MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG‘ONA FILIALI

5350100 – Telekommunikatsiya texnologiyalari ta’lim yo‘nalishi

IV– kurs, 633-20 guruhi talabasi

Norxo`jayev Komronbekning

Abanentga kirish tarmoqlari fanidan tayyorlagan

Referati

Mavzu: Mobil aloqa tarmoqlarning xafvsizligi

Qabul qildi: Xalilov.M

REJA:

1. Mobil Aloqa Tarmoqlarining Xavfsizligi
2. Mobil Qurilmalar Xavfsizligi
3. Ommaviy Wi-Fi Tarmoqlarida Mobil Aloqa Tarmoqlarining Xavfsizligi

Mobil aloqa tarmoqlarining xavfsizligi haqida gapiraylik. Mobil aloqa, kunlik hayotimizning ajralmas qismi bo'lganligi uchun shaxsiy ma'lumotlarimizni, moliyaviy ma'lumotlarimizni va aloqalarimizni himoya qilish uchun xavfsiz aloqa ta'minlash juda muhimdir.

Mobil aloqalardagi asosiy xavfsizlik muammolari ichida ma'lumotlarning shifrlanishi keladi. Shifrlash, ma'lumotlarning aloqa davomida xavfsiz tarzda o'tkazilishini ta'minlaydi. Mobil qurilmalar orasidagi aloqada odatda shifrlash algoritmlari ishlatiladi va bu orqali ma'lumotlarning ruxsat olishsiz kirishdan himoya qilinishi ta'minlanadi.

Bundan tashqari, mobil qurilmalar va mobil tarmoqlar ham muhim xavfsizlik xavf-xatarlari bilan boshqarish zarurligi mavjud. Masalan, yomon niyatdagi kishilar yoki dasturlar orqali amalga oshiriladigan hamloqlar, foydalanuvchilarning shaxsiy ma'lumotlarini olish yoki qurilmalarga zarar yetkazish maqsadida bo'lishi mumkin. Bu turlash hamloqlar orasida zararli dasturlar, espiyon dasturlar, shaxsiy ma'lumotlarni olish (phishing) hamloqlari va tarmoq hamloqlari kiritiladi.

Mobil qurilmalar xavfsizligi uchun muhim chora-tadbirlarni o'tkazish muhimdir. Ular quyidagilarni o'z ichiga oladi:

Ishonchli dasturlar ishlatish: Qurilmangizga faqat ishonchli manbalar orqali dastur yuklab oling va o'rnatib qo'ying. Rasmiy dastur do'konlari, odatda xavfsizlik tekshiruvi orqali zararli dasturlarni oldirishga harakat qiladi.

Kuchli parollar va biometrik tasdiqlashni ishlatish: Qurilmangiz uchun kuchli va farqli parol belgilang yoki qo'llanish bilan yuz tanish (fingerprint) kabi biometrik tasdiqlash usullaridan foydalaning.

Yangilanishlarni va to'ldirishlarni o'rnatish: Qurilmangizning operatsion tizimi va dasturlarini yangi versiyalarga o'rnatishni unutmang. Ishlab chiqaruvchilar, xavfsizlik bo'yicha bo'sh joylarni tuzatish uchun tez-tez yangilanishlar va to'ldirishlar tarqatishadi.

Ommaviy Wi-Fi tarmoqlarida ehtiyot bo'lish: Ommaviy Wi-Fi tarmoqlarida ko'rish vaqtlarida shaxsiy va maxfiy ma'lumotlaringizni bo'lishdan saqlang. Bu turidagi tarmoqlar, espiyon dasturlar yoki ma'lumot o'ziq-ovqatlar uchun hamloq nuqtasi bo'lishi mumkin.

Mobil xavfsizlik dasturlaridan foydalanish: Telefoningiz yoki planshetingiz uchun xavfsizlik dasturidan foydalanib, zararli dasturlarni aniqlash va qurilmangizni himoya qilishda qo'shimcha sahifa berishingiz mumkin.

Mobil aloqada xavfsizlik mavzusi doimiy ravishda rivojlanayotgan soha hisoblanadi va foydalanuvchilar xavfsizligi uchun ko'proq chora-tadbirlar o'tkazish zarurMobil aloqa tarmoqlarining xavfsizligi haqida gapiraylik. Mobil aloqa, kunlik hayotimizning ajralmas qismi bo'lganligi uchun shaxsiy ma'lumotlarimizni, moliyaviy ma'lumotlarimizni va aloqalarimizni himoya qilish uchun xavfsiz aloqa ta'minlash juda muhimdir.

Mobil aloqalardagi asosiy xavfsizlik muammolari ichida ma'lumotlarning shifrlanishi keladi. Shifrlash, ma'lumotlarning aloqa davomida xavfsiz tarzda o'tkazilishini ta'minlaydi. Mobil qurilmalar orasidagi aloqada odatda shifrlash algoritmlari ishlatiladi va bu orqali ma'lumotlarning ruxsat olishsiz kirishdan himoya qilinishi ta'minlanadi.

Bundan tashqari, mobil qurilmalar va mobil tarmoqlar ham muhim xavfsizlik xavf-xatarlari bilan boshqarish zarurligi mavjud. Masalan, yomon niyatdagi kishilar yoki dasturlar orqali amalga oshiriladigan hamloqlar, foydalanuvchilarning shaxsiy ma'lumotlarini olish yoki qurilmalarga zarar yetkazish maqsadida bo'lishi mumkin. Bu turlash hamloqlar orasida zararli dasturlar, espiyon dasturlar, shaxsiy ma'lumotlarni olish (phishing) hamloqlari va tarmoq hamloqlari kiritiladi.

Mobil qurilmalar xavfsizligi uchun muhim chora-tadbirlarni o'tkazish muhimdir. Ular quyidagilarni o'z ichiga oladi:

Ishonchli dasturlar ishlatish: Qurilmangizga faqat ishonchli manbalar orqali dastur yuklab oling va o'rnatib qo'ying. Rasmiy dastur do'konlari, odatda xavfsizlik tekshiruvi orqali zararli dasturlarni oldirishga harakat qiladi.

Kuchli parollar va biometrik tasdiqlashni ishlatish: Qurilmangiz uchun kuchli va farqli parol belgilang yoki qo'llanish bilan yuz tanish (fingerprint) kabi biometrik tasdiqlash usullaridan foydalaning.

Yangilanishlarni va to'ldirishlarni o'rnatish: Qurilmangizning operatsion tizimi va dasturlarini yangi versiyalarga o'rnatishni unutmang. Ishlab chiqaruvchilar, xavfsizlik bo'yicha bo'sh joylarni tuzatish uchun tez-tez yangilanishlar va to'ldirishlar tarqatishadi.

Ommaviy Wi-Fi tarmoqlarida ehtiyot bo'lish: Ommaviy Wi-Fi tarmoqlarida ko'rish vaqtlarida shaxsiy va maxfiy ma'lumotlaringizni bo'lishdan saqlang. Bu turidagi tarmoqlar, espiyon dasturlar yoki ma'lumot o'ziq-ovqatlar uchun hamloq nuqtasi bo'lishi mumkin.

Mobil xavfsizlik dasturlaridan foydalanish: Telefoningiz yoki planshetingiz uchun xavfsizlik dasturidan foydalanib, zararli dasturlarni aniqlash va qurilmangizni himoya qilishda qo'shimcha sahifa berishingiz mumkin.

Mobil aloqada xavfsizlik mavzusi doimiy ravishda rivojlanayotgan soha hisoblanadi va foydalanuvchilar xavfsizligi uchun ko'proq chora-tadbirlar o'tkazish zarur

Mobil qurilmalar xavfsizligi, mobil telefonlar, tablet kompyuterlar va boshqa portativ qurilmalar kabi mobil qurilmalar uchun xavfsizlikni ta'minlashning umumiy qoidalari va chora-tadbirlari bilan bog'liqdir. Bu, shaxsiy ma'lumotlar, moliyaviy ma'lumotlar, aloqalar va mobil qurilmalarning xavfsizlikka qarshi himoyalashini o'z ichiga oladi.

Quyidagi chora-tadbirlar mobil qurilmalar xavfsizligini ta'minlashda muhim ahamiyatga ega:

Parol va Kimlik Tekshiruvi: Mobil qurilmalarga kirish uchun parol yoki kimlik tekshiruvi sozlamalari o'rnatish kerak. Yuqori darajadagi parollar ishlatish, biometrik identifikatsiya (qo'l bilan, yuz bilan yoki boshqa biometrik ma'lumotlarni foydalanish) kabi usullar bilan mobil qurilmalarni himoya qilish tavsiya etiladi.

Yangilanish va Xavfsizlik Paketlarini O'rnatish: Mobil qurilmalardagi tizim va dasturlarni yangilash muhimdir. Tizim yangilanishlari, yangi ishlab chiqarilgan yangilanishlar va xavfsizlik paketlarini o'rnatish yordamida xavfsizlik bo'yicha kamchiliklarni bartaraf etishga yordam beradi.

Ma'lumotlarni Maxfiy Tuting: Shaxsiy ma'lumotlarni, bank kartalari raqamlarini, parollar va boshqa maxfiy ma'lumotlarni mobil qurilmalarda saqlash kerak. Ushbu ma'lumotlarni maxfiy saqlash uchun mobil qurilma xavfsizligi sozlamalaridan foydalanish va maxfiylik sozlamalarini ehtiyotkorlik bilan o'rnatish tavsiya etiladi.

Dastur Yuklab Olishda Ehtiyotkorlik: Mobil qurilmalarga dastur yuklab olishda ehtiyotkor bo'lish kerak. Yalpi to'plamlar, o'zi bilan yuklangan dasturlar va boshqa manbalar orqali dastur yuklashdan oldin ularning etkazib beradigan faoliyatlari, yuklab olinadigan dastur haqida fikr bildirishlari va ularga beriladigan ruxsatlarni ko'rib chiqish kerak.

Xavfsizlik Dasturlari va Mobil Antiviruslar: Mobil qurilmalarga xavfsizlik dasturlarini, mobil antiviruslar va maxfiylik dasturlarini o'rnatish tavsiya etiladi. Ushbu dasturlar qurilma xavfsizligini nazorat qilish, zararli dasturlarni aniqlash va o'chirish, xavfsizlik xatolarini to'g'rilash va hujjatlar uchun shifrlarni ta'minlash imkonini beradi.

Muhimliklar Tarafdorligi: Mobil qurilmalarni yoqish, mahrum etish yoki yoqish sozlamalarini faqat ruxsat berilgan muhitlarda amalga oshirish tavsiya etiladi. Bu, qurilmaning maxfiy ma'lumotlarga yoki hujjatlarga yuzasidan taqiqlovchi xavf-xatarlarni kamaytirishga yordam beradi.

Mobil qurilmalar xavfsizligi, foydalanuvchilar uchun muhim bir masaladir. Yukoridagi chora-tadbirlarni amalga oshirish, shaxsiy ma'lumotlar va mobil qurilmalarning xavfsizligini ta'minlashga yordam beradi. Buning bilan birga, mobil qurKechirasiz, men sizning so'rovingizni ma'nosiz yakunladi va kiritishni to'xtatdim. Agar sizga boshqa savollar yoki yordam kerak bo'lsa, menga ayting!

SWOT TAXLIL

Kuchli tomonlar

Yurtdan-yurtga bog'liqlik: Mobil aloqa tarmoqlari yanada kuchli bo'lib kelmoqda va yurtdan-yurtga bog'liqlikni osonlashtirib beradi. Bu, global aloqa tarmoqlari orqali dunyo bo'ylab bo'lgan ulkan ma'lumot almashinuvi imkoniyatini beradi.

Ko'p yoqilg'i va foydalanuvchilar soni: Mobil aloqa tarmoqlari yanada keng tarqalgan va katta yoqilg'i mavjud bo'lgan tarmoqlardir. Bu, katta foydalanuvchilar sonini olish, boshqa tashkilotlar bilan aloqada bo'lish va reklama va marketing kampaniyalarini samarali bajarish imkonini beradi.

Texnologik rivojlanish: Mobil aloqa tarmoqlari texnologik rivojlanish bilan birga o'sayotganligi uchun kuchli tomon hisoblanadi. Yangi aloqa protokollari, 5G tarmog'i, ishlab chiqaruvchilar tomonidan taklif etilayotgan innovatsiyalar va boshqalar kabi faktorlar, xavfsizlikni yanada yuqori darajada oshirishga yordam beradi.

Kamchiliklar

Xavfsizlik chegaralari: Mobil aloqa tarmoqlarida xavfsizlik chegaralari mavjud bo'lishi mumkin. Bu, shaxsiy ma'lumotlarni ushlab turish, identifikatsiya va autentifikatsiya muammolari, zararli dasturlar va viruslar, phishing hamjihatlar va boshqa xavf-xatarlarga oqibat bo'lishi mumkin.

Tizim ustida kontrol va monitoring: Mobil aloqa tarmoqlarida tizim ustida to'liq kontrol va monitoring olish qiyin bo'lishi mumkin. Bu,

xavfsizlik holatini kuzatish, zararli faoliyatni aniqlash va to'g'risidagi chora-tadbirlarni amalga oshirishni qiyinlashtirishi mumkin.

Qo'llab-quvvatlash va yangilanishlar: Mobil aloqa tarmoqlarining xavfsizligini yaxshilash, xavfsizlik sozlamalarini yangilash va xavfsizlik holatini takomillashtirish uchun qo'llab-quvvatlash va yangilanishlarga tegishli bo'lish kerak. Bu, resurslar va vaqtni talab qiladi.

Imkoniyatlar

Xavfsizlik texnologiyalaridagi rivojlanish: Xavfsizlik sohasidagi texnologik rivojlanish, mobil aloqa tarmoqlarining xavfsizligini yuqori darajaga oshirish imkonini beradi. Yangi xavfsizlik protokollari, biometrik identifikatsiya, end-to-end shifrlash va boshqa texnologik yechimlar, mobil aloqa tarmoqlarini xavfsizlashtirish uchun imkonlar yaratadi.

Xavfsizlik bilimlari va o'qitish: Xavfsizlik sohasidagi bilimlarning va o'qitishyurtlaridagi rivojlanish, mobil aloqa tarmoqlaridagi xavfsizlikga oid tajribalarni o'rgatish va xavfsizlikga qaratilgan kadrlarni ta'minlash imkonini beradi. Bu, mobil aloqa sohasidagi xavfsizlikning mustahkamlanishiga yordam beradi.

Tahlilga oid o'zgartirishlar

Xakkerlik va kiber-hujumlar: Mobil aloqa tarmoqlarining keng tarqalishi bilan birga, xakkerlar va kiber-hujumlar ham o'sganligi uchun xavfsizlikga xavf-xatarlar oshiradi. Xakkerlar shaxsiy ma'lumotlarni olish, identifikatsiya va autentifikatsiya protsesslarini yopish, zararli dasturlar va viruslar tarqatish kabi hujumlar bilan mobil aloqa tarmoqlariga zarar yetkazishi mumkin.

Maxfiylik va ma'lumotlarni boshqarish sohasidagi tartibotlar: Xavfsizlik sohasida o'zgartirishlar bilan birga, maxfiylik va ma'lumotlarni

boshqarish sohasida ham tartibotlar mavjud bo'lishi mumkin. Bu, maxfiylik normativ-huquqiy muammolari, ma'lumotlarni to'plash, saqlash va ishlatishga oid qonunlar va boshqa tartibotlarni o'z ichiga oladi.

GLOSSARY

Mobil aloqa tarmoqi: Kablosiz kommunikatsiya orqali mobil qurilmalar orqali ma'lumot almashish imkonini beruvchi tarmoq.

Xavfsizlik: Xavfsizlik, tizim, tarmoq yoki ma'lumotlarni hujum, zararli dasturlar, xakkerlik yoki boshqa xavf-xatarlardan himoya qilish jarayoni yoki holatidir.

Xavfsizlik protokollari: Mobil aloqa tarmoqlarida foydalaniladigan protokollar, ma'lumotlarni shifrlash, autentifikatsiya va autorizatsiya, shaxsiy ma'lumotlarni himoya qilish va hujumlar bilan kurashish uchun qo'llanishadi.

Shifrlash: Ma'lumotlarni maxfiylik qilish uchun ularni shifrlash protsessi. Shifrlanmagan ma'lumotlar xavfsizlik xavf-xatariga uchraydi, shuning uchun shifrlash, ma'lumotlarni yolg'iz o'qish imkonini beradi.

Biometrik identifikatsiya: Shaxslarning unikal biologik xususiyatlari, masalan, qo'l izi, yuz skani, retinasini skanlash, imzolash va boshqalar kabi asosli ma'lumotlarga asoslangan identifikatsiya usuli.

Zararli dasturlar: Kiber-hujumlarni bajarish, ma'lumotlarni olish, sistemlarni zarar yetkazish, xavfsizlikni buzish va boshqa xavf-xatarlarni oshirish maqsadida yaratilgan dasturlar.

Phishing: Foydalanuvchilarni aldadishga solish maqsadida yuborilgan so'rovnoma, e-pochta, SMS xabar yoki veb-sayt orqali shaxsiy ma'lumotlarni olishga harakat qiluvchi xakkerlik usuli.

Xakker: Kiber-hujumlarni bajaruvchi shaxs yoki guruh, tarmoqni buzish, ma'lumotlarni olish, zararli dasturlar o'rnatish va boshqa zararli faoliyatni bajarish maqsadida faoliyat yuritadigan kishi.

Maxfiylik: Shaxsiy ma'lumotlarni to'plash, saqlash va ishlatish jarayonlarida foydalanuvchilarning ma'lumotlarining maxfiylikni himoya qilinishi.

Identifikatsiya: Foydalanuvchining kimligini tasdiqlash jarayoni, masalan, foydalanuvchi nomi, paroli, biometrik ma'lumotlar yoki boshqa identifikatsiya faktorlarini qo'llash orqali.

Autentifikatsiya: Foydalanuvchining to'g'ri kimligini tasdiqlash jarayoni, masalan, parolni tekshirish, biometrik identifikatsiya, SMS kodi olish yoki boshqa autentifikatsiya usullari orqali.

Xavfsizlik monitoringi: Tizim, tarmoq yoki platformalardagi xavfsizlik holatini kuzatish va yo'qotishga oid tadbirlarni amalga oshirish uchun monitoring va tahlil vositasi.

End-to-end shifrlash: Ma'lumotni yuborishdan start bo'lib, qabul qilishgacha bo'lgan barcha kommunikatsiyalarni shifrlash protsessi.

Xavfsizlik sozlamalari: Tizim, tarmoq yoki dastur sozlamalarUzr oling, menimcha berilgan matn chegaralariga erishilmagan.

Foydalanilgan adabiyotlar ro`yhati

5. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetida kadrlar tayyorlash tizimini tubdan takomillashtirish va samaradorligini oshirish chora-tadbirlari to‘g‘risida. O‘zbekiston Respublikasi Vazirlar Mahkamasining qarori. Toshkent sh., 2018 yil 24 iyul, 569-son.

6. Axborot texnologiyalari va kommunikatsiyalarining jorim etilishini

nazorat kilish, ularni ximoya qilish tizimini takomillashtirish chora-tadbirlari to‘g‘risida. O‘zbekiston Respublikasi Prezidentining qarori. Toshkent sh., 2018 yil 21 noyabr, PK-4024. 7. O‘zR OO‘MTVning 2005-yil 21-fevraldagi 34-sonli «Talaba mustaqil ishini tashkil etish to‘g‘risida»gi buyruq bilan tasdiqlangan namunaviy nizom.

8. R.X.Alimov ,B.Yu.Xodiyev, K.Alimov va boshq. /S.S.G‘ulomovning umumiy tahriri ostida. Milliy iqtisodda axborot tizimlari va

texnologiyalari: Oliy o‘quv yurtlari talabalari uchun o‘quv qo‘llanma. T.: «Sharq»,2004. –320b.

9. Akbarov D.Ye. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning kullanilishi.- Toshkent, «O‘zbekiston markasi» nashriyoti, 2009-432 bet. 10. Ishmuxamedov R., Abduqodirov A., Pardaev A. Ta’limda innovatsion texnologiyalar (ta’lim muassasalari pedagog-o’qituvchilari uchun amaliy tavsiyalar)-T.: Iste’dod, 2008.-2008 – 180 b. 11. Aripov A.N., Mirzaxidov X.M., Shermatov Sh.X., Saidxodjayev S.R., Hasanov P.F., Amirov D.M., Bakirov O.A. Axborot – kommunikatsiya texnologiyalari. Izohli lug‘at. Toshkent-2004.-499 bet. 12. B.A.Begalov,N.R.Zaynalov, A.E.Davronov. Talabalarning mustaqil ishini tashkillashtirish. Uslubiy ko‘rsatma. SamISI, Samarkand,2006. –30 b.

Internet saytlari

1. http://www.gov.uz/- O‘zbekiston Respublikasi hukumat portali.

2. http://www.edu.uz/- O‘zbekiston Respublikasi oliy va o‘rta maxsus ta’lim vazirligi. 3. http://www.ziyonet.uz- Axborot ta’lim portali. 4. http://www.lex.uz/- O‘zbekiston Respublikasi qonun hujjatlari ma’lumotlari milliy bazasi. 5. http://www.ima.uz/- O‘zbekiston Respublikasi Intellektual mulk agentligi. 6. http://www.nuu.uz/- Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy

universiteti. 7. http://www.tuit.uz/- Toshkent axborot texnologiyalari universiteti. 8. http://www.samtuit.uz/- Toshkent axborot texnologiyalari universiteti Samarqand filiali. 9. http:// www.freesoft.ru /- Bepul dasturiy ta`minotlar. 10. http://www.uzinfocom.uz/- Kompyuter va axborot texnologiyalarini rivojlantirish va joriy etish markazi 11. http://www.infocom.uz/- Infocom ilmiy elektron jurnal. 12. http://www.iqtisodiyot.uz/- “Iqtisodiyot va innovatsion texnologiyalar” ilmiy elektron jurnal. 13. http:// www.uza.uz /- O‘zbekiston milliy axborot agentligi. 14. http://wikipedia.org - Erkin entsiklopediya 15. http://www.citforum.ru - Axborot texnologiyalar bo‘yicha axborot sayti. http://hozir.org

TEST

Mobil aloqa tarmoqlarida xavfsizlik nima?

a) Ma'lumotlarni uzatish uchun qo'llaniladigan mobil qurilmalar

b) Tizimni himoya qilish protokollari

c) Kablosiz tarmoqlarda ma'lumotlarni shifrlash va himoya qilish

d) O'zgartirishlarni kuzatish va baholash

Javob: c) Kablosiz tarmoqlarda ma'lumotlarni shifrlash va himoya qilish

Mobil aloqa tarmoqlarida foydalaniladigan xavfsizlik protokollari nima?

a) HTTP

b) HTTPS

c) SSL

d) FTP

Javob: b) HTTPS

Shifrlash nima uchun foydalaniladi?

a) Ma'lumotlarni shifrlash uchun

b) Tarmoqni boshqarish uchun

c) Qo'llanuvchilarni autentifikatsiya qilish uchun

d) Ma'lumotlarni saqlash uchun

Javob: a) Ma'lumotlarni shifrlash uchun

Biometrik identifikatsiya nima uchun foydalaniladi?

a) Foydalanuvchilarni autentifikatsiya qilish uchun

b) Tarmoqni boshqarish uchun

c) Ma'lumotlarni shifrlash uchun

d) Zararli dasturlarni aniqlash uchun

Javob: a) Foydalanuvchilarni autentifikatsiya qilish uchun

Mobil aloqa tarmoqlarida qaysi xavfsizlik usuli phishingga qarshi himoya qilishda muhimdir?

a) Shifrlash

b) Biometrik identifikatsiya

c) Zararli dasturlarni tan olish

d) Foydalanuvchilarni ta'lim berish

Javob: d) Foydalanuvchilarni ta'lim berish

Xakkerlik nima?

a) Xavfsizlikni ta'minlash tizimi

b) Zararli dasturlarni o'rganish tizimi

c) Kiber-hujumlar bilan shug'ullanuvchi shaxs yoki guruh

d) Ma'lumotlarni shifrlash protokollari

Javob: c) Kiber-hujumlar bilan shug'ullanuvchi shaxs yoki guruh

Xavfsizlik monitoringi nima uchun foydalaniladi?

a) Zararli dasturlarni o'chirish uchun

b) Tizimni boshqarish uchun

c) Xavfsizlik holatini kuzatish va yo'qotish uchun

d) Ma'lumotlarni yig'ish uchun

Javob: c) Xavfsizlik holatini kuzatish va yo'qotish uchun

End-to-end shifrlash nima?

a) Ma'lumotlarni uzatish uchun qo'llaniladigan mobil qurilmalar

b) Ma'lumotlarni shifrlash va uzatish protsessi

c) Tarmoqni boshqarish uchun protokollar

d) Ma'lumotlarni saqlash uchun protokollar

Javob: b) Ma'lumotlarni shifrlash va uzatish protsessi

Autentifikatsiya nima uchun foydalaniladi?

a) Ma'lumotlarni saqlash uchun

b) Tizimni boshqarish uchun

c) Foydalanuvchilarni autentifikatsiya qilish uchun

d) Zararli dasturlarni aniqlash uchunJavob: c) Foydalanuvchilarni autentifikatsiya qilish uchun

Mobil aloqa tarmoqlarida xavfsizlikni ta'minlash uchun qaysi faktorlar muhimdir?

a) Shifrlash protokollari va autentifikatsiya usullari

b) Tarmoqning fizikaviy himoyasi

c) Zararli dasturlarni aniqlash tizimlari

d) Foydalanuvchilarning xavfsizlik sozlamalari