TARMOQ XAVFSIZLIGI. ASOSIY TAHDIDLAR VA HIMOYA CHORALARI

Qodirov Farrux Ergash o'g'li
Shahrisabz davlat pedagogika instituti "Matematika va ta'limda axborot texnologiyasi kafedrasi mudiri, Ilmiy rahbar
Jomurodova Go'zal Abror qizi
Shahrisabz davlat pedagogika instituti matematik va informatika yo'nalishi 2-bosqich talabasi

https://doi.org/10.5281/zenodo.15117525

Annotatsiya. Tarmoq xavfsizligi tarmoqlar, ma'lumotlar va tizimlarni kiber tahdidlardan himoya qilishga mo'ljallangan amaliyotlar, siyosatlar va texnologiyalarni anglatadi. U ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlaydi. Uning ahamiyati ruxsatsiz kirish va ma'lumotlar buzilishining oldini oladi. Korxonalarni moliyaviy yo'qotishlardan va obro'siga putur yetkazishdan himoya qiladi.GDPR, HIPAA va ISO 27001 kabi qoidalarga muvofiqligini ta'minlaydi. Tarmoq xavfsizligiga asosiy tahdidlar. Ma'lumotlarni buzishi yoki o'g'irlashi mumkin bo'lgan zararli dastur. Hisob ma'lumotlarini o'g'irlash uchun ishlatiladigan aldamchi elektron pochta yoki xabarlar. Xizmatlar mavjud bo'lmasligi uchun tarmoqni ortiqcha yuklash. Ma'lumotlarni o'g'irlash yoki o'zgartirish uchun aloqani ushlab turish. Nozik ma'lumotlarga kirish uchun veb-ma'lumotlar bazasi zaifliklaridan foydalanish.Noma'lum dasturiy ta'minot zaifliklaridan foydalanadigan hujumlar. Xodimlar yoki pudratchilar tarmoqqa kirishdan noto'g'ri foydalanish. Himoya choralari:Ko'p faktorli autentifikatsiya (MFA) va rolga asoslangan kirishni boshqarish (RBAC). Ruxsatsiz trafikni bloklash va hujumlarni aniqlash. SSL/TLS va VPN bilan xavfsiz ma'lumotlarni uzatish. Dasturiy ta'minotdagi xavfsizlik bo'shliqlarini yopish. Xodimlarni kiberxavfsizlik bo'yicha eng yaxshi amaliyotlar bo'yicha o'rgatish. SIEM vositalaridan foydalanish va kirish testi. Antivirus dasturini o'rnatish va mobil qurilmalarni himoya qilish. Kiberhujumlar yuz berganda biznes uzluksizligini ta'minlash. Tarmoq xavfsizligi raqamli aktivlarni rivojlanayotgan kibertahdidlardan himoya qilish zarur. Kuchli siyosatlar, ilg'or xavfsizlik vositalari va foydalanuvchi xabardorligining kombinatsiyasi samarali mudofaa strategiyasi uchun juda muhimdir.

Ka'lit so'zlar. Tarmoq xavfsizligi, Kiberhujumlar ,DDOS hujumi, MITM (Man-in-the-Middle) hujumi , Zararli dasturlar ,Viruslar va troyanlar ,Ransomware, Ma'lumotlar o'g'irlanishi, Phishing, Credential stuffing, Firewall (tarmoqlararo ekran) , Intrusion Detection and Prevention Systems (IDPS), End-to-End shifrlash (E2EE), VPN (Virtual Private Network), Ko'p faktorli autentifikatsiya (MFA), Parol xavfsizligi, SIEM (Security Information and Event Management), Regulyar xavfsizlik tekshiruvlari, Monitoring va tahlil, Xavfsizlik protokollari.

Annotation. Network security refers to the practices, policies, and technologies designed to protect networks, data, and systems from cyber threats. It ensures the confidentiality, integrity, and availability of data. Its importance is in preventing unauthorized access and data breaches. It protects businesses from financial losses and reputational damage. It ensures compliance with regulations such as GDPR, HIPAA, and ISO 27001. Key threats to network security. Malware that can compromise or steal data. Spoofed emails or messages used to steal credentials. Overloading the network so that services are unavailable. Interception of connections to steal or modify data. Exploiting web database vulnerabilities to

access sensitive data. Attacks that exploit unknown software vulnerabilities. Misuse of network access by employees or contractors. Protection measures:

Keywords. Network Security, Cyber Attacks, DDOS Attack, MITM (Man-in-the-Middle) Attack, Malware, Viruses and Trojans, Ransomware, Data Theft, Phishing, Credential Stuffing, Firewall (internet screen), Intrusion Detection and Prevention Systems (IDPS), End-to-End Encryption (E2EE), VPN (Virtual Private Network), Multi-Factor Authentication (MFA), Password Security, SIEM (Security Information and Event Management), Regular Security Audits, Monitoring and Analysis, Security Protocols.

Аннотация. Сетевая безопасность — это практики, политики и технологии, предназначенные для защиты сетей, данных и систем от киберугроз. Он обеспечивает конфиденциальность, целостность и доступность данных. Его важность предотвращает несанкционированный доступ и утечку данных. Он защищает предприятия от финансовых потерь и репутационного ущерба. Он обеспечивает соблюдение таких правил, как GDPR, HIPAA и ISO 27001. Основные угрозы сетевой безопасности. Вредоносное программное обеспечение, которое может повредить или украсть данные. Фишинговые электронные письма или сообщения, используемые для кражи учетных данных. Перегрузка сети, из-за которой сервисы становятся недоступными. Перехват с целью кражи или изменения данных. Использование уязвимостей веб-баз данных для доступа к конфиденциальной информации Атаки, использующие неизвестные уязвимости программного обеспечения. Неправомерное использование доступа к сети сотрудниками или подрядчиками. Средства защиты: многофакторная аутентификация (MFA) и управление доступом на основе ролей (RBAC). Блокируйте несанкционированный трафик и обнаруживайте атаки. Безопасная передача данных с помощью SSL/TLS и VPN. Закрытие дыр в безопасности программного обеспечения. Обучайте сотрудников лучшим практикам кибербезопасности. Использование и тестирование на проникновение инструментов SIEM. Установка антивирусного ПО и защита мобильных устройств.

Ключевые слова. Сетевая безопасность, Кибератаки, DDOS-атака, Атака MITM (Человек посередине), Вредоносное ПО, Вирусы и трояны, Программы-вымогатели, Кража данных, Фишинг, Подстановка учетных данных, Межсетевой экран, Системы обнаружения и предотвращения вторжений (IDPS), Сквозное шифрование (E2EE), VPN (виртуальная частная сеть), Многофакторная аутентификация (MFA), Безопасность паролей, SIEM (Информация безопасности и управление событиями), Регулярные проверки безопасности, Мониторинг и анализ, Протоколы безопасности.

Zamonaviy dunyoda axborot texnologiyalari kundalik hayotimizning ajralmas qismiga aylanib bormoqda. Shaxsiy va korporativ ma’lumotlarning xavfsizligi esa tobora dolzarb masalaga aylanmoqda. Tarmoq xavfsizligi tarmoqlar, ma’lumotlar va tizimlarni turli kiber tahdidlardan himoya qilishga mo‘ljallangan amaliyotlar, siyosatlar va texnologiyalar majmuasini anglatadi. Uning asosiy maqsadi — ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashdir.

Tarmoq xavfsizligi – bu tarmoqlar, ma’lumotlar va tizimlarni kiber tahdidlardan himoya qilishga qaratilgan amaliyotlar, siyosatlar va texnologiyalar majmuasidir. Uning asosiy maqsadi ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashdir.Tarmoq xavfsizligini ta’minlash uchun firewall, VPN, shifrlash texnologiyalari, intrusion detection

systems (IDS), ko‘p faktorli autentifikatsiya (MFA) kabi vositalar ishlatiladi. Shu bilan birga, foydalanuvchilarning xabardorligi ham muhim rol o‘ynaydi.

Tarmoq xavfsizligi zamonaviy axborot texnologiyalari muhitida eng muhim masalalardan biri hisoblanadi. Rivojlangan tahdidlarga qarshi samarali kurashish uchun ilg‘or texnologiyalar va xavfsizlik amaliyotlarini qo‘llash zarur. Kiberxavfsizlikni ta’minlash faqat texnik vositalarga emas, balki foydalanuvchilarning xabardorligiga ham bog‘liq. Shu sababli, muntazam treninglar va xavfsizlik siyosatini takomillashtirish muhim hisoblanadi.

Tarmoq xavfsizligiga tahdid soluvchi kiberhujumlar va zararli harakatlar turli shakllarda namoyon bo‘lishi mumkin. Quyida eng keng tarqalgan tahdidlar keltirilgan:Viruslar, troyanlar, josus dasturlar va reklama dasturlari tarmoq va tizimlarga zarar yetkazadi. Foydalanuvchilarga yolg‘on elektron pochta yoki xabarlar yuborilib, login va parollarni o‘g‘irlashga harakat qilinadi. Bank, ijtimoiy tarmoqlar va korporativ tizimlar maqsadli hujum obyektlari bo‘lishi mumkin. Tarmoqlar yoki serverlarga ortiqcha trafik yuborish orqali xizmatlarni ishdan chiqaradi. Veb-saytlar va onlayn xizmatlarning ishlashini vaqtincha yoki doimiy ravishda to‘xtatishi mumkin.Xakerlar bir tizimdan o‘g‘irlangan login-parollarni boshqa tizimlarda sinab ko‘rishadi. Oddiy va takrorlanuvchi parollardan foydalanish xavfni oshiradi.Veb-saytning ma’lumotlar bazasiga zararli SQL buyruqlari yuborish orqali maxfiy ma’lumotlarga noqonuniy kirish. Moliyaviy va shaxsiy ma’lumotlarni o‘g‘irlash ehtimoli yuqori. Tarmoq xavfsizligini ta’minlash uchun quyidagi asosiy himoya choralari qo‘llaniladi: Firewall (Tarmoqlararo ekran) – tarmoqga ruxsatsiz kirishning oldini oladi va zararli trafikni filtrlaydi.Intrusion Detection and Prevention Systems (IDPS) – tarmoqda g‘ayritabiiy faoliyatni kuzatib borish va hujumlarning oldini olish. Virtual Private Network (VPN) – tarmoq orqali uzatilayotgan ma’lumotlarni shifrlash orqali xavfsiz ulanishni ta’minlaydi. End-to-End Encryption (E2EE) – ma’lumotlarning uzatilish jarayonida shifrlanishini ta’minlaydi. Ko‘p faktorli autentifikatsiya (MFA) – foydalanuvchilarning akkauntlariga kirish uchun qo‘shimcha tekshiruv (masalan, SMS yoki autentifikatsiya ilovalari). Raqamli sertifikatlar (SSL/TLS) – veb-sayt va foydalanuvchilar o‘rtasidagi ma’lumotlarni shifrlash orqali himoya qilish. Antivirus va Antimalware dasturlar – zararli dasturlarni aniqlash va yo‘q qilish. Yuklab olinadigan fayllarni skanerlash – zararli dasturlarni oldindan aniqlash uchun xavfsizlik tizimlaridan foydalanish. Kuchli parollar ishlatish – foydalanuvchilar kamida 12 ta belgidan iborat murakkab parollardan foydalanishi kerak. Fishing hujumlaridan ogohlantirish – shubhali elektron pochta va xabarlarga e’tiborli bo‘lish. Xodimlarni xavfsizlik bo‘yicha o‘qitish – kiberxavfsizlik bo‘yicha muntazam treninglar o‘tkazish. SIEM (Security Information and Event Management) – tarmoqda sodir bo‘layotgan barcha harakatlarni kuzatish va tahlil qilish.Xavfsizlik auditi – tarmoq xavfsizlik choralarining samaradorligini tekshirish va takomillashtirish.

Tarmoq xavfsizligini ta’minlash texnologik vositalar, xodimlar xabardorligi va muntazam xavfsizlik monitoringiga bog‘liq. Kiberhujumlardan samarali himoyalanish uchun shifrlash, autentifikatsiya, firewall, antivirus dasturlar va xavfsizlik protokollaridan foydalanish shart.

Foydalanilgan adabiyotlar/Используемая литература/References:

1. Кодиров, Ф. Э., and О. Д. Дониёров. "ЭФФЕКТИВНЫЕ МОДЕЛИ РАЗВИТИЯ МЕДИЦИНСКОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ КАШАКАДЬИНСКОЙ ОБЛАСТИ." Символ науки 7-2 (2022): 15-17.

2. 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.

3. Uzakov, Gulom, et al. "Simulation of a tubular pyrolysis reactor using comsol multiphysics software." International Scientific and Practical Conference Digital and Information Technologies in Economics and Management. Cham: Springer Nature Switzerland, 2023.

4. Қодиров, Ф. "ҲУДУДЛАРДА ТИББИЙ ХИЗМАТЛАРНИ ДАСТУРИЙ ПАКЕТЛАР ЁРДАМИДА ЭЛЕКТРОН ТИББИЙ БАЗАСИНИ ЯРАТИШ." O'zbekiston Respublikasi Oliy Va o'rta Maxsus ta'lim Vazirligi Namangan Muhandislik-Qurilish Instituti (2022).

5. 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.

6. Bozorova, Irina Jumanazarovna, and Dilfuzaxon Mamasharipovna Karayeva. "Modern programming technologies and their role." интеллектуальный капитал xxi века. 2020.

7. 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.

8. Qodirov, Farrux, and Muxlisa Mavlonova. "O'ZBEKISTONDA ZIYORATGOH VA QADAMJOLAR, TURIZM XIZMATLARINI JADAL RIVOJLANTIRISH ISTIQBOLLARI." YANGI O 'ZBEKISTONDA MILLIY TURIZM ISTIQBOLLARI 1.01 (2024).

9. Qodirov, F., N. Sirojev, and S. Negmatova. "FEATURES OF THE ANDROID STUDIO SOFTWARE PACKAGE." Академические исследования в современной науке 2.17 (2023): 130-146.

10. Қодиров, Ф. Э., et al. "ДЛЯ ПРОВЕРКИ МОДЕЛЕЙ АДЕКВАТНОСТИ, ЧУВСТВИТЕЛЬНОСТЬ И СОПРОТИВЛЕНИЯ." ИНТЕГРАЦИЯ НАУКИ, ОБЩЕСТВА, ПРОИЗВОДСТВА И ПРОМЫШЛЕННОСТИ. 2019.11. Qodirov, F. E., D. A. Akbarova, and S. H. Shokirov. "SOFTWARE FOR WORKING WITH COMPUTER GRAPHICS AND THEIR TASKS. APPLICATION OF DIGITAL IMAGE PROCESSING FIELDS." (2021): 57-58.

11. Jumanazarovna, Bozorova Irina, and Kodirov Farruh Ergash O'G'Li. "Principle of electrocardiographic work and its role in modern medicine." Вопросы науки и образования 15 (99) (2020): 31-36.

12. Kodirov, F. E., and J. E. Nematov. "BASIC TECHNOLOGY AND SERVICE MANAGEMENTMULTISERVICE NETWORKS." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 214.

13. Қодиров, Ф. Э., and Ж. Э. Нематов. "РАЗВИТИЕ ЛОКАЛЬНОЙ СЕТИ НА ОСНОВЕ ТЕХНОЛОГИИ GPON." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 288.

14. Кодиров, Ф. Э., and М. У. Маматмурадова. "РАЗРАБОТКА ЦИФРОВОЙ ПРОГРАММЫ ШИФРОВАНИЯ И ВНЕДРЕНИЕ В ПРАКТИКУ." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 275.

15. Абдирасулов, Ж. У., and Ф. Э. Кодиров. "ЭФФЕКТИВНОСТЬ ANGULAR JS ДЛЯ

СОЗДАНИЯ ДИНАМИЧЕСКИХ ВЕБ-САЙТОВ И ОПТИМИЗАЦИИ ИХ ПРОИЗВОДИТЕЛЬНОСТИ." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 228.

16. Qodirov, F. E., J. B. Zohidov, and H. I. Karamatova. "ADVANTAGES OF PROGRAMMING LANGUAGES JAVASCRIPT, JAVA AND PYTHON." МОДЕЛИРОВАНИЕ И АНАЛИЗ СЛОЖНЫХ ТЕХНИЧЕСКИХ И ТЕХНОЛОГИЧЕСКИХ СИСТЕМ. 2019.

17. Qodirov, F. E., J. U. Abdirasulov, and J. E. Nematov. "FORMING GOVERNMENT AGENCY WEBSITES WITH WORDPRESS CONTENT MANAGEMENT SYSTEM." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 219.

18. Турдиев, У. К., and Ф. Э. Кодиров. "Задача Коши Для Одномерной Системы Уравнений Типа Бюргерса Возникающей В Двухскоростной Гидродинамике." Инновации в технологиях и образовании: сб. ст. участников XI Между (2018): 349.

19. Qodirov, F. E. "Methodological aspects and importance of development of medical services through econometric modeling and forecasting options." academy. uz/index. php/yo.