**TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.13/30.12.2019.T.07.02 RAQAMLI ILMIY KENGASH**

**TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

**IMAMALIYEV AYBEK TURAPBAYEVICH**

# FOYDALANUVCHILARNI BIR MARTALIK PAROLLARGA ASOSLANGAN AUTENTIFIKATSIYALASH USULLARI VA ALGORITMLARI

**05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi**

**TEXNIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI AVTOREFERATI**

**Toshkent-2024**

**UDK: 004.056.53**

**Texnika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati mundarijasi**

**Оглавление автореферата диссертации доктора философии (PhD) по техническим наукам**

**Contents of dissertation abstract of the doctor of philosophy (PhD) on technical sciences**

**TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.13/30.12.2019.T.07.02 RAQAMLI ILMIY KENGASH**

**TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

**IMAMALIYEV AYBEK TURAPBAYEVICH**

# FOYDALANUVCHILARNI BIR MARTALIK PAROLLARGA ASOSLANGAN AUTENTIFIKATSIYALASH USULLARI VA ALGORITMLARI

**05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi**

**TEXNIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI AVTOREFERATI**

**Toshkent-2024**

**Texnika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida B2024.1.PhD/T4416 raqam bilan ro‘yxatga olingan.**

Dissertatsiya Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (rezume)) Ilmiy kengash veb-sahifasida (www.tuit.uz) va “Ziyonet” Axborot ta’lim portalida (www.ziyonet.uz) joylashtirilgan.

| | |
|---|---|
| **Ilmiy rahbar:** | **Xudoykulov Zarifjon Turakulovich**<br>texnika fanlari bo‘yicha falsafa doktori (PhD), dotsent |
| **Rasmiy opponentlar:** | **Juraev Gayrat Umarovich**<br>fizika-matematika fanlari doktori, professor |
| | **Normatov Sherbek Baxtiyarovich**<br>texnika fanlari bo‘yicha falsafa doktori (PhD), dotsent |
| **Yetakchi tashkilot:** | **“UNICON.UZ” Fan-texnika va marketing tadqiqotlari markazi MCHJ** |

Dissertatsiya himoyasi Toshkent axborot texnologiyalari universiteti huzuridagi DSc.13/30.12.2019.T.07.02 raqamli Ilmiy kengashning 2024-yil “___” _____da soat _____ dagi majlisida bo‘lib o‘tadi. (Manzil: 100084, Toshkent shahri, Amir Temur ko‘chasi, 108-uy.Tel.: (99871) 238-64-43, e-mail: tuit@tuit.uz).

Dissertatsiya bilan Toshkent axborot texnologiyalari universitetining Axborot-resurs markazida tanishish mumkin ( ____ raqam bilan ro‘yxatga olingan). (Manzil: 100084, Toshkent shahri, Amir Temur ko‘chasi, 108-uy. Tel.: (99871) 238-64-43).

Dissertatsiya avtoreferati 2024-yil “___” _____ da tarqatildi.

(2024-yil “___” _____ dagi ___ raqamli reestr bayonnomasi.)

**B.Sh. Maxkamov**
Ilmiy darajalar beruvchi ilmiy kengash raisi, i.f.d., professor

**M.S. Saitkamolov**
Ilmiy darajalar beruvchi ilmiy kengash ilmiy kotibi, i.f.d., dotsent

**S.K. Ganiyev**
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi ilmiy seminar raisi, t.f.d., professor

## KIRISH (falsafa doktori (PhD) dissertatsiyasining annotatsiyasi)

**Dissertatsiya mavzusining dolzarbligi va zarurati.** Jahonda yildan-yilga tizimdagi kamchiliklar va ijtimoiy injineriyaga asoslangan kiberhujumlar salmog‘i ortib bormoqda. Ularning aksariyati autentifikatsiya mexanizmlari, jumladan, parolga asoslangan autentifikatsiya, bilan aloqador kamchiliklar va zaifliklar asosida amalga oshmoqda. Xususan, National Cyber Security Alliance ma’lumotiga ko‘ra, “buzib kirishga aloqador holatlarning 81% o‘g‘irlangan yoki zaif parollar bilan bog‘liq”[1]. Bu esa parolga asoslangan autentifikatsiya usulidan voz kechishning imkonsizligini inobatga olgan holda, ulardagi kamchiliklarni bartaraf etish, xususan, parolga qo‘shimcha ravishda ikkinchi faktorlardan foydalanishning yangi usul va vositalarini yaratishni taqozo etmoqda. Hozirda AQSH, Rossiya Federatsiyasi va Xitoy Xalq Respublikasi kabi davlatlarda parolga asoslangan autentifikatsiya usullariga qo‘shimcha ravishda foydalaniluvchi bir martalik parollarni generatsiyalovchi tokenlar, smart kartalar va boshqa vositalarni yaratishda alohida e’tibor berilmoqda.

Jahonda parolga asoslangan autentifikatsiya usuliga qo‘shimcha ravishda bir qancha faktorlardan foydalanish tizim xavfsizligini oshirishga imkon bermoqda. Xususan, biometrik parametrlardan, parollarni hosil qiluvchi yoki turli hisoblashlarni amalga oshirib beruvchi tokenlardan, smart kartalardan keng foydalanilmoqda. Biroq, ushbu vositalarning qimmatligi yoki xavfsizlik talablarini to‘laqonli bajarmasligi natijasida ko‘plab kiberjinoyatlar amalga oshirilmoqda. Shu sababli, parolga qo‘shimcha ravishda foydalaniluvchi bir martalik parollarni hosil qilishning dasturiy va apparat tokenlarini yaratishga, ularga asoslangan autentifikatsiya usullarini yaratishga qaratilgan ilmiy-amaliy tadqiqotlarga alohida e’tibor qaratish zarur hisoblanadi.

2023-yil 20-dekabr kuni O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoyev raisligida o‘tkazgan yig‘ilishida IT sohasi rivojlangani sari kiberxavfsizlikni ta’minlash masalasining dolzarbligi oshayotganini ta’kidlab o‘tildi. Shuningdek, ushbu yig‘ilishda O‘zbekistonda 2023-yilning 11 oyida 5,5 mingta kiberjinoyat sodir etilganligi, shundan, 70 foizi bank kartalari bilan bog‘liq firibgarlik va o‘g‘rilik jinoyatlari ekanligini aytib o‘tilgan[2]. Respublikamizda kiberxavfsizlik sohasida jinoyatlarni oldini olish, fuqarolarni kiberjinoyatlar bo‘yicha bilimlarini shakllantirishga qaratilgan keng qamrovli chora tadbirlar amalga oshirilmoqda. Jumladan, 2022-2026-yillarga mo‘ljallangan yangi O‘zbekistonning taraqqiyot strategiyasida “Kiberjinoyatchilikning oldini olish tizimini yaratish” vazifasi qo‘yilgan bo‘lib, buni amalga oshirishda “2023 – 2026 – yillarga mo‘ljallangan O‘zbekiston Respublikasining kiberxavfsizlik strategiyasini ishlab chiqish”, “Kiberjinoyatchilik uchun jinoiy javobgarlikni qayta ko‘rib chiqish”, “Axborot maydonidagi kiberhujum va tahdidlarni monitoring qilish tizimini yanada takomillashtirish” kabi mexanizmlar belgilab qo‘yilgan. Ushbu vazifalarni

---

[1] National Cyber Security Alliance tomonidan berilgan ma’lumot. Sayt: https://logmeonce.com/resources/compromised-passwords-are-responsible-for-what-percentage-of-breaches/

[2] O‘zbekiston Respublikasi Prezidentining 2023 yil 20 dekabr kuni o‘tkazgan videoselektor yig‘ilishi. [Sayt]: https://www.gazeta.uz/oz/2023/12/21/cyber-crime/ (murojaat vaqti:30.05.2024)

amalga oshirishda autentifikatsiya muammosini hal etish, xususan, foydalanuvchilarni autentifikatsiyalashning samarali va xavfsiz usullarini ishlab chiqish muhim hisoblanadi.

O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi 2022-yil 15-apreldagi O‘RQ-764-son Qonuni, O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60-son “2022 – 2026 yillarga mo‘ljallangan yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi, 2023-yil 11-sentabrdagi PF-158-son ““O‘zbekiston – 2030” strategiyasi to‘g‘risida”gi, 2018-yil 14-martdagi PF-5379-son “O‘zbekiston Respublikasining davlat xavfsizligi tizimini takomillashtirish chora-tadbirlari to‘g‘risida”gi va 2018-yil 19-fevraldagi PF-5349-son “Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi Farmonlari, 2007-yil 3-apreldagi PQ-614-son “O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to‘g‘risida”gi Qarori hamda mazkur sohaga tegishli boshqa meyoriy-huquqiy hujjatlarida belgilangan vazifalarni amalga oshirishga mazkur dissertatsiya ishi muayyan darajada xizmat qiladi.

**Tadqiqotning respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi.** Mazkur tadqiqot respublika fan va texnologiyalar rivojlanishining IV. “Axborotlashtirish va axborot-kommunikatsiya texnologiyalarini rivojlantirish” ustuvor yo‘nalishi doirasida bajarilgan.

**Muammoning o‘rganilganlik darajasi.** Foydalanuvchilarni autentifikatsiyalash usullari va tizimlarini tadqiq etish, yaratish, takomillashtirish va ularga bo‘ladigan hujumlarni tahlil etish, jumladan, ikkinchi faktorga asoslangan autentifikatsiya usullari va vositalarini tadqiq etish, bir martalik parollarni generatsiyalash borasida X. Wang, W. Zheng, E. De Cristofaro, C. Katsini, D.I. Golenko va boshqa chet ellik olimlar tomonidan ilmiy-tadqiqot ishlari olib borilgan[3].

O‘zbekistonda S.K.Ganiyev, M.M.Karimov, D.Ya. Irgasheva, K.A.Tashev, O.P.Axmedova, Z.T.Xudoykulov va J.T.Arziyevalar boshchiligidagi ilmiy jamoalar tomonidan foydalanuvchilarni autentifikatsiyalash masalasiga, axborotni himoyalashning kriptografik mexanizmlariga oid ko‘plab tadqiqot ishlari olib borilgan[4].

---

[3] Wang X. et al. Attacks and defenses in user authentication systems: A survey. Journal of Network and Computer Applications. – 2021. – T. 188. – C. 103080. //Zheng, W., Jia, C., 2017. CombinedPWD: a new password authentication mechanism using separators between keystrokes. In: 2017 13th International Conference on Computational Intelligence and Security (CIS), Hong Kong, China, pp. 557 – 560. //De Cristofaro E. et al. A comparative usability study of two-factor authentication. arXiv preprint arXiv: 1309.5344. – 2013. //Katsini, C.; Belk, M.; Fidas, C.; Avouris, N.; Samaras, G. Security and Usability in Knowledge-based User Authentication: A Review. In Proceedings of the 20th Pan-Hellenic Conference on Informatics, Patras, Greece, 10–12 November 2016; ACM: New York, NY, USA, 2016; p. 63. //Д. И. Голенко Моделирование и статистический анализ псевдослучайных чисел на электронных вычислительных машинах. – Издательство" Наука", Главная редакция физико-математической литературы, 1965.

[4] С.К. Ганиев, А.Т. Имамалиев. Псевдотасодифий кетма-кетлик генератори асосида масофадан фойдаланувчининг аутентификаторини яратиш. “ТАТУ хабарлари” ilmiy-texnika va axborot-tahliliy jurnali. № 2(58)/2021. Toshkent-2021. -Б. 150-159. // M.M. Karimov, K.A. Tashev, J. Arziyeva, A.A. Abdurakhmanov, A.T. Imamliyev. About one of the authentication methods // “TATU xabarlari” ilmiy-texnika va axborot-tahliliy jurnali. № 3/2013. Toshkent-2013. -P. 5-12 K.A. // A.F. Verlan, M.M. Karimov, K.A. Tashev, A.T. Imamaliyev. Method of Authentication on Based Password Generators // 3 rd international conference on “Application of Information and Communication Technology and Statistics in Economy and Education”. Bulgaria, Sofia-2013. -

Shuning bilan bir qatorda, foydalanuvchilarning haqiqiyligini tekshirishda qo‘shimcha faktor sifatida qo‘llanilayotgan bir martalik parollarni hosil qilish usullari va vositalarini, ularga asoslangan foydalanuvchilarni autentifikatsiyalashning xavfsiz va samarali usullarini ishlab chiqish masalalariga yetarlicha e’tibor qaratilmagan.

**Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta’lim muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi.** Dissertatsiya tadqiqoti Toshkent axborot texnologiyalari universitetining ilmiy-tadqiqot ishlari rejasining №A5-061 – “Samarali yagona identifikatsiya texnologiyasi asosida “Elektron hukumat” tizimi xavfsizlik darajasini oshirish” (2015-2017) mavzusidagi loyihasi doirasida bajarilgan.

**Tadqiqotning maqsadi** bir martalik parollarni generatsiyalashning samarali algoritmlari, ularga asoslangan foydalanuvchilarni autentifikatsiyalash usullari va algoritmlarini tadqiq etishdan iborat.

**Tadqiqotning vazifalari:**

apparat-dasturiy va dasturiy vosita ko‘rinishida amalga oshirishga qulay bir martalik parollarni generatsiyalash algoritmlarini ishlab chiqish;

foydalanuvchilarni bir martalik parolga asoslangan autentifikatsiyalash algoritmlarini ishlab chiqish;

foydalanuvchilarni “savol-javob” mexanizmiga asoslangan autentifikatsiyalash usullarini ishlab chiqish;

mobil qurilma va parolga asoslangan ikki tomonlama autentifikatsiyalash usulini ishlab chiqish.

**Tadqiqotning obyekti** sifatida axborot-kommunikatsiya tizimlarida foydalanuvchilarning haqiqiyligini tekshirish jarayoni olingan.

**Tadqiqotning predmeti**ni bir martalik parollarni generatsiyalash algoritmlari, apparat-dasturiy va dasturiy vositalari hamda ularga asoslangan ikki faktorli autentifikatsiya usullari tashkil etadi.

**Tadqiqotning usullari.** Tadqiqot jarayonida axborotni kriptografik himoyalash tizimlari nazariyasi, ehtimollik nazariyasi, sonlar nazariyasi, matematik mantiq, modellashtirish va obyektga yo‘naltirilgan dasturlash usullaridan foydalanilgan.

**Tadqiqotning ilmiy yangiligi** quyidagilardan iborat:

foydalanuvchilarni xavfsiz va samarali autentifikatsiyalash maqsadida kam takrorlanish darajasiga ega qisqartirish funksiyasi va kalitli xesh funksiya asosida apparat-dasturiy va dasturiy vosita ko‘rinishida amalga oshirishga qulay, turli uzunlikdagi bir martalik parollarni generatsiyalash algoritmlari ishlab chiqilgan;

bir faktorli autentifikatsiyalash usullaridagi xavfsizlik muammolarini bartaraf etish maqsadida amalga oshirilgan apparat-dasturiy va dasturiy vosita

---

Р. 773-777. // О.П. Ахмедова, А.Т. Имамалиев. Фойдаланувчиларни аутентификациялаш усулларида хавфсизлик муаммолари. “Ахборот Коммуникациялар: Тармоқлар-Технологиялар-Ечимлар” ҳар чораклик илмий-техник журнал. № 2(62)2022. ISSN 2010-510X. -Б. 35-44. //Z. Khudoykulov, A.T. Imamaliyev. “Analysis Password-based Authentication Systems with Password Policy”. International Conference on Information Science and Communications Technologies: applications, trends and opportunities. ICISCT 2021. Tashkent, Urgench, Uzbekistan, -P. 1-3 //Arziyeva J.T. Psevdotasodifiy sonlar generatori asosida autentifikatsiyalash usullari va algoritmlari. Texnika fanlari bo‘yicha falsafa doktorlik (PhD) dissertatsiyasi, 2020 y.

ko‘rinishidagi tokenlardan ikkinchi faktor sifatida foydalanish orqali foydalanuvchilarni haqiqiyligini tekshirish algoritmlari ishlab chiqilgan;

hisoblash resurslaridan samarali foydalanish maqsadida kalitli xesh funksiyalarga asoslangan, “savol-javob” mexanizmida ishlovchi, mijoz-server o‘rtasida ikki tomonlama va ikki faktorli xavfsiz hamda samarali autentifikatsiyani amalga oshiruvchi usullar ishlab chiqilgan;

mobil qurilmadan ikkinchi faktor sifatida foydalanishga asoslangan foydalanuvchi va serverning o‘zaro autentifikatsiyasini xesh funksiya yordamida amalga oshirish usuli ishlab chiqilgan.

**Tadqiqotning amaliy natijasi** quyidagilardan iborat:

foydalanuvchilarni autentifikatsiyalashda qo‘llaniladigan bir martalik parollarni shakllantiruvchi apparat-dasturiy ko‘rinishdagi token ishlab chiqilgan;

foydalanuvchilarni autentifikatsiyalashda qo‘llaniladigan bir martalik parollarni shakllantiruvchi dasturiy vosita ko‘rinishidagi token ishlab chiqilgan;

foydalanuvchilarni OTP generatori asosida ikki faktorli autentifikatsiyalash tizimining sinov muhiti uchun dasturiy vosita ishlab chiqilgan.

**Tadqiqot natijalarining ishonchliligi.** Tadqiqot natijalarining ishonchliligi ishlab chiqilgan algoritmlar va usullar uchun olingan tajribaviy natijalar, qiyosiy tahlillash natijalari hamda tanlangan sharoitda qo‘lga kiritilgan hisoblash natijalari bilan, shuningdek, ishlab chiqilgan vositalar “Asakabank” aksiyadorlik jamiyatida, “UNICON.UZ” Fan-texnika va marketing tadqiaotlari markazi mas’uliyati cheklangan jamiyatida, “Turon information technology group” mas’uliyati cheklangan jamiyatida joriy qilinganligi bilan izohlanadi.

**Tadqiqot natijalarining ilmiy va amaliy ahamiyati.** Tadqiqot natijalarining ilmiy ahamiyati yuqori takrorlanmaslik darajasiga ega bir martalik parollarni generatsiyalash algoritmlari va ular asosida foydalanuvchilarni ikki faktorli autentifikatsiyalash usullari ishlab chiqilganligi bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati ishlab chiqilgan bir martalik parollarni generatsiyalash tokenlari va ularga asoslangan foydalanuvchilarni autentifikatsiyalash usullari parolga bog‘liq bo‘lgan tahdidlar sonini minimallashtirishga imkon berishi bilan izohlanadi.

**Tadqiqot natijalarining joriy qilinishi.** Foydalanuvchilarni bir martalik parollarni generatsiyalash algoritmlari asosida autentifikatsiyalash usullari, algoritmlari hamda dasturiy vositalari bo‘yicha olingan ilmiy natijalar asosida:

bir martalik parollardan ikkinchi faktor sifatida foydalanishga asoslangan foydalanuvchilarni autentifikatsiyalovchi “Xeshlash algoritmi asosida bir martalik parolni generatsiyalash tizimi” dasturiy vositasi “Asakabank” aksiyadorlik jamiyatida joriy qilingan (“Asakabank” AK 2024-yil 21-fevraldagi dalolatnomasi; O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligining 2024-yil 29-martdagi 2/17-944/22-2-son ma’lumotnomasi). Natijada dasturiy vositalarni mobayl bank xizmatlarida qo‘llash foydalanuvchilarga noqulaylik tug‘dirmagan va bir martalik parollarni takrorlanmaslik darajasi 62% ga teng, shuningdek, QR kodni, mobil qurilmani o‘g‘irlash va SMS xabarni tutib olish kabi hujumlarni oldini olishga imkon bergan.

apparat-dasturiy muhitda amalga oshirishga mo‘ljallangan xesh-funksiya asosida bir martalik parol generatori “UNICON.UZ” Fan-texnika va marketing tadqiqotlari markazi mas’uliyati cheklangan jamiyatida “Buyumlar Interneti ilovalarida maxfiylik va ma’lumotlar yaxlitligini ta’minlash algoritmi va dasturini ishlab chiqish” mavzusidagi innovatsion loyiha doirasida Buyumlar Interneti ilovalarida mijoz va server o‘rtasida xavfsiz ikki faktorli autentifikatsiyani amalga oshirish jarayonida qo‘llanildi (“UNICON.UZ” MCHJ 2024-yil 21-fevraldagi dalolatnomasi; O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligining 2024-yil 29-martdagi 2/17-944/22-2-son ma’lumotnomasi). Natijada ushbu algoritm generatsiyalagan 1 mln.ta 6 xonalik parolning 618 988 tasi takrorlanmagan va takrorlanmaslik darajasi 61,9% ni tashkil etgan.

HMAC algoritmi asosida ishlab chiqilgan bir tomonlama va ikki tomonlama autentifikatsiyalash usulida qo‘llanilgan “Xeshlash algoritmi asosida bir martalik parolni generatsiyalash tizimi” dasturiy vositasi “Turon information technology group” MCHJda “EduSmart” nodavlat o‘quv muassasalari ishini avtomatlashtirish axborot tizimida foydalanuvchilarni autentifikatsiyalash maqsadida joriy etilgan (“Turon information technology group” MCHJ 2024-yil 15-fevraldagi dalolatnomasi; O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligining 2024-yil 29-martdagi 2/17-944/22-2-son ma’lumotnomasi). Natijada ishlab chiqilgan dasturiy vosita yuqori tasodifiylik va takrorlanmaslik darajasiga ega bir martalik parollarni generatsiyalash imkonini bergan.

tasodifiylik va takrorlanmaslik darajasi yuqori bo‘lgan bir martalik parollarni generatsiyalash algoritmining dasturiy vositasi O‘zbekiston Respublikasi Ichki ishlar vazirligi tezkor-qidiruv departamenti Kiberxavfsizlik markazi amaliy faoliyatida tatbiq etilgan (Ichki ishlar vazirligining 2024-yil 23-fevraldagi 16/K5-2233-son ma’lumotnomasi). Ilmiy tadqiqot natijasida olti xona uzunlikdagi bir martalik parollarni generatsiyalashda takrorlanmaslik darajasi mavjud OTP generatorlariga qaraganda 28,4% ga yuqori ko‘rsatgichga erishilgan.

**Tadqiqot natijalarining aprobatsiyasi.** Mazkur tadqiqot natijalari 3 ta xalqaro va 11 ta respublika ilmiy-amaliy anjumanlarida muhokamadan o‘tkazilgan.

**Tadqiqot natijalarining e’lon qilinganligi.** Dissertatsiyaning mavzusi bo‘yicha jami 26 ta ilmiy ish chop etilgan, jumladan, O‘zbekiston Respublikasi Oliy attestatsiya komissiyasining dissertatsiyalarning asosiy ilmiy natijalarini chop etish tavsiya etilgan ilmiy nashrlarida, 4 tasi xorijiy va 6 tasi respublika jurnallarida nashr etilgan hamda 2 ta EHM uchun yaratilgan dasturiy vositalarni qayd qilish guvohnomalari olingan.

**Dissertatsiyaning tuzilishi va hajmi.** Dissertatsiya tarkibi kirish, to‘rtta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovalardan iborat. Dissertatsiya hajmi 117 betni tashkil etadi.

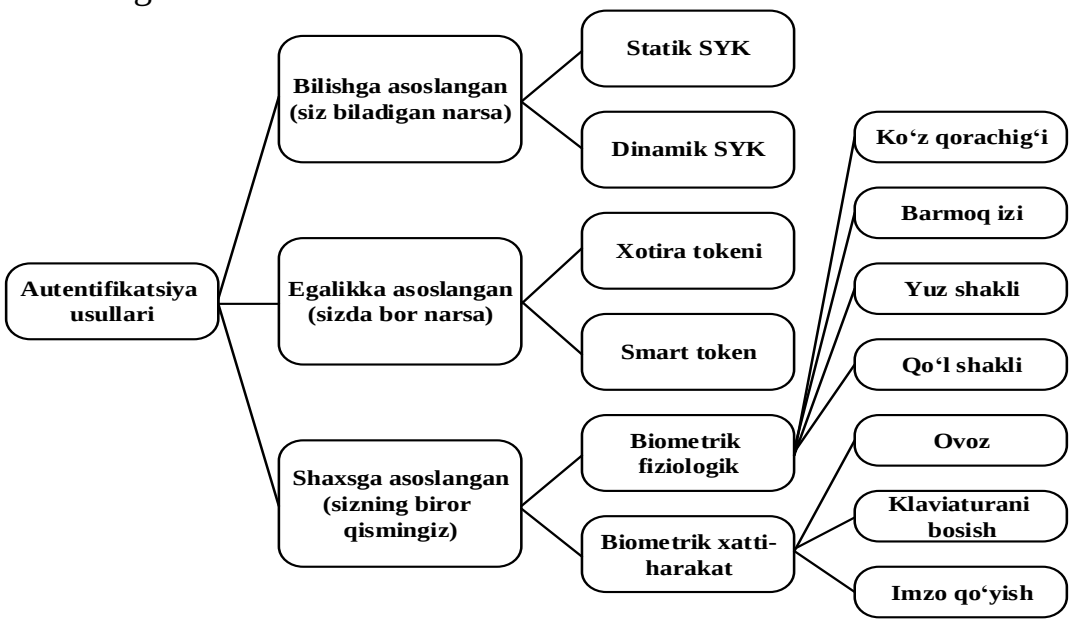
## DISSERTATSIYANING ASOSIY MAZMUNI

**Kirish** qismida dissertatsiya mavzusining dolzarbligi va zaruriyati asoslangan, tadqiqotning O‘zbekiston Respublika fan va texnologiyalari

rivojlanishining ustuvor yo‘nalishlariga mosligi ko‘rsatilgan, maqsad va vazifalari belgilab olingan hamda tadqiqot obyekti va predmeti aniqlangan, olingan natijalarning ishonchliligi asoslab berilgan, ularning nazariy va amaliy ahamiyati, tadqiqot natijalarini amalda joriy qilish holati, nashr etilgan ishlar va dissertatsiyaning tuzilishi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiyaning “**Foydalanuvchilarni autentifikatsiyalash usullari va ularda mavjud xavfsizlik muammolari”** deb nomlangan birinchi bobida foydalanuvchilarni haqiqiyligini tekshirishning zamonaviy usullari, ularda mavjud xavfsizlik muammolari, ko‘p faktorli autentifikatsiya usullari va ulardagi zaifliklar tahlil etilgan.·

*Birinchi paragraf*da foydalanuvchilarni autentifikatsiyalashning zamonaviy usullaridan: foydalanuvchi bilgan biror narsa asosida autentifikatsiya usuli, foydalanuvchi egalik qiladigan biror narsa asosidagi autentifikatsiya usuli, biometric autentifikatsiya usullari hamda ularga qaratilga hujumlar tahlili va tavsifi keltirilgan. 1-rasmda foydalanuvchilarni autentifikatsiyalash usullarining tasnifi keltirilgan.




**1-rasm. Foydalanuvchilarni autentifikatsiyalash usullarining tasnifi**

*Ikkinchi paragraf*da autentifikatsiya usullarida mavjud xavfsizlik muammolari tahlil qilingan. Autentifikatsiya tizimlariga bo‘ladigan hujumlar 1-jadvalda to‘rtta xususiyatga ko‘ra tasniflangan. Bunda hujumchining bilimiga ko‘ra, hujum maqsadiga ko‘ra, hujum shakliga ko‘ra va hujum kuchiga ko‘ra tahlili keltirilgan.

*Uchinchi paragrafda* yuqorida keltirilgan hujumlarga qarshi foydalanuvchilarni autentifikatsiyalashning turli usullarini taqqoslash va tahlil qilish uchun zarur bo‘lgan me’zonlarni tanlash, ular asosida olingan autentifikatsiya usullarini tahlil etish masalasi bilan tanishib chiqiladi. Yaxshi autentifikatsiya usuli nafaqat hujumlarga qarshi tura olishi, balki, samaradorlik va foydalanuvchanlik bo‘yicha ham yuqori ko‘rsatkichga ega bo‘lishi kerak. Shu bois autentifikatsiya usullarini taqqoslash uchun *bardoshlilik – robustness (aniqlik, samaradorlik, xavfsizlik, shaxsiylik), foydalanuvchanlik - usability (universallik, o‘rganuvchanlik, adaptivlik, foydalanuvchiga afzal bo‘lishi,*

*qo‘shimcha vosita talab qilishi)* va *ishonchlilik - reliability* kabi me’zonlar olindi. Shuningdek, baholash me’zonlarini uchta darajaga ajratish mumkin: yuqori (high, H), o‘rta (medium, M) va past (low, L).

**1-jadval**

**Autentifikatsiya tizimiga bo‘ladigan mavjud hujumlar**

| Hujumlar | Talab etiladigan bilim | Hujum nishoni | Hujum shakli | Hujum kuchi |
|---|---|---|---|---|
| Qo‘pol kuch (Brute force) hujumi | Kichik | Parol | - | O‘rtacha |
| Faraz qilishga asoslangan hujum | O‘rtacha | Parol | - | O‘rtacha |
| Yelka orqali qarash hujumi | O‘rtacha | Parol | - | O‘rtacha |
| Fishing hujumi | Kichik | Parol | - | Kuchli |
| Sun’iy sintez | Ko‘p | Biometrik parametr | Bevosita | O‘rtacha |
| Takrorlash hujumi | O‘rtacha | Biometrik parametr | Bilvosita | O‘rtacha |
| Zaharlash hujumi | Ko‘p | Biometrik parametr | Bilvosita | Zaif |

Quyida qator autentifikatsiya usullari yuqorida keltirilgan me’zonlar bo‘yicha tahlili bilan tanishib chiqiladi. Masalan, turli autentifikatsiya usullarini qo‘pol kuch hujumiga nisbatan himoyasining natijasi 2-jadvalda aks ettirilgan.

**2-jadval**

**Autifikatsiya usullarining qo‘pol kuch hujumiga nisbatan himoya darajasi**

| Autentifikatsiya usullari | RO | | | UA | RA |
|---|---|---|---|---|---|
| | AC | EF | SE | | |
| Matn asosidagi sxema | H | L | L | M | L |
| Grafik asosidagi sxema | M | M | L | M | L |
| Audio asosidagi sxema | M | L | L | M | L |
| Video asosidagi sxema | L | M | L | M | L |
| Boshqotirmaga asoslangan sxema | L | M | L | M | M |
| SMS asosidagi sxema | H | M | M | M | M |
| Savol-javob asosidagi sxema | H | M | M | H | M |

Autentifikatsiya tizimlarini taqqoslashda ularni to‘rt toifaga ajratish mumkin. Ular an’anaviy matnga asoslangan tizimlar, grafik tizimlar, tokenlar va biometrik tizimlar. Ushbu to‘rt turdagi tizimlarning afzalliklari va kamchiliklarini 3-jadvalda ko‘rish mumkin.

Yuqorida olingan xulosalardan bir faktorli autentifikatsiya usullarida jiddiy muammo mavjud bo‘lib, ularni bartaraf etishning yagona usuli bu – ko‘p faktorli autentifikatsiyadan foydalanish hisoblanadi. Shu sababli, keyingi paragrafda ko‘p faktorli autentifikatsiya usullarining tahlil etish masalasi bilan tanishib chiqiladi.

*Uchinchi paragrafda* Ko‘p faktorli autentifikatsiya usullari va ulardagi mavjud xavfsizlik muammolari o‘rganib chiqilgan. Faktorlarning kombinatsiyasiga ko‘ra amalda foydalanilayotgan ko‘p faktorli autentifikatsiya usullarining ulushiga foydalanish taqsimoti tahlil etildi. Bundan tashqari ko‘p faktorli autentifikatsiyalashning asosiy muammolari: foydalanuvchanlik, integratsiya, mustaxkamlik, maxfiylik, xavfsizlik kabilar o‘rganib chiqildi.

Yuqorida olingan tahlil natijalaridan quyidagi xulosalarni olish mumkin:

- biror narsani bilishga asoslangan va insonga tegishli ajralmas xususiyatlar asosidagi autentifikatsiya usullari bugungi kunda eng keng tarqalgan usullar hisoblansada, ular xavfsizlik nuqtai nazaridan yangi turdagi hujumlarga bardoshli emasligini ko‘rsatdi.

- SYK, SYH va SYaga asoslangan foydalanuvchilarni autentifikatsiyalash usullari asosida qurilgan tizimlar bir faktorga asoslanganda, yuqori xavfsizlikni ta’minlamasligi aniqlandi.

- bir faktorli autentifikatsiya usullarida mavjud kamchiliklarni bartaraf etishda faktorlar sonini oshirish samarali va xavfsiz usul ekanligi aniqlandi.

- amalga oshirish, foydalanuvchanlik, narx, xavfsizlik nuqtai nazaridan bir martalik tokenga asoslangan ikki faktorli autentifikatsiya usuli eng mosligi aniqlandi.

**3-jadval**

**Turli xil autentifikatsiya tizimlarini taqqoslash**

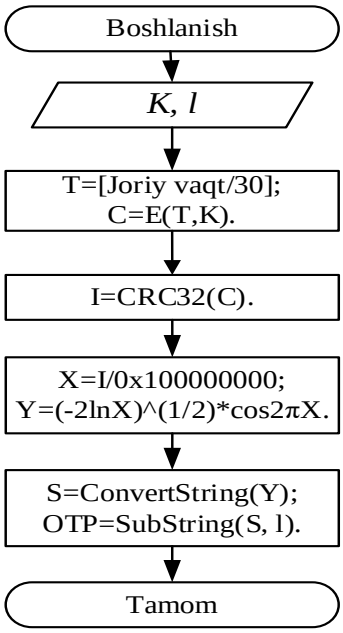
| Himoya turlari | Afzalliklari | Kamchiliklari |
|---|---|---|
| Matnga asoslangan tizimlar | Tezkor javob, amalga oshirish oson, foydalanuvchi uchun qulay. | Lug‘at hujumi, brute force hujumi, yelka orqali qarash hujumi, sotsial injinering hujumi |
| Grafikka asoslangan tizimlar | Eslab qolish oson, fishing hujumiga va boshqa sotsial injinering hujumiga zaif emas. | Parolda bo‘shliqlar bo‘lishini talab etadi. Matn parollarga qaraganda ushbu tizim yelka orqali qarash hujumiga zaif hisoblanadi. Tizimga kirish va parolni yaratish uzoq vaqtni talab etadi |
| Tokenga asoslangan tizimlar | Lug‘at hujumi, brute force hujumi, yelka orqali qarash hujumi, takrorlash hujumlariga bardoshli. Murakkab parollarni yodlash zarurati yo‘q. Xavfsizlik darajasi yuqori. | Qo‘shimcha qurilmani olib yurish zarur va ko‘p vaqt talab etadi. |
| Biometrik tizimlar | Murakkab parollarni yodlash zarurati yo‘q. Xavfsizlik va foydalanuvchanlik darajasi yuqori. | Odatda biologik shablonlarni saqlash uchun katta hajmli saqlagichlar zarur. Hususiyatlarni ajratib olish uchun qimmat qurilmalar talab etiladi. Bu tizimga qalbakilashtirish hujumlari va maxfiylikni oshkor etish hujumlari bo‘lishi mumkin. Ko‘p vaqt talab etadi. |

*Beshinchi paragraf*da tadqiqot maqsadi va vazifalarining qo‘yilishi keltirilgan.

Dissertatsiyaning **“Bir martalik parollarni generatsiyalash algoritmlari va akslantirishlari”** deb nomlangan ikkinchi bobida bir martalik parollarni generatsiyalashning mavjud algoritmlari tahlil qilingan, apparat-dasturiy va dasturiy vosita ko‘rinishida amalga oshirish uchun qulay bir martalik parollarni generatsiyalash algoritmlari taklif etilgan hamda “savol-javob” mexanizmiga asoslangan autentifikatsiya usuli uchun mos kriptografik akslantirishni tanlab olish bo‘yicha tavsiyalar berilgan.

*Birinchi paragrafda* sanoqni sinxronizatsiyalashga asoslangan HOTP algoritmi va vaqtga asoslangan TOTP algoritmi tahlil etilgan.

*Sanoqni sinxronizatsiyalashga asoslangan OTP*da hisoblagich mijoz va server tizimi o‘rtasida sinxronlashtiriladi. Hisoblagich har safar OTP so‘ralganda faollashtiriladi.




*1-bosqich.* Joriy vaqtni o‘zlashtirish.

$$\mathrm{T} = [\frac{\text{Joriy vaqt}}{30}].$$

*2-bosqich.* T qiymat uchun shifrlashni amalga oshirish. Xususiy holda, AES-128 shifrlash standarti. Umumiy holda

$$\mathrm{C} = \mathrm{E}(\mathrm{T}, \mathrm{K}).$$

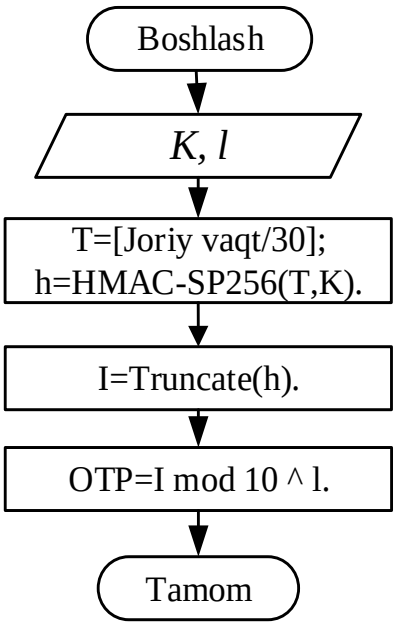
*3-bosqich.* Shifrmatnni 32 bitli qiymatga keltirish.

*4-bosqich.* Talab etilgan uzunlikdagi OTPni hosil qilish. Hosil bo‘lgan 32 bitli I butun sonni [0, 1] oraliqda ifodalash (X – hosil qilish) uchun $0\text{x}100000000$ qiymatga bo‘lish amalga oshiriladi:

$$\mathrm{X} = \mathrm{I}/0\text{x}100000000.$$
$$\mathrm{Y} = (-2\mathrm{lnX})^{1/2}\cos 2\pi\mathrm{X}$$
$$\mathrm{SubString}(\mathrm{S},\ \mathrm{l})$$

**2-rasm. *Algoritm_1* algoritmining blok-sxemasi**

*Vaqtni sinxronizatsiyalashga asoslangan OTP*da foydalanuvchi vaqt parametrini o‘z ichiga olgan parol qiymatini hisoblaydi va u ma’lum muddat ichida (odatda 30 sekund) amalda bo‘ladi. Belgilangan muddat tamomlanganidan so‘ng, parolni amal qilish muddati ham tugaydi va yangi parol generatsiyalanishi talab etiladi.




*1-bosqich.* Joriy vaqtni o‘zlashtirish.

*2-bosqich.* T qiymat uchun xeshlashni amalga oshirish.

$$\mathrm{h} = \mathrm{HMAC} - \mathrm{SP256}(\mathrm{T}, \mathrm{K})$$

*3-bosqich.* Xesh qiymatni 32 bitga qisqartirish.

1. $h$ qiymatning birinchi baytining eng kichik 4 biti ajratiladi va $d_1$ sifatida belgilanadi.
2. $h$ qiymatning o‘ninchi baytining eng kichik 4 biti ajratiladi va $d_2$ sifatida belgilanadi.
3. $d_1$ va $d_2$ qiymatlarni qo‘shish orqali $offset = d_1 + d_2$ qiymat hosil qilinadi.
4. 32 bitli $I$ kattalik quyidagicha hosil qilinadi:

$$I = \big(h[offset]\ \&0x7F\big) \ll 24 | \big(h[offset+1]\ \&0xFF\big) \ll 16 | \big(h[(offset+2) mod 32]\ \&0xFF\big) \ll 8 | (h[(offset+3) mod 32]\ \&\ 0xFF)$$

*4-bosqich.* 32 bitli qiymatdan l uzunlikdagi OTPni hosil qilish. $\mathrm{I}\bmod 10^{\mathrm{l}}$.

**3-rasm. *Algoritm_2* algoritmining blok-sxemasi**

*Ikkinchi paragrafda* simmetrik blokli shifrlash algoritmiga asoslangan dasturiy ko‘rinishda amalga oshirishga qulay OTP va apparat-dasturiy muhiti

uchun mo‘ljallangan xesh funksiya (spongent-256) asosidagi OTP algoritmini yaratish masalasi bilan tanishib o‘tiladi.

Simmetrik blokli shifrlash algoritmiga asoslangan dasturiy ko‘rinishda amalga oshirishga qulay OTP 2-rasmda va apparat-dasturiy muhiti uchun mo‘ljallangan xesh funksiya asosidagi OTP generatori esa 4-rasmda keltirilgan.

Tahlil natijasida taklif etilgan OTPni generatsiyalash algoritmlarini mavjudlariga nisbatan yuqori samaradorligini ko‘rsatib, bu quyidagilar bilan izohlangan:

- Algoritm_1 algoritmida CRC32 funksiyasidan foydalanilganligi va 32 bitli qiymatdan OTPni hosil qilish yondashuvi mavjud bo‘lgan yondashuvlardan takrorlanish darajasi yuqoriligi;
- Algoritm_2 algoritmida foydalanilgan Truncate() funksiyasini mavjudlaridan takrorlanish darajasi yuqoriligi.

**5-jadval**

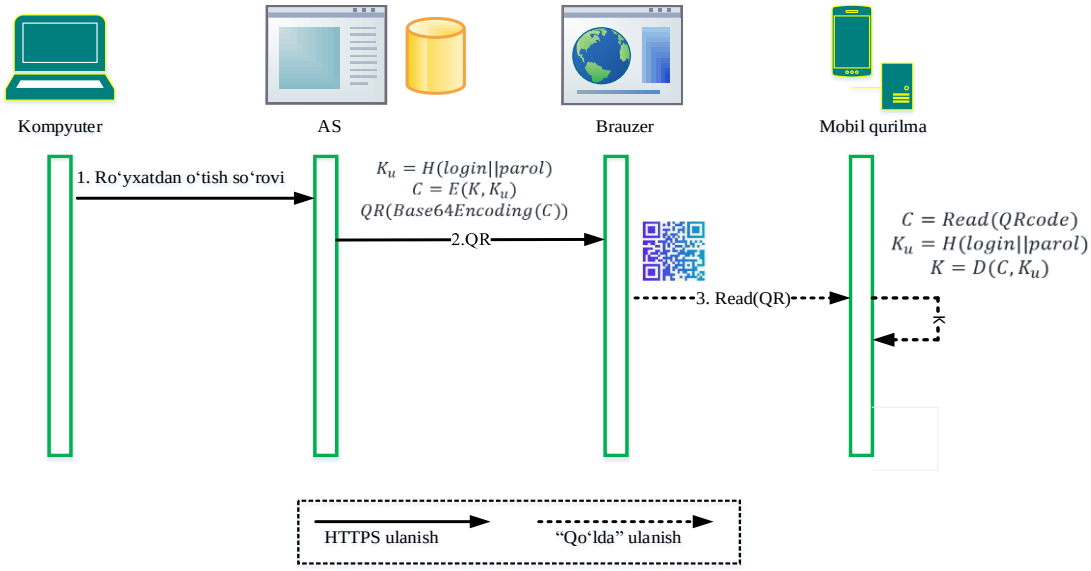
***Algoritm_1* va *Algoritm_2* algoritmlarida 1 mln. OTP orasidan faqat bir marta takrorlanganlarining ulushi (%)**

| № | Algoritm nomi | Matematik asosi | Ulush, % | |
|---|---|---|---|---|
| | | | 6 xonali OTP uchun | 7 xonali OTP uchun |
| 1. | HOTP [66] | HMAC, ikki tomon orasida sanoqni sinxronlash | 36.8 | 90.5 |
| 2. | TOTP [83] | HMAC, ikki tomon orasida vaqtni sinxronlash | 36.8 | 90.5 |
| 3. | [69] manba | PTSG, tub sonlar, bir tomonlama | 85.4 | 100.0 |
| 4. | Algoritm_1 | Simmetrik blokli shifrlash, CRC32, ikki tomon orasida vaqtni sinxronlash | 65.4 | 98.2 |
| 5. | Algoritm_2 | HMAC, ikki tomon orasida vaqtni sinxronlash | 62.5 | 95.3 |

*Uchinchi paragrafda* “savol-javob” mexanizmiga asoslangan mavjud autentifikatsiya usullarida foydalanilgan va uning asosini tashkil etgan kriptografik akslantirishlar (algoritmlar) xususiyatlarini tahlil qilish va bardoshli akslantirishlarni taklif etish masalasiga to‘xtalib o‘tiladi. “Savol-javob” mexanizmiga asoslangan mashhur autentifikatsiya protokollariga, OCRA, SCRAM, CHAP larni misol keltirish mumkin.

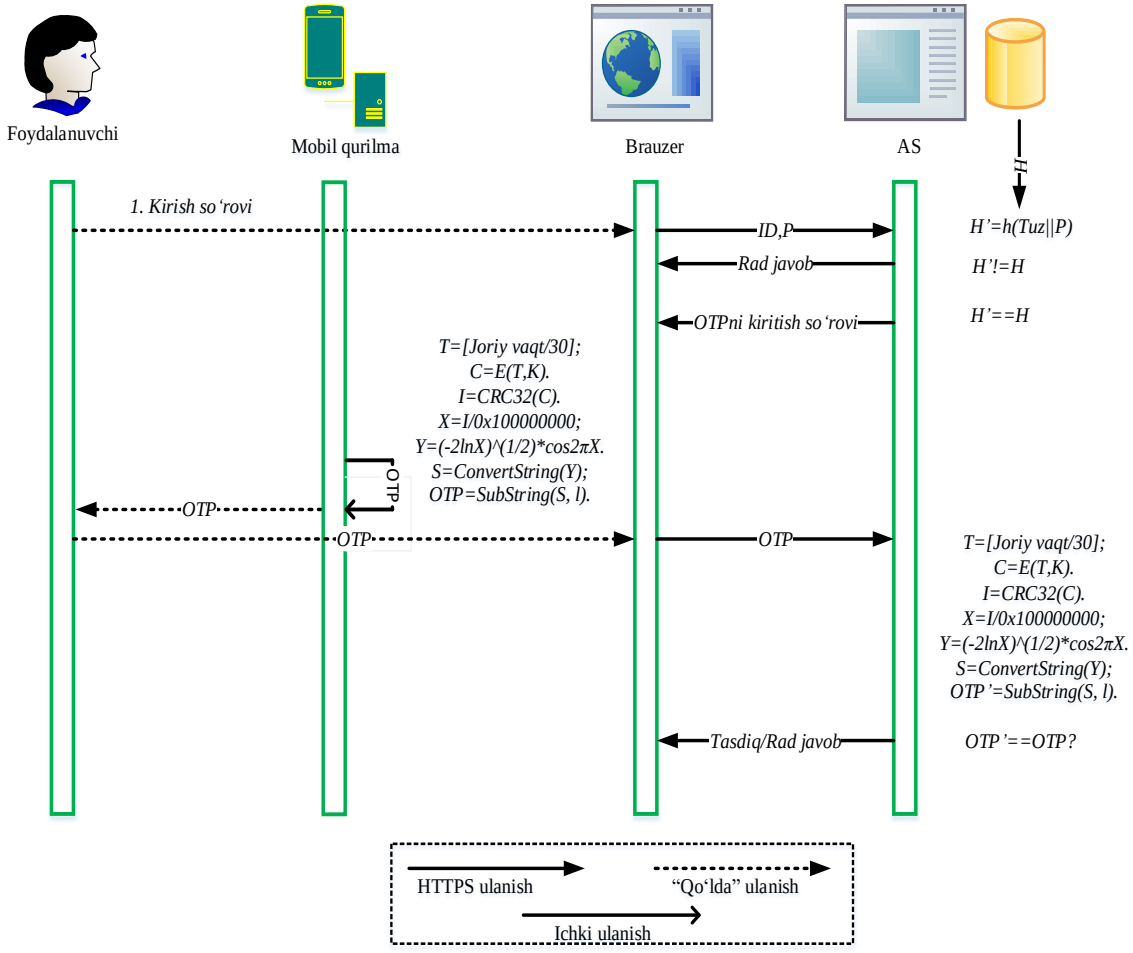
Dissertatsiyaning **“Bir martalik parolga asoslangan autentifikatsiya usullari va algoritmlarini ishlab chiqish”** deb nomlangan uchinchi bobda bir martalik parollarga asoslangan autentifikatsiya algoritmlari, “savol-javob” mexanizmiga asoslangan autentifikatsiya usullari hamda mobil qurilma va parolga asoslangan foydalanuvchilarni ko‘p faktorli autentifikatsiyalash usuli taklif etilgan.

*Birinchi paragraf*da dasturiy va apparat-dasturiy ko‘rinishda amalga oshirishga mo‘ljallangan bir martalik parollarni generatsiyalash asosida foydalanuvchilarni autentifikatsiyalash algoritmlarini ishlab chiqish masalasiga to‘xtalib o‘tiladi.



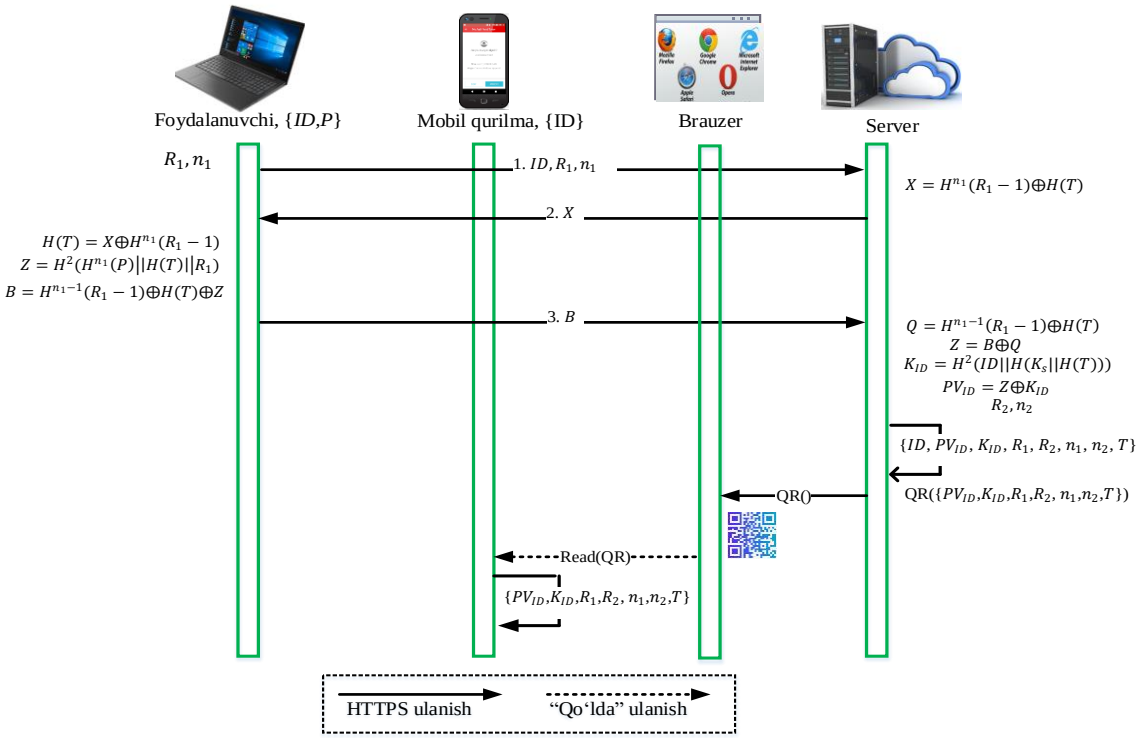

**4-rasm. Ro‘yxatga olish protsedurasi**

Algoritm_1 OTP generatoriga asoslangan foydalanuvchilarni autentifikatsiyalash algoritmi (Protokol_1) taklif etilgan. Ushbu autentifikatsiya algoritmi ikki bosqichdan iborat: foydalanuvchini ro‘yxatga olish (4-rasm) va kirish (5-rasm).



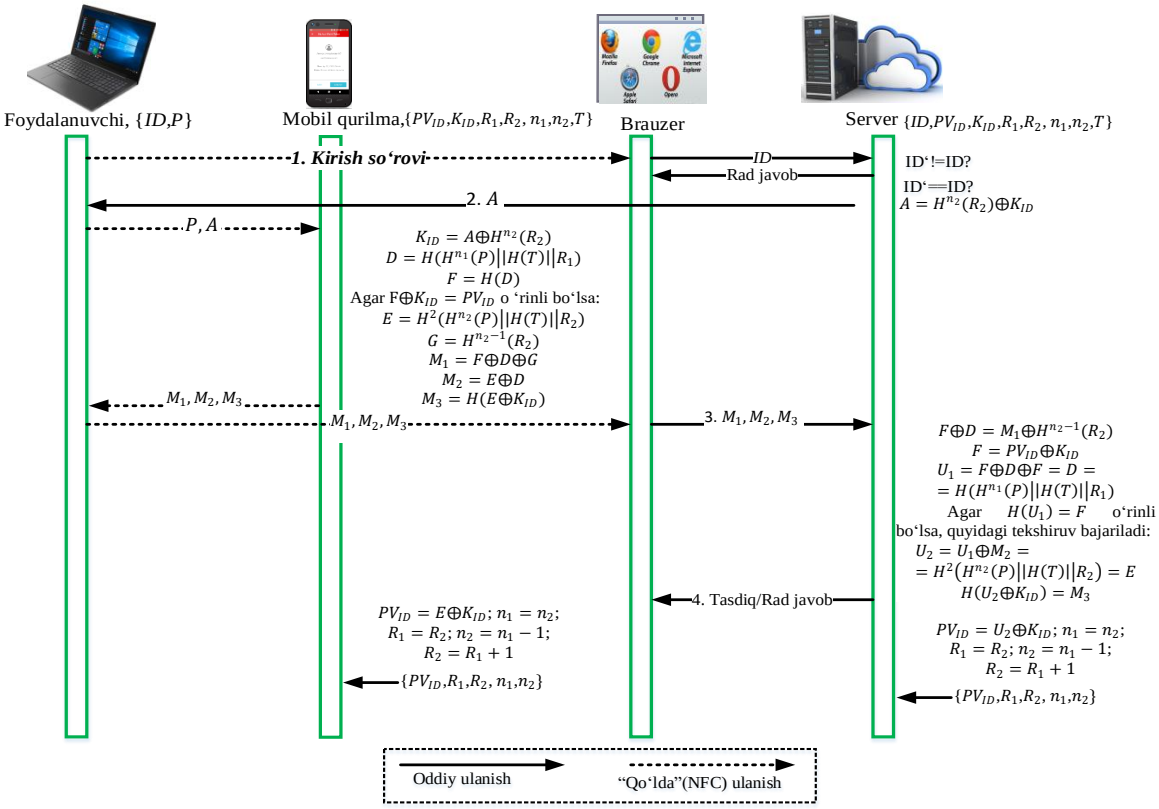

**5-rasm. Protokol_1 algoritmining kirish protsedurasi**

Algoritm_2 algoritmi asosida OTPlarni generatsiyalashning apparat-dasturiy vositasi yordamida foydalanuvchilarni autentifikatsiyalash algoritmi (Protokol_2) taklif etiladi.



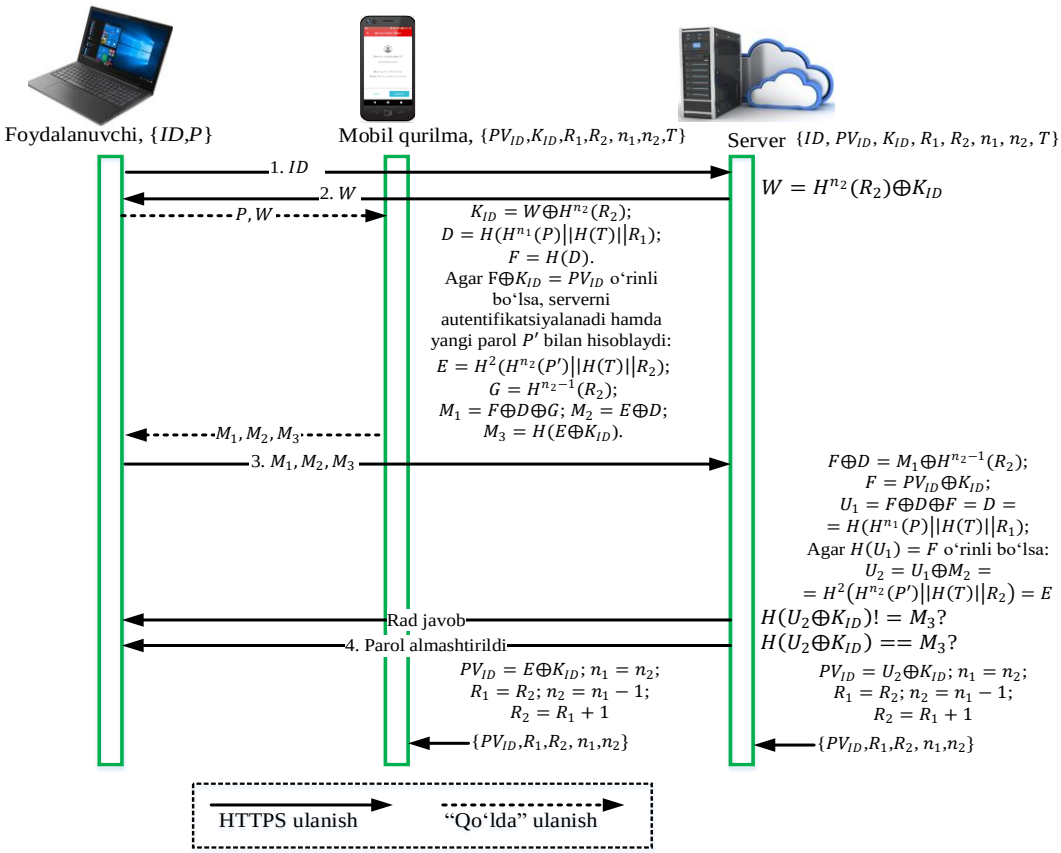

**6-rasm. Ro'yxatga olish protsedurasi**

Ushbu algoritmda ham **ro'yxatga olish** va **kirish** protseduralari mavjud bo'lsada, ro'yxatga olish protsedurasi tokenni foydalanuvchiga taqdim etishdan oldin amalga oshiriladi. Ushbu algoritmda foydalanuvchi tizimda ikkinchi faktorli qo'shish allaqachon tizimda ma'lumotlari xavfsiz qayd etilgan tokenga ega bo'lishi talab etiladi. Shundan so'ng, algoritmning kirish protsedurasi birinchi keltirilgan algoritmniki kabi amalga oshirilib, farqli ravishda OTP mobil qurilmadagi ilovani o'rniga apparat-dasturiy vositadan foydalaniladi.




**7-rasm. Protokol_6 usulining kirish protsedurasi**

*Uchinchi paragraf*da foydalanuvchining mobil qurilmasi yordamida ikki faktorli autentifikatsiyalash imkoniyatiga ega, serverni ham autentifikatsiyalash imkoniyatini beruvchi usulni yaratish masalasi keltirilgan. Taklif etilayotgan autentifikatsiya usuli xesh funksiyalarga asoslangan bo‘lib, bardoshli hisoblangan xesh funksiyalardan foydalanish mumkin. Bunda xesh qiymatning uzunligini 256 bitga teng va bardoshli algoritm bo‘lishi tavsiya etiladi. Autentifikatsiya usuli (Protokol_6) 3 ta protseduradan: foydalanuvchini ro‘yxatga olish, kirish va parolni almashtirishdan iborat.



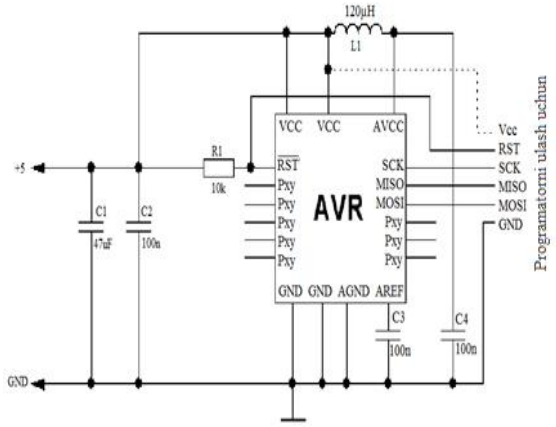

**8-rasm. Protokol_6 usulining parolni almashtirish protsedurasi**

Ushbu taklif etilgan usul mobil qurilma imkoniyatidan, xususan, NFC texnologiyasidan, foydalanib foydalanuvchilarni autentifikatsiyalashni amalga oshirib, ham parol ham mobil qurilmani talab etgani bois ikki faktorli, server ham foydalanuvchi ham bir-birini autentifikatsiyalash imkoniyatiga ega bo‘lgani bois ikki tomonlama autentifikatsiya deb aytish mumkin.

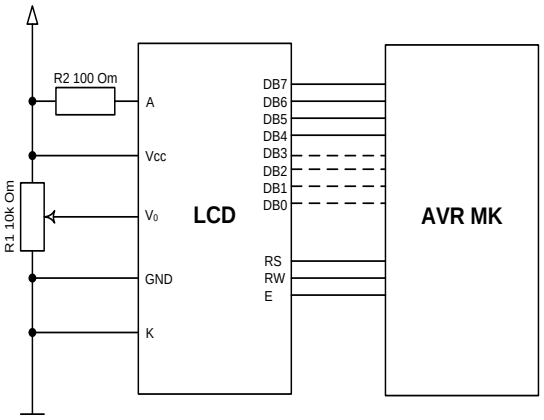
Dissertatsiyaning **“Ishlab chiqilgan autentifikatsiya usullarining qiyosiy tahlili va amalda tatbiqi”** deb nomlangan to‘rtinchi bobda bir martalik parollarni generatsiyalash algoritmini apparat-dasturiy va dasturiy vositada amalga oshirish tartibi, bir martalik parollarga asoslangan autentifikatsiyalash usullari va algoritmlarining tahlili, dissertatsiya ishidan olingan amaliy natijalarni amalda tatbiq etishdan olingan natijalar keltirilgan.

*Birinchi paragraf*da bir martalik parolga asoslangan autentifikatsiya qurilmasini yaratish muammosi tadqiq etiladi. Ushbu muammoni hal etishda mikrokontrollerlardan foydalaniladi. Mikrokontrollerlar kichik hisoblash qurilmasi bo‘lib, ular yordamidan turli xil qurilmalarni yaratish mumkin.

9-rasmda AVR mikrokontrollerni ta’minot blokiga ulanishi hamda unga dastur yozish interfeysi keltirilgan. 10-rasmda esa, LCD displeyni mikrokontrollerga ulash sxemasi keltirilgan.



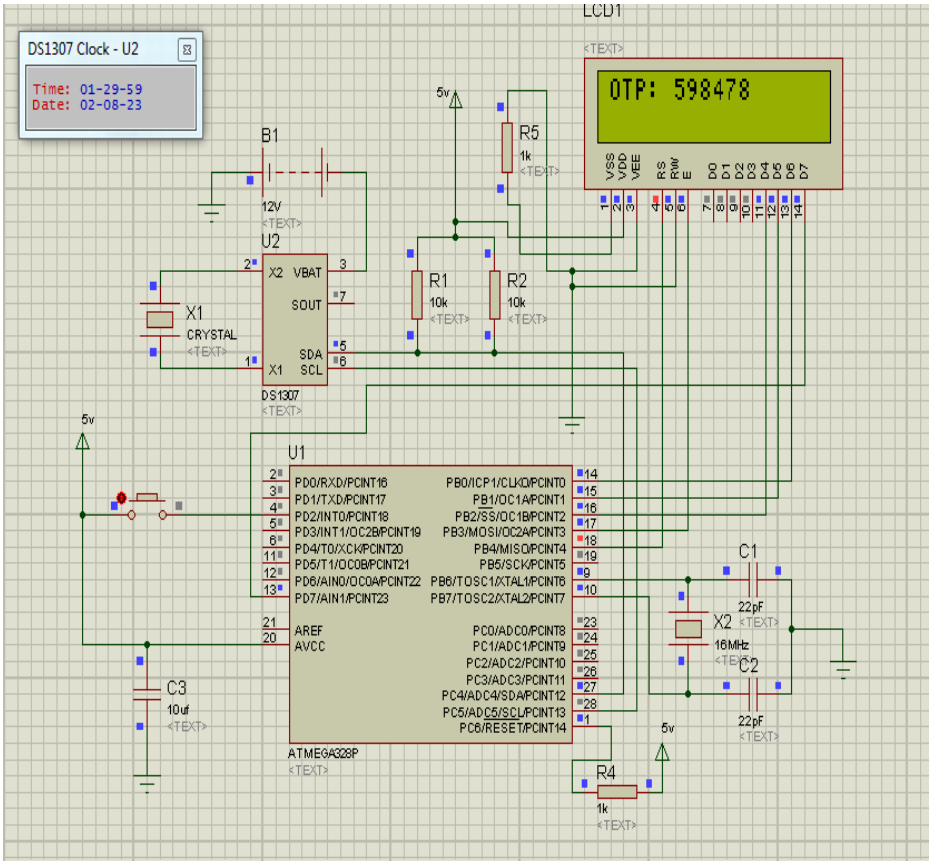

**9-rasm. Mikrokontrollerni ta’minot blokiga ulanish sxemasi**




**10-rasm. LCD displeyni mikrokontrollerga ulash sxemasi**

Taklif etilgan qurilma uchun CodeVisionAVR kompilyatori asosida dastur tuzishda mikrokontroller turiga qarab uning kutubxonasi tanlanadi. Ushbu mikrokontroller uchun zarur bo‘lgan ko‘plab funksiyalarni o‘z ichiga olgan.

Proteus dasturiy paketdan foydalanib, 11-rasmda keltirilgan sxema yordamida ushbu funksiyalarning natijasini ko‘rish mumkin.




**11-rasm. Bir martalik parol generatori apparat-dasturiy qurilmasining ish holati**

*Ikkinchi paragraf*da uchinchi bobda taklif etilgan autentifikatsiya usullari va algoritmlarining tahlili amalga oshiriladi (6-,7-,8-jadvallar).

**6-jadval**

**Protokol_1 va Protokol_2 algoritmlarining umumiy tahlil natijalari**

| № | Protokol nomi | Ro‘yxatga olishdagi almashinadigan xabarlar soni | Kirishda almashinadigan xabarlar soni | Seans kalitini xavfsiz almashinish | OTP generatorining tasodifiyligi |
|---|---|---|---|---|---|
| 1. | Google authenticator | 2 | 4 | - | O‘rtacha |
| 2. | Microsoft authenticator | 2 | 4 | - | O‘rtacha |
| 3. | Protokol_1 | 2 | 4 | + | Yuqori |
| 4. | Protokol_2 | 2 | 4 | + | Yuqori |

*Uchinchi paragraf*da ishlab chiqilgan dasturiy va dasturiy-apparat vositalarni amaliyotda joriy etishdan olingan natijalar tahlili keltirilgan. Ishlab chiqilgan usullar amaliyotda turli tashkilotlar faoliyatida tatbiq etildi.

**7-jadval**

**Protokol_3, Protokol_4 va Protokol_5 usullarining umumiy tahlil natijalari**

| № | Usul nomi | Ro‘yxatga olishdagi almashinadigan xabarlar soni | Kirishda almashinadigan xabarlar soni | Kriptografik akslantirish | Ikki tomonlama autentifikatsiya | Ikki faktorli autentifikatsiya | Ishonarli tomon ishtiroki |
|---|---|---|---|---|---|---|---|
| 1. | Nidxem-Shreder | NA | 5 | Shifrlash | + | - | + |
| 2. | Neuman-Stub. | NA | 4 | Shifrlash | - | - | + |
| 3. | Otvey-Riis | NA | 5 | Shifrlash | - | - | + |
| 4. | Kerberos | NA | 4 | Shifrlash | + | - | + |
| 5. | Protokol_3 | 2 | 4 | HMAC | + | - | - |
| 6. | Protokol_4 | 2 | 6 | HMAC | + | + | - |
| 7. | Protokol_5 | 3 | 4 | HMAC | + | - | - |

“Asakabank” aksiyadorlik jamiyatida “Xeshlash algoritmi asosida bir martalik parolni generatsiyalash tizimi” dasturiy vositasi joriy qilindi. Ilmiy tadqiqot natijasida dasturiy vositalarni mobayl bank xizmatlarida qo‘llash foydalanuvchilarga noqulaylik tug‘dirmagan va bir martalik parollarni takrorlanmaslik darajasi 62% ga teng.

**8-jadval**

**Protokol_6 usulini mavjud analoglari bilan xavfsizlik talablari bo‘yicha qiyosiy tahlili**

| № | Protokol nomi | Xavfsizlik talabi nomeri | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1. | M.Jan va bosh [71] | + | + | + | + | + | + | + | - | + | + |
| 2. | J. Arziyeva [53] | + | + | + | + | + | + | + | - | + | - |
| 3. | Ku [70] | + | + | + | + | - | - | - | - | + | - |
| 4. | Protokol-6 | + | + | + | + | + | + | + | + | + | + |

“UNICON.UZ”-Fan-texnika va marketing tadqiaotlari markazi mas’uliyati cheklangan jamiyatida “Buyumlar interneti ilovalarida maxfiylik va ma’lumotlar

yaxlitligini ta’minlash algoritmi va dasturini ishlab chiqish” mavzusidagi innovatsion loyiha doirasida buyumlar interneti ilovalarida mijoz va server o‘rtasida xavfsiz ikki faktorli autentifikatsiyani amalga oshirish jarayonida sinovdan o‘tkazildi.

“Turon information technology group” MCHJda “Xeshlash algoritmi asosida bir martalik parolni generatsiyalash tizimi” dasturiy vositasi “EduSmart” nodavlat o‘quv muassasalari ishini avtomatlashtirish axborot tizimida foydalanuvchilarni autentifikatsiyalash maqsadida joriy etilgan.

Ishlab chiqilgan bir martalik parollarni generatsiyalash algoritmining dasturiy vositasi O‘zbekiston Respublikasi Ichki ishlar vazirligi tezkor-qidiruv departamenti Kiberxavfsizlik markazi amaliy faoliyatida tatbiq etilgan. Ilmiy tadqiqot natijasida 6 xona uzunlikdagi parollarning takrorlanmaslik darajasi mavjud HOTP va TOTP generatorlariga qaraganda 28,4% ga yuqori bo‘lgan ko‘rsatgichga erishilgan.

## XULOSA

“Foydalanuvchilarni bir martalik parollarga asoslangan autentifikatsiyalash usullari va algoritmlari” mavzusidagi dissertatsiya ishi bo‘yicha olib borilgan tadqiqotlar natijasida quyidagi xulosalar taqdim etildi:

1. Kam takrorlanish darajasi bilan qisqartirish funksiyasi va kalitli xesh funksiyaga asoslangan apparat-dasturiy ko‘rinishida amalga oshirishga qulay bir martalik parollarni generatsiyalash algoritmi ishlab chiqildi. Ishlab chiqilgan algoritm 62,5% takrorlanmaslik darajasi bilan olti xonali parollarni generatsiyalashga imkon bergan.
2. Kriptografik algoritm yordamida qisqartirish va simmetrik blokli shifrlashga asoslangan dasturiy ko‘rinishda amalga oshirishga qulay bir martalik parollarni generatsiyalash algoritmi ishlab chiqildi. Ishlab chiqilgan algoritm 65,4% takrorlanmaslik darajasi bilan olti xonali parollarni generatsiyalashga imkon bergan.
3. Ishlab chiqilgan generator yordamida shakllantirilgan 6 va 7 xona uzunlikdagi parollarning takrorlanmaslik darajasi mavjud HOTP va TOTP generatorlarga qaraganda yuqori ko‘rsatkichga erishilgan.
4. Bir martalik parollarni generatsiyalovchi apparat-dasturiy va dasturiy vosita ko‘rinishida amalga oshirilgan tokenlardan ikkinchi faktor sifatida foydalanishga asoslangan foydalanuvchilarni autentifikatsiyalash algoritmlari ishlab chiqildi. Ishlab chiqilgan algoritmlar foydalanuvchilarni tokenga asoslangan ikkinchi faktor bo‘yicha ham autentifikatsiyalashga imkon bergan.
5. Kalitli xesh funksiyalarga asoslangan “savol-javob” mexanizmida ishlovchi foydalanuvchilarni ikki tomonlama va ikki faktorli autentifikatsiyalash usullari ishlab chiqildi. Ishlab chiqilgan usullar tomonlarni o‘zaro autentifikatsiyalashda ikkinchi faktor bo‘yicha ham haqiqiylikni tekshirish imkonini bergan.
6. Mobil qurilmadan ikkinchi faktor sifatida foydalanish asosida foydalanuvchi va serverni o‘zaro autentifikatsiyasini ta’minlovchi, xesh funksiyaga asoslangan xavfsizlik usuli ishlab chiqildi. Ishlab chiqilgan usul zaif paroldan foydalanilganda ham bardoshlikni ta’minlashini ko‘rsatgan.

**НАУЧНЫЙ СОВЕТ DSc. 13/30.12.2019.T.07.02 ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**ИМАМАЛИЕВ АЙБЕК ТУРАПБАЕВИЧ**

# МЕТОДЫ И АЛГОРИТМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ОДНОРАЗОВЫХ ПАРОЛЕЙ

**05.01.05 – Методы и системы защиты информации. Информационная безопасность**

**АВТОРЕФЕРАТ ДИССЕРТАЦИИ**
**ДОКТОРА ФИЛОСОФИИ (PhD) ПО ТЕХНИЧЕСКИМ НАУКАМ**

**Ташкент-2024**

**Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Министерство Высшего образования, науки и инноваций Республики Узбекистан за № B2024.1.PhD/T4416.**

Диссертация выполнена в Ташкентском университете информационных технологий имени Мухаммада ал-Хоразмий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб-странице Научного совета (www.tuit.uz) и на Информационно-образовательном портале «ZiyoNet» (www.ziyonet.uz).

| | |
|---|---|
| **Научный руководитель:** | **Худойкулов Зарифжон Туракулович**<br>доктор философии по техническим наукам (PhD), доцент |
| **Официальные оппоненты:** | **Жураев Гайрат Умарович**<br>доктор физико-математических наук, профессор |
| | **Норматов Шербек Бахтиярович**<br>доктор философии по техническим наукам (PhD), доцент |
| **Ведущая организация:** | **ООО «UNICON.UZ» - Центр научных-технических и маркетинговых исследований** |

Защита диссертации состоится «__» _____2024 года в _____ часов на заседании Научного совета DSc. 13/30.12.2019.T.07.02 при Ташкентском университете информационных технологий. (Адрес: 100084, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер №___). (Адрес: 100084, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43).

Автореферат диссертации разослан «___» _____ 2024 года.

(протокол рассылки №__ от «___» _____ 2024 года.)

**Б.Ш. Махкамов**
Председатель научного совета по присуждению ученых степеней, д.э.н., профессор

**М.С.Саиткамолов**
Ученый секретарь научного совета по присуждению ученых степеней, д.э.н., доцент

**С.К. Ганиев**
Председатель научного семинара при научном совете по присуждению ученых степеней, д.т.н., профессор

## ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

**Актуальность и востребованность темы диссертации.** В мире с каждым годом возрастает масштаб кибератак, основанных на системных уязвимостях и социальной инженерии. Большинство из них реализуются на основе недостатков и уязвимостях, связанных с механизмами аутентификации, включая аутентификацию на основе пароля. В частности, по данным National Cyber Security Alliance, «81% инцидентов взлома связаны с кражей или слабыми паролями»[1]. Это, учитывая невозможность отказаться от метода аутентификации на основе пароля, требует устранения имеющихся в них недостатков, в частности, создания новых способов и средств использования второго фактора в дополнение к паролю. В настоящее время особое внимание уделяется созданию токенов, смарт-карт и других инструментов, генерирующих одноразовые пароли, которые используются в таких странах, как США, Российская Федерация и Китайская народная республика, В настоящее время в таких странах, как США, Российская Федерация и Китайская Народная Республика особое внимание уделяется созданию токенов, смарт-карт и других инструментов генерации одноразовых паролей, которые используются в дополнение к методам аутентификации на основе паролей.

В мире, помимо парольного метода аутентификации, использование нескольких факторов позволяет повысить безопасность системы. В частности, широко применяются биометрические параметры, токены, генерирующие пароли или выполняющие различные вычисления, и смарт-карты. Однако многие киберпреступления совершаются из-за того, что эти средства стоят дорого или не полностью отвечают требованиям безопасности. Поэтому необходимо уделить особое внимание научно-практическим исследованиям, направленным на создание программных и аппаратных токенов для генерации одноразовых паролей, которые могут использоваться в дополнение к паролям, и методов аутентификации на их основе.

На совещании под председательством Президента Республики Узбекистан Шавката Мирзиёева 20 декабря 2023 года было подчеркнуто, что вопрос кибербезопасности становится все более актуальным по мере развития IT-сектора. На этой встрече также было отмечено, что за 11 месяцев 2023 года в Узбекистане было совершено 5500 киберпреступлений, из которых 70% составили мошенничества и кражи, связанные с банковскими картами[2]. В нашей республике реализуются комплексные меры, направленные на профилактику преступлений в сфере кибербезопасности и формирование у граждан знаний о киберпреступлениях. В частности, в новой стратегии развития Узбекистана на 2022-2026 годы поставлена задача «Создание системы профилактики киберпреступлений. выход», «Пересмотр уголовной ответственности за

[1] Информация предоставлена National Cyber Security Alliance. Сайт: https://logmeonce.com/resources/compromised-passwords-are-responsible-for-what-percentage-of-breaches/

[2] Видеоселекторное совещание Президента Республики Узбекистан состоялось 20 декабря 2023 года. Сайт: https://www.gazeta.uz/oz/2023/12/21/cyber-crime/ (murojaat vaqti:30.05.2024)

киберпреступления», «Дальнейшее совершенствование системы мониторинга кибератак и угроз в информационной сфере». При реализации этих задач важно решить проблему аутентификации, в частности, разработать эффективные и безопасные методы проверки подлинности пользователей.

Данное диссертационное исследование в определенной степени нацелено на решение задач, обозначенных Законом Республики Узбекистан «О Кибербезопасности», указами Президента Республики Узбекистан от 28 января 2022 года № УП-60 «О Стратегии развития Нового Узбекистана на 2022-2026 годы», от 11 сентября 2023 года УП-158 «О стратегии «Узбекистан - 2030», от 14 марта 2018 года УП-5379 «О мерах по совершенствованию системы государственной безопасности Республики Узбекистан» и от 19 февраля 2018 года УП-5349 «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций», постановлением Президента Республики Узбекистан от 3 апреля 2007 года № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан», а также задач, определенных в других нормативно-правовых актах, связанных с данной деятельностью.

**Соответствие исследования приоритетным направлениям развития науки и технологий республики.** Данное исследование выполнено в соответствие с приоритетным направлением развития науки и технологий Республики IV. «Информатизация и развитие информационно-коммуникационных технологий».

**Степень изученности проблемы.** Со стороны X. Wang, W. Zheng, E. De Cristofaro, C. Katsini, D.I. Golenko и других зарубежных ученых были проведены научные исследования по изучению, созданию, совершенствованию методов аутентификации пользователей и анализу атак на них, в том числе изучению методов и инструментов двухфакторной аутентификации, генерации одноразовых паролей[3].

В Узбекистане со стороны научных групп под руководством С.К.Ганиева, М.М.Каримова, Д.Я.Иргашевой, К.А.Ташева, О.П.Ахмедовой, З.Т.Худойкулова и Ж.Т.Арзиевой проведены множество исследований по вопросу аутентификации пользователей и криптографических механизмов защиты информации[4].

---

[3] Wang X. et al. Attacks and defenses in user authentication systems: A survey. Journal of Network and Computer Applications. – 2021. – Т. 188. – С. 103080. //Zheng, W., Jia, C., 2017. CombinedPWD: a new password authentication mechanism using separators between keystrokes. In: 2017 13th International Conference on Computational Intelligence and Security (CIS), Hong Kong, China, pp. 557 – 560. //De Cristofaro E. et al. A comparative usability study of two-factor authentication. arXiv preprint arXiv: 1309.5344. – 2013. //Katsini, C.; Belk, M.; Fidas, C.; Avouris, N.; Samaras, G. Security and Usability in Knowledge-based User Authentication: A Review. In Proceedings of the 20th Pan-Hellenic Conference on Informatics, Patras, Greece, 10–12 November 2016; ACM: New York, NY, USA, 2016; p. 63. //Д. И. Голенко Моделирование и статистический анализ псевдослучайных чисел на электронных вычислительных машинах. – Издательство" Наука", Главная редакция физико-математической литературы, 1965.

[4] С.К. Ганиев, А.Т. Имамалиев. Псевдотасодифий кетма-кетлик генератори асосида масофадан фойдаланувчининг аутентификаторини яратиш. “ТАТУ хабарлари” ilmiy-texnika va axborot-tahliliy jurnali. № 2(58)/2021. Toshkent-2021. -Б. 150-159. // M.M. Karimov, K.A. Tashev, J. Arziyeva, A.A. Abdurakhmanov, A.T. Imamliyev. About one of the authentication methods // “TATU xabarlari” ilmiy-texnika va axborot-tahliliy

Наряду с этим, недостаточное внимание уделяется разработке методов и средств генерации одноразовых паролей, которые используются в качестве дополнительного фактора проверки подлинности пользователей, а также на их основе безопасных и эффективных методов аутентификации пользователей.

**Связанность диссертационного исследования с научно-исследовательскими планами высшего учебного заведения, в котором была выполнена диссертация.** Диссертационное исследование выполнено согласно плану научно-исследовательских работ №А5-061 - «Повышение уровня безопасности системы «Электронного правительства» на основе эффективной технологии единой идентификации» (2015-2017) Ташкентсткого университета информационных технологий.

**Целью исследования** является исследование эффективных алгоритмов генерации одноразовых паролей, а также методов и алгоритмов аутентификации пользователей, основанных на них.

**Задачи исследования:**

разработка простых в реализации алгоритмов генерации одноразовых паролей в виде аппаратно-программных и программных средств;

разработка алгоритмов аутентификации пользователей на основе одноразового пароля;

разработка методов аутентификации пользователей на основе механизма «вопрос-ответ»;

разработка метода двусторонней аутентификации на основе мобильного устройства и пароля.

**Объектом исследования** является процесс проверки подлинности пользователей в информационно-коммуникационных системах.

**Предметом исследования** является исследование эффективных алгоритмов генерации одноразовых паролей, а также методов и алгоритмов аутентификации пользователей, основанных на них.

**Методы исследования.** В процессе исследования использовались теория систем криптографической защиты информации, теория вероятностей, теория чисел, математическая логика, моделирование и объектно-ориентированное программирование.

**Научная новизна исследования** заключается в следующем:

для безопасной и эффективной аутентификации пользователей разработаны алгоритмы генерации одноразовых паролей различной длины, которые легко реализуются в виде аппаратных и программных средств на

---

jurnali. № 3/2013. Toshkent-2013. -P. 5-12 K.A. // A.F. Verlan, M.M. Karimov, K.A. Tashev, A.T. Imamaliyev. Method of Authentication on Based Password Generators // 3 rd international conference on “Application of Information and Communication Technology and Statistics in Economy and Education”. Bulgaria, Sofia-2013. -P. 773-777. // О.П. Ахмедова, А.Т. Имамалиев. Фойдаланувчиларни аутентификациялаш усулларида хавфсизлик муаммолари. “Ахборот Коммуникациялар: Тармоқлар-Технологиялар-Ечимлар” ҳар чораклик илмий-техник журнал. № 2(62)2022. ISSN 2010-510X. -Б. 35-44. //Z. Khudoykulov, A.T. Imamaliyev. “Analysis Password-based Authentication Systems with Password Policy”. International Conference on Information Science and Communications Technologies: applications, trends and opportunities. ICISCT 2021. Tashkent, Urgench, Uzbekistan, -P. 1-3 //Arziyeva J.T. Psevdotasodifiy sonlar generatori asosida autentifikatsiyalash usullari va algoritmlari. Texnika fanlari bo‘yicha falsafa doktorlik (PhD) dissertatsiyasi, 2020 y.

основе функции сокращения с низким уровнем повторения и хэш-функции с ключом;

алгоритмы проверки подлинности пользователей с помощью токенов в виде аппаратных и программных средств в качестве второго фактора были разработаны для устранения проблем безопасности в методах однофакторной аутентификации;

для эффективного использования вычислительных ресурсов были разработаны методы, основанные на ключевых хэш-функциях, работающие по механизму «вопрос-ответ» и реализующие двустороннюю и двухфакторную безопасную и эффективную аутентификацию между клиентом и сервером;

разработан метод взаимной аутентификации пользователя и сервера, основанный на использовании мобильного устройства в качестве второго фактора с помощью хэш-функции.

**Практические результаты исследования** заключаются в следующем:

разработан токен в виде аппаратно-программного обеспечения, генерирующий одноразовые пароли, используемые при аутентификации пользователей;

разработан токен в виде программного обеспечения, генерирующий одноразовые пароли, используемые при аутентификации пользователей;

разработано программное средство для тестовой среды системы двухфакторной аутентификации на основе генератора OTP пользователя.

**Достоверность результатов исследования.** Достоверность результатов исследования объясняется экспериментальными результатами, полученными по разработанным алгоритмам и методам, результатами сравнительного анализа и результатами расчетов, полученных в выбранных условиях, а также объясняется тем, что разработанные средства были внедрены в АО «Асакабанк», ООО “UNICON.UZ”-Центр научно-технических и маркетинговых исследований, ООО “Turon information technology group”.

**Научная и практическая значимость результатов исследования.**

Научная значимость результатов исследования объясняется тем, что на их основе разработаны алгоритмы генерации одноразовых паролей с высоким уровнем неповторяемости и методы двухфакторной аутентификации пользователей.

Практическая значимость результатов исследования объясняется тем, что разработанные токены генерации одноразовых паролей и разработанные на их основе методы аутентификации пользователей позволяют минимизировать количество угроз, связанных с паролями.

**Внедрение результатов исследования.** На основании полученных научных результатов о методах, алгоритмах и программных средствах аутентификации пользователей на основе алгоритмов генерации одноразовых паролей:

программное средство аутентификации пользователей «Система генерации одноразовых паролей на основе алгоритма хеширования», основанное на использовании одноразовых паролей в качестве второго

фактора внедрено в АО «Асакабанк» (справка № 2/17-944/22-2 от 29 марта 2024 года Министерства высшего образования, науки и инноваций Республики Узбекистан). В результате использование программных средств в услугах мобильного банкинга не причинило неудобств пользователям и процент неповторения одноразовых паролей был равен 62%, а также позволило предотвратить такие атаки, как кража QR-кода, мобильного устройства и перехват SMS-сообщений.

генератор одноразовых паролей на основе хеш-функции, предназначенный для реализации в аппаратно-программной среде использован в процессе реализации безопасной двухфакторной аутентификации между клиентом и сервером в приложениях Интернета вещей в рамках инновационного проекта «Разработка алгоритма и программы обеспечения конфиденциальности и целостности данных в приложениях Интернета вещей» в Обществе с ограниченной ответственностью «UNICON.UZ»-Центр научных-технических и маркетинговых исследований (справка № 2/17-944/22-2 от 29 марта 2024 года Министерства высшего образования, науки и инноваций Республики Узбекистан). Из 1 миллиона паролей, сгенерированных данным генератором одноразовых паролей, была подсчитана доля повторяющихся только один раз паролей. По результатам расчета данный алгоритм сгенерировал. В результате из 1 миллиона 6-значных паролей, сгенерированных этим алгоритмом, 618 988 не повторялись, а уровень неповторяемости составил 61,9%.

Программное средство «Система генерации одноразовых паролей на основе алгоритма хеширования», разработанное на основе алгоритма HMAC и примененное методом односторонней и двусторонней аутентификации, внедрено в ООО «Turon information technology group» в целях аутентификации пользователей в информационной системе автоматизации работы негосударственных образовательных учреждений «EduSmart» (справка № 2/17-944/22-2 от 29 марта 2024 года Министерства высшего образования, науки и инноваций Республики Узбекистан). В результате разработанное программное средство позволило генерировать одноразовые пароли с высоким уровнем случайности и неповторяемости.

программное средство алгоритма генерации одноразового пароля с высокой степенью случайности и неповторяемости внедрен в практическую деятельность Центра кибербезопасности оперативно-розыскного департамента Министерства внутренних дел Республики Узбекистан (справка № 16/K5-2233 от 23 февраля 2024 года Министерства внутренних дел Республики Узбекистан). В результате научного исследования показатель неповторения при генерации одноразовых 6-значных паролей составила на 28,4% выше, чем у существующих генераторов OTP.

**Апробация результатов исследования.** Результаты данного исследования были обсуждены на 3 международных и 11 республиканских научно-практических конференциях.

**Публикация результатов исследования.** По теме диссертации опубликовано в общей сложности 26 научных работ, из них 10 статей в

научных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан, в том числе 4 – в иностранных и 6 – в республиканских журналах, а также получены 2 свидетельства о регистрации программных продуктов для ЭВМ.

**Структура и объем диссертации.** Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложения. Объем диссертации составляет 117 страниц.

## ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

**В введении** обоснованы актуальность и востребованность темы диссертации, показано соответствие с приоритетными направлениями развития науки и технологий Республики Узбекистан, формулируются цель и задачи, также объект и предмет исследования, изложены научная новизна и практические результаты исследования, обоснована достоверность полученных результатов, раскрыта их теоретическая и практическая значимость, приведен перечень внедрений в практику результатов исследования, сведения об опубликованных работах и структура диссертации.

В первой глава диссертации, озаглавленной как "**Методы аутентификации пользователей и проблемы их безопасности"** анализируются современные методы проверки пользователей, наличие в них проблемы безопасности, методы многофакторной аутентификации и их уязвимости.

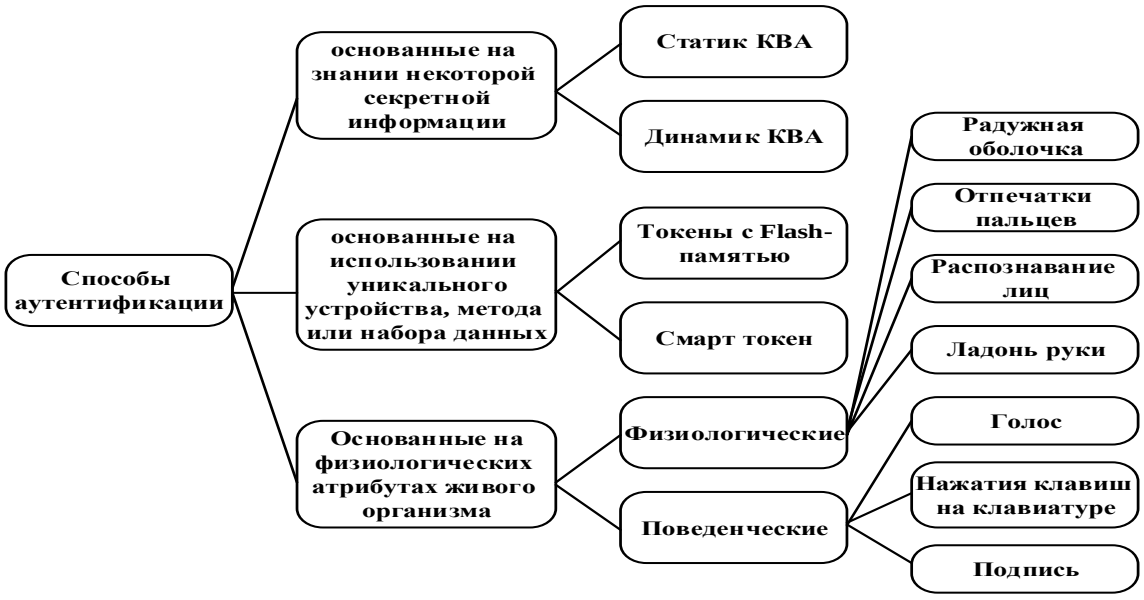



**Рисунок 1. Классификация методов аутентификации пользователей**

*В первом параграфе* из современных способов аутентификации пользователей представлены: метод аутентификации, основанный на том, что знает пользователь, метод аутентификации, основанный на чем-то, принадлежащем пользователю, биометрические методы аутентификации и анализ, и описание атак на них. На рисунке 1 представлена классификация методов аутентификации пользователей.

*Во втором параграфе* анализируются существующие проблемы безопасности в методах аутентификации. Атаки на системы

аутентификации классифицируются в Таблице 1 по четырем характеристикам. Где приведен анализ, основанный на знаниях злоумышленника, в зависимости от цели атаки, формы атаки и силы атаки.

*В третьем параграфе* поставлена задача выбора критериев, необходимых для сравнения и анализа различных методов аутентификации пользователей на фоне вышеупомянутых атак, а также анализа полученных на их основе методов аутентификации. Хороший метод аутентификации должен не только противостоять атакам, но также обладать высокой производительностью и удобством использования. Поэтому для сравнения методов аутентификации были выделены следующие критерии: *прочность – robustness (точность, эффективность, безопасность, конфиденциальность), удобство использования - usability (универсальность, обучаемость, адаптируемость, предпочтение пользователю, требующее дополнительного средство)* и *надежность – reliability.* Также критерии оценки можно разделить на три уровня: высокий (high, H), средний (medium, M) и низкий (low, L).

**Таблица 1**

**Существующие атаки на систему аутентификации**

| **Атаки** | **Требуемые знания** | **Цель атаки** | **Форма атаки** | **Сила атаки** |
|---|---|---|---|---|
| Атака полным перебором (Brute force) | Минимальное | Пароль | - | Средняя |
| Атака, основанная на предположении | Среднее | Пароль | - | Средняя |
| Атака подсматривание через плечо | Среднее | Пароль | - | Средняя |
| Фишинговые атаки | Минимальное | Пароль | - | Высокая |
| Исскуственный синтез | Низкое | Биометрический параметр | Прямая | Средняя |
| Атаки с повторением | Среднее | Биометрический параметр | Прямая | Средняя |
| Вирусные атаки | Высокое | Биометрический параметр | Прямая | Слабая |

Ниже представлен ряд методов аутентификации с их анализом по вышеуказанным критериям. Например, результат защиты различных методов аутентификации от атаки полным перебором приведен в Таблице 2.

**Таблица 2**

**Уровень защиты методов аутентификации от атаки полным перебором**

| **Методы аутентификации** | **RO** | | | **UA** | **RA** |
|---|---|---|---|---|---|
| | **AC** | **EF** | **SE** | | |
| Схема на основе текста | H | L | L | M | L |
| Схема на основе графики | M | M | L | M | L |
| Схема на основе аудио | M | L | L | M | L |
| Схема на основе видео | L | M | L | M | L |
| Схема на основе головоломки | L | M | L | M | M |
| Схема на основе SMS | H | M | M | M | M |
| Схема на основе вопроса-ответа | H | M | M | H | M |

При сравнении систем аутентификации их можно разделить на четыре категории. Это системы на основе традиционного текста, графические системы, токены и биометрические системы. Преимущества и недостатки этих четырех типов систем можно увидеть в Таблице 3.

Из приведенных выше выводов следует, что существует серьезная проблема с методами однофакторной аутентификации, и единственным способом ее рещения является использование многофакторной аутентификации. Поэтому в следующем параграфе можно ознакомится с вопросом анализа методов многофакторной аутентификации.

*В четвертом параграфе* изучаены методы многофакторной аутентификации и существующие проблемы их безопасности. Исходя из комбинаций факторов проанализировано распределенное использование доли методов многофакторной аутентификации на практике. Кроме того, были изучены основные проблемы многофакторной аутентификации: удобство использования, интеграция, надежность, конфиденциальность, безопасность и т. д.

**Таблица 3**

**Сравнение различных систем аутентификации**

| **Виды защиты** | **Преимущества** | **Недостатки** |
|---|---|---|
| Системы на основе текста | Быстрое реагирование, простота реализации, удобство для пользователя. | Атаки с подбором по словарю, brute force, подсматривание через плечо, атаки социальной инженерии |
| Графические системы | Легко запомнить, неуязвим для фишинга и других атак социальной инженерии. | Пароль требует пробелов. По сравнению с текстовыми паролями, эта система более уязвима для атаки «подсматривание через плечо». Требуется много времени, чтобы войти в систему и создать пароль |
| Системы на основе токена | Устойчив к атакам с подбором по словарю, brute force, подсматривание через плечо, с повторением. Нет необходимости запоминать сложные пароли. Уровень безопасности высокий. | Необходимость ношение с собой дополнительного устройства и требует много времени. |
| Биометрические системы | Нет необходимости запоминать сложные пароли. Уровень безопасности высокий. | Как правило, хранение биологических шаблонов требует больших объемов памяти. Для извлечения признаков требуется дорогостоящее оборудование. Возможны атаки с подделкой и атаки на раскрытие конфиденциальной информации. Требует много времени. |

По результатам вышеизложенного анализа можно сделать следующие выводы:

- хотя методы аутентификации, основанные на знании чего-либо и основанные на неотъемлемых свойствах человека, сегодня являются

наиболее распространенными, они показали, что они не устойчивы к новым типам атак с точки зрения безопасности.

- было выявлено, что системы, построенные на методах аутентификации пользователей на основе SYK, SYH и SYA, не обеспечивают высокую безопасность при использовании одного фактора.

- было выявлено, что увеличение количества факторов является эффективным и безопасным способом преодоления недостатков методов однофакторной аутентификации.

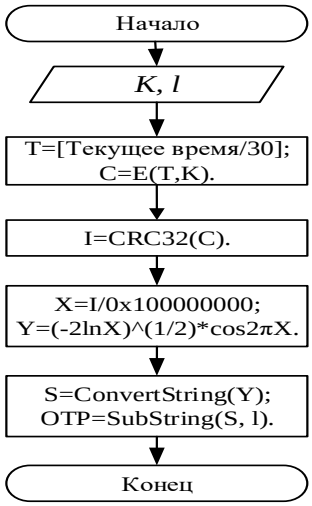
- было выявлено, что с точки зрения реализации, удобства использования, стоимости, безопасности метод двухфакторной аутентификации на основе одноразового токена оказался наиболее совместимым.

*В пятом параграфе* представлены постановка цели и задачи исследования.

Во второй главе диссертации, озаглавленной как **«Алгоритмы и преобразование генерации одноразовых паролей»** проанализированы существующие алгоритмы формирования одноразовых паролей, предложены простые в реализации алгоритмы формирования одноразовых паролей в виде аппаратно-программных и программных средств, а также даны рекомендации по выбору подходящего криптографического преобразования для метода аутентификации на основе механизма «вопрос-ответ».

*В первом параграфе* анализированы алгоритм HOTP, основанный на синхронизации счета и алгоритм TOTP, основанный на времени.

*На OTP, основанным на синхронизации счета* счетчик синхронизируется между клиентской и серверной системой. Счетчик активируется каждый раз, когда запрашивается OTP.




*1-й этап.* Освоение текущего времени.

$$T = [\frac{\text{Текущее время}}{30}].$$

*2-й этап.* Шифрование для значения T. В частном случае, стандарт шифрования AES-128. В общем случае

$$C = E(T, K).$$

*3-й этап.* Преобразование зашифрованного текста в 32-битное значение.

*4-й этап.* Сгенерирование OTP требуемой длины. Для того, чтобы представить (сгенерировать - X) сгенерированное 32-битное целое число I в диапазоне [0, 1] выполняется деление на 0x100000000:

$$X = I/0x100000000.$$

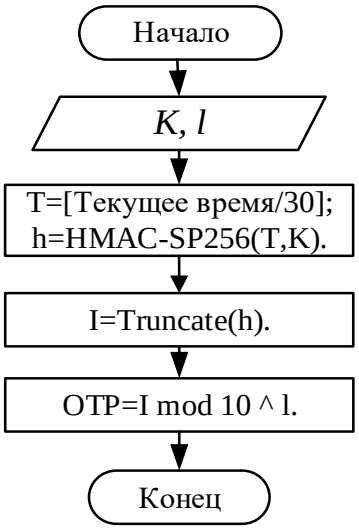
$$Y = (-2\ln X)^{1/2}\cos 2\pi X$$

$$SubString(S, l)$$

**Рисунок 2. Блок-схема алгоритма *Algoritm_1***

*На OTP, основанным на времени* пользователь вычисляет значение пароля, которое включает параметр времени и действует в течение определенного периода времени (обычно 30 секунд). По истечении

указанного периода срок действия пароля также истечет, и потребуется сгенерировать новый пароль.




*1-й этап.* Освоение текущего времени.

*2-й этап* хеширование для значения T.

$$h = HMAC - SP256(T, K)$$

*3-й этап.* Уменьшение хеш-значения до 32 бит.

1. выделяются наименьшие 4 бита первого байта значения $h$ и обозначаются как $d_1$.
2. выделяются наименьшие 4 бита десятого байта значения $h$ и обозначаются как $d_2$.
3. сложив значении $d_1$ и $d_2$ можно получить

$$offset = d_1 + d_2$$

4. 32-битная величина $I$ генерируется следующим образом:

$$I = \big(h[offset]\ \&0x7F\big) \ll 24 | \big(h[offset+1]\ \&0xFF\big) \ll 16 | \big(h[(offset+2) mod 32]\ \&0xFF\big) \ll 8 | (h[(offset+3) mod 32]\ \&\ 0xFF)$$

*4-й этап.* генерация OTP с длиной l из 32-битного значения. $I \bmod 10^l$.

**Рисунок 3. Блок-схема алгоритма *Algoritm_2***

*Во втором параграфе* можно ознакомиться с задачей создания простого в реализации OTP на основе симметричного блочного алгоритма шифрования и OTP алгоритма на основе хеш-функции (spongent-256), предназначенного для аппаратно-программной среды.

Простой в виде программной реализации OTP на основе алгоритма симметричного блочного шифрования показан на рисунке 2, а генератор OTP на основе хеш-функции, предназначенный для аппаратно-программной среды, представлен на рисунке 4.

**Таблица 5**

**Доля повторяющихся только один раз среди 1 млн. OTP в алгоритмах *Algoritm_1* и *Algoritm_2* (%)**

| № | Наименование алгоритма | Математическая основа | Доля, % | |
|---|---|---|---|---|
| | | | для 6 значной OTP | для 7 значной OTP |
| 1. | HOTP [66] | HMAC, синхронизация счета между двумя сторонами | 36.8 | 90.5 |
| 2. | TOTP [83] | HMAC, синхронизация времени между двумя сторонами | 36.8 | 90.5 |
| 3. | [69] источник | PTSG, простые числа, односторонние | 85.4 | 100.0 |
| 4. | Algoritm_1 | Симметричное блочное шифрование, CRC32, синхронизация времени между двумя сторонами | 65.4 | 98.2 |
| 5. | Algoritm_2 | HMAC, синхронизация времени между двумя сторонами | 62.5 | 95.3 |

В результате анализа предложенные алгоритмы генерации OTP показывают более высокую эффективность по сравнению с существующими, что объясняется следующим:

- Алгоритм CRC32 использованный в алгоритме Algoritm_1 и подход к генерации OTP из 32-битного значения имеет более высокая повторяемость, чем существующие подходы;

- Алгоритм Truncate() использованный в алгоритме Algoritm_2 имеет более высокая повторяемость, чем существующие подходы.

*Третий параграф* посвящен анализу особенностей криптографического преобразования (алгоритмов), используемых в существующих методах аутентификации, основанных на механизме «вопрос-ответ», и вопросу предложения устойчивого преобразования. Примерами популярных протоколов аутентификации, основанных на механизме «вопрос-ответ», являются OCRA, SCRAM, CHAP.

В третьей главе диссертации, озоглавленной как **«Разработка методов и алгоритмов аутентификации на основе одноразового пароля»** предложены алгоритмы аутентификации на основе одноразовых паролей, методы аутентификации на основе механизма «вопрос-ответ» и метод многофакторной аутентификации пользователей на основе мобильных устройств и паролей.

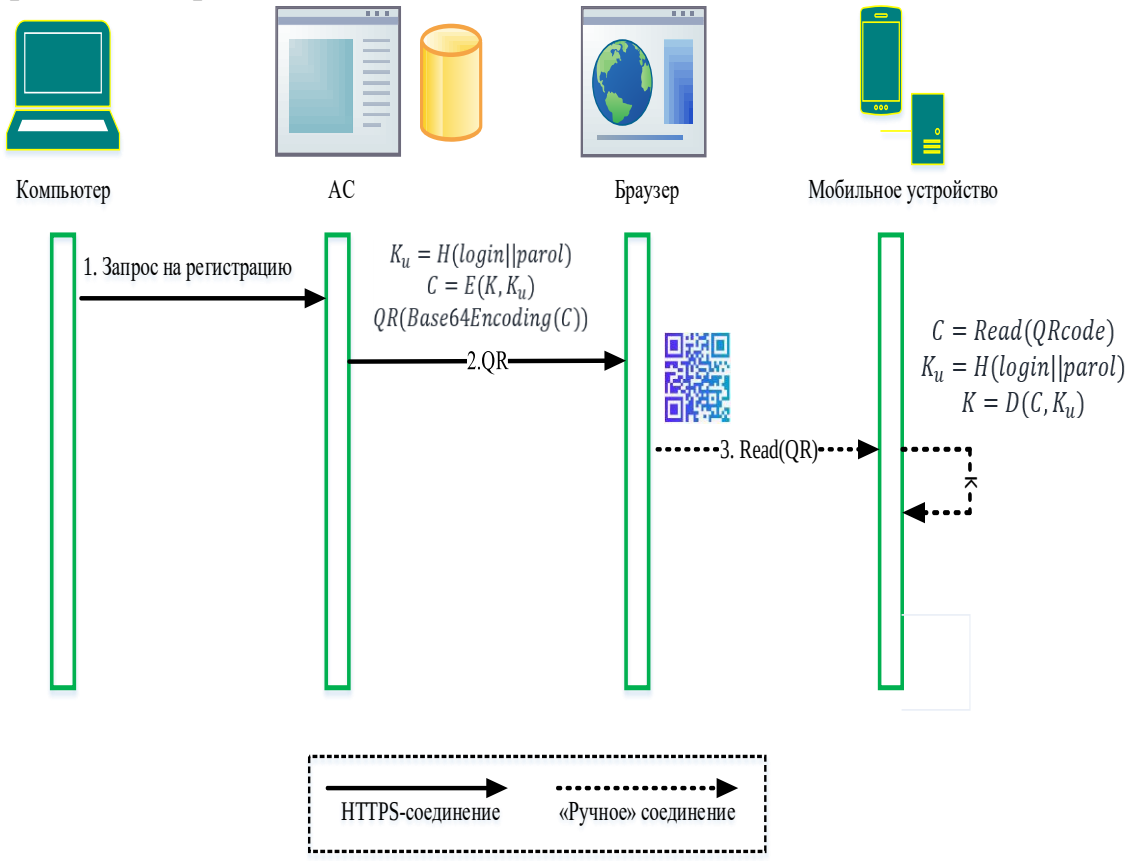



**Рисунок 4. Процедура регистрации**

*В первом параграфе* обсуждены вопросы по разработке алгоритмов аутентификации пользователей на основе генерации одноразовых паролей, предназначенных для реализации в программном и аппаратно-программном виде.

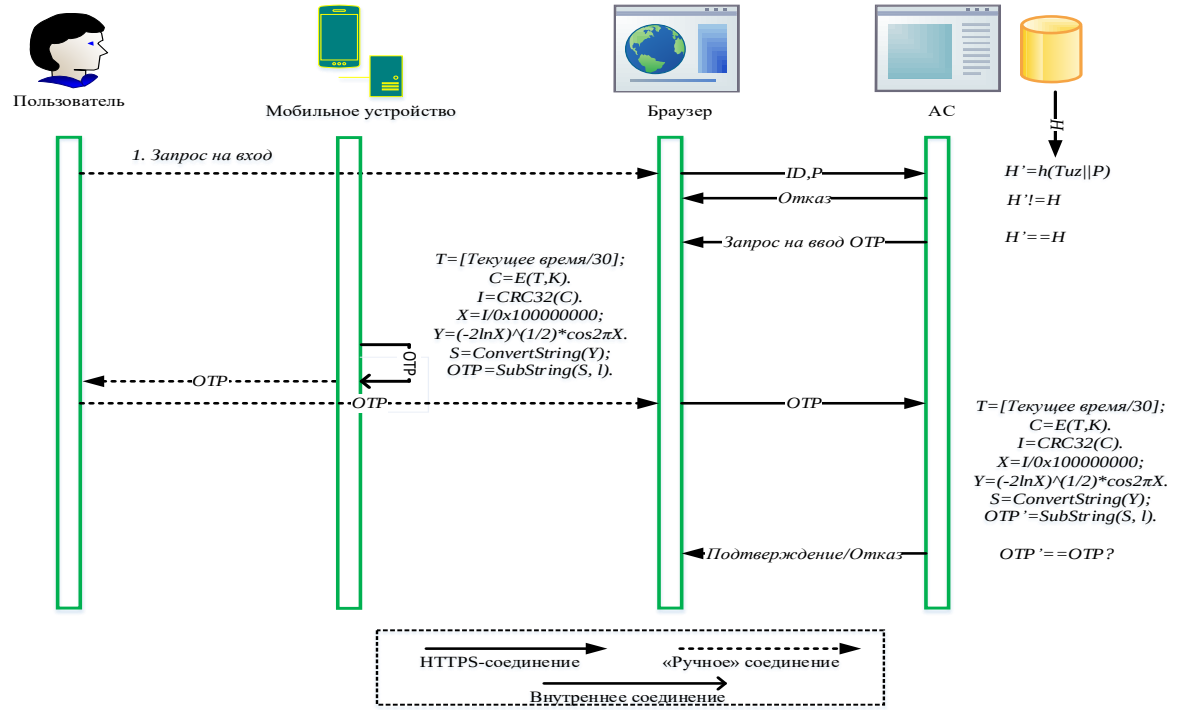



**Рисунок 5. Процедура входа в алгоритм Protokol_1**

Предложен алгоритм аутентификации пользователя (Protokol_1) на основе генератора OTP алгоритма Algoritm_1. Этот алгоритм аутентификации состоит из двух этапов: регистрация пользователя (рисунок 4) и вход в систему (рисунок 5).

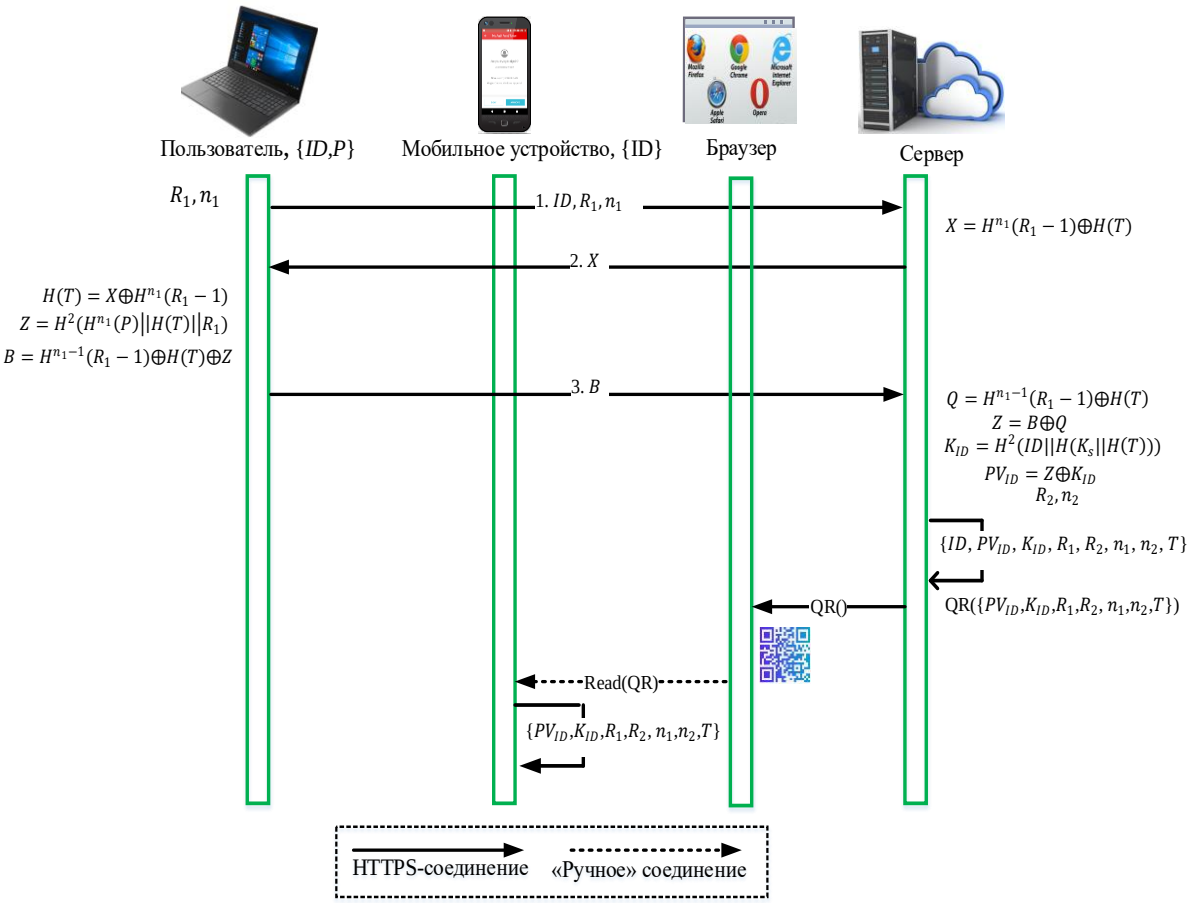



**Рисунок 6. Процедура регистрации**

На основе алгоритма Алгоритм_2 предложен алгоритм аутентификации пользователя (Protokol_2) с использованием аппаратно-программного средства генерации OTP. Хотя этот алгоритм также имеет процедуры **регистрации** и **входа**, процедура регистрации выполняется до того, как токен будет представлен пользователю. В этом алгоритме пользователю требуется, чтобы в момент добавления второго фактора в систему у пользователя уже был токен, информация о котором надежно записана в системе. После этого процедура ввода алгоритма производится так же, как и в первом представленном алгоритме, с той лишь разницей, что вместо приложения на мобильном устройстве OTP используется аппаратно-программное средство.

*В третьем параграфе* представлена задача создания метода с возможностью двухфакторной аутентификации с использованием мобильного устройства пользователя и возможностью аутентификации на сервере. Предлагаемый метод аутентификации основан на хеш-функциях, при котором могут использоваться хэш-функции, которые считаются надежными. При этом рекомендуется хеш-функция с длиной 256 бит и с надежным алгоритмом. Метод аутентификации (Protokol_6) состоит из 3 процедур: регистрация пользователя, вход и смена пароля.

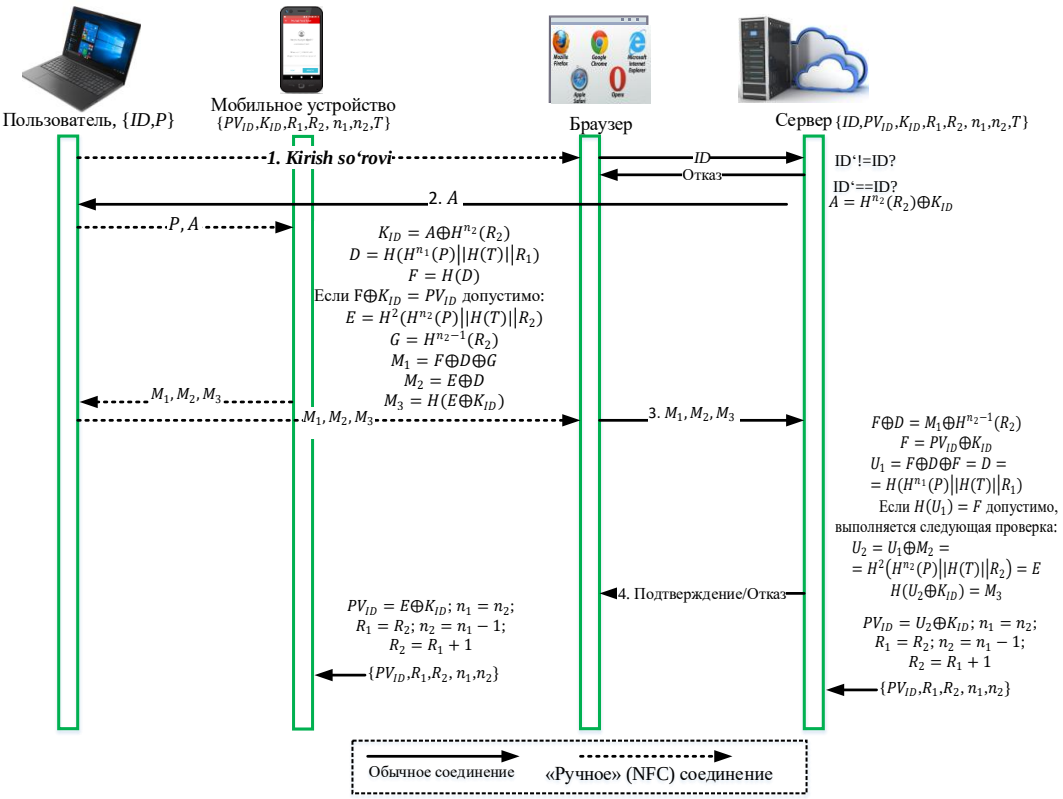



**Рисунок 7. Процедура входа в методе Protokol_6**

Этот предлагаемый метод реализует аутентификацию пользователя с использованием возможностей мобильного устройства, в частности технологии NFC, и его можно назвать двухфакторной аутентификацией, поскольку требуются и пароль, и мобильное устройство, также и двухфакторной аутентификацией, поскольку и сервер, и пользователь могут аутентифицировать друг друга.

В четвертой главе диссертации, озоглавленной как **“Сравнительный анализ и практическое применение разработанных методов аутентификации”** представлены порядок реализации алгоритма генерации одноразового пароля в аппаратно-программных и программных средствах, анализ методов и алгоритмов аутентификации на основе одноразовых паролей, реализации на практике полученных в диссертации практических результатов.

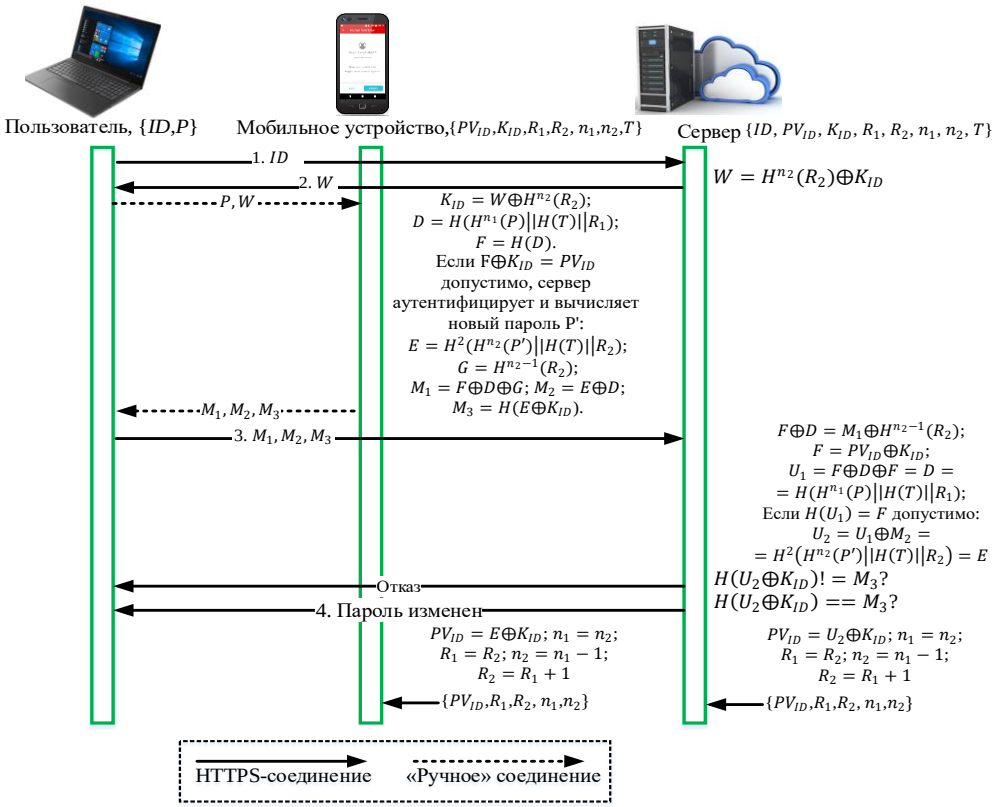



**Рисунок 8. Процедура смена пароля в методе Protokol_6**

*В первом параграфе* исследуется проблема создания устройства аутентификации на основе одноразового пароля. Для решения этой проблемы используются микроконтроллеры. Микроконтроллеры — это небольшие вычислительные устройства, которые можно использовать для создания различных устройств.

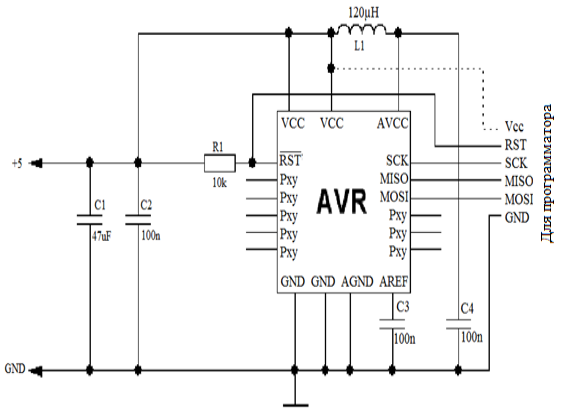



**Рисунок 9. Схема подключения микроконтроллера к блоку питания**

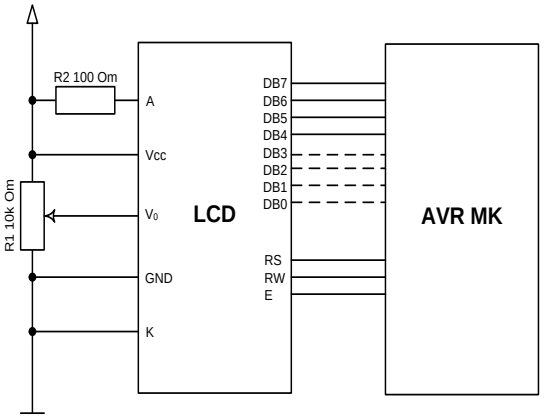



**Рисунок 10. Схема подключения LCD дисплея к микроконтроллеру**

На рисунке 9 показано подключение микроконтроллера AVR к блоку питания и интерфейс записи программы для него. А на рисунке 10 представлена схема подключения LCD дисплея к микроконтроллеру.

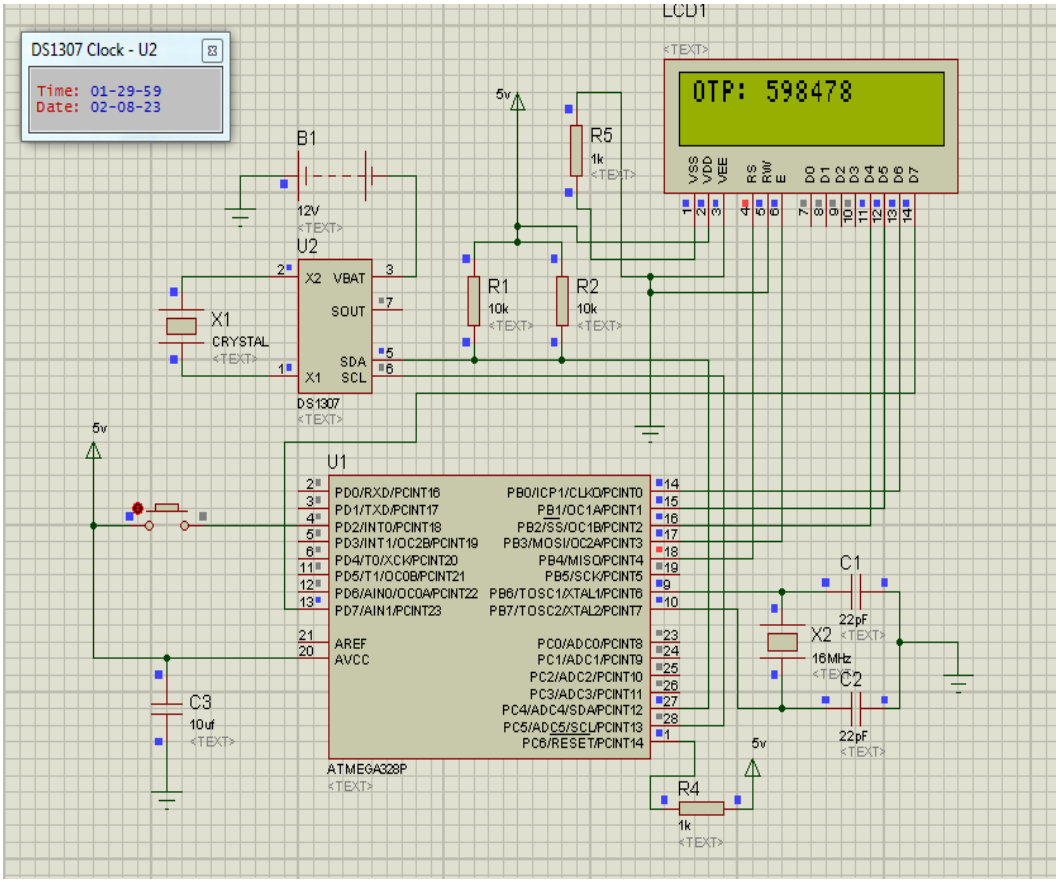



**Рисунок 11. Рабочее состояние аппаратно-программного устройства генератора одноразовых паролей**

При создании программы на основе компилятора CodeVisionAVR для предлагаемого устройства ее библиотека подбирается в зависимости от типа микроконтроллера. Он содержит множество функций, необходимых для микроконтроллера. Используя пакет программного обеспечения Proteus, с помощью схемы, показанной на рисунке 11, можно увидеть результаты этих функций.

*Во втором параграфе* анализируются методы и алгоритмы аутентификации, предложенные в третьей главе (таблицы 6, 7, 8).

**Таблица 6**

**Общие результаты анализа алгоритмов Protokol_1 и Protokol_2**

| № | Наименование протокола | Количество сообщений, обмениваемые при регистрации | Количество сообщений, обмениваемые при входе | Безопасный обмен сеансовыми ключами | Случайность генератора OTP |
|---|---|---|---|---|---|
| 1. | Google authenticator | 2 | 4 | - | Средняя |
| 2. | Microsoft authenticator | 2 | 4 | - | Средняя |
| 3. | Protokol_1 | 2 | 4 | + | Высокая |
| 4. | Protokol_2 | 2 | 4 | + | Высокая |

*В третьем параграфе* представлен анализ результатов, полученных от внедрения разработанных программных и аппаратно-программных средств на практике. Разработанные методы были внедрены на практике в деятельности различных организаций.

**Таблица 7**

**Общие результаты анализа методов Protokol_3, Protokol_4 и Protokol_5**

| № | Наименование метода | Количество сообщений, обмениваемые при регистрации | Количество сообщений, обмениваемые при входе | Криптографическое преобразование | Двухсторонняя аутентификация | Двухфакторная аутентификация | Участие достоверной стороны |
|---|---|---|---|---|---|---|---|
| 1. | Nidxem-Shreder | NA | 5 | Shifrlash | + | - | + |
| 2. | Neuman-Stub. | NA | 4 | Shifrlash | - | - | + |
| 3. | Otvey-Riis | NA | 5 | Shifrlash | - | - | + |
| 4. | Kerberos | NA | 4 | Shifrlash | + | - | + |
| 5. | Protokol_3 | 2 | 4 | HMAC | + | - | - |
| 6. | Protokol_4 | 2 | 6 | HMAC | + | + | - |
| 7. | Protokol_5 | 3 | 4 | HMAC | + | - | - |

В акционерном обществе «Асакабанк» внедрено программное средство «Система генерации одноразовых паролей на основе алгоритма хеширования». В результате научного исследования использование программных средств в услугах мобильного банкинга не причинило неудобств пользователям и процент неповторения одноразовых паролей был равен 62%.

**Таблица 8**

**Сравнительный анализ метода Protokol_6 с существующими аналогами с точки зрения требований безопасности**

| № | Наименование протокола | Номер требования безопасности | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1. | M.Jan va b. [71] | + | + | + | + | + | + | + | - | + | + |
| 2. | J. Arziyeva [53] | + | + | + | + | + | + | + | - | + | - |
| 3. | Ku [70] | + | + | + | + | - | - | - | - | + | - |
| 4. | Protokol-6 | + | + | + | + | + | + | + | + | + | + |

Протестирован в процессе реализации безопасной двухфакторной аутентификации между клиентом и сервером в приложениях Интернета вещей в рамках инновационного проекта «Разработка алгоритма и программы обеспечения конфиденциальности и целостности данных в приложениях Интернета вещей» в Обществе с ограниченной ответственностью «UNICON.UZ»-Центр научных-технических и маркетинговых исследований.

Программное средство «Система генерации одноразовых паролей на основе алгоритма хеширования» внедрено в ООО «Turon information technology group» в целях аутентификации пользователей в

информационной системе автоматизации работы негосударственных образовательных учреждений «EduSmart».

Программное средство алгоритма генерации одноразового пароля с высокой степенью случайности и неповторяемости внедрен в практическую деятельность Центра кибербезопасности оперативно-розыскного департамента Министерства внутренних дел Республики Узбекистан. В результате научного исследования показатель неповторения при генерации одноразовых 6-значных паролей составила на 28,4% выше, чем у существующих генераторов HOTP и TOTP.

## ЗАКЛЮЧЕНИЕ

В результате исследования, проведенного по теме «Методы и алгоритмы аутентификации пользователей на основе одноразовых паролей», были представлены следующие выводы:

1. Разработаны простые в реализации алгоритмы генерации одноразовых паролей в виде аппаратно-программных и программных средств на основе функции сокращения и ключевой хеш-функции с низким уровнем повторения. Разработанный алгоритм позволил генерировать шестизначные пароли с неповторяемостью 62,5%.
2. Разработан простой в реализации алгоритм генерации одноразового пароля на основе сокращения и симметричного блочного шифрования с использованием криптографического алгоритма. Разработанный алгоритм позволил генерировать шестизначные пароли с неповторяемостью 65,4%.
3. Степень неповторяемости 6- и 7-значных длинных паролей, генерируемых с помощью разработанного генератора, было достигнуто выше, чем у существующих генераторов HOTP и TOTP.
4. Разработаны алгоритмы аутентификации пользователей, основанные на использовании токенов в качестве второго фактора, реализованные в виде аппаратно-программных и программных средств, генерирующих одноразовые пароли. Разработанные алгоритмы позволили пользователям пройти аутентификацию по второму фактору на основе токена.
5. Разработаны методы двухсторонней и двухфакторной аутентификации пользователей, работающих в механизме «вопрос-ответ» на основе ключевых хеш-функций. Разработанные методы позволили проверить достоверность второго фактора при взаимной аутентификации сторон.
6. Разработан метод, основанный на хеш-функции, осуществляющий взаимную аутентификацию пользователя и сервера на основе использования мобильного устройства в качестве второго фактора. Разработанный метод показал, что обеспечивает устойчивость даже при использовании слабого пароля.

**SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.13/30.12.2019.T.07.02 AT TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES**

**TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES**

**IMAMALIYEV AYBEK TURAPBAYEVICH**

# USER AUTHENTICATION METHODS AND ALGORITHMS BASED ON ONE-TIME PASSWORDS

**05.01.05 – Methods and systems of information protection. Information security**

**DISSERTATION ABSTRACT**
**OF THE DOCTOR OF PHILOSOPHY (PhD) ON TECHNICAL SCIENCES**

**Tashkent-2024**

**The theme of doctor of philosophy (PhD) on technical sciences was registered at with the Higher attestation commission under the Ministry of Higher education, science and innovations of the Republic of Uzbekistan under No. B2024.1.PhD/T4416.**

The dissertation has been prepared at Tashkent university of information technologies named after Muhammad al-Khwarizmi.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (resume)) on the website of Scientific council (www.tuit.uz) and on the website of "ZiyoNet" Information and educational portal (www.ziyonet.uz).

| | |
|---|---|
| **Scientific adviser:** | **Khudoykulov Zarifjon Turakulovich**<br>doctor of philosophy in technical sciences (PhD), associate professor |
| **Official opponents** | **Juraev Gayrat Umarovich**<br>doctor of physics and mathematics, professor |
| | **Normatov Sherbek Bakhtiyarovich**<br>doctor of philosophy in technical sciences (PhD), associate professor |
| **Leading organization:** | **Scientific, technical and marketing research center "UNICON.UZ" LLC** |

The defense will take place "____" _____ 2024 at _____ the meeting of Scientific council No. DSc.13/30.12.2019.T.07.02 at Tashkent University of Information Technologies (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of the Tashkent University of Information Technologies (is registered under No.___). (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43).

Abstract of dissertation sent out on "____" _____ 2024 y.

(mailing report No. ___ on "____" _____ 2024 y.).

**B.Sh. Makhkamov**
Chairman of the scientific council awarding scientific degrees, doctor of economical sciences, professor

**M.S. Saitkamolov**
Scientific secretary of scientific council awarding scientific degrees, doctor of economical sciences, associate professor

**S.K. Ganiyev**
Chairman of the academic seminar under the scientific council awarding scientific degrees, doctor of technical sciences, professor

## INTRODUCTION (abstract of PhD thesis)

**The aim of the research work** is to investigate efficient algorithms for generating one-time passwords and user authentication methods and algorithms based on them.

**The object of the research work** is the process of verifying the authenticity of users in information and communication systems.

**The scientific novelty of the research work** is as follows:

for the purpose of secure and effective authentication of users, algorithms for generating one-time passwords of different lengths have been developed, which are easy to implement in the form of hardware and software based on the reduction function with a low repetition rate and the hash function with a key;

algorithms for verifying the authenticity of users by using tokens in the form of hardware and software as a second factor have been developed in order to eliminate security problems in one-factor authentication methods;

in order to efficiently use computing resources, methods have been developed that are based on key hash functions, work in the "question-answer" mechanism, and implement two-way and two-factor secure and effective authentication between the client and the server;

a method of mutual authentication of the user and the server based on the use of a mobile device as a second factor using a hash function has been developed.

**Implementation of research results.** Based on the scientific results obtained on the methods, algorithms and software tools of user authentication based on one-time password generation algorithms:

The "one-time password generation system based on the hashing algorithm" software tool that authenticates users based on the use of one-time passwords as a second factor was introduced in the joint-stock company "Asakabank" (Order of the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan dated March 29, 2024 2/ reference No. 17-944/22-2). As a result, the use of software tools in mobile banking services did not cause inconvenience to users, and the rate of non-repetition of one-time passwords equaled 62%, as well as prevented attacks such as QR code, mobile device theft, and SMS message interception.

A one-time password generator based on a hash function designed to be implemented in a hardware-software environment was developed at the "UNICON.UZ" Center for Science, Technology and Marketing Research Limited Liability Company, innovative project of "Algorithm and software for ensuring privacy and data integrity in Internet of Things applications", was used in the process of implementing secure two-factor authentication between the client and the server in Internet of Things applications (order of the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan dated March 29, 2024 2/ reference No. 17-944/22-2). As a result, out of 1 million 6-digit passwords generated by this algorithm, 618,988 were not repeated and the rate of non-repetition was 61,9%.

Used in one-way and two-way authentication method developed on the basis of HMAC algorithm "One-time password generation system based on hashing

algorithm" software tool "Turon information technology group" LLC was introduced in the "EduSmart" non-state educational institution automation information system in order to authenticate users (order of the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan dated March 29, 2024 2/17-944/ Reference No. 22-2). As a result, the software tool developed made it possible to generate one-time passwords with a high level of randomness and non-repetition.

The software tool of the one-time password generation algorithm with a high level of randomness and non-repeatability was implemented in the practical activities of the Cyber Security Center of the Rapid Investigation Department of the Ministry of Internal Affairs of the Republic of Uzbekistan (Ministry of Internal Affairs dated February 23, 2024 reference number 16/K5-2233). As a result of scientific research, the rate of non-repetition in the generation of one-time passwords with a length of six digits is 28,4% higher than that of existing OTP generators.

**Structure and volume of the dissertation.** The structure of the dissertation consists of an introduction, four chapters, conclusion, references and appendix. The volume of the thesis is 117 pages.

**E’LON QILINGAN ISHLAR RO‘YXATI**
**СПИСОК ОПУБЛИКОВАННЫХ РАБОТ**
**LIST OF PUBLISHED WORKS**

**I bo‘lim (I часть; I part)**

1. А.Т. Имамалиев. Проблема разработки механизма аутентификации ближней связи // International scientific journal of “The Way of Science”. № 7(77), 2020. Volgograd-2020. -С. 8-10. (5, Global Impact Factor).
2. С.К. Ганиев, А.Т. Имамалиев. Псевдотасодифий кетма-кетлик генератори асосида масофадан фойдаланувчининг аутентификаторини яратиш // “ТАТУ хабарлари” ilmiy-texnika va axborot-tahliliy jurnali. № 2(58)/2021. Toshkent-2021. -Б. 150-159. (05.00.00; №31).
3. Z. Khudoykulov, A.T. Imamaliyev. “Analysis Password-based Authentication Systems with Password Policy” // International Conference on Information Science and Communications Technologies: applications, trends and opportunities. ICISCT 2021. Tashkent, Urgench, Uzbekistan, -P. 1-3 (05.00.00; 30.10.2021, №308/6-son rayosat qarori). (3, **Scopus**).
4. О.П. Ахмедова, А.Т. Имамалиев. Фойдаланувчиларни аутентификациялаш усулларида хавфсизлик муаммолари // “Ахборот Коммуникациялар: Тармоқлар-Технологиялар-Ечимлар” ҳар чораклик илмий-техник журнал. № 2(62)2022, ISSN 2010-510X, -Б. 35-44. (05.00.00; №2).
5. A.T. Imamaliyev, S.K. Ganiyev, S. Usmanov. Algorithm of Generating One-Time Passwords for Two-Factor Authentication of Users // 12th World Conference on “Intelligent System for Industrial Automation” (WCIS-2022), Volume 2, Uzbekistan, Tashkent-2022. -P. 132-139. (3, **Scopus**).
6. Imamaliyev A.T. “Mobil telefonlar yordamida autentifikatsiyalash tizimining tahlili” // International scientific journal of “Innovative Development in Educational Activities”. VOLUME 2, ISSUE 11, 2023/11, -B. 439–443. (23, Scientific journal impact factor).
7. Imamaliyev A.T. ““SAVOL-JAVOB” mexanizmiga asoslangan HMAC algoritmi yordamida foydalanuvchilarni autentifikatsiyalash usuli” // “IQRO” jurnali. VOLUME 10, ISSUE 2, 2024, -B. 11–16, (slib.uz).
8. M.M. Karimov, K.A. Tashev, J. Arziyeva, A.A. Abdurakhmanov, A.T. Imamliyev. About one of the authentication methods // “TATU xabarlari” ilmiy-texnika va axborot-tahliliy jurnali. № 3/2013. Toshkent-2013. -P. 5-12. (05.00.00; №31).
9. Ташев, А.А. Абдуракҳманов, А.Т. Имамалиев, Ж. Арзиева. Парол генераторининг аппарат воситасини яратиш муаммоси // “TATU xabarlari” ilmiy-texnika va axborot-tahliliy jurnali. № 3/2013. Toshkent-2013. -Б. 19-24. (05.00.00; №31).
10. N.B. Nasrullaev, Sh.R. Gulomov, A.T. Imamaliyev. Approach to implementation of software and hardware control system activity protection // “TATU xabarlari” ilmiy-texnika va axborot-tahliliy jurnali. № 3(31)/2014. Toshkent-2014. -P. 125-129. (05.00.00; №31).

11. A.F. Verlan, M.M. Karimov, K.A. Tashev, A.T. Imamaliyev. Method of Authentication on Based Password Generators // 3rd international conference on “Application of Information and Communication Technology and Statistics in Economy and Education”. Bulgaria, Sofia-2013. -P. 773-777.

12. З.Т. Худойкулов, У.У. Тожиакбарова, А.Т. Имамалиев. Проблемы аутентификации при электронном голосовании // Электронный сборник научных статей по материалам Международной научно-технической конференции “Энергетика, инфокоммуникационные технологии и высшее образование”. Том 2. Алматы, Казань-2023. -С. 620-629.

13. З.Т. Худойкулов, А.Т. Имамалиев. Методы многофакторной аутентификации и связанные с ними проблемы безопасности // Электронный сборник научных статей по материалам Международной научно-технической конференции “Энергетика, инфокоммуникационные технологии и высшее образование”. Том 2. Алматы, Казань-2023. -С. 595-603.

14. С.К.Ганиев, А.Т. Имамалиев. Қисқа масофада боғланишли аутентификация масаласига доир // “Иқтисодиётнинг тармоқларини инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти” Республика илмий-техник анжуманининг маърузалар тўплами. Тошкент-2020. -Б. 376-378.

15. А.Т. Имамалиев. Псевдотасодфий кетма-кетлик генераторларига асосланган бир мартали паролларни шакллантириш муаммоси // “Иқтисодиётнинг тармоқларини инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти” Республика илмий-техник анжуманининг маърузалар тўплами. 2-қисм. Тошкент-2021. -Б. 305-308.

16. С.К.Ганиев, А.Т. Имамалиев. Аутентификация усулларининг қиёсий таҳлили // “Iqtisodiyot tarmoqlarining innovatsion rivojlanishida axborot-kommunikatsiya texnologiyalarining ahamiyati” Respublika ilmiy-texnik anjumanining ma’ruzalar to‘plami. Toshkent-2022. -Б. 374-377.

17. A.T. Imamaliyev. Ikki faktorga asoslangan autentifikasiya algoritmi // “Kompyuter ilmlari va muhandislik texnologiyalari” xalqaro ilmiy-texnik konferensiya materiallari to‘plami. 2-qism. Jizzax-2022. -B. 44-47.

18. Z.T. Xudoykulov, A.T. Imamaliyev, U.U. Tojiakbarova. Barmoq izi orqali identifikatsiya va utentifikatsiya tizmini amalga oshirish // “Кибермаконда содир этилаётган жиноятларга қарши кураш: муаммолар ва ечимлар” мавзусидаги Республика илмий-амалий конференция материаллари тўплами. Тошкент-2022. -B. 344-350.

19. A.T. Imamaliyev, U.U. Tojiakbarova, I.U. Xolimtayeva. RFID tizimi orqali identifikatsiya vautentifikatsiyani amalga oshirish // “Кибермаконда содир этилаётган жиноятларга қарши кураш: муаммолар ва ечимлар” мавзусидаги Республика илмий-амалий конференция материаллари тўплами. Тошкент-2022. -B. 333-338.

20. А.Т. Имамалиев. Елка орқали кўриш ҳужумига қарши ҳимоя усуллари // “Axborot xavfsizligi sohasida raqamlashtirish muammolari va

istiqbollari” Respublika ilmiy-amaliy konferensiya matyeriallari to‘plami. Toshkent - 2022. -Б. 94-96.

21. A.T. Imamaliyev, O. Ro‘zimov. Qo‘riqlash tizimlarida qo‘llaniladigan identifikatsiya vositalari // “Integrallashgan qo‘riqlash tizimlari – xavfsizlikni ta’minlovchi vositalarining rivojlanish istiqbollari” respublika ilmiy-amaliy konferensiya materiallari. Toshkent-2023. -B. 50-57.

22. A.T. Imamaliyev. Parolga asoslangan autentifikatsiya muammolari va yechimlari // “Integrallashgan qo‘riqlash tizimlari – xavfsizlikni ta’minlovchi vositalarining rivojlanish istiqbollari” respublika ilmiy-amaliy konferensiya materiallari. Toshkent-2023. -B. 57-62.

23. A.T. Imamaliyev. Bir martali parolni shakllantirish algorimlari asosida yaratilgan dasturiy moduli // “Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari” respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami. Toshkent-2023. -B. 30-35

24. A.T. Imamaliyev. Bir martali parolga asoslangan autentifikator qurilmasini ishlab chiqish // “Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari” respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami. Toshkent-2023. -B. 285-291

25. A.T. Imamaliyev, Z.T. Xudoyqulov. ATmega 16 mikrokontrollerida bir martali parolni generatsiyalash tizimi // Dasturga guvohnoma № DGU18805. 18.10.2022.

26. A.T. Imamaliyev, Z.T. Xudoyqulov, B.M. Shamshiyeva, U.U. Tojiakbarova, O.O. Tursunov, A.A. Karimov, I.S. Olimov. Heshlash algoritmi asosida bir martali parolni generatsiyalash tizimi // Dasturga guvohnoma № DGU18806. 18.10.2022.

Avtoreferat “Muhammad al-Xorazmiy avlodlari” ilmiy jurnali tahririyatida tahrirdan o‘tkazildi va o‘zbek, rus va ingliz tillaridagi matnlarini mosligi tekshirildi.

Bosishga ruxsat etildi: 22.09.2024-yil
Bichimi 60x84 1/16, «Times New Roman»
garniturada raqamli bosma usulida bosildi.
Nashriyot bosma tabog‘i: 2.5. Adadi: 100. Buyurtma № 60.
Bahosi kelishuv asosida

Nizomiy nomidagi Toshkent davlat pedagogika
universiteti bosmaxonasida chop etildi.
Manzil: Toshkent shahri, Chilonzor tumani,
Bunyodkor ko‘chasi 27-uy