

**MANAGEMENT AND ECONOMICS
SCIENTIFIC RESEARCH JOURNAL**

**MENEJMENT VA IQTISODIYOT
ILMIY-TADQIQOT JURNALI**

**НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЖУРНАЛ
МЕНЕДЖМЕНТА И ЭКОНОМИКИ**



MANAGEMENT AND ECONOMICS SCIENTIFIC RESEARCH JOURNAL

☎ +998 95 651 90 00

✉ journals@timeedu.uz

📍 Shota Rustaveli ko'chasi, 114

🌐 tmijournals.ndc-agency.uz

✈ @TMII_ilmiy_bolim

Bosh muharrir:

Narbayev Sharafatdin Kengeshovich

Bosh muharrir o'rinbosari:

Nosirova Nargiza Jamoliddin qizi

Muharrir:

Qarshiyeva Shahnoza Davlatovna

Tahrir hay'ati:

1. Sharipov Kongratbay Avezimbetovich – O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vaziri, t.f.d., prof.;
2. Axmedov Xojiakbarxon Dilshatovich – Toshkent menejment va iqtisodiyot instituti rektori i.f.n., dotsent;
3. Gulyamov Saidasror Saidaxmedovich – O'zbekiston Fanlar akademiyasi akademigi, i.f.d, professor;
4. Gulyamov Saidaxror Saidaxmedovich – O'zbekiston Fanlar akademiyasi akademigi i.f.d, professor;
5. Sultanov Mansur Qilichovich – Oliy ta'lim, fan va innovatsiyalar vazirligi huzuridagi "Inno" innovatsion o'quv-ishlab chiqarish texnoparki bosh direktori, t.f.f.d., dotsent;
6. Chertovitskiy Aleksandr Stepanovich - „Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muxandislari instituti“ Milliy tadqiqot universiteti professori, iqtisodiyot fanlari doktori;
7. Popkova Yelena Gennadyevna - Rossiya Federatsiyasi avtonom notijorat tashkiloti "Ilmiy kommunikatsiyalar instituti" prezidenti, iqtisodiyot fanlari doktori, professor;
8. Dr Goh Khang Wen – Malaziyaning INTI Xalqaro universiteti prorektori;
9. Wang Cheng – XXR "Hebei Institute of Mechanical and Electrical Technology" instituti i.f.f.d., dotsent;
10. Yo'ldoshev Nuriddin Qurbonovich – Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasini i.f.d., professor;
11. Akramov Tohir Abdirahmonovich Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasini i.f.d., professor;
12. Temirov Abdulaziz Alimjonovich – Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasini i.f.n., professor;
13. Rajabov Nazirjon Razzaqovich – Toshkent menejment va iqtisodiyot instituti Iqtisodiyot kafedrasini mudiri, i.f.n., dotsent;
14. Xotamov Ibodullo Sadulloyevich – Toshkent menejment va iqtisodiyot instituti Iqtisodiyot kafedrasini i.f.n., professor;
15. Sobirov Aziz Avazbekovich – Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasini mudiri, i.f.f.d., dotsent;
16. Raximova Shahlo Baxtiyorovna – Ta'lim sifatini nazorat qilish bo'limi boshlig'i, p.f.f.d., dotsent;
17. Kadirova Istora Bobirovna – Toshkent menejment va iqtisodiyot instituti Karyera markazi direktori, i.f.f.d.;
18. Turakulov Otabek Xolmirzayevich – Toshkent menejment va iqtisodiyot instituti Muhandislik va axborot texnologiyalari kafedrasini mudiri, t.f.f.d.

MUHANDISLIK OYLIGI

“RAQAMLI TEXNOLOGIYALARNI RIVOJLANTIRISH VA INNOVATSION MUHANDISLIK YECHIMLARI: ZAMONAVIY TENDENSIYALAR VA ISTIQBOLLAR” MAVZUSIDA RESPUBLIKA ILMIY-AMALIY ANJUMANI TO‘PLAMI MATERIALLARI

17-18 APREL, 2025

TOSHKENT

MUNDARIJA

1.	Primova X.A., Xaniyev N.M., Nodirov M.T. RFID TEXNOLOGIYASI ORQALI OLINGAN MA'LUMOT ASOSIDA QORAMOL KASALLIKLARINI ANIQLASHNING LOYIHALASH	6
2.	Doshanova M.Y., Otaxanova B.I., Aliyev R.R. USING ARTIFICIAL INTELLIGENCE TO AUTOMATE THE PROCESS OF COLLECTING AND ANALYZING DATA FROM ONLINE JOB POSTINGS	10
3.	Eshonqulov E.Sh., Abdiyeva H.S., Abdurahmonov M.S. SUN'IY YO'LDOSH TASVIRLARIDA PANSARPENING YONDASHUVI NATIJALARINI BAHOLASH BAYONNOMALARI	23
4.	Abduraxmanova Z.T. O'ZBEKISTONDA QISHLOQ XO'JALIGINING RAQAMLI TRANSFORMATSIYASI	26
5.	Abdiyeva K.S., Shamsiyeva K., Oblokulov S. GOMPERTZ ALGORITHM FOR THE DETECTION OF BREAST CANCER USING MAMMOGRAPHIC IMAGES	31
6.	Abdiyeva K.S., Shamsiyeva K., Olimjonova S. TOPOGRAPHIC MAP BASED SEGMENTATION OF MEDICAL IMAGES	35
7.	Radjabov B.A. O'ZBEKISTONNING TASHQI SAVDODA LOGISTIKA XARAJATLARI: RAQAMLI YECHIMLAR VA ULARNING EKSPORT RAQOBATBARDOSHLIGIGA TA'SIRI	39
8.	Primova X.A., Vaydullayeva M.F. SUN'IY INTELLEKTNI TALQIN QILISH VA QAROR QABUL QILISH: NORAVSHAN FIKRLASH TIZIMLARINI HISOBLASH MODELLARINI CHUQUR O'RGANISH	49
9.	Ulashov A.E., Obilov H.X. MATEMATIK MASALALARNI ZAMONAVIY DASTURLASH TILLARI YORDAMIDA YECHISH	57
10.	Mamatov N.S., Asqarov A.A. HAVO SIFATI INDEKSINI BASHORATLASHNING REGRESSION MODEL	69
11.	Mirpulatova L.M. AXBOROT TEXNOLOGIYALARI VA RAQAMLI TRANSFORMATSIYANING BANK FAOLIYATIDAGI ROLI	75
12.	Ниезматова Н.А., Жалелов Қ.А., Абдуллаева Б.М. НУТҚ СИГНАЛЛАРИДАН ШОВҚИНЛАРНИ БАРТАРАФ ЭТИШДА ФИЛЬТРЛАР ЖУФТЛИГИНИ ҚЎЛЛАШ ЁНДАШУВИ	84
13.	Mamatov N.S., Jo'rayev I.A., Jalelova M.M., Usarov J.A. TIBBIY TASVIRLAR BAZALARI TAHLILI	88
14.	Mamatov N.S., Jo'rayev I.A., Jalelova M.M., Jumayev B.J. TIBBIY TASVIRLARNI TAHLIL QILISH USUL VA ALGORITMLARI	92
15.	Mamatov N.S., Jalelova M.M., Jo'rayev I.A., Turakulova Sh.A. TIBBIY 2D TASVIRLAR ASOSIDA 3D TASVIRLARNI SHAKLLANTIRISH USULLARI	96
16.	Niyozmatova N.A., Madaminjonov A.D. INSON HIS-TUYG'ULARINI ANIQLASH DASTURIY VOSITALARI VA QURILMALARI	99

17.	Мухамедиева Д.Т., Маматов Н.С., Маматов А.А. МАТНЛИ МАЪЛУМОТЛАРНИ ТАСНИФЛАШДА БЕЛГИЛАРНИ ШАКИЛЛАНТИРИШ УСУЛ ВА АЛГОРИТМЛАРИ	103
18.	Raximov M. KASB KOMPETENSIYASIDA RAQAMLI TA'LIM TRANSFORMATSIYASI	106
19.	Turakulov O.X. MATNLI MA'LUMOTLARNI QAYTA ISHLASH BOSQICHLARI	110
20.	Turakulov O.X., Jalelov R.M. MATNLI MA'LUMOTLARGA DASTLABKI ISHLOV BERISH ALGORITMLARI	116
21.	Мухамедиева Д.К. ПОСТРОЕНИЕ ДЕРЕВА МЕРКЛА	123
22.	Mamatov N.S., Nuritdinov N.D., Almuradova N.A. IJTIMOIY TIZIMLARDA RAQAMLI TRANSFORMATSIYA JARAYONLARINI MODELLASHTIRISH	127
23.	Kabildjanov A.S., Pulatov G'.G. OB-HAVO OMILLARINING YURAK-QON TOMIR KASALLIKLARIGA TA'SIRINING SUN'IY INTELLEKT ASOSIDA TAHLILI	130
24.	Mamatov N.S., Kodirov E.S KAFT TASVIRI ASOSIDA SHAXSNI TANIB OLIH YONDASHUVLARI TAHLILI	133
25.	Raximov I.M. MAHALLIY ISHLAB CHIQUVCHILARNING XALQARO STANDARTLARGA MOSLASHUVI – IMKONIYATLAR, YUTUQLAR VA BARQAROR STRATEGIK YECHIMLAR	136
26.	Raximov F.J. TABIIY VA SUN'IY TOLALAR ASOSIDA QAYTA ISHLANGAN MAHSULOTLARNING TEXNOLOGIK SIFATI VA IQTISODIY SAMARADORLIGI	143
27.	Mamatov N.S., Dusanov X.T. NUTQ SIGNALINI XALAQITLARDAN TOZALASH USULLARI	150
28.	Dauletov A.Y., Sabirova S.T., Oydinov S.SH. ARXIVDA MATNLARNI QIDIRISH USULLARI TAHLILI	155
29.	Toshpulatov M. UNVEILING TOMORROW: EXPLORING THE FRONTIERS OF INNOVATION	162
30.	Маматов Н.С., Ниёзматова Н.А., Тожибоева Ш.Х., Яхяев Б.Ю., Машанпин Т.В. ИНСОН ҲИС-ТУЙҒУЛАРИНИ ЮЗ ТАСВИРИ ОРҚАЛИ АНИҚЛАШ ДАСТУРИЙ ВОСИТАЛАРИ ВА ҚУРИЛМАЛАРИ	165
31.	Ниёзматова Н.А., Маматов Н.С., Турғунова Н.М. МАТНЛИ МАЪЛУМОТЛАРНИ ТАСНИФЛАШ УСУЛ ВА АЛГОРИТМЛАРИ ТАҲЛИЛИ	172
32.	Маматов Н.С., Валижонов И.Х., Шукруллоев Б.Р. ТАСВИРЛАРНИ ТАСНИФЛАШДА ҚўЛЛАНИЛАДИГАН УСУЛЛАР	185
33.	Niyozmatova N.A., Xoitqulov A.A., Mamatov A.A. MATNLI MA'LUMOTLARDAN FAKTLARNI AJRATISH TEXNOLOGIYALARI	178
34.	Buribaeva Z.R. DIGITAL TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE IN EDUCATION: CHALLENGES AND OPPORTUNITIES	181

35.	Anarova Sh.A., Ibrohimova Z.E., Boliyeva D.N. R-FUNKSIYA USULINI (RFM) QO'LLAGAN HOLDA KO'P O'LCHOVLI FRAKTAL TUZILISHDAGI TASVIRLARNI GEOMETRIK MODELLARINI ISHLAB CHIQUISH	188
36.	Ibrohimova Z.E., Qarshiboyev J.O', Xaniyev N.M. KOMPYUTER GRAFIKASINING GEOMETRIK ALMASHTIRISHLARI ASOSIDA MURAKKAB FRAKTAL TUZILISHLARNI MATEMATIK VA RAQAMLI MODELLASHTIRISHNI AMALGA OSHIRISH	192
37.	Xalimov A.A. SANOAT KORXONALARIDA QAYTA TIKLANUVCHI ENERGIYA MANBALARIDAN FOYDALANISH YO'LLARI	198
38.	Rustamova M.M. INNOVATIVE TECHNOLOGIES AND INVESTMENT EFFICIENCY IN COTTON- TEXTILE CLUSTERS: OPTIMIZING COSTS THROUGH INDUSTRY 4.0 SOLUTIONS.	204
39.	Suyarov A.M. AXBOROTLARNI VIZUAL TAQDIM ETISHDA INFOGRAFIKA VOSITALARINI YARATISH USULLARI	214
40.	Saminjonov N.A. CHAKANA SAVDO FAOLIYATIDA RAQAMLI VA NEYROMARKETING STRATEGIYALARINING INTEGRATSIYASI	219
41.	Alimov A.A. INDUSTRY 4.0 TALABLARI ASOSIDA MUHANDISLIK TA'LIMINI TASHKIL ETISH MASALALARI	224
42.	Sobirov A.A., Zaripbayeva A.A. SANOAT KLASSTERLARINI SHAKLLANISH MEXANIZMLARI VA ZAMONAVIY MODELLARI	228
43.	Sharipov K.A., Karimov V.A. AQLLI ENERGIYA TIZIMLARI VA QAYTA TIKLANADIGAN ENERGIYA MANBALARIDAN FOYDALANISH USULLARI VA SAMARADORLIGI	237
44.	Маматов Н.С., Самижонов А.Н., Самижонов Б.Н. ИНСОН ЭХТИЁЖЛАРИНИ АНГЛОВЧИ ВА УЛАРГА ЖАВОБ БЕРИШ ҚОБИЛИЯТИГА ЭГА ЭМПАТИК РОБОТЛАР	246
45.	Yusupov R.A., G'ulomov A.X. MAYSALARNI O'RISH VA QOR TOZALASH MASHINASINI MASOFADAN BOSHQARISHNI AVTOMATLASHTIRISH	251
46.	Yusupov R.A., Qurbonov Sh.B. HELIX: FOYDALANUVCHIGA MOSLASHA OLADIGAN, KUNDALIK HAYOTDA YORDAM BERUVCHI SUN'IY INTELLEKT	254
47.	Haydarov E.D., Dusmurodov Q.A. OCHIQ WI-FI TARMOQLAR XAVFSIZLIGI	257
48.	Haydarov E.D., Dusmurodov Q.A. SIMSIZ TARMOQDA XAVFSIZLIK	265
49.	Ro'ziyeva F.K. MAISHIY KIMYO TOVARLARI B2B TAQSIMOTIDA KO'P KANALLI MARKETING STRATEGIYASINING AHAMIYATI	269
50.	Qudratov U.I., Abdullayeva N.R. MASHINANI O'QITISH USULLARIDAN FOYDALANGAN HOLDA ZARARLI DASTURLARNI ANIQLASH	277

51.	Muhamediyeva D.T., Raupova M. ELLIPTIK EGRI CHIZIQ ASOSIDA XAVFSIZ KALIT ALMASHINUVI	279
52.	Muhamediyeva D.T., Raupova M. POST-KVANT KRIPTOGRAFIYA ASOSIDA POLINOMLAR BILAN SHIFRLASH	282
53.	Muhamediyeva D.T., Raupova M. KVANT KALIT ALMASHINUVI BILAN INTEGRATSIYALANGAN RSA SHIFRLASH	285
54.	Mamayusupov A.A. ZAMONAVIY RAQAMLI MUHITDA KIBERXAVFSIZLIK TAHDIDLARI VA ULARNING OLDINI OLISH YO'LLARI	288
55.	Тоиров Ш. А. ОПТИМИЗАЦИЯ ФУНКЦИЙ С ПРИМЕНЕНИЕМ ЭВОЛЮЦИОННЫХ АЛГОРИТМОВ	291
56.	Toirov Sh. A. ARCHITECTURE OF OPERATORS IN QUANTUM ALGORITHMS	397
57.	Olimov S.A. TALABALARNING O'ZLASHTIRISH NATIJALARINI BAHOLASHDA RAQAMLI TEXNOLOGIYALARNING O'RNI	302
58.	Olimov S.A. OLIIY TA'LIM MUASSASALARIDA O'QUV JARAYONINI BOSHQARISHDA RAQAMLI TEXNOLOGIYALARNING AHAMIYATI	309
59.	Uzakova G.Z. ENGAGING ESP LEARNERS: STRATEGIES FOR PRODUCTIVE LESSONS	316
60.	Shafkarov F.X. SANATORIY-SOQ'LOMLASHTIRISH MUASSASALARINING ICHKI AUDITINI FUNDAMENTAL ASOSDA TASHKIL ETISH	321
61.	Raximov Sh.F. TIJORAT BANKLARIDA MIJOZLARNING SODIQLIK DASTURLARI ASOSIDA DEPOZITLARNI OSHIRISH YO'LLARI	329
62.	Туракулова Ш.А., Суюнова Н. ОПИСАНИЕ КРАЙНИХ ГИББОВСКИХ МЕР ДЛЯ МОДЕЛИ ИЗИНГА С НЕНУЛЕВЫМ ВНЕШНИМ МАГНИТНЫМ ПОЛЕМ НА РЕШЕТКЕ БЕТЕ	337
63.	Ulashov A.E. ZAMONAVIY TA'LIM TIZIMINING RAQAMLI TRANSFORMATSIYASI: TENDENSIYALAR, MUAMMOLAR VA YECHIMLARI	344
64.	Radjabov B.A. O'ZBEKISTONDA TA'LIMNING RAQAMLI TRANSFORMATSIYASI VA SUN'IY INTELLEKT	353
65.	Mamatov N.S., Ibroximov S.R., Almuradova N.A. O'QUV JARAYONIDA SUN'IY INTELLEKT VOSITALARIDAN FOYDALANISH	359
66.	Kuvandikov J.T., Tojiyev A.H. Axborot resurslaridan foydalanish ko'rsatkichlarini normallashtirish asosida bilim oluvchilarning bilim darajasini obyektiv baholash usullari	364
67.	Saidov S.F. TA'LIMDA SUN'IY INTELLEKTDAN SAMARALI FOYDALANISH MASALALARI	374
68.	Suyunova N.A. TA'LIMDA MANTIQ TUSHUNCHASI VA O'QUVCHILARDA MANTIQIY FIKRLASHNI RIVOJLANTIRISHNING INNOVATSION TEXNOLOGIYALARI	382

69.	Kuvandikov J.T. Tojiyev A.H. TA'LIM OLUVCHILAR BILIMINI BAHOLASHDA NORAVSHAN MANTIQDAN FOYDALANISH	389
70.	Djabbarova M.D. KASB-HUNAR TA'LIMIDA ELEKTRON TA'LIMNING PEDAGOGIK VA PSIXOLOGIK ASOSLARI	393
71.	Anarkulova G.M., Abduraxmanova F.N. OLIIY TA'LIMDA MAXSUS FANLAR BO'YICHA MASHG'ULOTLARDA ISHCHAN VA ROLLI O'YINLAR METODINI QO'LLASH INNOVATSION YONDASHUV	396
72.	Анаркулова Г.М., Абдиганиева З.С. ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ МЕТОДОВ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ И НАВЫКОВ СТУДЕНТОВ КАК ФАКТОР УСПЕВАЕМОСТИ	406
73.	Obidov R.A. TA'LIMDA KEYS TEXNOLOGIYALARINING AHAMIYATI	417
74.	Narbayev Sh.K., Maxkamova N.X. MAXSUS FANLARNI O'QITISHDA RAQAMLI VA INNOVATSION TEXNOLOGIYALARIDAN FOYDALANISHNING METODIK SHART-SHAROITLARI	422
75.	Erhanova N.A. MAKTABGACHA TA'LIM TASHKILOTLARIDA MULTIMEDIA RESURLARIDAN FOYDALANISH SAMARADORLIGI	430
76.	Xidoyatov M.B. OLIIY TA'LIM MUASSASALARIDA RAQAMLI MARKETING FAOLIYATINI BAHOLASH: AXBOROT TEXNOLOGIYALARIGA ASOSLANGAN YONDASHUVLAR	435
77.	Темиров А.А. АКЦИЯДОРЛИК ЖАМИЯТЛАРИ ФАОЛИЯТИГА РАҚАМЛИ БОШҚАРУВНИ ЖОРИЙ ЭТИШ ИСТИҚБОЛЛАРИ	444
78.	В.А.Ахмадалиев ЧОРВАЧИЛИК ХЎЖАЛИКЛАРИНИ ТАШКИЛ ЭТИШ ВА УЛАРГА ЕР АЖРАТИШ ТАРТИБИ	454
79.	Носирова Н.Дж. ЭКСПОРТНЫЙ ПОТЕНЦИАЛ СУБЪЕКТОВ МАЛОГО БИЗНЕСА УЗБЕКИСТАНА: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ (2018–2025 ГГ)	459
80.	Матлюбов Х.Ж. ТРАНСФОРМАЦИЯ ПРОМЫШЛЕННОЙ ПОЛИТИКИ: ОСНОВНЫЕ ТЕНДЕНЦИИ И ВЫЗОВЫ	463
81.	Sa'dulloyev H. I. SANOAT KORXONALARINING EKO-MARKETING TIZIMINI BAHOLAH AMALIYOTI	469

SIMSIZ TARMOQDA XAVFSIZLIK

Haydarov E.D.,

Muhammad Al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Axborot xavfsizligi kafedrası mudiri, PhD.

Dusmurodov Q.A.

Muhammad Al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Kriptologiya kafedrası 2-kurs magistranti

Annotatsiya. Ushbu maqolada simsiz tarmoqlarda xavfsizlik konsepsiyalari va usullari qisqacha tahlil qilinadi, WEP, WPA, WPA2 va WPA3 kabi boshqa shifrlash protokollari xavfsizroq va kriptobardoshliroqli ularga nisbatan hujum turlari keltirib o'tilgan. Protokollarga qarshi ba'zi hujumlar va himoya choralariga ham qarab o'tilgan.

Kalit so'zlar: Simsiz tarmoq, protokol, Wi-Fi, WEP, WPA, WPA2.

Abstract. This research briefly analyzes security concepts and methods in wireless networks. It provides an overview of encryption protocols such as WEP, WPA, WPA2, and WPA3, focusing on their security and cryptographic resistance. The study also presents various types of attacks against these protocols and discusses corresponding defense mechanisms.

Keywords: Wireless network, protocol, Wi-Fi, WEP, WPA, WPA2.

Аннотация. В данном исследовании кратко анализируются концепции и методы безопасности в беспроводных сетях. Рассматриваются шифровальные протоколы, такие как WEP, WPA, WPA2 и WPA3, с акцентом на их безопасность и криптостойкость. Также приведены типы атак на данные протоколы и меры защиты от них.

Ключевые слова: Беспроводная сеть, протокол, Wi-Fi, WEP, WPA, WPA2.

Kirish.

1997 yilda Elektron va Elektrika Muhandislari Instituti (IEEE) o'zining birinchi IEEE 802.11 standarti versiyasini chiqardi. Bu foydalanuvchilarga fizik tarmoq kabeli talab qilmasdan, tarmoqlarga simsiz kirish imkoniyatini beruvchi birinchi simsiz LAN standarti edi. Bu foydalanuvchilarga erkin harakatlanish davomida resurslarga ulanishni davom ettirish imkoniyatlarini taqdim etadi. Bu tarmoqqa kirishni osonlashtirishi va murakkab hududlarda tarmoqqa ulanishni ta'minlashi mumkin. Lekin

simsiz tarmoqni tinglovchi qurilma uzatuvchining geografik chegarasida bo'lsa, tarmoqdagi signallarni ushlashi mumkin bo'lgan xavfni yuzaga keltiradi[1]. Signallarning tarqalishi turli omillarga ta'sir qiladi, ammo sezgirlik va uzatuvchi kuchiga qarab, ular uzatuvchi qurilmadan yuzlab metr masofada ushlanishi mumkin. Bugungi kunda Internetda bepul mavjud bo'lgan paket analizatorlari va paket snifferslari ko'plab mavjud. Budan dasturlarga Wireshark, nmap va Tcpdump kabi dasturlarni misol keltirish mumkin.

Adabiyotlar tahlili

Uzatilgan signallarni shifrlash, axborotni tinglash va ushlab olishdan himoya qilish uchun zarurdir. Shifrlash axborotni ruxsatsiz shaxslar uchun o'qilmas holga keltiradi, ammo bu qurilmaning ishlash samaradorligi va protsessor kuchini talab qiladi. Shifrlashsiz simsiz tarmoqlardan foydalanish, shaxslarning shaxsiy ma'lumotlarini, masalan, fotosuratlar, videolar, elektron pochta xabarlar va moliyaviy axborotlarni oshkor qilish xavfini tug'diradi. Hech qanday shifrlashsiz, har kim tarmoqqa ulanishi va zararli trafikni ushlab yoki yuborishi mumkin. Uzatilgan paketlarni shifrlash uchun oddiygina Wi-Fi parolini yaratish kerak, ammo texnologiyaning foydalanuvchi uchun qulayligi ham muhim, chunki bu uning to'g'ri ishlatilish ehtimolini oshiradi. Demak, xavfsizlik faqat odamlarning kuchli parolni amalga oshirish ko'nikmalariga bog'liq bo'lmasligi kerak. Simsiz qurilmalar sonining oshishi bilan, masalan, IoT qurilmalari, aqlli televizorlar, simsiz printerlar, smartfonlar va noutbuklar, xavfsiz aloqaga ehtiyoj mavjud. 2024-yilga kelib dunyo bo'yicha umumiy ijtimoiy tarmoqlardan foydalanuvchilar soni 5,17 milliard kishiga yetdi, Xitoy, Hindiston va Qo'shma Shtatlar esa eng ko'p foydalanuvchiga ega mamlakatlar [2]. Foydalanuvchilarning katta o'sishi bilan, yuqori miqdordagi trafikni boshqarishi va uni samarali va xavfsiz tarzda himoya qilish texnologiyalariga ehtiyoj ortib bormoqda. Wi-Fi allaqachon Internet va elektr

energiyasi kabi muhim texnologiya hisoblanmoqda.

Metodologiya

Simsiz tarmoqlar mashhur bo'la boshlagach, turli xavfsizlik jamoalari standartdagi zaifliklarni topa boshladilar. Birinchi hujumlar 2001 yilda aniqlangan. WEP shifrlash halokatli darajada zaif ekanligi aniqlangan. WEP shifrlashni buzishning algoritmlari ishlab chiqilganidan boshlab, ular yanada samarali bo'ldi. WPA, WPA2 va WPA3 kabi boshqa shifrlash protokollari xavfsizroq va kriptobardoshliroq hisoblanadi. WPA2 - WPA protokolinining yaxshilangan versiyasidir va AES (Advanced Encryption Standard) shifrlashni taklif qiladi.

WPA (Wi-Fi Protected Access), WPA2, va WPA3 protokollariga qarshi turli hujum turlari mavjud.

- **Brute Force Attack (qupol kuch hujumi)** WPA o'zida o'rtacha kuchli shifrlash usulini taklif qilgan bo'lsa-da, agar parol juda oddiy bo'lsa, hujumchi parolni aniqlash uchun barcha mumkin bo'lgan kombinatsiyalarni sinab ko'rish mumkin.

- **Dictionary Attack** hujumchi so'zlar ro'yxatini (dictionary) ishlatib, parolni aniqlashga urinishadi. Bu hujum WPA protokoli bo'yicha zaif bo'lgan tizimlarda amalga oshirilishi mumkin.

- **KRACK (Key Reinstallation Attack)** Bu hujum WPA2 protokoli uchun 2017-yilda topilgan. KRACK hujumi, "4-way handshake" jarayonidagi zaifliklardan

foydalanadi. Hujumchi ma'lumotlarni qayta ishlatib yoki kalitlarni qayta o'rnatib, shifrlashni buzishi mumkin.

- **Dragonblood Attack**

WPA3'ning ba'zi xususiyatlariga qarshi, ayniqsa "Simultaneous Authentication of Equals" (SAE) (yangi "Handshake") zaifliklar mavjud. 2019-yilda Dragonblood deb nomlangan hujum topildi. Bu hujum, key exchange jarayonida xavfsizlikni buzishga imkon beradi.

- **Downgrade Attack**

Hujumchi, tarmoqni WPA3 protokolidan WPA2 yoki WPA versiyasiga tushirib, ularga hujum qilish imkoniyatini yaratishi mumkin. Bunday hujumlarda, WPA3ning yangi xavfsizlik imkoniyatlari buziladi.

Har bir protokolning o'ziga xos zaifliklari mavjud, lekin WPA3 protokoli, boshqa protokollarga nisbatan eng kuchli xavfsizlikni ta'minlaydi. Ammo, har bir tarmoqda to'g'ri xavfsizlik choralarini ko'rish va kuchli parollarni ishlatish juda muhimdir. Hujumlar asosan parolning zaifligiga tayanadi, shuning uchun tarmoq paroli har doim murakkab va uzun bo'lishi kerak.

WEP protokolining birinchi kamchiliklaridan biri **initsializatsiya vektori** (IV)dir. Kriptografik maqsadlar uchun ishlatilganda, 24-bit IV maydoni juda kichik bo'lib, protokolda katta cheklovlarni keltirib chiqaradi. Faqatgina 24 bit bilan WEP kaliti uchun faqat $2^{24} = 16\,777\,216$ xil turli shifrlash oqimlari mavjud. Trafik juda ko'p bo'lgan tarmoqlarda IVlar kam bitli bo'lgani uchun qayta ishlatiladi. Ba'zi oqim shifrlashlari, agar

hujumchi ishlatilgan kalit oqimini topa olsa, kriptografik tahlilga nisbatan zaif bo'ladi. Ba'zi hujumlar bu zaiflikni ekspluatatsiya qilib, tarmoqqa qo'shimcha trafik yuborib, ko'proq IVlar yaratadi, shunday qilib, parchalash jarayonini tezlashtiradi. IVlar qachon va qanday o'zgartirilishi protokolda ko'rsatilmagan, IVlar albatta qayta ishlatiladi. Agar IVlar tasodifiy tanlansa, faqat 5000 ta uzatilgan paketdan so'ng, qayta ishlatish ehtimoli 50% ni tashkil etadi.

RC4 40-bitli umumiy kalit va 24-bitli tasodifiy IV (Initsializatsiya Vektori)dan foydalanadi, bu esa 64-bitli RC4 kalitini yaratadi. Qisqa 40-bitli kalit esa qupol kuch hujumiga zaif. Agar bir nechta foydalanuvchilar bir xil kalitni ishlatssa, bu deshifrlash imkoniyatlarini oshiradi [4], chunki kalitlarni o'zgartirish kamdan-kam amalga oshiriladi. Ba'zi ishlab chiqaruvchilar kalit o'lchamini 104 bitgacha kengaytirdi, bu IV bilan birgalikda 128 bitli kalitni beradi.

WEP protokoli ma'lumotlar trafikini shifrlash uchun RC4 (Rivest Cipher 4) oqim shifrlashini ishlatadi. Bu algoritim DES va 3DES shifrlashidan tezroq va samaraliroq hisoblanadi, ammo kalitlari zaif. Oqimli shifrlashda blokli shifrlashlarga qaraganda kamroq hisoblash ishlatadi.

Natijalar va muhokama

Har bir tarmoq boshqaruvchisi o'zining MAC (Media Access Control) manziliga ega bo'lib, bu 6 baytli / 48-bitli qiymat bo'lib, o'nlik raqamlar va harflardan tashkil topgan. Ushbu raqamlar NIC ning qaysi ishlab chiqaruvchiga tegishli ekanligini

ko'rsatadi va manzil ko'pincha apparat yoki yoqilgan manzil deb ataladi. Faqat tasdiqlangan MAC manzillarini filtrlash orqali biz autentifikatsiya jarayoniga yana bir qatlam qo'shamiz, chunki router tarmoqqa qo'shilgan har bir MAC manzilini ichki ro'yxat bilan solishtiradi. Agar ular ichki ro'yxatdagi manzillar bilan mos kelmasa, qurilma tarmoqqa qo'shilishiga yo'l qo'yilmaydi. Ammo MAC-filtrlash xavfsizlik mexanizmi sifatida samarasizdir, chunki hujumchi osonlik bilan kirish nuqtasi va mijoz orasidagi trafikni kuzatishi mumkin. MAC manzillarini kuzatib, biror dastur yordamida ehtimoliy "oq ro'yxat"dagi MAC manzillarini soxtalashtirish mumkin. Bunga misol sifatida macchanger, iproute2, Technitium

MAC Address Changer va EtherChange kabi dasturlarni keltirish mumkin[4,5].

Xulosa

Simsiz tarmoqlar jamiyatda tizimlar va xizmatlarga ulanish nuqtayi nazaridan katta foyda keltiradi. Ular simli tarmoqlarga nisbatan o'rnatilishi kamroq xarajat talab qiladi va oson kengaytiriladi. Simsiz tarmoqlar, simli tarmoqlarga qaraganda, hujumlarga nisbatan zaifroq bo'lishi mumkin. Har kim simsiz tarmoqqa kirishga urinish qilishi mumkin, agar ular kirish nuqtasining geografik doirasida bo'lsa ishni yanada osonlashtiradi. Simsiz tarmoqlar, butun tarmoqqa kirishning qo'shimcha tahdidlarini keltirib chiqarishi mumkin. Aynan bu tadqiqot ishida ham shu zaifliklar tahlil qilib o'tildi.

Foydalanilgan adabiyotlar ro'yxati:

1. B.P. Crow, I. Widjaja, J.G. Kim, and P.T. Sakai. *IEEE 802.11 Wireless Local Area Networks*. *IEEE Communications Magazine*, 35(9):116–126, September 1997. ISSN 1558-1896. doi: 10.1109/35.620533. Conference Name: *IEEE Communications Magazine*.
2. Wireshark · Go Deep., . URL <https://www.wireshark.org/>.
3. The Tcpdump Group. *Tcpdump/Libpcap public repository*. URL <https://www.tcpdump.org>. Library Catalog: www.tcpdump.org Publisher: The Tcpdump Group.
4. Aircrack-ng, . URL <https://www.aircrack-ng.org/>.
5. Smartphone users worldwide 2020,. URL <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>. Library Catalog: www.statista.com.

Ingliz tili muharriri: Nosirova Nargiza Jamoliddin qizi
Musahhih: Vahobova Marfua Mirkamalovna
Sahifalovchi va dizayner: Zoirov Sardor Ziyodin o'g'li

1-maxsus son

© Materiallar ko'chirib bosilganda **"Management and Economics Scientific Research Journal"** jurnali manba sifatida ko'rsatilishi shart. Jurnalda bosilgan material va reklamalardagi dalillarning aniqligiga mualliflar ma'sul. Tahririyat fikri har vaqt ham mualliflar fikriga mos kelamasligi mumkin. Tahririyatga yuborilgan materiallar qaytarilmaydi.

Mazkur jurnalda maqolalar chop etish uchun quyidagi havolalarga maqola, reklama, hikoya va boshqa ijodiy materiallar yuborishingiz mumkin.
Materiallar va reklamalar pullik asosda chop etiladi.

El. pochta: journals@timeedu.uz

Tel.: [+998 95 651 90 00](tel:+998956519000)

"Management and Economics Scientific Research Journal" jurnali 19.09.2024-yildan O'zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan 404368-son reyestr raqami tartibi bo'yicha ro'yxatdan o'tkazilgan. Litsenziya raqami: C-5669639
PNFL: 308906510

Manzilimiz: Toshkent shahar, Yakkasaroy tumani
Shota Rustaveli ko'chasi, 114