

исследования актуальные проблемы и развитие тенденции: решения и перспективы, 1(1), 215–217. извлечено от <https://inlibrary.uz/index.php/zitdmrt/article/view/5164>

13. Zhomurodov, D. ., Ulashev, A. ., & Tozhiyev, A. (2023). THE SYSTEM FOR DETERMINING THE QUALIFICATIONS OF INDUSTRY EXPERTS. Евразийский журнал академических исследований, 3(4 Special Issue), 280–289. извлечено от <https://in-academy.uz/index.php/ejar/article/view/14519>

14. Xolbutayevich T. O., Mamasoliyevich J. D. O‘QUV JARAYONIDA TO‘LDIRILGAN REALLIK TEXNOLOGIYALARIDAN FOYDALANISH //International Journal of Contemporary Scientific and Technical Research. – 2022. – С. 334-338.s

15. Баратов Ж.Р. (2021). ИСПОЛЬЗОВАНИЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА ПРИ ВЫПОЛНЕНИИ ДИАГНОСТИКИ. Экономика и социум, (3-1 (82)), 458-464.

16. Alisher T., Asrorjon U. APPLICATION AND RESULTS OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN EDUCATION //International Journal of Contemporary Scientific and Technical Research. – 2023. – С. 28-30.

17. Norqo‘ziyev , Q. (2023). MOBIL ROBOTLAR UCHUN YO‘LNI REJALASHTIRISH ALGORITMI. Research and Implementation. извлечено от <https://fer-teach.uz/index.php/rai/article/view/746>

18. Rustamov Maxammadi Jabborovich, Irgasheva Umida Abdimal kizi, and Iskandarov Azizbek Ilxom o‘g‘li. “BIR JINSLI BO‘LMAGAN ISSIQLIK TARQALISH TENGLAMASINI FURYE (O‘ZGARUVCHILARNI AJIRATISH) USULI YORDAMIDA YECHISH”. RESEARCH AND EDUCATION, vol. 2, no. 2, Feb. 2023, pp. 79-84, <https://researchedu.org/index.php/re/article/view/1796>.

19. Maxkamov Shohruh Sarvar o‘g‘li “MA’LUMOTLAR BAZASI (MB) VA MA’LUMOTLAR BAZASINI BOSHQARISH TIZIMI (MBBT)NING NAZARIY ASOSLARI” KOMPYUTER ILMLARI VA MUHANDISLIK TEXNOLOGIYALARI mavzusidagi Xalqaro ilmiy-texnik anjuman materiallari 13.10.2023. 90-94 bet.

WEB ILOVALARDA AUTENTIFIKATSIYA DASTURIY VOSITALARINI ISHLAB CHIQISH VA QO‘LLASH

t.f.f.d., dots. Abdumalikov Akmaljon Abduxoliq o‘g‘li

O‘zbekiston Milliy Universitetining Jizzax filiali

Gulmurodova Dinora Akram qizi

O‘zbekiston Milliy Universitetining Jizzax filiali magistranti

akmalabdumalikov6@gmail.com

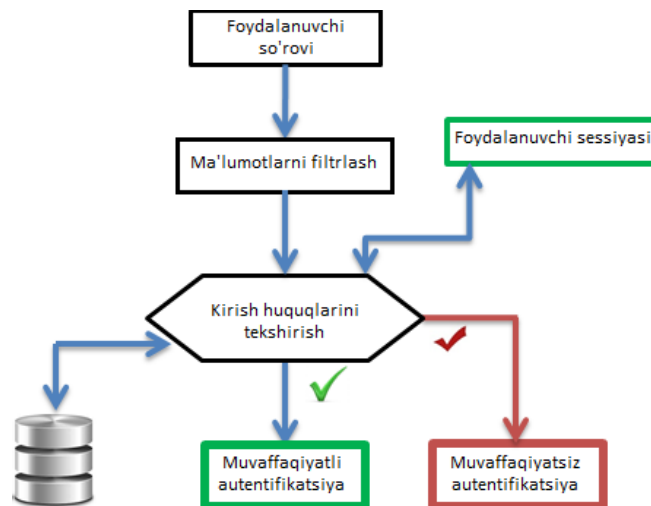
Hozirgi kunda dunyo miqyosida axborot texnologiyalarining jadal sur‘atlar bilan rivojlanib borishi ko‘plab qulayliklar bilan bir qatorda yangi muammolarni o‘rtaga qo‘ymoqda. Avtomatlashtirilgan axborot tizimlarida va telekommunikatsiya tizimlarida aylanayotgan axborotlar hamda ularning xavfsizligiga bo‘ladigan

tahdidlarning soni bugunga kelib keskin darajada oshib ketdi. Ushbu muammoli xolatlar hozirda nafaqat Respublikamizda balki butun dunyoda axborot texnologiyalari sohasining texnik va dasturiy majmualari kirib borgan xar bir tashkilot va korxonaning asosiy bo'g'inlaridan biriga aylangan.

Tizimga kirgan foydalanuvchi tomonidan yuborilgan so'rovlar IS avtorizatsiya qilish tartib-qoidalariga muvofiq qayta ishlanadi. 1.-rasmda veb-ga asoslangan axborot tizimlarida foydalanuvchini avtorizatsiya qilish uchun ishlatiladigan algoritmi ko'rsatilgan.

Quyidagi algoritmi taklif etiladi:

1. Foydalanuvchi so'rovi yuboriladi.
2. Yuborilgan so'rov filtrlashdan o'tadi. Filtrlash axborot tizimi talablari va spetsifikatsiyalariga muvofiq amalga oshiriladi.
3. Kirish huquqlari tekshiriladi. Agar tekshirish muvaffaqiyatli bo'lsa, foydalanuvchi tizimga kiradi, aks holda kirish taqiqlanadi.
4. Kirish taqiqlangandan keyin markazlashgan monitoring tizimlariga tashqi tomondan kirishga urunganligi holati yuzasidan axborot boradi.



1-rasm. Veb-axborot tizimi uchun avtorizatsiya algoritmi

Autentifikatsiya qilingan shifrlash zarurati alohida konfidensiallik va autentifikatsiya bloki shifrining ishlash rejimlarini xavfsiz tarzda birlashtirish xatoga moyil va qiyin bo'lishi mumkinligini kuzatish natijasida paydo bo'ldi. Bu noto'g'ri amalga oshirish yoki autentifikatsiyaning yo'qligi (shu jumladan SSL/TLS) tufayli ishlab chiqarish protokollari va ilovalariga kiritilgan bir qator amaliy hujumlar bilan tasdiqlangan. Taxminan 2000-yilda standartlashtirish rejimlari tushunchasi atrofida to'g'ri amalga oshirilishini ta'minlaydigan bir qator harakatlar rivojlandi. Xususan, 2000 -yilda Charanjit Jutla'ning yaxlitlikdan xabardor CBC va yaxlitlikni biladigan parallelizable , IAPM, rejimlar nashr etilishi mumkin bo'lgan xavfsiz rejimlarga kuchli qiziqish uyg'otdi. Olti xil autentifikatsiya qilingan shifrlash usullari (masalan, ofset kod kitobi rejimi 2.0, OCB 2.0; Key Wrap; CBC-MAC , CCM bilan hisoblagich; shifrlash, keyin autentifikatsiya qilish, keyin tarjima qilish , EAX; shifrlash-keyin-MAC, EtM; va Galois/counter rejimi, GCM) ISO/IEC 19772:2009 da

standartlashtirilgan. NIST so'roviga javoban ko'proq autentifikatsiyalangan shifrlash usullari ishlab chiqilgan.

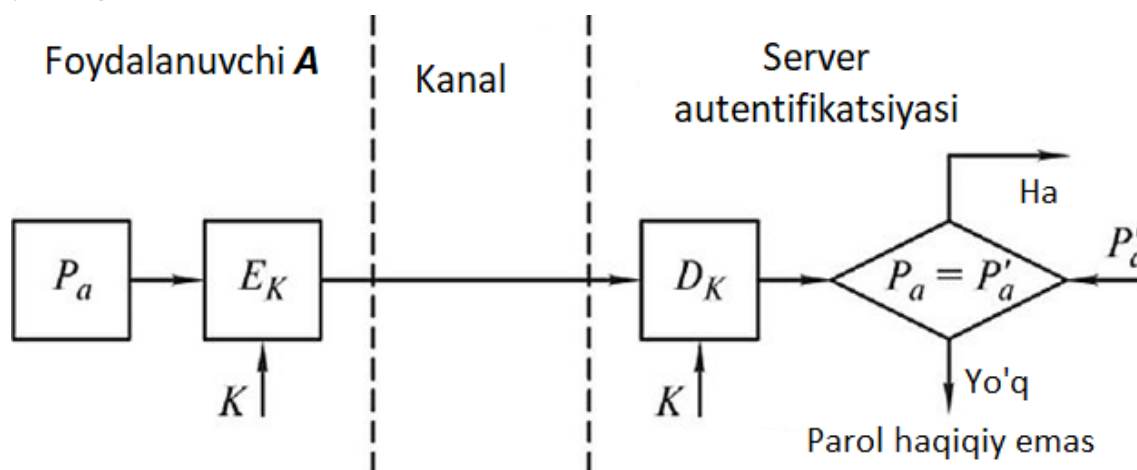
Autentifikatsiyaning keng tarqalgan sxemalaridan biri oddiy autentifikatsiya bo'lib, u an'anaviy qayta ishlatiladigan parollardan foydalanish va qayta ishlash vositalarini bir vaqtning o'zida kelishib olishga asoslangan.

"Yagona tizimga kirish" ning asosiy printsipli foydalanuvchining barcha tarmoq resurslariga kirishi uchun bir martalik autentifikatsiya protsedurasidan o'tishi etarliligini nazarda tutadi.

Parol va foydalanuvchi identifikatorini o'tkazish quyidagi usullar bilan amalga oshirilishi mumkin:

1) shifrlanmagan shaklda; masalan, PAP (Password Authentication Protocol) parolni autentifikatsiya qilish protokoliga muvofiq, parollar aloqa liniyasi orqali ochiq, himoyalangan shaklda uzatiladi;

2) himoyalangan; barcha uzatilgan ma'lumotlar (foydalanuvchi identifikatori va parol, tasodifiy raqam va vaqt belgilari) shifrlash yoki bir tomonlama funksiya bilan himoyalangan bo'ladi.



2-rasm. Parolga asoslangan oddiy autentifikatsiya

Kiberjinoyatlardan yo'qotishlarni kamaytirish uchun foydalanuvchilarning xavfsizligini ta'minlash usullarini takomillashtirish zarur. Hozirgi vaqtda kuchli xavfsizlik strategiyasini amalga oshirishga yordam beradigan ko'plab autentifikatsiya va avtorizatsiya usullari mavjud, Ular orasida ko'plab mutaxassislar tokenga asoslangan avtorizatsiyani eng yaxshisi deb ajratib ko'rsatishadi.

Ushbu tizimlarni biometrik identifikatsiya tizimlari, masalan, haydovchining yuzini aniqlash tizimlari va biometrik vaqtni kuzatish tizimlari bilan aralashtirib yubormaslik kerak. Biometrik autentifikatsiya tizimlari passiv emas, balki faol rejimda ishlaydi va deyarli har doim avtorizatsiyani o'z ichiga oladi. Ushbu tizimlar avtorizatsiya tizimlari bilan bir xil bo'lmasa-da, ular ko'pincha kombinatsiyalangan holda qo'llaniladi (masalan, barmoq izini tekshirish bilan eshik qulflarida).

Biometrik autentifikatsiya yordamida ko'zning to'r pardasi ham, barmoq izi ham maxfiy foydalanuvchi ma'lumotlari bo'lib xizmat qilishi mumkin, Ushbu biometrik tasvirlar har bir foydalanuvchi uchun o'ziga xos bo'lib, axborotga kirishni yuqori darajada himoya qiladi. Oldindan tuzilgan protokollarga ko'ra, foydalanuvchining

biometrik namunalari ma'lumotlar bazasida ro'yxatga olinadi, "Biometriya" atamasi - biometrika ingliz tilidagi adabiyotlarda biometrikaning yangi tarmog'i sifatida paydo bo'lib, u insonning shaxsiy jismoniy va xulq-atvor xususiyatlarini o'lchash usullarini va ulardan identifikatsiya yoki autentifikatsiya qilish uchun foydalanish usullarini ifodalovchi bilim sohasini qamrab oladi.

Foydalanilgan adabiyotlar ro'yxati:

1. O'zbekiston Respublikasini rivojlantirish bo'yicha taraqqiyot strategiyasi.
2. Archana, B. S., Chandrashekar, A., Bangi, A. G., Sanjana, B. M. and Akram, S. (2017) Survey on us-able and secure two-factor authentication.
3. Tatli, E. I. (2015) Cracking More Password Hashes With Patterns.
4. Rouse, M. (2015). knowledge-based authentication (KBA). Available: <https://searchsecurity.techtarget.com/definition/knowledge-based-authentication>. Last accessed 7th November 2019.
5. Elets News Network. (2018). From July 1, authenticate Aadhaar through face recognition. Available: <https://egov.eletsonline.com/2018/01/from-july-1-authenticate-aadhaar-through-face-recognition/>. Last accessed 9th November 2019.
6. Muppidi, S. (2017) Companies Need More Than Two-Factor Authentication to Keep Users Safe. Harvard Business Review Digital Articles, 2-4.
7. Hayot faoliyati xavfsizligi. G'.Yo.Yormatov, O.R.Yuldashev, A.L.Hamrayeva, Toshkent-2018.
8. Olim Turakulov, Oybek Kayumov, & Nazokat Kayumova. (2023). MANAGEMENT OF THE INTELLECTUAL RESOURCES OF THE ENTERPRISE BASED ON ARTIFICIAL INTELLIGENCE DURING THE DEVELOPMENT OF THE DIGITAL ECONOMY IN UZBEKISTAN. International Journal of Contemporary Scientific and Technical Research, (Special Issue), 145–154. Retrieved from <https://journal.jbnuu.uz/index.php/ijcstr/article/view/338>
9. Xolbutayevich T. O., Mamasoliyevich J. D. O'QUV JARAYONIDA TO'LDIRILGAN REALLIK TEXNOLOGIYALARIDAN FOYDALANISH //International Journal of Contemporary Scientific and Technical Research. – 2022. – C. 334-338.s
10. Oybek Kayumov, Nazokat Kayumova, & Aliyeva Rayxona, Yo'ldosheva Madina. (2023). THE STRATEGIC SIGNIFICANCE OF HUMAN RESOURCE MANAGEMENT IN UZBEKISTAN ENTERPRISES ON THE BASIS OF ARTIFICIAL INTELLIGENCE. International Journal of Contemporary Scientific and Technical Research, 268–272. Retrieved from <https://journal.jbnuu.uz/index.php/ijcstr/article/view/588>
11. Тоджиев, М., Улугмуродов, Ш., & Ширинбоев, Р. (2022). Tasvirlar sifatini yaxshilashning chiziqli kontrast usuli. Современные инновационные исследования актуальные проблемы и развитие тенденции: решения и перспективы, 1(1), 215–217. извлечено от <https://inlibrary.uz/index.php/zitdmrt/article/view/5164>
12. Maxkamov Shohruh Sarvar o'g'li "MA'LUMOTLAR BAZASI (MB) VA MA'LUMOTLAR BAZASINI BOSHQARISH TIZIMI (MBBT)NING NAZARIY ASOSLARI" KOMPYUTER ILMLARI VA MUHANDISLIK

TEKNOLOGIYALARI mavzusidagi Xalqaro ilmiy-texnik anjuman materiallari 13.10.2023. 90-94 bet.

13. Ахатов, А., Улугмуродов, Ш. А., & Таджиев, . М. . (2022). Аудио для фонетической сегментации и речи для речи. Современные инновационные исследования актуальные проблемы и развитие тенденции: решения и перспективы, 1(1), 146–149. извлечено от <https://inlibrary.uz/index.php/zitdmrt/article/view/5273>

14. Баратов Ж.Р. (2021). ИСПОЛЬЗОВАНИЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА ПРИ ВЫПОЛНЕНИИ ДИАГНОСТИКИ. Экономика и социум, (3-1 (82)), 458-464.

15. Alisher T., Asrorjon U. APPLICATION AND RESULTS OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN EDUCATION //International Journal of Contemporary Scientific and Technical Research. – 2023. – С. 28-30.

16. Norqo'ziyev , Q. (2023). MOBIL ROBOTLAR UCHUN YO'LNI REJALASHTIRISH ALGORITMI. Research and Implementation. извлечено от <https://fer-teach.uz/index.php/rai/article/view/746>

17. Rustamov Maxammadi Jabborovich, Irgasheva Umida Abdimal kizi, and Iskandarov Azizbek Ilxom o'g'li. "BIR JINSI BO'LMAGAN ISSIQLIK TARQALISH TENGLAMASINI FURYE (O'ZGARUVCHILARNI AJIRATISH) USULI YORDAMIDA YECHISH". RESEARCH AND EDUCATION, vol. 2, no. 2, Feb. 2023, pp. 79-84, <https://researchedu.org/index.php/re/article/view/1796>.

18. Zhomurodov, D. ., Ulashev, A. ., & Tozhiyev, A. (2023). THE SYSTEM FOR DETERMINING THE QUALIFICATIONS OF INDUSTRY EXPERTS. Евразийский журнал академических исследований, 3(4 Special Issue), 280–289. извлечено от <https://in-academy.uz/index.php/ejar/article/view/14519>

19. Abduraxmanov Ravshan Anarbayevich, Parmonov Abdutolib Abdurahob o'g'li. (2022). BO'LG'USI MUTAXASSISNING SHAXS SIFATIDAGI QOBILIYATINI OSHRISHDA PEDAGOGIK VA AXBOROT TEKNOLOGIYALARINING O'RNI. International Journal of Contemporary Scientific and Technical Research, 1(2), 673–676. Retrieved from <https://journal.jbnuu.uz/index.php/ijcstr/article/view/305>.

20. Maxamadaliyevich S. B. YER TUZISH LOYIHALARIDA GEOAXBOROT TEKNOLOGIYALARINING AGROLANDSHAFT ASOSLARI //International Journal of Contemporary Scientific and Technical Research. – 2022. – С. 197-200.

21. Akhatov A., Saidaliyev B., Quvondikov J. Simulation modeling for optimizing the crops structure in the conditions of the Jizzakh region //2021 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2021. – С. 1-4.

22. Ахатов А., Сайдалиев Б. Qishloq xo'jalik ekinlarining avtomatlashgan tasnifini yaratishda yuqori aniqlikdagi kosmik tasvir materiallarini qo'llanish tajribasi //Современные инновационные исследования актуальные проблемы и развитие тенденции: решения и перспективы. – 2022. – Т. 1. – №. 1. – С. 144-146.

23. Hayot faoliyati xavfsizligi. M.X.Tojiyev, I.Nigmatov, Toshkent-2015

24. <https://digitalcommons.unf.edu>

25. <https://dataprot.net/statistics/two-factor-authentication-statistics>
26. <https://www.techtarget.com>
27. <https://www.okta.com>

BUL ALGEBRASI FUNKSIYALARI SISTEMASINI POST TEOREMASI ASOSIDA TO'LIQLIKKA TEKSHIRISH

Xolmatov Javlon Yusupovich

O'zbekiston Milliy universiteti Jizzax filiali

Xudoyshukurova Ruxsora Shuxrat qizi,

Ibadullayev Shohruh Sherali o'g'li

O'zbekiston Milliy universiteti Jizzax filiali talabalari

javlonolmatov@jbnuu.uz

Annotatsiya: Maqolada to'liq funksiyalar sistemasiga ta'rif va Post teoremasi yordamida funksiyalar sistemasini to'liqlikka tekshirishning chinlik jadvali asosida yaratilgan yangi algoritmlari qo'llanilgan. Murakkablik darajasi o'rtacha bo'lgan misol shu algoritmlar asosida yechilgan va natijalari olingan.

Kalit so'zlar: Funksiyalar sistemasining to'liqligi, yopiq sinflar, Post teoremasi, Post jadvali, P_0 - nol saqllovchi funksiyalar sinfi, P_1 - bir saqllovchi funksiyalar sinfi, M - monoton funksiyalar sinfi, S - o'z-oziga ikki taraflama-dual funksiya sinfi, L - chiziqli funksiyalar sinfi.

Kirish

Mantiq algebrasining $F=(f_1, f_2, \dots, f_n)$ funksiyalar sistemasi berilgan bo'lsin.

Agar mantiq algebrasining istalgan funksiyasini $F=(f_1, f_2, \dots, f_n)$ sistemadagi funksiyalar superpozitsiyasi orqali ifodalash mumkin bo'lsa, u holda F sistema to'liq funksiyalar sistemasi deb ataladi.

Mantiq algebrasida hammasi bo'lib beshta maksimal funksional yopiq sinf mavjud. Bular quyidagilardir: P_0 - nol saqllovchi, P_1 - bir saqllovchi, M - monoton, S - o'z-o'ziga ikki taraflama, L - chiziqli.

Post teoremasi yordamida funksiyalar sistemasi to'liqlikka tekshiriladi.

Asosiy qism

Amerikalik olim E.Post tomonidan funksiyalar sistemasi to'liqligining yetarli va zarur shartlari topilgan.

Post teoremasi. $F = \{f_1, f_2, f_3, \dots, f_n\}$ funksiyalar sistemasi to'liq bo'lishi uchun bu sistemada P_0, P_1, M, S, L maksimal funksional yopiq sinflarning har biriga kirmaydigan kamida bitta funksiya mavjud bo'lishi yetarli va zarur (ya'ni $F = \{f_1, f_2, f_3, \dots, f_n\}$ funksiyalar sistemasi faqat P_0, P_1, M, S, L maksimal funksional yopiq sinflardan birortasining ham qism to'plami bo'lmaganda va faqat shundagina to'liq sistema bo'ladi).

Post jadvali