. Misol uchun, smart avtomobillar, o'z-o'zini boshqaruvli energetika tizimlari, o'z-o'zini boshqaruvli uyotish tizimlari kabi vositalar bu sohada ishlatiladi. Bu qurilmalar o'zaro ma'lumot almashinuvi, avtomatik ishga tushirish, o'z-o'zini tuzatish, o'z-o'zini o'rganish va o'z-o'zini optimallashtirish imkoniyatlarini ta'minlaydi.

21. Uzluksizlik: IoT qurilmalari, uzluksizlik sohasida ham yutuq beradi. Uzluksizlik tizimlari va qurilmalari orqali avtomatik xavfsizlik monitoringi, uzluksizlik nazorati, muvozanat va o'zaro ishonch tizimlari, muvozanatning avtomatik ravishda ta'minlanishi va boshqalar amalga oshiriladi. Bu qurilmalar masofaviy nazorat, muvozanat analitikasi, havfsizlik kameralari, uzluksizlik sensorlari va boshqalar kabi vositalar orqali uzluksizlikni ta'minlashga yordam beradi.

22. Markaziy boshqaruv: IoT qurilmalari markaziy boshqaruv sohasida ham yutuq beradi. Qurilmalar o'rtasidagi ma'lumot almashinuvi va kommunikatsiya, ma'lumotlar tahlili, ma'lumotlarni birlashtirish, ma'lumotlarni boshqarish va boshqalar amalga oshirish uchun markaziy boshqaruv vositalari va platformalardan foydalaniladi. Bu, avtomatlashtirilgan ma'lumot analitikasi, ma'lumot almashinuvi platformalari, boshqaruv paneli va boshqalar kabi vositalar orqali asosiy jarayonlarni boshqarish va birlashtirish imkoniyatlarini ta'minlaydi.

23. Kreativlik va innovatsiya: Simsiz qurilmalar kreativlik va innovatsiya sohasida ham yutuq beradi. Bu, innovatsiyalarni oshirish, yangiliklarni taklif qilish, yangi biznes modellari va mahsulotlar yaratish uchun avtomatlashtirilgan texnologiyalardan foydalanishni ta'minlaydi.

24. Saqlash va logistika: IoT qurilmalari saqlash va logistika sohasida ham yutuq beradi. Bu qurilmalar orqali omborlar, transport tizimlari, loyihalash va resurs boshqaruv tizimlari avtomatlashtiriladi. Bu imkoniyatlar orqali xaridorlarga to'g'ri vaqtda mahsulot taqdim etish, omborlar va logistika jarayonlarini nazorat qilish, ma'lumotlarni saqlash va boshqarish, ta'kidlash va boshqalar amalga oshirish uchun foydalaniladi.

25. Sog'liqni saqlash: IoT qurilmalari sog'liqni saqlash sohasida ham yutuq beradi. Bu qurilmalar tibbi uskunalar, shifoxonalar, klinikalar, shaxsiy sohalar va boshqa sohalarda foydalaniladi. Sog'liqni monitoring qilish, tibbi ma'lumotlar to'plamini o'rganish, shaxsiy

tarbiyalash va takliflar berish, avtomatik kasalliklar diagnositi, narxlarni monitoring qilish va boshqalar kabi vazifalarda IoT qurilmalardan foydalaniladi.

26. O'qish va ta'lim: IoT qurilmalari o'qish va ta'lim sohasida ham yutuq beradi. Bu qurilmalar maktablar, oliy o'quv yurtlari, universitetlar, darsliklar, yangi ta'lim usullari va boshqalar orqali ta'lim jarayonlarini avtomatlashtirish, o'quv ma'lumotlarini birlashtirish, ta'limni monitoring qilish, o'quvchilarga ma'lumotlarni taqdim etish va boshqalar kabi vazifalarda foydalaniladi.

27. Akidalar va restoranlar: IoT qurilmalari akidalar va restoranlar sohasida ham yutuq beradi. Bu qurilmalar orqali restoranlar o'rtasidagi ma'lumot almashinuvi, xaridorlarga xizmat ko'rsatish, kuzatuv va nazorat, atrofdagi muhitning monitori va boshqalar amalga oshiriladi. Akidalar tarmoqlari, restoran tizimlari, buyurtma va yetkazib berish tizimlari va boshqalar kabi vositalar IoT asosida ishlab chiqariladi.

28. Transport va logistika: IoT qurilmalari transport va logistika sohasida ham keng qo'llaniladi. Bu qurilmalar orqali transport tizimlarini monitoring qilish, loyihalash, navigatsiya, transportning ish vaqtini va o'zaro aloqani ta'minlash, transportning xavfsizligini nazorat qilish

29. Energohavo sohasi: Simsiz qurilmalar energohavo sohasida ham yutuq beradi. Bu qurilmalar orqali energiya iste'moli, energiya tarmoqlari, boshqaruv tizimlari va havosozlikning avtomatlashtirilishi amalga oshiriladi. Energiya ta'minoti, energiya iste'molining monitoringi, qulaylik va energiya samaradorligini oshirish, energiya sarfiyatini kamaytirish va boshqalar uchun IoT qurilmalardan foydalaniladi.

30. Kishilarga xizmat ko'rsatish: Simsiz qurilmalar, kishilarga xizmat ko'rsatish sohasida ham rivojlanmoqda. Bu qurilmalar orqali xususiy xizmatlarni avtomatlashtirish, xaridorlarga shaxsiy xizmat ko'rsatish, shaxsiy ko'rsatkichlar va talablar to'g'risidagi ma'lumotlarni yig'ish, shaxsiy tahlillar va takliflar berish, shaxsiy tajriba va tanishlikni oshirish va boshqalar amalga oshiriladi.

Bu yutuqlar faqat bir necha sohalardan iborat bo'lib, simsiz qurilmalar asosan biznes, kommunikatsiya, xavfsizlik, o'zaro bog'liqlik, ma'lumotlar analitikasi, o'z-o'zini boshqaruv, uzluksizlik va boshqa sohalarda o'rnatiladi. Har bir sohada yutuqlar va imkoniyatlar kengayib borayotganidek, bu sohalardagi innovatsiyalar va yangiliklar jamiyatning turli sohalarida o'z o'rnatishini topmoqda.

SIMSIZ QURILMALAR QO'LLANISH SOHASIDAGI YUTUQLAR

Simsiz qurilmalar (IoT) qo'llanish sohasidagi yutuqlar quyidagilardir:

1. Barcha qurilmalarni birlashtirish: Simsiz qurilmalar qo'llanish sohasida, barcha qurilmalarni birlashtirish va ularga alohida to'plamlar yaratish muhimdir. Ushbu to'plamlar tarmoq asosida aks ettiriladi va ularga boshqarish tizimi orqali qo'llaniladi.

2. Ma'lumotlar to'plami tahlili: Simsiz qurilmalar ko'plab ma'lumotlarni to'playdi. Bu ma'lumotlar IoT tizimlarda tahlil qilinishi, ma'lumotlar analitikasi va tahlili jarayonlarida muhim rol o'ynayadi. Ma'lumotlar to'plami tahlili tizimga yaxshi tushuntirish, narx tahlili, foydalanuvchi odatlari va talablarini aniqlash va boshqalar kabi maqsadlarda foydalaniladi.

3. Xavfsizlik va farovonlik: Simsiz qurilmalar qo'llanish sohasida xavfsizlik va farovonlikning kuzatilishi muhim ahamiyatga ega. Tizimdagi qurilmalarning xavfsizlik protokollarini qo'llab-quvvatlash, ma'lumotlarni shifrlash, autentifikatsiya usullarini amalga oshirish, tizimdan tashqariga nusha saqlash va boshqalar kabi chora-tadbirlar xavfsizlik va farovonlikni ta'minlash uchun zarurdir.

4. Otomatlashtirish va oddiylik: IoT tizimlari oddiylikni oshirish, ish faolligini oshirish va yordam berishda muhim rol o'ynayadi. Tizimdagi qurilmalar avtomatik ravishda xodimlar bilan kommunikatsiya qilish, topshiriqlarni bajarish, holatlarni avtomatik nazorat qilish, oddiy hisob-kitobni bajarish va boshqalar kabi vazifalarni muximlashtirish uchun ishlatiladi.

5. Energia samaradorligi: IoT qurilmalari kuchli energiya iste'mol qiladi, shuning uchun energiya samaradorligini yuqori tutish muhimdir. Qurilmalar energiya samaradorligini yuqori tutish orqali batafsil hisobot berish, kuchli energetikalar bilan ishlash, energiya iste'moli monitoringini amalga oshirish va energiya sarflarini minimalizatsiya qilishga yordam beradi.

6. Protokollar va standardlar: IoT tizimlari uchun mavjud protokollar va standardlar orqali birlashtirish va interoperatsiya tarmoqlar.

7. Bulut xizmatlardan foydalanish: Simsiz qurilmalar qo'llanish sohasida bulut xizmatlardan foydalanish muhimdir. Bulut xizmatlar, ma'lumotlarni saqlash, ma'lumotlar analitikasi, ma'lumotlar o'zaro almashinuvini ta'minlash va boshqalar kabi amalga oshiriladigan funksiyalarni taqdim etishda foydalaniladi.

8. Ma'lumotlar tomoshabinligi va avtomatik analitika: Simsiz qurilmalar tomonidan to'plangan ma'lumotlar avtomatik ravishda tahlil qilinadi va bu ma'lumotlardan foydalanuvchilarga foydali ma'lumotlar olib chiqariladi. Ma'lumotlar tomoshabinligi va avtomatik analitika, yo'nalishlarni aniqlash, iste'molchilar odatlari va talablarini tahlil qilish, maslahatlar berish va boshqalar kabi vazifalarda foydalaniladi.

9. Kommunikatsiya va tarmoq protokollari: Simsiz qurilmalar bir-biriga va kengaytirilgan tarmoqlarga bog'liq bo'lishi uchun kommunikatsiya va tarmoq protokollari muhimdir. Bu protokollar, qurilmalar orasidagi ma'lumot almashishni, komanda berishni, ma'lumotlar almashinuvi va sinxronizatsiyani amalga oshirishda foydalaniladi.

10. Integatsiya va yo'qotish: Simsiz qurilmalar qo'llanish sohasida mavjud tizimlarga integratsiya qilish va ularga bog'liqlikni yo'qotish muhimdir. Bu yo'qotish jarayonida eskirgan, muzlatilgan yoki ishlamaydigan qurilmalar erkakini identifikatsiya qilish, qurilmalarning avtomatik ravishda to'plamlar bilan bog'lanishini yo'qotish va boshqalar kabi muammolarni hal qilish uchun foydalaniladi.

11. Xavf-xatarlarni tahlil qilish va xavf-xatarlarga qarshi tadbirlar: Simsiz qurilmalar qo'llanish sohasida xavf-xatarlarni tahlil qilish va ularga qarshi tadbirlarni amalga oshirish muhimdir. Xavf-xatarlarni tahlil qilish, qurilmalarning xavf-xatarlarga qarshi hisob-kitobini o'rnatish, ularga qarshi tadbirlarni amalga oshirish, yonishlar yoki yangilanishlar uchun ta'limlarni tuzish va boshqalar kabi vazifalarda foydalaniladi.

Ushbu yutuqlar:

12. Dasturiy ta'minot: Simsiz qurilmalar qo'llanish sohasidagi dasturiy ta'minot ham muhimdir. Qurilmalarga moslashuvchan dasturlar va to'plamlar yaratish, ularga yangilash va yangilanishlarga tez reagirov berish, dasturlar ustida to'plam, skriptlar yoki interfeyslar yaratish va boshqalar kabi muammolar yechish uchun foydalaniladi.

13. Boshqaruv va monitoring: Simsiz qurilmalar qo'llanish sohasida tizimni boshqarish va monitoring amaliyotlari muhimdir. Qurilmalar ustida monitoring qilish, holatlarni nazorat qilish, qurilmalar orqali ishga tushirish va boshqarishni avtomatlashtirish, xavf-xatarlarni aniqlash, alarm va bildirishnomalar tashlash va boshqalar kabi vazifalarda foydalaniladi.

14. Tashqi aloqalar va integratsiya: Simsiz qurilmalar qo'llanish sohasidagi tashqi aloqalar va integratsiya ham muhimdir. Qurilmalar tashqi tizimlarga integratsiya qilinishi, uchuvchi vositalar bilan aloqalar, API va protokollar orqali tizimlarga ulanish, tashqi ma'lumotlar bazalariga kirish va boshqalar kabi vazifalarda foydalaniladi.

15. Sifat va iste'molchilar odatlari: Simsiz qurilmalar qo'llanish sohasida sifat va iste'molchilar odatlari ham muhimdir. Qurilmalar sifatini ta'minlash, ishga tushirish, to'g'ridan-to'g'ri qo'llash, foydalanuvchi interfeysi va tajribasi, foydalanuvchilarning odatlari va talablari bilan moslashuvchan bo'lish va boshqalar kabi vazifalarda foydalaniladi.

Bu yutuqlar, simsiz qurilmalar qo'llanish sohasidagi asosiy muammolar va vazifalarga oiddir. Xususan, tizimning birlashtirilishi, ma'lumotlar to'plami tahlili, xavfsizlik va farovonlik, energiya samaradorligi, protokollar va standardlar, ma'lumotlar tomoshabinligi, kommunikatsiya protokollari, integatsiya va yo'qotish, dasturiy ta'minot, boshqaruv va monitoring, tashqi aloqalar va integratsiya, sifat va iste'molchilar odatlari kabi muhim tushunchalar va amaliyotlar keng qo'llaniladi.

Xulosa: Xulosa qilinganda, simsiz tarmoqlar xavfsizligi protokollarining muhim bir qismi mavjud bo'lib, ulardan foydalanish tarmoq muloqotlarini va ma'lumotlarini shifrlash, autentifikatsiya qilish, himoya qilish va hujumlarga qarshi himoya qilishni ta'minlaydi. Bu protokollar, HTTPS, OpenVPN, IPsec, WPA2/WPA3, SSH, SFTP, SRTP, DNSSEC, IKEv2 va boshqalar kabi nomlarni o'z ichiga oladi.

Barcha protokollar kamchiliklarga ega bo'lishi mumkin, masalan, shifrlash protokollari eski yoki zayl sifatida shifrlash algoritmalari va protokollarini qo'llaydigan versiyalarda kamchiliklarga uchrayishi mumkin. Autentifikatsiya jarayonlarida kamchiliklar, konfiguratsiya xatoliklari, protokollar va qurilmalar orasidagi uyumsizliklar kabi muammo va kamchiliklar xavfsizlik protokollarida yuzaga kelishi mumkin.

Simsiz tarmoqlar xavfsizligi uchun protokollar bir yondan muloqotlar va ma'lumotlar ustida yolg'on amallar va hujumlar bilan kurashishga imkon beradi, boshqacha aytganda, ularga ishonchli va xavfsiz bir tarmoq tuzishining muhim qismlarini ta'minlash maqsadga

muvofiq. Xavfsizlikni ta'minlashda protokollar yalpi, barcha tarmoq operatorlari va foydalanuvchilar tomonidan to'liq ishlatishga va yangilanishga e'tibor berilishi lozim.

FOYDALANILAGAN ADABIYOTLAR:

1. Axborot xavfsizligi tizimini qurish metodologiyasi va xavf-xatarlarni tahlil qilish va boshqarish sohasida foydalaniladigan bazilar adabiyotlar:

2. Rossouw, R., & von Solms, R. (2016). Information Security Governance: A Practical Development and Implementation Approach. Auerbach Publications.

3. Whitman, M. E., & Mattord, H. J. (2016). Principles of Information Security. Cengage Learning.

4. Pfleeger, C. P., & Pfleeger, S. L. (2018). Security in Computing. Pearson.

5. Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology (NIST) Special Publication.

6. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.

7. ISO/IEC 27002:2013. Information technology — Security techniques — Code of practice for information security controls.

8. NIST Special Publication 800-53. Security and Privacy Controls for Federal Information Systems and Organizations.

9. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.

10. Anderson, R. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

11. «Axborot texnologiyasi. Ma’lumotlami kriptografik muho- fazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari» O‘zbekiston Davlat standard. 0‘z DSt 1092:2005.

12. «Axborot texnologiyasi. Axborotlami kriptografik muhofazasi. Ma’lumotlami shifrlash algoritmi» 0‘zbekiston Davlat standard. 0‘zDSt 1105:2006

13. «Axborot texnologiyasi. Ochiq tizimlar o‘zaro bogMiqligi. Elek tron raqamli imzo ochiq kaliti sertifikati va atribut sertifikatining tuzil- masi» 0‘zbekiston Davlat standarti. 0‘zDSt 1108:2006.

14. С.В. Симонов. Анализ рисков в информационнмх систе- мах. Практические советь! // Конфидент. -2001. -№2.

15. S.S.Qosimov. Axborot texnologiyalari. 0‘quv qoMlanma. - T.: «Aloqachi», 2006.

16. S.K.G‘aniyev, M.M. Karimov. Hisoblash sistemalari va tar- moqlarida informatsiya himoyasi. Oliy o‘quv yurt.talab. uchun o‘quv qoMlanma. —Toshkent Davlat texnika universiteti, 2003.

17. "Information Security Management Handbook" - Harold F. Tipton va Micki Krause tomonidan yozilgan bu kitob, umumiy xavfsizlik prinsiplarini va xavfsizlikni tahlil qilishning asosiy aspektlarini o'z ichiga oladi.

18. "Principles of Information Security" - Michael E. Whitman va Herbert J. Mattordning ushbu kitobi, xavfsizlikni qo'llab-quvvatlashning amaliyotga yo'naltirilgan prinsiplarini, tahlil qilish usullarini va xavf-xatarlarni boshqarishning muhim aspektlarini taqdim etadi.

19. "Security Engineering: A Guide to Building Dependable Distributed Systems" - Ross J. Andersonning bu kitobi, xavfsizlikni tizimni qurish va boshqarishning muhim xususiyatlari, tahlil qilish usullari, xavf-xatarlarni identifikatsiya qilish va ularga javob berishning yollari haqida tafsilotlar beradi.

20. "The Art of Computer Virus Research and Defense" - Peter Szorning ushbu kitobi, xavf-xatarlarni tahlil qilish va ularga qarshi ko'rsatkichlarni ishlab chiqishning yollari, viruslarni aniqlash va ularga qarshi muomala qilishning tajribali usullarini taqdim etadi.