INTERNET XAVFSIZLIGI VA ASOSI TAXDIDLAR

Qodirov Farrux Ergash o'g'li
Shahrisabz davlat pedagogika instituti "Matematika va ta'limda axborot texnologiyasi kafedrasi mudiri, Ilmiy rahbar
Jabborova O'g'iloy Husan qizi
Shahrisabz davlat pedagogika instituti matematika va informatika yo'nalishi 2-bosqich talabasi
https://doi.org/10.5281/zenodo.15117962

Annotatsiya. Internet xavfsizligi bugungi kunda eng dolzarb muammolardan biri bo'lib, u shaxsiy ma'lumotlarni himoya qilish, tarmoq infratuzilmasining barqaror ishlashini ta'minlash va kiberjinoyatlarga qarshi kurashish bilan bog'liq. Zamonaviy texnologiyalar rivojlanishi bilan internetga bog'liq tahdidlar ham ko'payib, ularning murakkabligi oshmoqda. Ushbu mavzu internet xavfsizligining asosiy tamoyillari, global tahdidlar va ularga qarshi kurash usullarini qamrab oladi. Internet xavfsizligi – bu kompyuter tizimlari, tarmoq infratuzilmalari va foydalanuvchilarning ma'lumotlarini zararli dasturlar, kiberhujumlar, fishing (phishing), zararli kodlar (malware) va boshqa xavflardan himoya qilish tizimidir. Ushbu mavzu doirasida eng keng tarqalgan tahdidlar, jumladan, DDoS hujumlari, MITM (Man-in-the-Middle) hujumlari, ransomware dasturlari, shaxsiy ma'lumotlarning buzilishi, ijtimoiy muhandislik (social engineering) va IoT (Internet of Things) qurilmalarining himoyasizligi kabi muammolar ko'rib chiqiladi. Mavzu, shuningdek, internet xavfsizligini ta'minlash usullarini tahlil qiladi. Masalan, shaxsiy va korporativ ma'lumotlarni himoya qilish uchun shifrlash texnologiyalari (encryption), ikki faktorli autentifikatsiya (2FA), antivirus va firewall tizimlaridan foydalanish, muntazam dasturiy ta'minot yangilanishlarini amalga oshirish va kiberhujumlarga qarshi himoya strategiyalarini ishlab chiqish muhim ahamiyatga ega.

Kalit so'zlar: Internet xavfsizligi , Kiberxavfsizlik, Kiberhujumlar, Zararli dasturlar (Malware), Fishing (Phishing), Ijtimoiy muhandislik (Social Engineering) DDoS hujumi , MITM hujumi (Man-in-the-Middle), Ransomware, Antivirus, Firewall, Shifrlash (Encryption), Ikki faktorli autentifikatsiya (2FA), Tarmoq xavfsizligi, IoT xavfsizligi, Shaxsiy ma'lumotlarni himoya qilish.

Kirish. Kiberhujumlar turli xil maqsadlarda amalga oshirilishi mumkin, jumladan, ma'lumotlarni o'g'irlash, tizimlarni ishdan chiqarish yoki pul ishlash maqsadida zarar yetkazish.

Eng keng tarqalgan kiberhujum turlari:

1.DDoS (Distributed Denial of Service) hujumlari – Xizmatlarni ishlamay qolishiga sabab bo'luvchi tarmoq resurslariga haddan tashqari yuklash.

MITM (Man-in-the-Middle) hujumlari – Foydalanuvchi va server o'rtasidagi ma'lumotlarni yashirincha o'g'irlash yoki o'zgartirish.

Zero-day hujumlar – Dastur yoki operatsion tizimlardagi hali aniqlanmagan zaifliklardan foydalanish.

2. Zararli dasturlar (Malware)Zararli dasturlar foydalanuvchi yoki korporativ tizimlarga zarar yetkazish maqsadida yaratiladi.

Asosiy zararli dastur turlari: Viruslar – O'zini ko'paytiradigan va tizim fayllariga zarar yetkazuvchi dasturlar.

Troyan dasturlar – Foydali dastur sifatida ko'rinadigan, ammo tizimni buzuvchi dasturlar.

Ransomware (Shantaj dasturlari) – Foydalanuvchi fayllarini shifrlab, uni qayta tiklash uchun pul talab qiluvchi zararli dasturlar.

Spyware (Josus dasturlar) – Foydalanuvchi faoliyatini yashirin kuzatib boradigan dasturlar.

3. Fishing (Phishing) va ijtimoiy muhandislik (Social Engineering)

Fishing – bu foydalanuvchini aldash yo‘li bilan maxfiy ma’lumotlarini (login, parol, bank kartasi raqami) qo‘lga kiritish.

Fishing usullari:

E-mail fishing – Soxta elektron pochta xabarlari orqali foydalanuvchini aldash.

Vishing (Voice phishing) – Telefon qo‘ng‘iroqlari orqali aldash.

Smishing (SMS phishing) – Soxta SMS xabarlar orqali ma’lumotlarni o‘g‘irlash.

Ijtimoiy muhandislik esa foydalanuvchilarning e’tiborsizligi yoki psixologik zaif tomonlarini ekspluatatsiya qilish orqali ma’lumotlarini olishga qaratilgan hujum turidir.

4. Ma’lumotlarning maxfiyligi va buzilishi

Bugungi kunda ko‘plab kompaniyalar va tashkilotlar katta hajmdagi shaxsiy ma’lumotlarni saqlaydi. Ushbu ma’lumotlar: Hackerlar tomonidan buzilishi – Kompaniyalarning ma’lumotlar bazalari buzilib, mijozlarning shaxsiy ma’lumotlari sotilishi yoki tarqatilishi mumkin.

Ichki xodimlar tahdidi – Ba’zan kompaniya xodimlari ham ma’lumotlarni sotish yoki zarar yetkazish maqsadida foydalanishi mumkin.

5. IoT (Internet of Things) xavfsizligi

IoT qurilmalarining keng tarqalishi bilan yangi xavfsizlik muammolari yuzaga kelmoqda: Himoyasiz IoT qurilmalar – Ko‘plab IoT qurilmalar parolsiz yoki zaif himoya bilan ishlaydi, bu esa hackerlar uchun oson nishonga aylanadi.

Botnetlar – IoT qurilmalarining zararli dasturlar tomonidan buzilishi va DDoS hujumlar uchun ishlatilishi.

6. Wi-Fi va tarmoq xavfsizligi tahdidlari

Jamoat Wi-Fi tarmoqlari va shifrlanmagan internet aloqalari hackerlar uchun qulay sharoit yaratadi.

Mavzuga doir adabiyotlar tahlili.

1. Ilmiy maqolalar va tadqiqotlar

Kiberxavfsizlikning asosiy tamoyillari

William Stallings – "Network Security Essentials: Applications and Standards" (2020)

Ushbu kitob tarmoq xavfsizligining asosiy tamoyillarini tushuntiradi. U tarmoq protokollari, kriptografiya, autentifikatsiya va ruxsatsiz kirishga qarshi himoya usullarini o‘z ichiga oladi. Kitobda ma’lumotlarni shifrlash (AES, RSA, ECC) va xavfsizlik devorlari (firewall) haqida ham batafsil ma’lumot berilgan.

Bruce Schneier – "Applied Cryptography: Protocols, Algorithms, and Source Code in C" (2015) Ushbu kitob kiberxavfsizlikda muhim bo‘lgan kriptografik usullarni tahlil qiladi. Internet xavfsizligining muhim jihatlaridan biri bo‘lgan shifrlash va autentifikatsiya algoritmlari haqida keng ma’lumot beriladi.

Zararli dasturlar va kiberhujumlar Kevin Mitnick – "The Art of Deception: Controlling the Human Element of Security" (2002) . Bu kitobda kiberjinoyatchilar tomonidan ishlatiladigan ijtimoiy muhandislik usullari (social engineering) haqida ma’lumot berilgan.

Hujumchilar foydalanuvchilarni qanday aldashi va bu tahdidlarga qarshi qanday himoyalanish mumkinligi tushuntiriladi. Nicholas Weaver – "A Deep Dive into Ransomware Attacks and Defense Mechanisms" (2021, IEEE Journal). Ushbu maqola ransomware dasturlarining ishlash mexanizmlari va ularga qarshi kurash strategiyalarini tahlil qiladi. Tahlil qilingan ransomware turlari: WannaCry, Ryuk, REvil. Tarmoq xavfsizligi va himoya usullari Andrew S. Tanenbaum – "Computer Networks" (2021) Bu kitobda tarmoq xavfsizligi va tarmoq protokollari (TCP/IP, VPN, SSL/TLS) haqida batafsil tushuntirilgan. DDoS hujumlariga qarshi kurashish texnologiyalari haqida ham ma'lumot berilgan. Cisco Networking Academy – "CCNA Cybersecurity Operations" (2020) Cisco sertifikati uchun tayyorlov kitobi bo'lib, unda kiberxavfsizlik va tarmoq xavfsizligi bo'yicha amaliy usullar bayon etilgan. Ma'lumotlarni tarmoqda qanday himoya qilish va xavfsizlik devorlarini qanday sozlash kerakligi tushuntiriladi.

2. Xalqaro tashkilotlar va ularning hisobotlari

Kiberxavfsizlik bo'yicha yirik xalqaro tashkilotlar, NIST (National Institute of Standards and Technology) "NIST Cybersecurity Framework" – kiberxavfsizlik bo'yicha xalqaro standart sifatida foydalaniladi Ma'lumotlarni himoya qilish va tizim xavfsizligini ta'minlash bo'yicha ko'rsatmalar mavjud. ENISA (European Union Agency for Cybersecurity) Har yili e'lon qilinadigan "Threat Landscape Report" – Yevropadagi kiberxavfsizlik tahdidlari va ularning rivojlanish tendensiyalari haqida ma'lumot beradi. Cybersecurity & Infrastructure Security Agency (CISA, AQSh) CISA kiberxavfsizlik tahdidlarini kuzatib boruvchi va ularni oldini olish bo'yicha tavsiyalar beruvchi tashkilot hisoblanadi. "Ransomware Protection Guide" va "DDoS Attack Mitigation" bo'yicha hisobotlari muhim manbalardir.

3. Zamonaviy tahdidlar va ularning tahlili. DDoS va IoT tahdidlari .

"The Evolution of DDoS Attacks and Defense Mechanisms" – IEEE Security & Privacy Journal (2022) Maqolada DDoS hujumlarining rivojlanishi, Mirai botnet kabi keng tarqalgan hujum usullari va ularga qarshi samarali choralar haqida ma'lumot berilgan. "IoT Security Challenges and Solutions" – ACM Computing Surveys (2021) IoT qurilmalarining zaifliklari va kiberhujumlarga nisbatan zaif tomonlari tahlil qilingan. IoT qurilmalarida ishlatiladigan shifrlash algoritmlari va xavfsizlik protokollari muhokama qilingan.

"Phishing Attack Trends and Countermeasures" – Journal of Cybersecurity Research (2020) Dunyo bo'ylab sodir bo'lgan yirik ma'lumot buzilishlari va ularga sabab bo'lgan omillar haqida batafsil hisobot. Internet xavfsizligi bo'yicha adabiyotlar va tadqiqotlar tahlili shuni ko'rsatadiki, kiberxavfsizlik nafaqat texnik, balki ijtimoiy va huquqiy jihatlarga ham bog'liqdir. Ilmiy kitoblar va maqolalar asosan texnik himoya choralariga e'tibor qaratadi (shifrlash, autentifikatsiya, firewall), xalqaro tashkilotlar esa real tahdidlar va ularning oldini olish strategiyalarini ishlab chiqadi.

Mavzu bo'yicha eng muhim yo'nalishlar quyidagilardir:

Tarmoq xavfsizligi – shifrlash, VPN, firewall va boshqa himoya choralarini o'rganish.

Kiberjinoyatchilik – fishing, ransomware va ijtimoiy muhandislik tahdidlariga qarshi kurash.

Zamonaviy tahdidlar – IoT, DDoS va ma'lumot buzilishlari tahlili.

Xalqaro standartlar va huquqiy bazalar – NIST, ENISA va CISA kabi tashkilotlarning tavsiyalari.

Kelajakda internet xavfsizligi yanada murakkablashib borishi kutilmoqda, shuning uchun yangi himoya texnologiyalari va xavfsizlik protokollarini doimiy ravishda takomillashtirish zarur

Natija muhokama. Tahlil qilingan adabiyotlar va ilmiy tadqiqotlar internet xavfsizligiga turli nuqtai nazardan yondashgan bo‘lsa-da, umumiy fikr shundaki, eng katta xavf inson omili bilan bog‘liq. Ijtimoiy muhandislik (social engineering) va fishing hujumlari texnik himoya choralaridan ko‘ra, insonlarning beparvoligi tufayli muvaffaqiyatli bo‘lmoqda. Shu sababli, foydalanuvchilarni xabardor qilish va kiberxavfsizlik bo‘yicha o‘qitish muhim ahamiyatga ega. Internet xavfsizligi bugungi kunda axborot texnologiyalarining eng muhim yo‘nalishlaridan biri bo‘lib, kiberjinoyatchilikning ko‘payishi bilan uni ta’minlash zarurati ortib bormoqda. Tahlil shuni ko‘rsatadiki, zamonaviy tahdidlar (DDoS hujumlari, fishing, ransomware, IoT zaifliklari) tobora murakkablashib, nafaqat individual foydalanuvchilar, balki biznes va davlat tashkilotlari uchun ham jiddiy xavf tug‘dirmoqda.

Xulosa va takliflar. Tadqiqot natijalariga ko‘ra, tarmoq texnologiyalarining rivojlanishi axborot almashinuvi tizimlarini tubdan o‘zgartirib, global iqtisodiyot, ta’lim, tibbiyot, biznes va kundalik hayotning ajralmas qismiga aylanganligi aniqlandi. Tarmoq texnologiyalarining evolyutsiyasi quyidagi asosiy bosqichlarni o‘z ichiga oladi:

Dastlabki bosqich (1950–1980-yillar): Kompyuter tarmoqlari faqat ilmiy va harbiy sohalar uchun ishlatilgan. Internetning rivojlanishi (1980–2000-yillar): TCP/IP protokollarining joriy etilishi bilan internet global tizimga aylandi. Simsiz va yuqori tezlikdagi tarmoqlar (2000–2010-yillar): Wi-Fi va mobil internet texnologiyalarining ommaviylashishi kuzatildi. Zamonaviy bosqich (2010-yildan hozirgi kungacha): Bulutli hisoblash, sun’iy intellekt va 5G texnologiyalarining rivojlanishi kuzatilmoqda. Tahlil shuni ko‘rsatadiki, zamonaviy tarmoq texnologiyalari: Tezkor va samarali axborot almashinuvi imkoniyatini yaratmoqda.

Turli sohalarning rivojlanishiga katta ta’sir ko‘rsatmoqda.

Axborot xavfsizligi, raqamli tengsizlik va tarmoq infrastrukturasi bilan bog‘liq muammolarni hal qilish zaruriyatini tug‘dirmoqda. Kelajakda 6G texnologiyalari, kvant tarmoqlar, IoT, sun’iy intellekt asosida boshqariladigan avtonom tarmoqlar kabi innovatsiyalarni joriy etish tarmoq texnologiyalarini yangi bosqichga olib chiqishi kutilmoqda.

- Kiberxavfsizlik bo‘yicha yangi algoritmlar va shifrlash texnologiyalarini joriy etish.
- Sun’iy intellekt asosida xavfsizlik monitoringini kuchaytirish.
- Yuqori tezlikdagi internetdan foydalanish imkoniyatlarini kengaytirish.
- Optik tolali tarmoqlar va 5G bazaviy stansiyalarini ko‘paytirish.
- Qishloq hududlari va rivojlanayotgan mintaqalarga tarmoq texnologiyalarini joriy etish.
- Ta’lim va kasbiy rivojlanish uchun bepul onlayn resurslar yaratish.
- Tarmoq texnologiyalari bo‘yicha ilmiy izlanishlarni kengaytirish.
- Sun’iy intellekt va kvant hisoblash sohasida tadqiqotlarni rag‘batlantirish.
- Kam energiya sarflovchi tarmoq qurilmalarini ishlab chiqish.

Foydalanilgan adabiyotlar/Используемая литература/References:

1. Ergash o’g’li, Qodirov Farrux, and Berdiyev Sardor Sobir o’g’li. "DEVELOPMENT OF MATHEMATICAL APPLICATIONS IN THE PROGRAM OF EXISTING SCRIPT LANGUAGE."

2. Qodirov, F. E., S. S. Jo'rayev, and V. N. Qalandarov. "INFORMATION ARCHITECTURE IN SITE DESIGN." НАУКА И НАУЧНЫЙ ПОТЕНЦИАЛ-ОСНОВА УСТОЙЧИВОГО ИННОВАЦИОННОГО РАЗВИТИЯ ОБЩЕСТВА. 2019.
3. Qodirov, F. E., et al. "FEATURES OF INTEL CORE i9 X-SERIES PROCESSORS AND ITS ADVANTAGE FROM OTHER PROCESSORS." ПУТИ ПОВЫШЕНИЯ РЕЗУЛЬТАТИВНОСТИ СОВРЕМЕННЫХ НАУЧНЫХ ИССЛЕДОВАНИЙ. 2019.
4. Ergash o'g'li, Qodirov Farrux, and Bozorova Irina Jumanazarovna. "METHODS OF DISPLAYING MAIN MEMORY ON CACHE." Ответственный редактор (2020): 6.
5. Qodirov, F. E. "Methodological aspects and importance of development of medical services through econometric modeling and forecasting options." academy. uz/index. php/yo.
6. Ergash o'g'li, Qodirov Farrux. "Hududlarni ijtimoiy-iqtisodiy rivojlantirishda har bir hududning o 'ziga xos xususiyatlari." Scientific Journal of Actuarial Finance and Accounting 4.09 (2024): 178-183.
7. Qodirov, F. E., O. D. Doniyorov, and H. Shokirov Sh. "Basic concepts of information security in information systems. Wide threats and their consequences." концепции устойчивого развития науки в современных условиях (2021): 153-155.
8. Қодиров, Ф. "ЗАМОНАВИЙ КОМПЬЮ ТЕР УЙИНЛАРИ ВА УЛАРНИНГ СИНФЛАНИШИ." МУХАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ КАРШИ ФИЛИАЛИ (2019).
9. Qodirov, F. "YOSHLAR MA'NAVIYATINI YUKSALTIRISHDA MILLIY ONLAYN KITOB DO'KONINI ISHLAB CHIQISH VA TADBIQ ETISH." МУХАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ КАРШИ ФИЛИАЛИ (2019).
10. Qodirov, F. "MASOFAVIY TA'LIMDA O'QISHNING QULAYLIKLARI VA KAMCHILIKLARI." МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҚАРШИ ФИЛИАЛИ (2020).
11. Ergash o'g'li, Qodirov Farrux. "ECONOMETRIC MODELING OF THE DEVELOPMENT OF MEDICAL SERVICES TO THE POPULATION OF THE REGION." Berlin Studies Transnational Journal of Science and Humanities 2.1.1 Economical sciences (2022).
12. Кодиров, Ф. "АНАЛИЗ БИОСИГНАЛОВ В ЭЛЕКТРОКАРДИОГРАФИИ И МЕТОДЫ ИХ ОБРАБОТКИ." МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҚАРШИ ФИЛИАЛИ (2020).
13. Қодиров, Ф. "СОЗДАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И АППАРАТА ЭЛЕКТРОННОЙ БИБЛИОТЕЧНОЙ СИСТЕМЫ НА ОСНОВЕ QR-КОДОВОЙ ТЕХНОЛОГИИ." Kokand University (2020).
14. Bozorova, Irina Jumanazarovna, and Dilfuzaxon Mamasharipovna Karayeva. "Modern programming technologies and their role." интеллектуальный капитал xxi века. 2020.
15. Qodirov, F. "Aholiga tibbiy xizmat ko 'rsatish sohasining kelgusi holatini bashoratlash." Samarqand iqtisodièt va servis instituti (2022).
16. Qodirov, F. "QR-kod texnologiyasi asosida elektron kutubxona tizimini dasturiy va apparat taminotini yaratish." Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Qarshi filiali (2021).
17. Қодиров, Фаррух, and Х. Мухитдинов. "АҲОЛИГА ТИББИЙ ХИЗМАТ КЎРСАТИШДАН ОЛИНГАН ДАРОМАД ВА ХАРАЖАТЛАРНИ БИЗНЕС ИННОВАЦИОН МОДЕЛИ." Raqamli iqtisodiyot va axborot texnologiyalari 2.3 (2022): 136-141.

18. Qodirov, F. "Optimum solutions for the development of medical services in private clinics." Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Qarshi filiali (2022).
19. Qodirov, F. "Қашқадарё ҳудуди аҳолисига хизмат кўрсатиш тармоқлари ва уларга таъсир этувчи омиллар." O ‘zbekiston Qishloq Va Suv xo ‘jaligi” Jurnali (2022).
20. Қодиров, Ф. "Вилоят аҳолисига соғлиқни сақлаш хизматлари кўрсатиш тармоқлари ривожланиш механизмининг статистик таҳлили." Andijon Mashinasozlik Instituti (2022).
21. Қодиров, Ф. "Аҳолига тиббий хизмат кўрсатиш соҳасининг келгуси ҳолатини башоратлаш." Самарқанд иқтисодиѐт ва сервис институти (2022).
22. Қодиров, Фаррух, and Х. Мухитдинов. "АҲОЛИГА ТИББИЙ ХИЗМАТ КЎРСАТИШДАН ОЛИНГАН ДАРОМАД ВА ХАРАЖАТЛАРНИ БИЗНЕС ИННОВАЦИОН МОДЕЛИ." Raqamli iqtisodiyot va axborot texnologiyalari 2.3 (2022): 136-141.
23. Қодиров, Ф. "Қашқадарё вилояти аҳолисига тиббий хизмат кўрсатиш тармоқларини ривожлантиришнинг истиқболлари." o ‘zbekiston qishloq va suv xo ‘jaligi» âà «Agro ilm (2022).
24. Бозорова, Ирина Жуманазаровна. "Создание программного обеспечения электронной библиотечной системы на основе QR-кодовой технологии." Теория и практика современной науки. 2020.
25. Zoxidov, J. B., F. E. Qodirov, and I. J. Bozorova. "QUARTUS II PROJECT CONCEPT AND ITS OPPORTUNITIES AND PROBLEMS." АКТУАЛЬНЫЕ ПРОБЛЕМЫ ТЕХНИЧЕСКОГО И ТЕХНОЛОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИННОВАЦИОННОГО РАЗВИТИЯ. 2019.
26. Маматмурадова, М. У., И. Ж. Бозорова, and Ф. Э. Кодиров. "СОЗДАНИЕ И ЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ И РЕСУРСОВ ЭЛЕКТРОННОГО ОБУЧЕНИЯ В НЕПРЕРЫВНОМ ОБРАЗОВАНИИ." Инновации в технологиях и образовании. 2019.
27. Ergash o’g’li, Qodirov Farrux, and Bozorova Irina Jumanazarovna. "METHODS OF DISPLAYING MAIN MEMORY ON CACHE." Ответственный редактор (2020): 6.