ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.13/30.12.2019.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

АРЗИЕВА ЖАМИЛА ТИЛЕУБАЕВНА

ПСЕВДОТАСОДИФИЙ СОНЛАР ГЕНЕРАТОРИ АСОСИДА АУТЕНТИФИКАЦИЯЛАШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2020

УДК: 004.056.53

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси автореферати мундарижаси

Оглавление автореферата диссертации доктора философии (PhD) по техническим наукам

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

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.13/30.12.2019.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

АРЗИЕВА ЖАМИЛА ТИЛЕУБАЕВНА

ПСЕВДОТАСОДИФИЙ СОНЛАР ГЕНЕРАТОРИ АСОСИДА АУТЕНТИФИКАЦИЯЛАШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2020

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2019.1.PhD/T996 рақам билан рўйхатга олинган.

Диссертация Тошкент ахборот технологиялари университетида бажарилган.

Диссертация автореферати уч тилда (ўзбек, рус, инглиз (резюме)) Илмий кенгаш веб-саҳифасида (www.tuit.uz) ва «Ziyonet» Ахборот таълим порталида (www.ziyonet.uz) жойлаштирилган.

Илмий раҳбар:	**Каримов Маджит Маликович** техника фанлари доктори, профессор
Расмий оппонентлар:	**Ганиев Салим Каримович** техника фанлари доктори, профессор
	Жўраев Гайрат Умарович физика-математика фанлари доктори, доцент
Етакчи ташкилот:	**«UNICON.UZ» – фан-техника ва маркетинг тадқиқотлари маркази**

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.13/30.12.2019.T.07.01 Илмий кенгашнинг 2020 йил «08» сентябрь соат 16⁰⁰ даги мажлисида бўлиб ўтади. (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43, факс: (99871) 238-65-52, e-mail: tuit@tuit.uz).

Диссертация билан Тошкент ахборот технологиялари университети Ахборот-ресурс марказида танишиш мумкин (2820 рақам билан рўйхатга олинган.). (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-ўй. Тел.: (99871) 238-65-44).

Диссертация автореферати 2020 йил «25» сентябрь да тарқатилди.
(2020 йил «24» август даги 14 рақамли реестр баённомаси.)

Р.Х. Хамдамов
Илмий даражалар берувчи илмий кенгаш раиси, т.ф.д., профессор

Ф.М. Нуралиев
Илмий даражалар берувчи илмий кенгаш илмий котиби, т.ф.д., доцент

С.К. Ганиев
Илмий даражалар берувчи илмий кенгаш қошидаги илмий семинар раиси, т.ф.д., профессор

КИРИШ (фалсафа доктори (PhD) диссертациясининг аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. Жаҳонда аутентификациянинг анъанавий усулларида заифликларни ортиб бориши натижасида ташкилотларда қатъий ёки кўп факторли аутентификация усулларидан фойдаланиш кўламини кенгайтиришга алоҳида эътибор қаратилмоқда. Ахборот – коммуникация тизимлари ривожининг ҳозирги замон босқичида фойдаланувчиларни ҳақиқийлигини текширишда кўп факторли аутентификация усулларидан фойдаланиш муҳим ҳисобланади. Хусусан, Mircosoft компаниясининг хавфсизлик бўйича ходими, Алекс Вайнерт сўзларига кўра «Кўп факторли аутентификация усулларидан фойдаланиш натижасида автоматик равишда амалга оширилувчи ҳужумларнинг 99.9%и блокланган»[1]. Бу йўналишда ривожланган мамлакатларда, жумладан, АҚШ, Англия, Япония, Франция, Нидерландия ва бошқа давлатларда фойдаланувчиларни кафолатли аутентификациясини таъминловчи аппарат ва дастурий воситаларни ишлаб чиқиш муҳим аҳамият касб этмоқда.

Жаҳонда фойдаланувчи ҳақиқийлигини кафолатли текшириш имкониятини берувчи, фойдаланишга қулай ва кам харажатли кўп факторли аутентификация усулларини яратишга йўналтирилган илмий тадқиқот ишлари олиб борилмоқда. Бу борада, амалда кенг қўлланилувчи паролга асосланган аутентификация усулида мавжуд хавфсизлик муаммоларини бартараф этишда қўшимча фактор сифатида бир мартали пароллардан фойдаланишнинг самарали ва хавфсиз усулларини ишлаб чиқиш муҳим вазифалардан бири ҳисобланади. Шу билан бирга, бир мартали парольларни яратиш усулларини ва унга асосланган мавжуд аутентификация усулларининг бардошлигини таҳлил қилиш ҳамда такомиллаштириш зарур бўлмоқда.

Республикамизда давлат ва хўжалик бошқарув органларида фойдаланувчиларни ҳақиқийлигини текширишда ва молиявий операцияларни кафолатли амалга оширишда жараён хавфсизлигини таъминлашга қаратилган кенг қамровли чора-тадбирлар амалга оширилмоқда. 2017-2021 йилларда Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегиясида, жумладан «...ахборот хавфсизлигини таъминлаш ва ахборотни ҳимоялаш тизимини такомиллаштириш, ахборот соҳасидаги таҳдидларга қарши ўз вақтида ва муносиб қаршилик кўрсатиш»[2] вазифалари белгиланган. Мазкур вазифаларни бажаришда фойдаланувчиларни ҳақиқийлигини текширишнинг самарали, хавфсиз ва паролга асосланган усуллари ҳамда воситаларини ишлаб чиқиш муҳим вазифалардан бири ҳисобланади.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида»ги, 2018 йил 14 мартдаги ПФ-5379-сон

[1] https://www.zdnet.com/article/microsoft-using-multi-factor-authentication-blocks-99-9-of-account-hacks/

[2] Ўзбекистон Республикаси Президенти 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида» ги Фармони

«Ўзбекистон Республикасининг давлат хавфсизлиги тизимини такомиллаштириш чора-тадбирлари тўғрисида»ги, 2018 йил 19 февралдаги ПФ-5349-сон «Ахборот технологиялари ва коммуникациялари соҳасини янада такомиллаштириш чора-тадбирлари тўғрисида»ги Фармонлари ва 2007 йил 3 апрелдаги ПҚ-614-сон «Ўзбекистон Республикасида ахборотни криптографик муҳофаза қилишни ташкил этиш чора-тадбирлари тўғрисида»ги Қарори ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишда мазкур диссертация тадқиқоти маълум даражада хизмат қилади.

Тадқиқотнинг республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги. Мазкур тадқиқот республика фан ва технологиялар ривожланишининг IV. «Ахборотлаштириш ва ахборот-коммуникация технологияларини ривожлантириш» устувор йўналиши доирасида бажарилган.

Муаммонинг ўрганилганлик даражаси. Аутентификация тизимлари учун бир мартали паролларни генерациялаш, хусусан, паролларни сақлаш, уларни узатиш ва хавфсизлик хусусиятлари бўйича таҳлил қилиш соҳасида L.Lamport, M.Sandirigama, A.Shimizu, W.C.Ku ва бошқа чет эллик олимлар ҳамда RSA лабораторияси (John Brainard, Ari Juels, Michael Szydlo, Moti Yung ва бошқалар), Microsoft лабораторияси (Stuart Schechter, Serge Egelman, Serge Egelman) каби халқаро ташкилотлар томонидан инженерлик-тадқиқот ишлари олиб борилмоқда.

Ўзбекистонда С.К.Ганиев, М.М.Каримов, П.Ф.Хасанов, Д.Е.Акбаров бошчилигидаги илмий жамоалар томонидан ахборот тизимларининг ҳимояланганлигини таҳлил қилиш, аутентификация воситаларини ишлаб чиқиш, аутентификация усулларини такомиллаштириш ва паролларни хавфсиз узатиш усуллари ўрганиб чиқилган.

Шунинг билан бирга, ҳозирда фойдаланувчилар ҳақиқийлигини текширишда қўшимча фактор сифатида қўлланилаётган бир мартали паролларни псевдотасодифий сонлар генератори асосида ҳосил қилиш усуллари, уларга асосланган «савол-жавоб» механизми кўринишидаги қатъий аутентификация усуллари етарли даражада ўрганилмаган.

Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация тадқиқоти Тошкент ахборот технологиялари университетининг илмий-тадқиқот ишлари режасининг №17-007 – “Компьютер тармоқларида суқилиб киришларини аниқловчи ва бартараф этувчи тизимларни самарадорлигини оширувчи усул ва воситалар” (2009-2011) мавзусидаги лойиҳа доирасида бажарилган.

Тадқиқотнинг мақсади тасодифийлик даражаси юқори бўлган псевдотасодифий сонлар генератори асосида самарали, хавфсиз қатъий аутентификация усул ва алгоритмларини ишлаб чиқишдан иборат.

Тадқиқотнинг вазифалари:

тасодифийлик даражаси юқори бўлган псевдотасодифий сонларни генерациялаш усулини ишлаб чиқиш;

тасодифийлик даражаси юқори бўлган бир мартали паролларни генерациялаш усули ва алгоритмини ишлаб чиқиш;

бир мартали паролларга асосланган аутентификация усуллари ва алгоритмларини такомиллаштириш;

бир мартали паролларни самарали етказишга асосланган кўп факторли аутентификация усули ва алгоритмини ишлаб чиқиш;

бир мартали паролларга асосланган қатъий аутентификация протоколини такомиллаштириш.

Тадқиқотнинг объекти сифатида ахборот тизимларида фойдаланувчиларни ҳақиқийлигини текшириш жараёни олинган.

Тадқиқотнинг предметини псевдотасодифий сонлар генераторига асосланган қатъий аутентификация усуллари ва алгоритмлари ташкил этади.

Тадқиқотнинг усуллари. Тадқиқот жараёнида алгоритмлаш, эҳтимоллар назарияси, сонлар назарияси, қиёсий таққослаш, хавфсизликка таҳлиллаш ва объектга йўналтирилган дастурлаш усулларидан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

бир мартали паролларни юқори тасодифийлик даражасига эга бўлишини ҳисобга олган ҳолда псевдотасодифий сонлар генератори ишлаб чиқилган;

иррационал сонлар хусусиятидан фойдаланиб юқори такрорланмаслик даражасига эга бир мартали паролларни генерациялаш усули ва алгоритми ишлаб чиқилган;

мавжуд хавфсизлик муаммоларини бартараф этиш мақсадида TOTP/HOTP алгоритмига ва SMS хабарда юборилувчи бир мартали паролларга асосланган аутентификация усуллари такомиллаштирилган;

бир мартали паролни QR код кўринишида етказишга асосланган аутентификация усули ва алгоритми ишлаб чиқилган;

икки томонлама аутентификациялаш ва сеанс калитини тақсимлаш имкониятини мавжуд эмаслигини инобатга олган ҳолда бир мартали паролга асосланган аутентификация протоколи такомиллаштирилган.

Тадқиқотнинг амалий натижаси қуйидагилардан иборат:

бардошли симметрик блокли шифрлаш алгоритмлари асосида юқори тасодифийлик даражасига эга псевдотасодифий сонлар генератори ва унга асосланган бир мартали пароллар генераторининг дастурий воситаси ишлаб чиқилган;

TOTP/HOTP алгоритмига асосланган аутентификация тизимларида тақсимланган калитларни хавфсиз узатиш ва сақлаш имкониятига эга мобил дастурий восита ишлаб чиқилган;

SMS хабарда бир мартали паролларни шифрланган кўринишга етказиб берувчи мобил дастурий восита ишлаб чиқилган;

QR код кўринишида тақдим қилинган бир мартали парол ёрдамида “савол-жавоб” механизмига асосланган аутентификация усулининг мобил дастурий воситаси ишлаб чиқилган.

Тадқиқот натижаларининг ишончлилиги. Тадқиқот натижаларининг ишончлилиги ахборот тизимларда зарур бўлган псевдотасодифий кетма-кетликларни ҳосил қилиш усули, бир мартали паролларни генерациялаш усули, тақсимланган калитларни хавфсиз узатиш, сақлаш, таҳдидлардан ҳимоялаш усуллари ва алгоритмларидан олинган реал ҳамда тажрибавий таҳлиллар билан изоҳланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти тасодифийлик даражаси юқори бўлган псевдотасодифий сонларни ва унинг асосида бир мартали паролларни генерациялаш усулини ишлаб чиқиш, унга асосланган аутентификация усулларини ва алгоритмларини ишлаб чиқиш ҳамда такомиллаштириш билан изоҳланади.

Тадқиқот натижаларининг амалий аҳамияти ахборот тизимларида паролга боғлиқ таҳдидларни минималлаштириш, тақсимланган калитларни хавфсиз узатиш ва сақлаш имконияти билан изоҳланади.

Тадқиқот натижаларининг жорий қилиниши. Ишлаб чиқилган бир мартали паролларни генарациялаш, унга асосланган аутентификация усуллари, алгоритмлари ва дастурий воситаларини ишлаб чиқиш бўйича олинган натижалар асосида:

юқори тасодифийлик ва такрорланмаслик даражасига эга бир мартали паролларни генерациялаш усулининг дастурий воситаси Қорақалпоғистон Республикаси Давлат солиқ бошқармаси Нукус тумани Давлат Солиқ инспекциясининг амалий фаолиятида жорий қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 9 июндаги 33-8/3105-сон маълумотномаси). Илмий тадқиқот натижасида олти хона узунликдаги бир мартали паролларни генерациялашда 36,865% тўлиқ такрорланмаслик даражасига эришилган;

бир мартали пароллардан иккинчи фактор сифатида фойдаланишга асосланган фойдаланувчиларни аутентификацияловчи “Secure SMS Authenticator” ва “Secure OTP Authenticator” дастурий воситалари “Микрокредитбанк”нинг Қорақалпоғистон Республикаси филиалига жорий қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 9 июндаги 33-8/3105-сон маълумотномаси). Илмий тадқиқот натижасида дастурий воситаларни мобайл банк хизматларида қўллаш фойдаланувчиларга ноқулайлик туғдирмасдан QR кодни ўғирлаш, мобил қурилмани ўғирлаш ва SMS хабарни тутиб олишга қаратилган ҳужумларни олдини олишга имкон берган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари 2 та халқаро ва 10 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Диссертациянинг мавзуси бўйича жами 26 та илмий иш чоп этилган, жумладан, Ўзбекистон Республикаси Олий аттестация комиссиясининг диссертацияларнинг асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларида 8 та мақола, 2 таси хорижий ва 6 таси республика журналларида нашр этилган ҳамда 3 та ЭҲМ учун яратилган дастурий воситаларни қайд қилиш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация таркиби кириш, тўртта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертация ҳажми 119 бетни ташкил этади.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида диссертация мавзусининг долзарблиги ва зарурияти асосланган, тадқиқотнинг Ўзбекистон Республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги кўрсатилган, мақсад ва вазифалари белгилаб олинган ҳамда тадқиқот объекти ва предмети аниқланган, олинган натижаларнинг ишончлилиги асослаб берилган, уларнинг назарий ва амалий аҳамияти, тадқиқот натижаларини амалда жорий қилиш ҳолати, нашр этилган ишлар ва диссертациянинг тузилиши бўйича маълумотлар келтирилган.

Диссертациянинг «**Ахборот-коммуникацион тизимларида аутентификация муаммолари»** деб номланган биринчи боби ахборотни ҳимоялашда аутентификациялаш усулларининг ўрни, аутентификация усуллари ва уларда мавжуд таҳдидлар таҳлили ва бир мартали паролларга асосланган аутентификация усулларининг таҳлилига бағишланган.

Фойдаланувчиларни аутентификациялаш усуллари 3 туркумга: фойдаланувчи билган бирор билим, фойдаланувчида мавжуд бирор нарса ва фойдаланувчини характерловчи бирор нарса асосида аутентификациялашга бўлинади. Аутентификация усуллари орасида содда паролларга асосланган усулнинг оммавийлиги ва фойдаланиш учун осонлик даражаси юқори ҳисоблансада, жуда паст хавфсизлик даражасига эга ҳамда эсда сақлаш заруриятини талаб этади. Токенга асосланган аутентификация усуллари эса юқори хавфсизлик даражасини таъминлаб, инфратузилма ва қурилма нархининг юқорилиги сабабли оммавийлик даражаси паст ҳамда ҳар доим бирга олиб юришни талаб этади. Биометрик параметрларга асосланган аутентификациялаш усуллари эсда сақлаш ва олиб юриш каби заруриятларни талаб этмасада, веб ресурслардан фойдаланишда ноқулай, оммавийлик даражаси паст ва юқори нархга эга.

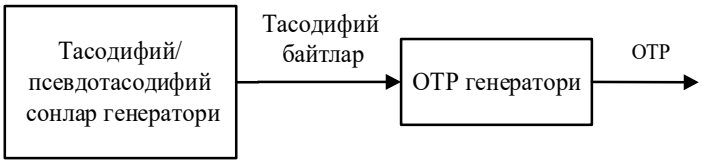
Амалда биринчи туркумга тегишли аутентификация усуллари кенг тарқалгани боис, мавжуд оммавийликни сақлаб туриш учун ундаги хавфсизлик муаммоларини бартараф этишга катта эътибор қаратилмоқда. Бирор нарсани билишга асосланган аутентификация усулларига қаратилган ҳужумларни олдини олишга қарши таклиф этилган усуллар тўлақонли равишда ҳимояни таъминламайди. Бироқ, олинган таҳлил натижаларидан бир

мартали пароллар (One time password, OTP) га асосланган аутентификация усуллари мавжуд ҳужумларга қарши муҳим восита эканлигини кўриш мумкин.

Диссертациянинг **«Самарали паролларни генерациялаш усули ва алгоритми»** деб номланган иккинчи бобида бир мартали паролларни генерациялаш усуллари таҳлил қилинган ва псевдотасодифий сонлар генератори, унга асосланган бир мартали паролларни генерациялаш усули ва алгоритми таклиф этилган.

Бир мартали паролларни генерациялашда турли усуллардан фойдаланилиб, уларга вақт меткасидан кирувчи параметр сифатида фойдаланувчи псевдотасодифий сонлар генераторига асосланган, санокдан кирувчи параметр сифатида фойдаланувчи псевдотасодифий сонлар генераторига асосланган, маълум белгилар тўпламидан фойдаланиб паролларни генерациялашга асосланган ва тасодифий сонлар генераторидан паролларни генерациялашга асосланган усулларни келтириш мумкин.

Биринчи ва иккинчи гуруҳлар асосан ҳар иккала томонда бир хил ОТРни ҳосил қилиш учун фойдаланилса, кейинги гуруҳлар сервер томонда ОТРни генерациялаш ва уни мижозга узатишга асосланган аутентификация усулларида кенг қўлланилади. Псевдотасодифий сонлар генераторига (ПТСГ) асосланган ОТРларни генерациялаш ўзига хос хусусиятга эга бўлиб, бу уларда криптографик акслантиришлардан фойдаланилгани билан изоҳланади. Тўртинчи гуруҳга тегишли ОТРларни генерация қилишнинг умумий кўриниши 1-расмда келтирилган.

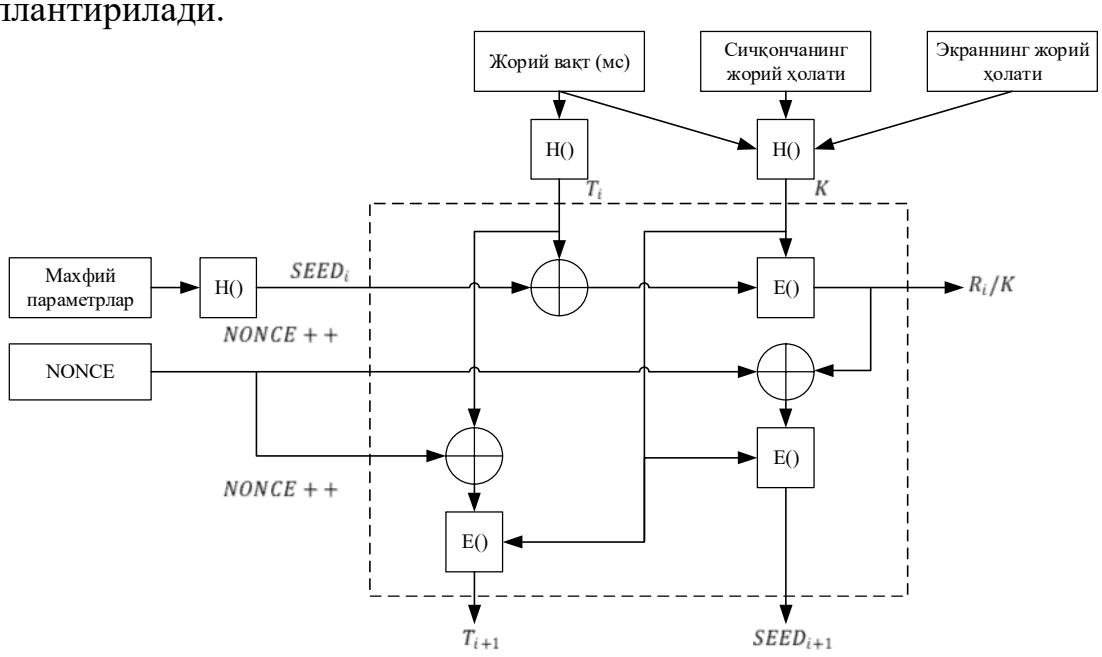


1-расм. ПТСГ асосида ОТРларни генерациялаш

Таклиф этилган ёндашувга асосан ОТРни генерациялаш усули учун псевдотасодифий кетма-кетликларни ҳосил қилувчи генераторнинг функционал кўриниши 2 - расмда келтирилган. Таклиф этилаётган ПТСГ учун тўпланиши осон бўлган сичқончанинг жорий ҳолати, операцион тизимнинг юқори аниқликдаги вақт меткаси, фойдаланувчи ишчи столининг жорий ҳолати каби параметрлар энтропия манбаси сифатида олинди. Бундан ташқари, таклиф этилган ПТСГ учун қўшимча кириш қийматлари сифатида 128 битли *nonce* катталигидан ва махфий параметр сифатида қурилманинг MAC (Media Access Control) манзили, IP (Internet Protocol) манзили, қаттиқ дискнинг серия рақами каби катталикдан фойдаланилди.

ПТСГ учун ички ҳолатни бошқариш муҳим аҳамиятга эга бўлиб, бунда ички функциялар деб аталувчи функциялардан фойдаланади. Инициализация функцияси 2-расмдан келиб чиқиб, бирор бир томонлама функция $H()$ ёрдамида жорий вақт T_i қиймати, жорий вақт, сичқончанинг жорий ҳолати ва экраннинг жорий ҳолати асосида калит K қиймати, махфий параметрлар асосида $SEED_i$ параметр қиймати ва бирор криптографик бўлмаган сонлар

генератори (ёки фойдаланувчи киритган) асосида $NONCE$ қиймати шакллантирилади.



2 – расм. Таклиф этилган ПТСГ функциональ кўриниши

Қийматларни генерациялаш функцияси талаб қилинган ҳажмдаги псевдотасодифий кетма-кетликларни жорий ички ҳолатдан фойдаланган ҳолда ҳосил қилади ва кейинги сўров учун ички ҳолатни янгилайди. 2-расмга асосланган ҳолда қийматларни генерациялаш функциясини бир блок учун қуйидагича ифодалаш мумкин:

- $R_i = E_K(T_i \oplus SEED_i)$;
- $SEED_{i+1} = E_K(R_i \oplus NONCE++)$;
- $T_{i+1} = E_k(T_i \oplus NONCE++)$.

Бу ерда, $E_K()$ – бардошли симметрик шифрлаш алгоритми бўлиб, унда K – битли калитдан фойдаланилади ва калит K нинг узунлиги $H()$ – бир томонлама (хэш функция) функция қийматига тенг бўлиши талаб қилинади. Масалан, 128 – бит хэш қийматни ҳосил қилувчи MD5 - хэш функцияси ва 128 – бит калит улчамли ихтиёрий симметрик блокли шифрлардан фойдаланиш мумкин. Ёки, $H()$ – бир томонлама хэш функция қийматидан $E()$ – симметрик блокли шифрлаш учун калитни ҳосил қилишнинг алтернатив усулидан фойдаланиш талаб этилади.

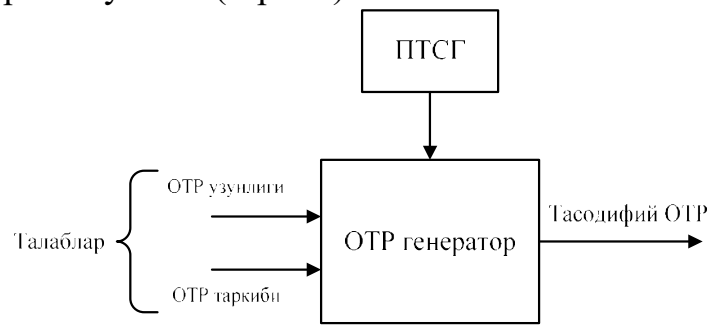
ПТСГлардан ҳосил бўладиган кетма-кетликларни тасодифийликка текширишнинг қатор усуллари мавжуд бўлиб, улар орасидан статистик тестларга асосланган усуллар кенг қўлланилади. Шу сабабли, 2-расмда келтирилган ПТСГдан олинган натижаларнинг тасодифийлик даражасини текшириш учун NIST SPECIAL PUBLICATION 800-22 статистик тестлар тўпламидан фойдаланилди. Бунинг учун, ПТСГдан 5 марта 2 миллион битдан бўлган намуналар олинди. Мазкур тестлар тўпламида 15 та тест мавжуд бўлиб, таклиф этилган ва мавжуд генераторларнинг тестлаш натижалари жадвалда a/b кўринишида берилган. Бунда b – жами тестлар сони, яъни 15 га тенг. a – кетма-кетликнинг нечтаси тестдан ўтганини англатади (1-жадвал).

1– жадвал

Генераторларнинг тестлаш натижалари

Генератор номи	Тетслаш наъмуналари				
	1	2	3	4	5
CryptGenRandom	14/15	15/15	14/15	13/15	15/15
/dev/urandom	15/15	15/15	15/15	15/15	15/15
Java Random()	15/15	15/15	15/15	15/15	14/15
Python Random()	14/15	15/15	15/15	15/15	15/15
Таклиф этилган ПТСГ	14/15	15/15	15/15	15/15	15/15

Статистик тестлар натижаси таклиф этилган ПТСГнинг тасодифийлик даражасини мавжудлари орасида юқорилигини кўриш мумкин. Таклиф этилган псевдотасодифий сонлар генераторини ПТСГ сифатида белгилаган ҳолда, унга асосланган паролларни генерациялаш усулининг функционал схемасини келтириш мумкин (3-расм).



3-расм. Тизим ПТСГга асосланган ОТР генераторининг умумий кўриниши

ОТР генераторлари учун ҳосил бўлаётган бир мартали паролларни *текис тақсимот* функциясига (continuous uniform distribution) бўйсиниши муҳим ҳисобланади. *Текис тақсимот* ёки *тўртбурчак тақсимот* бу – ўзгармас эҳтимолликка эга бўлган тақсимот бўлиб, чиқувчи қийматларни аниқ бир оралиқда ётишини англатади. Узлуксиз текис тақсимотнинг эҳтимоллик зичлик функцияси (Probability density function, PDF) қуйидагига тенг:

$$f(x) = \begin{cases} \frac{1}{b-a}, & x \in [a,b] \\ 0, & x \notin [a,b] \end{cases} \quad (1)$$

(1) тенгликда $a = 0$ ва $b = 1$ га тенг бўлса, у ҳолда $U(a,b)$ тақсимот стандарт текис тақсимот функцияси деб аталади.

Текис тақсимот қонуниятига асосланган кетма-кетликларни олишнинг қатор усуллари мавжуд бўлиб, улар орасидан иррациональ сонларга асосланган ёндашув алоҳида аҳамиятга эга. Хусусан, Д.И.Голенко томонидан псевдотасодифий сонларни генерациялашнинг Нейман усули айнан иррациоанал сонлар хусусиятидан келиб чиққан ҳолда модификацияланган. Бунда муаллиф назарий текис тақсимот функциясидан кичик фарқ қилувчи қуйидаги функцияни келтирган:

$$\xi_i = \{i\Theta\} \quad (2)$$

Бу ерда, Θ – иррационал сон бўлиб, муаллиф томонидан унга мисол сифатида $\sqrt{2}$, $\frac{\sqrt{2}}{2}$, $\frac{\sqrt{3}}{3}$, $\sqrt{3}$ ва $\frac{\sqrt{5}-1}{2}$ иррационал сонлари келтирилган. Мазкур ёндашувчи тўғрилигини текшириш учун $1 \le i \le 1000000$ ораликда Θ – иррационал соннинг юқорида келтирилган қийматлари ва таҳлиллар асосида танлаб олинган $\sqrt{7}$, $\frac{\sqrt{7}}{7}$ иррационал сонлари ва π сони учун (2) тенглик қийматлари ҳисобланиб, олинган натижаларнинг каср қисмларидан 6 та ва 7 тадан сонлар олиниб, уларни текис тақсимот қонунига асосланиши текширилди. Таҳлил натижасида $\sqrt{7}$ иррационал сони 6 та ва 7 та узунликдаги сонларни ҳосил қилишда мос равишда 88,3% ва 100% такрорланмасликни қайд этиб, текис тақсимот функциясига энг кўп бўйсиниши кўрсатди.

Иррационал сонларнинг текис тақсимланганлик хусусиятида келиб чиқиб, тасодифийлик таъминлаш учун ПТСГ ёрдамида i саноқни танлаш зарур бўлади. Мазкур бир мартали паролларни генерациялаш усули қуйида келтирилган.

Бу ерда қуйидаги бегиланишлар қабул қилинган:

1. $S_0 = \{0, \dots, 9\}, S_1 = \{0, \dots, 9, A, \dots, Z\}, S_2 = \{0, \dots, 9, a, \dots, z, A, \dots, Z\}$ белгилар тўплами. Бунда ҳар бир тўпламдаги белгилар сони $len(S_0) = 10, len(S_1) = 36, len(S_2) = 62$ га тенг.

2. $R = \{L, S_i\}$ – бир мартали парол учун талаблар бўлиб, L – бир мартали парол узунлигини ($L \in [6, 10]$), S_i – белгилар тўпламини билдиради ($i \in [0,2]$).

3. C_j^l – ПТСГдан ҳосил бўлган $j-$тасодифий қиймат бўлиб, l – унинг битдаги ўлчамини кўрсатади.

4. P_j – генерация қилинган j – бир мартали парол.

5. $F(R, C_j^l)$ – бир мартали паролни ҳосил қилиш функцияси бўлиб, бу ерда, $P_j = F\left(R, C_j^l\right) = F(\{L, S_i\}, C_j^l)$ тенглик ўринли.

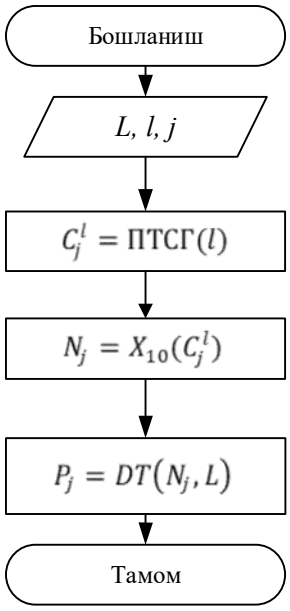
6. $DT(N_j, L)$ – динамик қисқартириш функцияси бўлиб, ОТР узунлигига L боғлиқ ҳолда P_j бир мартали паролни ҳосил қилиб беради:

$$DT\left(N_j, L\right) = S(M\left(N_j * \Theta\right), L)$$

Бу ерда, $M()$ – функция, $Nonce$ тасодифий қийматни Θ - иррационал сонга кўпайтириб, каср қисмини қайтаради. $S()$ – функция эса, $M()$-функция натижасининг ўнг томонидан L та рақамни қайтаради.

Таклиф этилаётган ОТР генератори учта S_0, S_1 ва S_2 тўпламдаги белгилардан иборат бўлган паролларни генерация қилиш имкониятига эга бўлиб, S_0 тўплам элементларидан иборат ОТРни ҳосил қилиш усулининг блок схемаси 4-расмда келтирилган.

Фақат рақамдан иборат бўлган ОТРлар амалда энг кенг қўлланилади. S_0 тўплам элементларидан иборат бўлган ОТРларни генерация қилиш функцияси $F\left(R, C_j^l\right) = F\left(\{L, S_0\}, C_j^l\right)$ га тенг. Бу ҳолда талаб этилувчи ОТРни узунлиги L нинг ихтиёрий мумкин бўлган қийматлари учун ПТСГдан бир блок узунлигидаги тасодифий қиймат олинади. Бу ҳолда ОТРни генерация қилишнинг умумий кетма-кетлиги қуйидагича:



4-расм. S_0 тўплам белгиларидан иборат паролларни ҳосил қилиш усулининг блок схемаси

a. Талаб этилган P_j бир мартали паролни генерация қилиш учун ПТСГидан l бит узунлигидаги C_j^l генерация қилинади.
b. C_j^l битлар кетма-кетлигидан ўнлик саноқ тизимидаги $N_j = X_{10}(C_j^l)$ ҳосил қилинади.
c. Талаб этилган P_j бир мартали паролни ҳосил қилиш учун $P_j = DT(N_j, L)$ тенгликдан фойдаланилади.

Таклиф этилган OTP генераторининг такрорланмаслик даражаси HOTP генератори ва $random()$ функцияси билан таққосланди. Ҳар бир алгоритм ёрдамида 6 ва 7 узунликдаги 1 миллионта OTP ҳосил қилинди. Олинган тажриба натижалари 2-жадвалда акс эттирилган.

2-жадвал

S_0 тўплам элементларини ҳосил қилиш натижалари

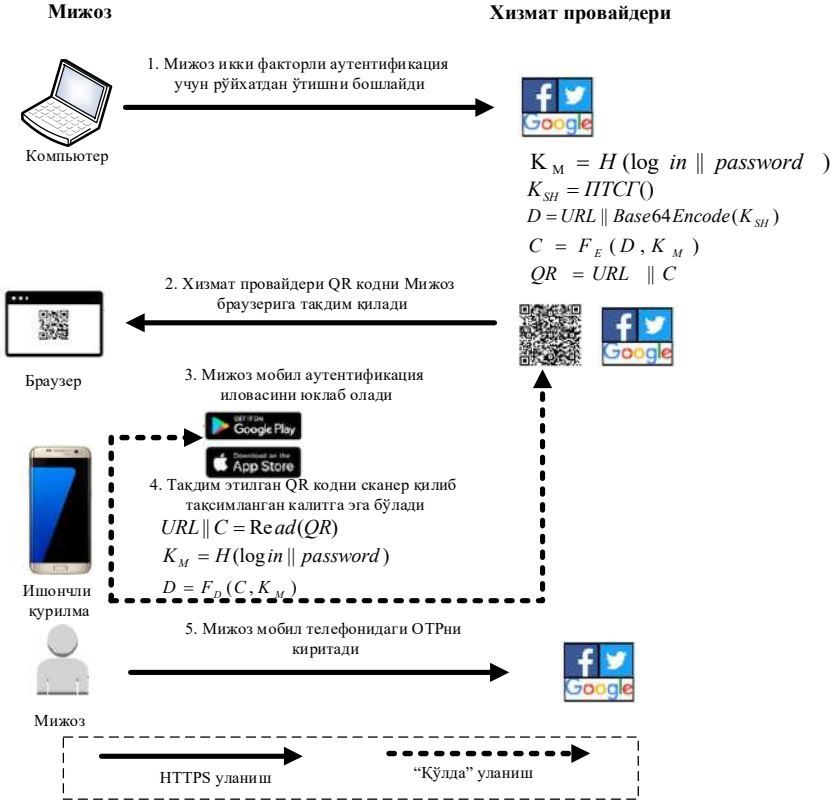
OTP генераторлари	**Такрорланишлар сони**										**Такрорланмаслик**
	2 марта	3 марта	4 марта	5 марта	6 марта	7 марта	8 марта	9 марта	9 дан ортиқ	жами	
HOTP (6)	184085	61208	15331	3080	490	71	11	0	0	264276	367957
$random()(6)$	183757	61646	15322	3078	517	72	8	2	0	264402	367182
1-алгоритм(6)	68394	2898	0	0	0	0	0	0	0	71292	854518
HOTP (7)	44964	1547	43	0	0	0	0	0	0	46554	905253
$random()(7)$	44923	1472	40	0	0	0	0	0	0	46435	905578
1-алгоритм(7)	0	0	0	0	0	0	0	0	0	0	1000000

Олинган тажриба натижаси таклиф этилган OTPни генерациялаш усули мавжудларига қараганда юбори такрорланмаслик даражасига эгалигини кўрсатади.

Диссертация ишининг «**Бир мартали паролга асосланган аутентификация протоколини ишлаб чиқиш**» номли учинчи бобида бир мартали пароллар генератори асосида аутентификация усулларидаги хавфсизлик муаммоларини бартараф этишга ва уларни таҳлил қилишга бағишланган бўлиб, дастлаб амалда фойдаланилаётган бир мартали паролларга асосланган аутентификация усулларидаги хавфсизлик муаммолари келтирилган ва шундан сўнг, уларни бартараф этиш усули таклиф этилади.

HOTP ёки TOTP (Time-based One-time Password) алгоритмига асосланган усуллар. TOTP алгоритмига асосланган икки томонлама аутентификациялашни амалга оширувчи иловаларда тақсимланган калитнинг хавфсизлигини таъминлашга эътибор қаратилмаган. Бу эса веб браузер кукиларида сақланувчи QR (Quick Response) код кўринишидаги тақсимланган калитни бузғунчи томонидан қўлга киритиш имконини яратади. Шу сабабли,

тақсимланган калитни биринчи фактор параметрлари асосида ҳимоялашга асосланган усулнинг рўйхатдан ўтиш босқичи 5-расмда келтирилган.

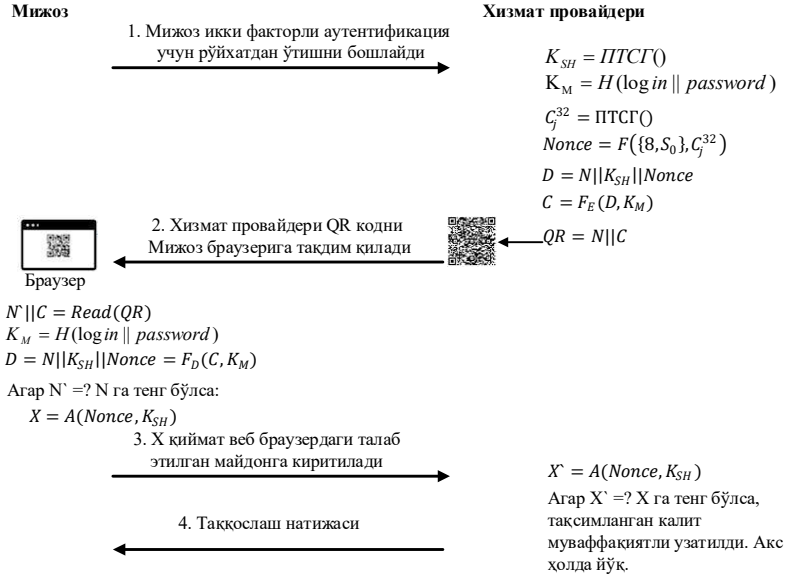


5-расм. Такомиллаштирилган TOTP асосланган аутентификация протоколида рўйхатдан ўтиш босқичи

Бу ерда, $H()$ –ихтиёрий бир томонлама функция бўлиб, бардошли бўлиши талаб этилади ва биринчи аутентификациялаш омиллари асосида ҳисобланади. K_{SH} – тақсимланган калит бўлиб, ПТСГидан генерация қилинади. $F_E()$ – симметрик блокли шифрлаш алгоритми бўлиб, фойдаланувчи томонидан танланади. URL – фойдаланилган хизмат номи ёки манзилини кўрсатувчи катталик бўлиб, қатор кўринишда тақдим этилади. Барча тўпланган маълумотлар фойдаланувчи томонидан ўқиб олишга қулай бўлиши учун QR код кўринишида тақдим этилган.

"Савол-жавоб" механизмига асосланган бир мартали парол ёрдамида аутентификация усули. Ушбу усул вазифаси нуқтаи назаридан HOTP ёки TOTP протоколларига ўхшаш, бироқ "савол-жавоб" механизмига асосланган бир мартали пароллар асосида аутентификация усулини ишлаб чиқилган. Ушбу усулда ҳам тақсимланган калитга эга бўлиш жараёни 5-расмдаги каби амалга оширилади. Кириш босқичи эса 6-расмдаги каби амалга оширилади. Таклиф этилган усулнинг умумий моҳияти сервер томонидан QR код кўринишида "савол"ни тақдим этиш ва унинг "жавобини" фойдаланувчи мобил иловаси ёрдамида топишдан иборат. Мазкур ҳолда $H()$ ва $A()$ – функциялар бардошли бир томонлама хэш функция ҳамда N – кўрсатилаётган хизмат номини кўрсатади. Аутентификация усулининг тасдиғи сервер ва мижоз томонда ягона $A()$ – функция фойдаланилганда ва унга кирувчи

параметрларнинг тенг бўлганда, унинг натижаси бир хил бўлиши билан изоҳланади.



6-расм. “Савол-жавоб” механизмига асосланган бир мартали парол ёрдамида аутентификация усулининг рўйхатдан ўтиш босқичи

SMS (Short Message Service) хабар ёрдамида ОТРни юборишга асосланган усул. Амалда банк-молия соҳасида фойдаланувчиларни ҳақиқийлигини текширишда ва тўловларни тасдиқлашда бир мартали паролларни SMS орқали узатишга асосланган усулдан фойдаланилади. Бироқ, ушбу усулда SMS хабарни ўқиш мумкинлиги сабаб жиддий хавфсизлик муаммоси юзага келиши мумкин. Шу сабабли, мавжуд бир мартали паролни узатиш усули такомиллаштирилган.

Дастлаб рўйхатдан ўтиш босқичида 5-расмдаги каби томонлар ўртасида тақсимланган калит K_{SH} га эга бўлинади. Шундан сўнг, кириш босқичи қуйидагича амалга оширилади:

1. Фойдаланувчи дастлаб хизмат провайдерида бирор операцияни амалга оширади. Масалан, тўловни амалга ошириш тасдиғи талаб этилганда.

2. Хизмат провайдери II бобда келтирилган ОТР генератори орқали зарур бўлган ОТРни ҳосил қилади ва у асосида умумий юборилувчи хабар M ни яратади. Хабарни фойдаланувчига рўйхатдан ўтиш жараёнида тақсимланган калит K_{SH} билан бирор симметрик блокли шифрлаш алгоритми F_E - асосида шифрлайди: $C = F_E(M, K_{SH})$. Бу ерда, F_E - симметрик блокли шифрлаш алгоритмининг шифрлаш функцияси.

3. Ушбу босқичда шифрланган хабар C бирор SMS шлюзига юборади.

4. SMS шлюз орқали шифрматн C фойдаланувчи мобайл қурилмасига узатилади.

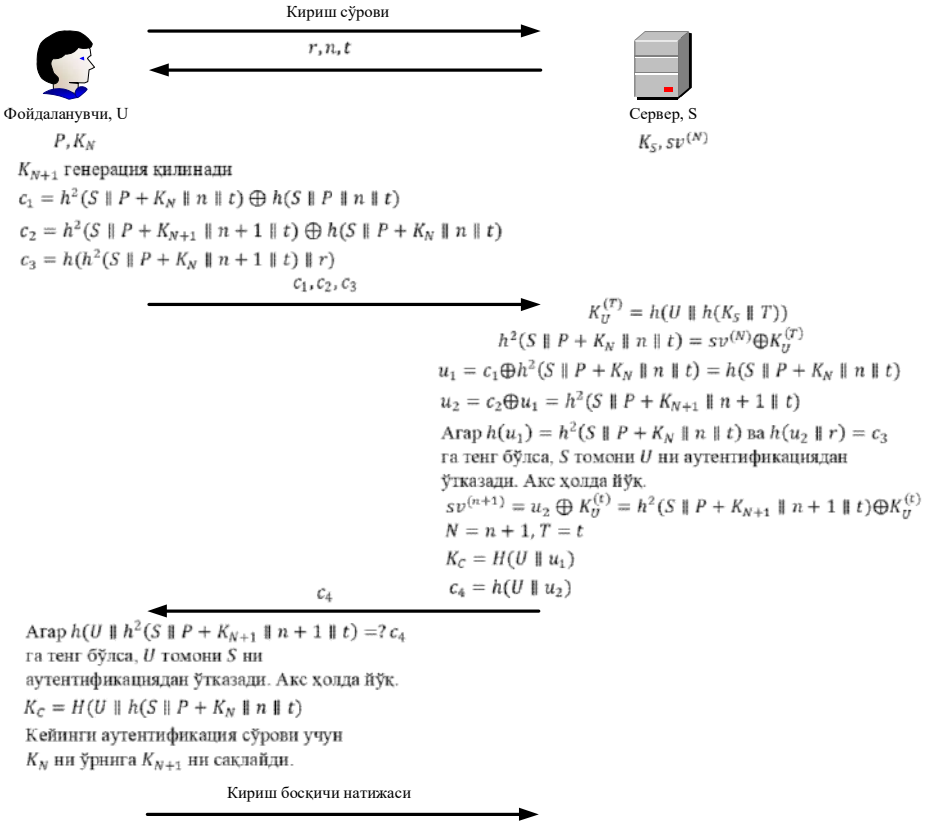
5. Мобил иловадаги махсус илова ёки мобайл банкинг иловасининг модули орқали шифрланган хабар C дешифрланади: $M = F_D(C, K_{SH})$. Бу ерда, F_D - симметрик блокли шифрлаш алгоритмининг дешифрлаш функцияси.

6. Дешифрланган хабар M дан ОТР сўралган манзилга киритилади.

7. Ушбу босқичда хизмат провайдеридан олинган аутентификация натижаси фойдаланувчига тақдим этилади.

SMS орқали OTPни юбориш усулини такомиллаштириш учун таклиф этилган усул, ҳозирда мобил қурилмаларнинг етарлича имкониятга эгалигига асосланади. Хусусан, мобил қурилмада талаб этилган иловани ўрнатиш ва ундан фойдаланиш имконияти мавжуд бўлиши керак.

Такомиллаштирилган W.C.Ku аутентификация усули. W.C.Ku томонидан ишлаб чиқилган аутентификация усули фақат бир томонлама аутентификацияни таъминлаб, бир томонлама функцияларга асосланган ҳамда “фараз қилиш” бўйича ҳужумга бардошсизлиги, икки томонлама аутентификацияни таъминламаслиги, сеанс калитини узатмаслиги ва паролларни алмаштириш имкониятларга эга эмаслиги каби камчиликларга эга. Шу сабабли, мазкур диссертация ишида келтирилган камчиликлар икки хил ёндашувда бартараф этилди. Биринчиси, W.C.Ku томонидан тақдим этилган протоколни модификациялаш бўлса, иккинчиси уни SAS-2 (Simple and Secure) протоколи шаклида ифодалашдир. Биринчи ёндашувда рўйхатдан ўтиш жараёнида қўшимча тасодифий катталик K_N киритилади. Кириш босқичи эса 7-расмда келтириб ўтилган.

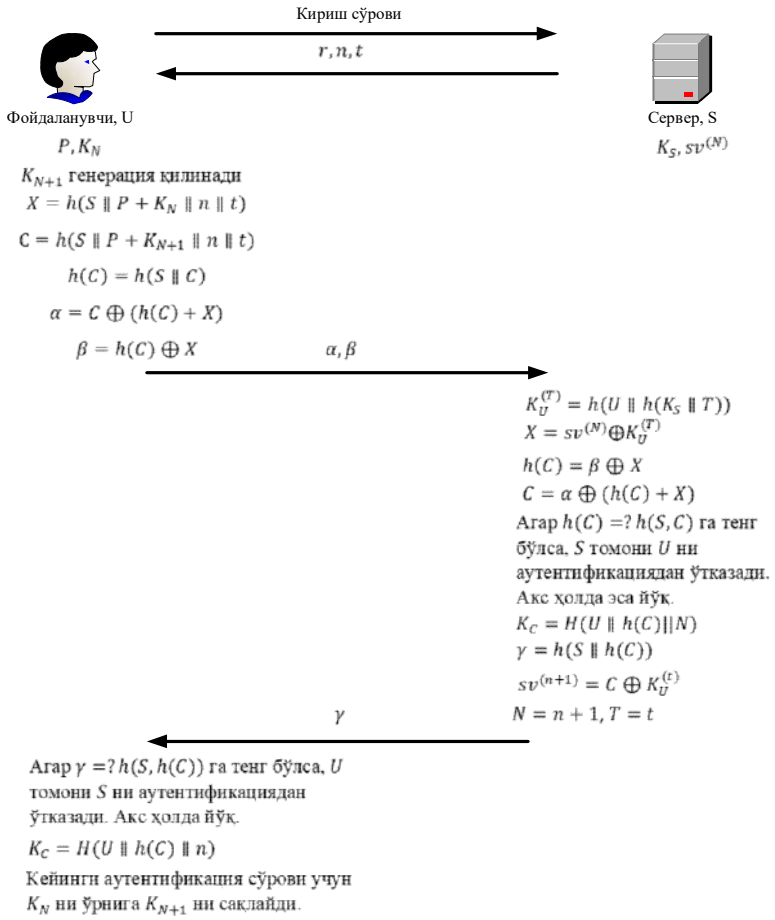


7-расм. Модификацияланган W.C.Ku усулининг кириш босқичи

Бу ерда, $h()$ – функция бир томонлама бардошли хэш функция бўлиб, унинг кўрсаткичи хэшлашлар сонини кўрсатади. N бутун сон бўлиб, U ни рўйхатдан ўтказиш учун 1 дан бошланади ва ҳар бир аутентификациядан ўтиш жараёнида ортиб боради. P фойдаланувчи U нинг бардошли пароли. K_S сервер S нинг махфий калити. T вақт меткаси бўлиб, фойдаланувчи U рўйхатдан

ўтказилган ёки қайта ўтказилган вақтни билдиради. $\oplus$ – белгиси XOR амалини ва || - белгиси бирлаштириш амалини англатади.

W.C.Ku усулининг SAS-2 протоколи кўринишидаги шакли ҳам юқорида келтирилган камчиликларни ўзида мужассамлаштирган бўлиб, унинг кириш босқичи 8-расмда келтирилган.



8-расм. SAS-2 кўринишидаги W.C.Ku усулининг кириш босқичи

W.C.Ku томонидан яратилган протоколнинг икки такомиллаштирилган версияси ҳам икки томонлама аутентификация ва сеанс калитини алмашиниш имкониятини тақдим этади.

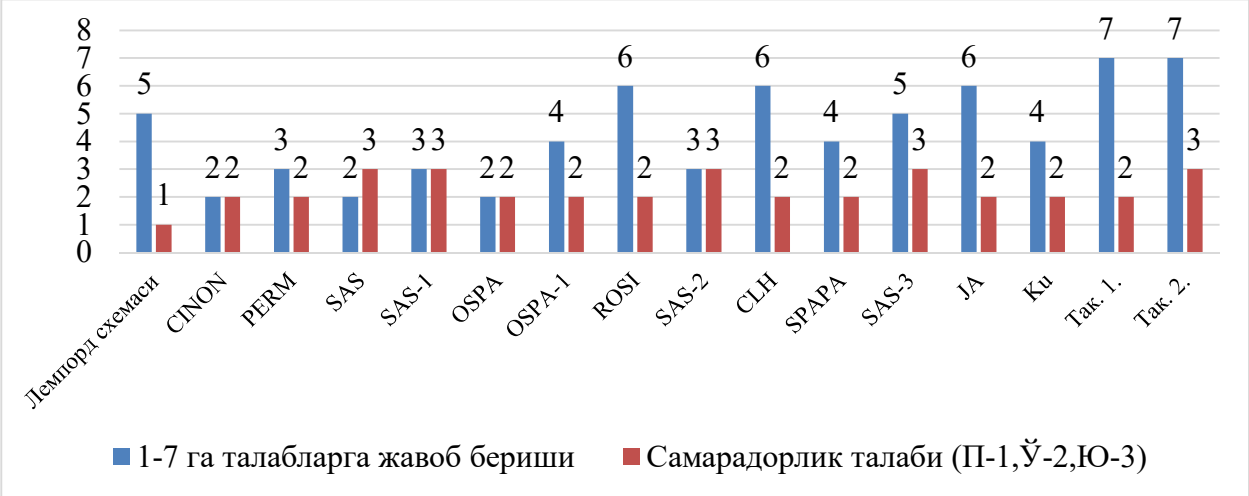
Бундан ташқари, паролни алмаштириш имкониятини мавжудлиги протоколдан амалда фойдаланиш имкониятини янада кенгайтиради. Ушбу икки кўринишнинг хавфсизлик ва ҳисоблаш бўйича самарадорлик таҳлиллари кейинги бобда келтирилган.

Диссертациянинг «**Аутентификация протоколларининг таҳлили ва амалда тадбиқи»** номли тўртинчи бобида юқорида келтирилган бир мартали паролларга асосланган аутентификация протоколларининг таҳлилига ва тадбиқига бағишланган.

Такомиллаштирилган TOTP/HOTP алгоритмини таҳлил қилиш натижасида QR кодни ўғирлаш ва “Мобил қурилмани ўғирлаш” каби ҳужумларни олдини олгани аниқланди. SMS хабар ёрдамида OTPни юборишга асосланган аутентификация усули эса SMS хабарни тутиб олиш, тинглаш ва қўлга киритиш ҳужуми, генерация қилинган OTPни қўлга киритишни мақсад қилган қўпол куч ҳужуми, тақсимланган калитни топишга қаратилган ҳужумлар ва SIM (Subscriber Identification Module) картани қалбакилаштиришга асосланган ҳужумларга бардошлиги аниқланди.

“Савол-жавоб” механизмига асосланган бир мартали парол ёрдамида аутентификация усули такрорлаш ҳужуми, қалбакилаштириш ҳужуми, ўртага турган одам ҳужуми ва тақсимланган калитни билишга қаратилган ҳужумларга бардошлиги аниқланди.

W.C.Ku усулининг модификацияланган кўринишларини мавжудларига нисбатан таҳлил қилишда: (1) “хизмат кўрсатишдан вос кечишга ундаш (Denial of Service)” ҳужуми, (2) “қалбакилаштириш” ҳужуми, (3) “ўртада турган одам” ҳужуми, (4) такрорлаш ҳужуми, (5) “фараз қилиш бўйича” ҳужум, (6) “ўғирланган верификатор” ҳужуми ва (7) икки томонлама аутентификациялашни мавжудлиги каби омиллар танлаб олинди. Бундан ташқари, протоколларнинг самарадорлигини баҳолаш учун сервер ва мижоз томондаги амаллар сони ва улар орасида узатилувчи маълумот ўлчамларига ҳам эътибор берилди. Танлаб олинган 7 та омил ва самарадорлик талаби бўйича таҳлил натижалари 9-расмда келтирилган. Таҳлил натижаси такомиллаштирилган усуллар танлаб олинган талабларнинг барчасига жавоб берган ҳамда юқори самарадорлик натижаларини қайд қилган.



9-расм. Мавжуд ва такомиллаштирилган алгоритмларнинг таҳлили

Такомиллаштирилган икки усул мос ҳолда ўрта ва юқори самарадорлик кўрсаткичларини қайд этган бўлиб, улар батафсил ҳолатда 3-жадвалда кетирилган.

3-жадвал

Такомиллаштирилган бир мартали паролларга асосланган аутентификация усулларининг самарадорлик омиллари бўйича таҳлили

	Серверда		Мижозда		Мижоз→ Сервер	
	Хэшлаш-лар сони (марта)	Сақланувчи маълумотлар	Хэшлаш-лар сони (марта)	Сақланувчи маълумотлар	Узитилиш-лар сони	Узатилувчи маълумот ҳажми
Так. 1.	4 ($mutual$ 6)	$sv^{(N)}, T, N, K_S$	6 ($mutual$ 7)	K_N	1	$L(log.req) + 3L(H)$
Так. 2.	3 ($mutual$ 6)	$sv^{(N)}, T, N, K_S$	3 ($mutual$ 4)	K_N	1	$L(ID) + 2L(H)$

Бир мартали паролларга асосланган W.C.Ku протоколига янги тасодифий қийматни киритиш унда мавжуд бўлган такрорлаш ҳужуми ва паролни фараз қилишга асосланган ҳужумга бардошли бўлиши таъминлаши аниқланди. Бундан ташқари, модификацияланган усул икки томонлама аутентификацияни таъминлаши ва унда паролларни алмашиниш

имкониятининг мавжудлиги протоколни фойдаланувчанлик даражасини ортишига хизмат қилади.

ХУЛОСА

«Псевдотасодифий сонлар генератори асосида аутентификациялаш усуллари ва алгоритмлари» мавзусидаги диссертация иши бўйича олиб борилган тадқиқотлар натижасида қуйидаги хулосалар тақдим этилди:

1. Бардошли симметрик блокли шифрлаш алгоритмлари асосида псевдотасодифий сонлар генератори ишлаб чиқилди. Ишлаб чиқилган псевдотасодифий сонлар генератори юқори тасодифийлик даражасини кўрсатди.
2. Ишлаб чиқилган псевдотасодифий сонлар генераторлари асосида иррационал сонлар хусусиятидан фойдаланган ҳолда бир мартали паролларни ҳосил қилиш усули ва алгоритми ишлаб чиқилди. Ишлаб чиқилган генератор 85,4% тўлиқ такрорланмаслик даражасига эга 6 хона узунликдаги паролларни ҳосил қилиш имконини берди.
3. Тақсимланган калитларни хавфсиз узатиш ва хавфсиз сақлаш орқали TOTP/HOTP алгоритми асосида ишлаб чиқилган аутентификация усули ва алгоритми такомиллаштирилди. Такомиллаштирилган усул турли зарарли дастурий воситалар ёрдамида амалга ошириладиган ҳужумларга бардошликни ошириш имконини берди.
4. Бир мартали паролларни шифрлаш орқали SMS хабар ёрдамида етказиш усули такомиллаштирилди. Такомиллашган усул рухсат этилмаган тутиб олиш ва SS7 протоколидаги заифлик натижасида амалга оширилувчи таҳдиддан ҳимоялаш имконини берди.
5. Бир мартали паролни QR код кўринишида тақдим этиш орқали етказишга асосланган аутентификация усули ва алгоритми ишлаб чиқилди. Ишлаб чиқилган усул бир мартали парол асосида аутентификация усулларига қаратилган ҳужумларни олдини олиш ва қулай фойдаланиш имконини берди.
6. W.C.Ku томонидан тақдим этилган бир мартали паролга асосланган аутентификация протоколи янги тасодифий катталикни киритиш ва икки томонлама аутентификациялаш имкониятини яратиш орқали такомиллаштирилди. Такомиллаштирилган усул аслида мавжуд бўлган такрорлаш ҳужуми ва паролни фараз қилиш ҳужумини олдини олиш имконини берган.

**НАУЧНЫЙ СОВЕТ DSc.13/30.12.2019.T.07.01
ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

АРЗИЕВА ЖАМИЛА ТИЛЕУБАЕВНА

МЕТОДЫ И АЛГОРИТМЫ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ГЕНЕРАЦИИ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

05.01.05 – Методы и системы защиты информации. Информационная безопасность.

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

Ташкент-2020

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за № B2019.1.PhD/T996.

Диссертация выполнена в Ташкентском университете информационных технологий.

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:	**Каримов Маджит Маликович** доктор технических наук, профессор
Официальные оппоненты:	**Ганиев Салим Каримович** доктор технических наук, профессор
	Жураев Гайрат Умарович доктор физико-математических наук, доцент
Ведущая организация:	**«UNICON.UZ» – центр научно-технических и маркетинговых исследований**

Защита диссертации состоится «08» октября 2020 года в 16⁰⁰ часов на заседании Научного совета DSc.13/30.12.2019.T.07.01 при Ташкентский университет информационных технологий. (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер №1620). (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «25» сентября 2020 года.
(протокол рассылки №14 от «24» августа 2020 года.)

Р.Х. Хамдамов
Председатель научного совета по присуждению ученых степеней, д.т.н., профессор

Ф.М. Нуралиев
Ученый секретарь научного совета по присуждению ученых степеней, д.т.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 результате увеличения уязвимостей в традиционных способах аутентификации, в мире особое внимание уделяется расширению использования строгих или многофакторных методов аутентификации в организациях. На современном этапе развития информационных-коммуникационных систем использование методов многофакторной аутентификации является важным для проверки подлинности пользователей. В частности, по словам Алекса Вайнерта, сотрудника службы безопасности Microsoft, «99,9% автоматических атак блокируются в результате использования методов многофакторной аутентификации»[3]. По данному направлению в развитых странах, таких как США, Англия, Япония, Франция, Нидерланды и др. создаются множества важных новизны по разработке аппаратных и программных средств, обеспечивающих гарантированную аутентификацию пользователей.

Во всем мире ведутся исследования по созданию удобных, недорогих многофакторных методов аутентификации, обеспечивающих гарантированную аутентификацию. В этом направлении одной из важных задач является разработка эффективных и безопасных способов использования одноразовых паролей в качестве дополнительного фактора в предотвращении существующих проблем безопасности в широко используемом методе аутентификации на основе паролей. В то же время существует необходимость научно обосновать анализ и совершенствование методов создания одноразовых паролей и устойчивость существующих методов аутентификации на их основе.

В нашей республике предпринимаются масштабные меры по обеспечению безопасности информационной безопасности, так как в государственных учреждениях, улицах и в общественных местах устанавливаются камеры наблюдения, который выводит на передний фланг по актуальности. В Стратегии действий по дальнейшему развитию Республики Узбекистан в 2017-2021 гг. отмечены задачи, в том числе «...совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере»[4]. Одной из важных задач при выполнении исследовательских работ является разработка эффективных, безопасных и основанных на паролях методов, и инструментов для проверки подлинности пользователей.

Данное диссертационное исследование, в определенной степени вносит вклад в выполнении задач, предусмотренных Указами Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 года «О Стратегии действий по дальнейшему развитию Республики Узбекистан», №УП-5379 от 14 марта 2018 года «О мерах по совершенствованию системы государственной

[3] https://www.zdnet.com/article/microsoft-using-multi-factor-authentication-blocks-99-9-of-account-hacks/

[4] Указ Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 г. «О Стратегии действий по дальнейшему развитию Республики Узбекистан»

безопасности Республики Узбекистан», №УП-5349 от 19 февраля 2018 года «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций» и Постановлением Президента Республики Узбекистан №ПП-614 от 03 апреля 2007 года «О мерах по организации криптографической защиты информации в Республике Узбекистан» и других нормативно-правовых документов, принятых в данной сфере.

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. В области генерации одноразовых паролей для систем аутентификации в частности хранение паролей, передача паролей и анализ их по свойствам безопасности ведут свои научные исследования ученые L.Lamport, M.Sandirigama, A.Shimizu, W.C.Ku и др. А также проложается инженерно-исследовательские работы со стороны таких компаний, как RSA лаборатория (John Brainard, Ari Juels, Michael Szydlo, Moti Yung ва бошқалар) и Microsoft лаборатория (Stuart Schechter, Serge Egelman, Serge Egelman).

В Узбекистане со стороны научных групп под руководством С.К.Ганиева, М.М. Каримова, П.Ф. Хасанова, Д.Е. Акбарова изучены вопросы по анализу защищенности информационных систем, разработка средств аутентификации, совершенствование методов аутентификации и методы безопасной передачи паролей.

Вместе с тем, методы генерации одноразовых паролей на основе генераторов псевдослучайных чисел, которые в настоящее время используются в качестве дополнительного фактора при аутентификации пользователей в виде основанного на них механизма «вопрос-ответ», и методы строгой аутентификации изучены недостаточно.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация. Диссертационное исследование выполнено в рамках научного проекта согласно плану научно-исследовательских работ Ташкентского университета информационных технологий №Ф17-007 - «Методы и средства повышения эффективности систем обнаружения и предотвращения атак в компьютерных системах» (2009-2011).

Цель исследования является разработка эффективных, безопасных метода и алгоритмов строгой аутентификации на основе генераторов псевдослучайных чисел с высокой степенью случайности.

Задачи исследования:

разработать метод генерации псевдослучайных чисел с высокой степенью случайности;

разработать метод и алгоритм генерации одноразовых паролей с высокой степенью случайности;

усовершенствовать методов и алгоритмов аутентификации, основанные на одноразовые пароли;

разработать метод и алгоритмов многофакторной аутентификации на основе эффективного предоставления одноразовых паролей;

усовершенствовать протокол строгой аутентификации, основанный на одноразовые пароли;

Объектом исследования является процесс проверки удостоверения подлинности в информационных системах.

Предмет исследования составляет методы и алгоритмы строгой аутентификации, основанные на генераторы псевдослучайных чисел.

Методы исследования. В процессе исследования использованы алгоритмизация, теория вероятностей, теория чисел, сравнительный анализ, анализ на безопасность и методы объектно-ориентированного программирования.

Научная новизна исследования заключается в следующем:

разработан генератор псевдослучайных чисел с учетом имения высокой степени случайности одноразовых паролей;

разработан метод и алгоритм генерации одноразовых паролей, имеющий высокой степень неповторимости с использованием свойств иррациональных чисел;

усовершенствованы методы аутентификации с учетом проблем безопасности, на основе алгоритма TOTP/HOTP и одноразовых паролей, отправляемых в SMS-сообщениях;

разработан метод и алгоритм аутентификации, основанный на передачи одноразовых паролей в виде QR-кода;

усовершенствован протокол аутентификации, основанный на одноразовом пароле, с учетом возможностей двухсторонней аутентификации и распределения сеансового ключа.

Практические результаты исследования заключаются в следующем:

разработано программное средство генератора псевдослучайных чисел с высокой степенью случайности на основе алгоритмов стойких симметричных блочных шифровании и генератора одноразового пароля, которое основывается на генераторе псевдослучайных чисел;

Разработано мобильное программное средство позволяющий безопасно распределит клуючей и хранит их в системах аутентификации, основанный на алгоритме TOTP/HOTP;

Разработано мобильное программное средство передачи одноразовых паролей в шифрованном виде в SMS-сообщении;

Разработано мобильное программное средство метода аутентифкации основанный на механизм «вопрос-ответ» с помощью одноразового пароля, который предоставляется в виде QR-кода.

Достоверность результатов исследования. Достоверность результатов исследования подтверждается реальным и экспериментальным анализом, полученным из метода генерации псевдослучайных последовательностей, метода генерации одноразовых паролей, методов и алгоритмов безопасной передачи распределенных ключей, безопасного хранения и защиты от угроз, необходимых в информационных системах.

Научная и практическая значимость результатов исследования. Научная значимость полученных результатов исследований заключается в том, что разработка методов и алгоритмов, защищающие от фальсификации образов лица и повысить точность распознавания, позволяют создавать методов повышения эффективности образов лица для систем идентификации и аутентификации.

Практическая значимость полученных результатов исследования заключается в том, что за счет применения программных средств, который разработаны на основе предложенных методов и алгоритмов в входных контрольных пунктах организаций, позволяет автоматизировать процессов идентификации человека.

Научная значимость результатов исследования объясняется разработкой метода генерации псевдослучайных чисел с высокой степенью случайности и метода генерации одноразовых паролей на его основе, разработкой и совершенствованием методов и алгоритмов аутентификации на основе генераторов одноразовых паролей.

Практическая значимость результатов исследования объясняется возможностью минимизирования связанных угрозы с паролями в информационных системах, а также безопасное передача и хранение распределенных ключей.

Внедрение результатов исследования. На основе полученных научных результатов по разработке методов, алгоритмов и программных средств аутентификации, которые основаны на разработанном методе генерации одноразовых паролей:

программное средство метода генерации одноразовых паролей, имеющий высокий степень случайности и неповторимости внедрено в практическую деятельность Нукусского районного Государственной Налоговой инспекции Государственного Налогового Управления Республики Каракалпакстан. (справка Министерства по развитию информационных технологий и коммуникаций от 9 июня 2020 года, №33-8/3105). В результате научного исследования была достигнута степень полной неповторимости 36,865% при генерации 6 знатных одноразовых паролей.

программные средства “Secure SMS Authenticator” и “Secure OTP Authenticator”, которые основаны на использование одноразовых паролей в качестве второго фактора внедрены в Каракалпакский Республиканский филиал «Микрокредитбанк»а (справка Министерства по развитию информационных технологий и коммуникаций от 9 июня 2020 года, №33-8/3105). В результате научного исследования, использование данных

программных средств в мобильных банковских приложениях позволило, не предоставляя неудобств пользователям предотвратить атак, таких как кража QR-кода, кража мобильного устройства и перехват SMS-сообщений.

Апробация результатов исследования. Результаты данного исследования были обсуждены на 2 международных и 10 республиканских научно-практических конференциях.

Публикация результатов исследования. По теме исследования опубликованы всего: 26 научная работа, из них 8 статей в журнальных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан, в том числе 2 - в иностранных и 6 - в республиканских журналах, а также получены 3 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 119 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обосновываются 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 первая глава диссертации, озаглавленная как **«Проблемы аутентификации в информационно-коммуникационных системах»,** посвящена к вопросам, такие как роль методов аутентификации при защите информации, анализ методов аутентификации и существующих угроз в них, а также анализ методов аутентификации, основанные на одноразовые пароли.

Методы аутентификации пользователей делятся на три класса: на основе знания что-то пользователем, на основе имения что-то пользователем и на основе что-то характеризующий пользователя. Среди методов аутентификации метод основанный на обычном пароле является широко распространенным и удобным для пользования, но степень безопасности является очень низким и требует сохранить в памяти человека. Методы аутентификации, основанные на токены обеспечивают высокую степень безопасности, но не распространены широко из-за высокой стоимостью инфраструктуры и устройства, также требует постоянного ношения с собой. Методы аутентификации, основанные на биометрических параметрах хоть и не требуют хранения в памяти и постоянного ношения с собой, но не удобен при использовании в веб ресурсах и не распространены широко из-за высокой стоимости.

В практике из-за широкого распространения методов аутентификации первого класса большое внимание уделяется к преодолению существующих проблем для поддержания масштабности. Предложенные метода для предотвращения атак направленные на методы аутентификации, основанные на знания что-то пользователем, не обеспечивают полноценную защиты. Но при этом из полученных результатов анализа можно увидеть, что методы аутентификации на основе одноразовых паролей (One time password, OTP) являются важным средством при предотвращении существующих атак.

Во второй главе диссертации под названием «**Методы и алгоритмы генерации эффективных паролей»,** анализирована методы генерации одноразовых паролей и предложена метод и алгоритм генератора псевдослучайных чисел и метод и алгоритм генерации одноразовых паролей на основе их.

При генерации одноразовых паролей применяется различные методы, и в качестве примера можно привести методы, основанные на генераторы псевдослучайных чисел, использующие временную метку в качестве входного параметра, основанные на генераторы псевдослучайных чисел, использующие счетчика как входного параметра, основанные на генерации паролей, использующие набор определенных символов и основанные на генерации паролей, использующие генератор псевдослучайных чисел.

На основе методов первой и второй группы методы аутентификации широко применяется для создания одинаковых OTP у обеих сторон, а следующие группы применяются для создания OTP в сервере и передачи его к пользователям. Генерирование OTP на основе генератора псевдослучайных чисел (ГПСЧ) имеет своеобразное свойство и это объясняется тем, что в них применяется криптографические преобразования. Общая схема генерации OTP, входящий в четвертую группу приведена на рисунке 1.

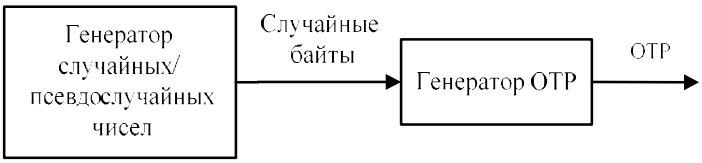


Рис-1. Генерирование OTP на основе ГПСЧ

На основе предложенного подхода на рисунке 2 приведена функциональная схема генератора создающий псевдослучайных последовательностей для метода генерации OTP. Для предлагаемого ГПСЧ в качестве источника параметров энтропии были выбраны текущая локация курсора компьютерной мышки, сверхточная временная метка операционной системы и текущее состояние рабочего стола пользователя. Кроме этого, для предложенного ГПСЧ в качестве добавочного входного значения было использована 128 битное *nonce* и в качестве конфиденциального параметра MAC (Media Access Control) адрес, IP (Internet Protocol) адрес и серийный номер жесткого диска.

Для ГПСЧ управление двумя состояниями является весьма важными и при этом используется функции, называемые внутренними. Исходя из рисунка

2 функция инициализации формирует *NONCE* значение с помощью определённой $H()$ односторонной функцией на основе значения текущей времени T_i, текущее время, значение K на основе текущего местоположения курсора компьютерный мышки и текущее состояние экрана, значение $SEED_i$ параметра на основе конфиденциальных параметров и не криптографического генератора (или введенный пользователем).

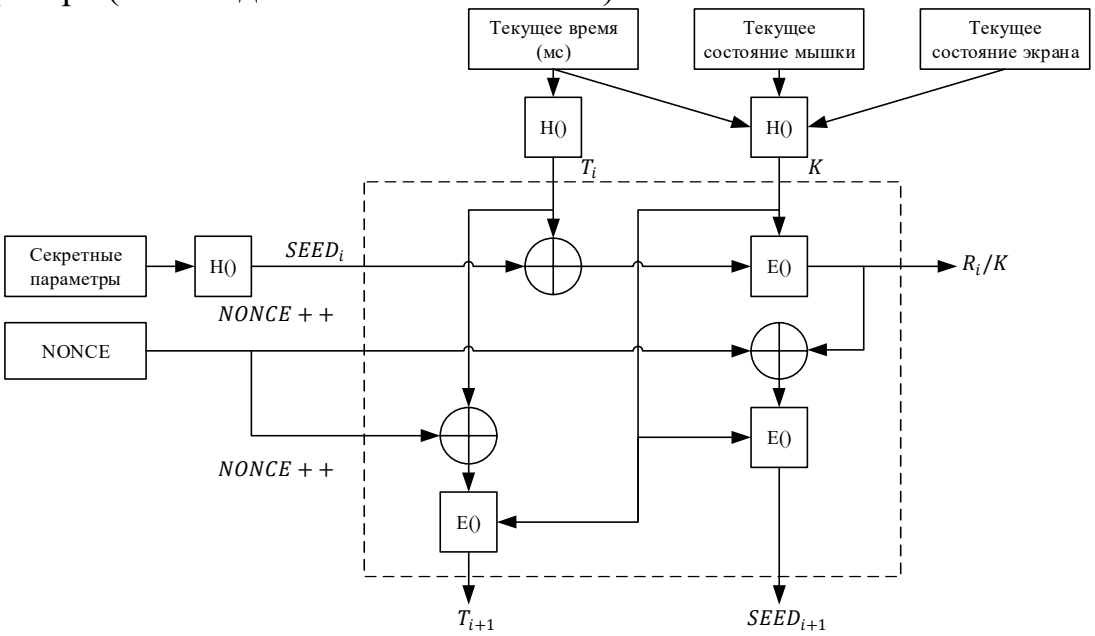


Рис.2. Функциональный вид предложенного ГПСЧ

Функция генерирования значений создает псевдослучайные числа требованной длины используя текущее внутреннее состояние и обновляет внутреннее состояние для следующего запроса. На основе рисунка 2 функцию генерирования значений для одного блока можно описывать следующем образом:

- $R_i = E_K(T_i \oplus SEED_i)$;
- $SEED_{i+1} = E_K(R_i \oplus NONCE++)$;
- $T_{i+1} = E_k(T_i \oplus NONCE++)$.

Здесь, $E_K()$ – алгоритм стойкого блочного шифрования, внем используется K битный ключ и требуется длина K ключа должна соответствовать длине значения $H()$ односторонней функции (хэш функции). Например, можно использовать MD5 хэш функцию, который создает 128 битное значение и любой симметричный блочное шифрование с 128 битным ключом. Или требуется использование с алнернативного метода генерации ключа для $E()$ – симметричного блочного шифрования с значения $H()$ - односторонней хэш функции.

Существует ряд методов тестирования на случайность последовательностей генерированных с ГПСЧ, но среди них широко распространены методы основанные на статистические тесты. Поэтому, для тестирования на степень случайности результатов полученных от ГПСЧ, которое приведена на рисунке 2, было использована статисические тесты NIST SPECIAL PUBLICATION 800-22. Для этого было получена 5 раз двух битные

образцы с ГПСЧ. В данном наборе тестов существует 15 тестов и результаты тестирования предложенного и существующих генераторов в таблице приведена a/b виде. При этом b – количества всех тестов, т.е она равна на 15. a – означает пройденных тестов последовательностей (таблица 1).

Таблица 1

Результаты тестирования генераторов

Название генератора	Образцы тестирования				
	1	2	3	4	5
CryptGenRandom	14/15	15/15	14/15	13/15	15/15
/dev/urandom	15/15	15/15	15/15	15/15	15/15
Java Random()	15/15	15/15	15/15	15/15	14/15
Python Random()	14/15	15/15	15/15	15/15	15/15
Предложенный ГПСЧ	14/15	15/15	15/15	15/15	15/15

В результате статистических тестов можно увидеть что предложенный ГПСЧ имеет высокую степень случайности в среди существующих. На основе предложенного генератора псевдослучайных чисел ГПСЧ можно иллюстрировать функциональную схему метода генерации паролей (рис.3).

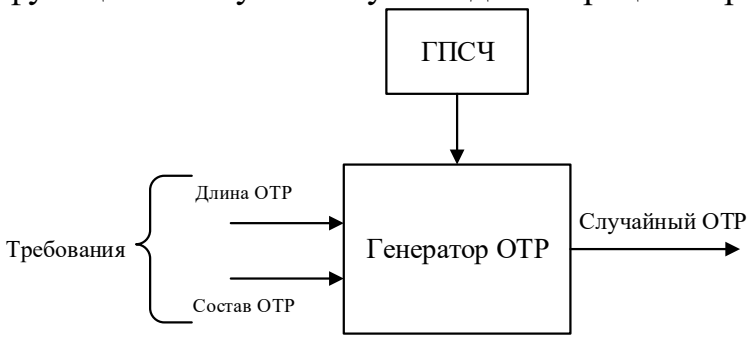


Рис.3. Общий вид OTP генератора, основанный на ГПСЧ системы

Создаваемые одноразовые пароли для генератора OTP должны подчинятся функцию неприрывного равномерного распределения (continuous uniform distribution) и это являеться важным. Равномерное распределение или четыреуголное распределение это распределение с неизменной вероятностью и означает, что исходящие значения стоят в определенном диапазоне. Функция плотности вероятности (Probability density function, PDF) неприрывного равномерного распределения равна следующему:

$$f(x) = \begin{cases} \frac{1}{b-a}, & x \in [a,b] \\ 0, & x \notin [a,b] \end{cases} \quad (1)$$

В (1) функции если $a = 0$ и $b = 1$ равна, тогда $U(a,b)$ называется функцией стандартное равномерное распределение.

Существует ряд методов получения последовательностей, основанные на законодательства равномерного распределения, но среди них подход, основанный на иррациональные числа имеет особую значимость. В частности, именно Неймановский метод генерации псевдослучайных чисел, разработанный со стороны Д.И.Голенко, модифицирован исходя из свойств иррациональных чисел. При этом со стороны автора приведена функция,

которая мало отличается от функции теоретического равномерной распределения:

$$\xi_i = \{i\Theta\} \quad (2)$$

Здесь, Θ – иррациональное число, со стороны автора при этом в качестве примера приведены $\sqrt{2}$, $\frac{\sqrt{2}}{2}$, $\frac{\sqrt{3}}{3}$, $\sqrt{3}$ и $\frac{\sqrt{5}-1}{2}$ иррациональные числа. Для проверки правильность данного подхода в диапазоне $1 \leq i \leq 1000000$ вычислены значения (2) уравнения для иррациональные числа Θ, которые приведены выше и $\sqrt{7}$, $\frac{\sqrt{7}}{7}$ выбранные на основе анализов и для числа π, из дробной части полученных результатов выбраны 6 и 7 чисель и проведена проверка основание на закономерность равномерного распределения. В результате анализа иррациональное число $\sqrt{7}$ при создании 6 и 7 разряднқх чисел показал 88,3% и 100% неповторимости, соответственно и большое подчинение к функции равномерного распределения.

Учитывая свойство равномерного распределения иррациональных чисел, необходимо будет выбрать число i с помощью ГПСЧ, чтобы гарантировать случайность. Ниже приведен метод генерирования данных одноразовых паролей.

Здесь приняты следующие определения:

1. $S_0 = \{0, \dots, 9\}, S_1 = \{0, \dots, 9, A, \dots, Z\}, S_2 = \{0, \dots, 9, a, \dots, z, A, \dots, Z\}$ набор символов. При этом количества символов в каждом набора равна $len(S_0) = 10, len(S_1) = 36, len(S_2) = 62$.

2. $R = \{L, S_i\}$ – требования к одноразовому паролю, L – длина одноразового пароля ($L \in [6, 10]$), S_i – означает набор символов ($i \in [0,2]$).

3. C_j^l – случайное значение j, которое получены из ГПСЧ, l – показывает длину в битах ее.

4. P_j – генерированное j одноразовый пароль.

5. $F(R, C_j^l)$ – функция создания одноразового пароля, здесь, $P_j = F\left(R, C_j^l\right) = F(\{L, S_i\}, C_j^l)$ равенство уместно.

6. $DT(N_j, L)$ – функция динамического сокращения, исходя из длины ОТР L генерирует одноразовый пароль P_j:

$$DT\left(N_j, L\right) = S(M\left(N_j * \Theta\right), L)$$

Здесь, $M()$ – функция, возвращает дробную часть умножая случайное значение $Nonce$ на иррациональное число Θ. $S()$ – функция, которая возвращает L цифр с правой стороны результата функции $M()$.

Предлагаемый генератор ОТР способен генерировать пароли, состоящие из трех наборов символов S_0, S_1 и S_2, а блок-схема метода генерации ОТР, состоящего из элементов набора S_0, показана на рисунке 4.

На практике чаще всего используются ОТР, состоящие только из цифр. Функция генерации ОТР, состоящих из элементов множества S_0, равна $F\left(R, C_j^l\right) = F\left(\{L, S_0\}, C_j^l\right)$. В этом случае случайное значение длины одного блока получается из ГПСЧ для произвольных возможных значений требуемой

длины L OTP. В этом случае общая последовательность генерации OTP следующая:

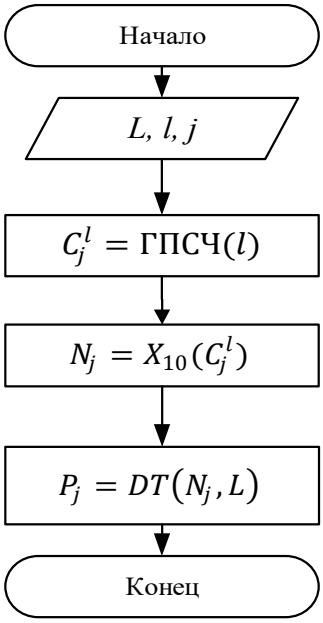


Рис.4. Блок схема генерирования паролей, состоящих из символов набора S_0

a. для генерации требуемого одноразового пароля P_j, вычисляется C_j^l с l бит длиной из ГПСЧ.
b. из последовательности C_j^l битов создается $N_j = X_{10}(C_j^l)$ в десятичном системе считывания.
c. для создания требуемого одноразового пароля P_j применяется уравнение $P_j = DT(N_j, L)$.

Проведено сравнений предложенного генератора OTP на степень неповторимости с генератором HOTP и функцией $random()$. С помощью каждого алгоритма было сгенерирована 1 миллион OTP с длиной 6 и 7 разрядов. Полученные результаты эксперимента отражены в таблице 2.

Таблица 2

Результаты генерирования элементов набора S_0

Генераторы OTP	Число повторения										Неповторимость
	2 раз	3 раза	4 раза	5 раза	6 раза	7 раза	8 раза	9 раза	9 раз и больше	Итого	
HOTP (6)	184085	61208	15331	3080	490	71	11	0	0	264276	367957
$random()$(6)	183757	61646	15322	3078	517	72	8	2	0	264402	367182
1-алгоритм(6)	68394	2898	0	0	0	0	0	0	0	71292	854518
HOTP (7)	44964	1547	43	0	0	0	0	0	0	46554	905253
$random()$(7)	44923	1472	40	0	0	0	0	0	0	46435	905578
1-алгоритм(7)	0	0	0	0	0	0	0	0	0	0	1000000

Результаты проведенных экспериментов показывают, что предлагаемый метод генерации OTP имеет более высокую степень неповторимости, чем существующие.

В третьей главе диссертации по названию **«Разработка протокола аутентификации на основе одноразовых паролей»** приводятся данные, которые посвящены поиску и устранению неисправностей, и анализу проблем безопасности в методах аутентификации на основе генератора одноразовых паролей, сначала представляет проблемы безопасности в методах аутентификации на основе одноразовых паролей, используемых на практике, а затем предлагает способ их решения.

Методы, основанные на алгоритмах HOTP или TOTP (Time-based One-Time Password). В приложения двухсторонней аутентификации, основанные на TOTP алгоритмы не удалено внимание на обеспечение безопасности распределенных ключей. Это дает возможность получить распределенного ключа в виде QR (Quick Response), которые хранятся в куки браузерах со

стороны злоумышленника. На рисунке 5, этап регистрации метода основанный на защите распределенного ключа с помощью параметров первого фактора.

Здесь, $H()$ - это произвольная односторонняя функция, при этом требуется стойкость и вычисляется на основе первых факторов аутентификации. K_{SH} – это распределенный ключ, который генерируется из ГПСЧ. $F_E()$ – это алгоритм симметричного блочного шифрования, который выбирается пользователем. URL – значение, указывающий название или адрес используемой службы и представлен в виде строк. Вся собранная информация предоставляется в виде QR-кода для удобства чтения пользователем.

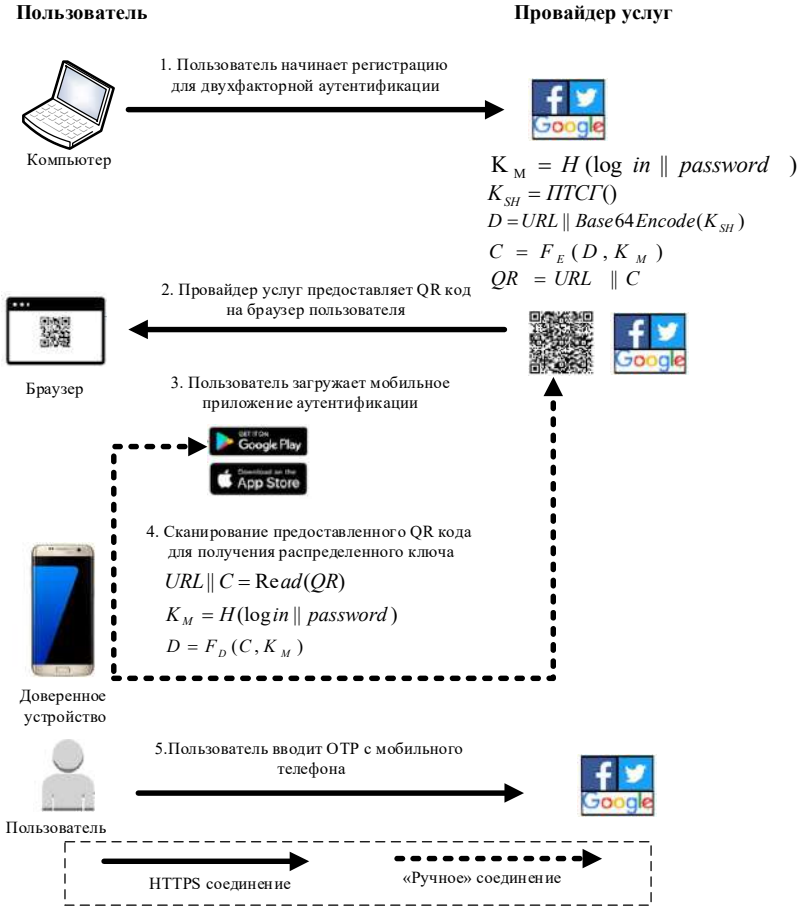


Рис.5. Этап регистрации в протоколе аутентификации, основанный на усовершенствованный TOTP

Метод аутентификации с помощью одноразового пароля, основанный на механизм "Вопрос-ответ". Данный метод с точки зрения функционирования похож протоколам HOTP или TOTP, но разработан метода аутентификации на основе одноразовых паролей, использующий механизм "вопрос-ответ". В данном методе процесс получения распределенного ключа выполняет как на рисунке 5. Процесс входа осуществляется как на рисунке 6. Общая сущность предложенного метода заключается в том, что «вопрос» в виде QR кода предоставляется со стороны сервера и «ответ» получается с помощью мобильного приложения пользователя. В данном случает $H()$ и $A()$ – это стойкие односторонние хэш функции и N показывает название оказываемой службы. Удостоверение метода аутентификации объясняется

тем, что при использовании одного $A()$на стороне сервера и клиента и введенные в него параметры равны, результат будет одинаковым.

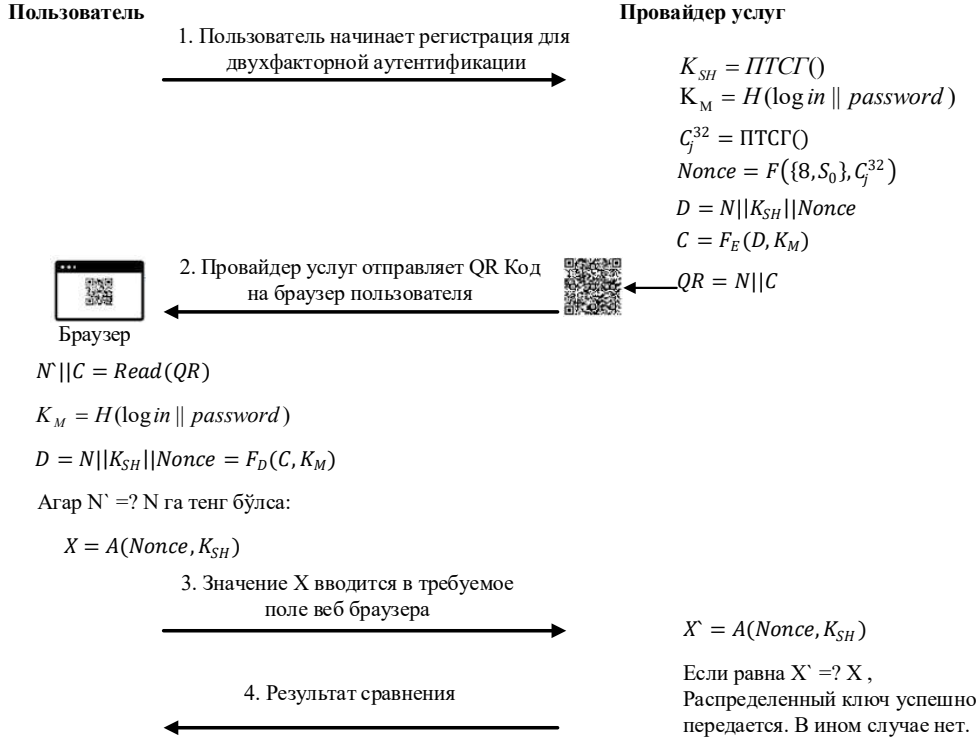


Рис.6. Этап регистрации метода аутентификации с помощью одноразового пароля на основе механизма «вопрос-ответ»

Метод основанный отправки OTP с помощью SMS-сообщения (Short Message Service). На практике в сфере банковского дела и финансов для проверки подлинности пользователей и подтверждения платежей используется метод, основанный на передаче одноразовых паролей посредством SMS. Однако возможность чтения SMS-сообщения таким образом может вызвать серьезные проблемы с безопасностью. Таким образом, существующий способ передачи одноразового пароля был улучшен.

Первоначально, на этапе регистрации, получается распределенный ключ K_{SH} между сторонами, как показано на рисунке 5. После этого этап входа проходит следующим образом:

1. Сначала пользователь выполняет операцию с поставщиком услуг. Например, когда требуется подтверждение оплаты.

2. Провайдер услуг генерирует требуемый OTP с помощью генератора, описанный в главе II, и создает на его основе общее сообщение M. Сообщение шифруется на основе алгоритма симметричного блочного шифрования F_E с ключом K_{SH}, выдаваемым пользователю при регистрации: $C = F_E(M, K_{SH})$. Здесь F_E - функция алгоритма симметричного блочного шифрования.

3. На этом этапе зашифрованное сообщение C отправляется на шлюз SMS.

4. Шифрованный текст C передается на мобильное устройство пользователя через шлюз SMS.

5. Зашифрованное сообщение C шифруется с помощью специального приложения в мобильном устройстве или модуле приложения мобильного

банкинга: $M = F_D(C, K_{SH})$. Здесь F_D - функция дешифрования алгоритма симметричного блочного шифрования.

6. Из расшифрованное сообщение *M,* OTP вводится на запрашиваемый адрес.

7. На этом этапе пользователю предоставляется результат аутентификации, полученный от поставщика услуг.

Предлагаемый метод улучшения способа отправки OTP через SMS основан на том, что мобильные устройства теперь имеют достаточные возможности. В частности, мобильное устройство должно иметь возможность устанавливать и использовать необходимое приложение.

Усовершенствованный метод аутентификации W.C.Ku. Метод аутентификации, разработанный W.C.Ku, обеспечивает только одностороннюю аутентификацию, и основан на односторонних функциях и имеет такие недостатки, как уязвимость к «предположительной» атаке, не обеспечивает двустороннюю аутентификацию, не передает ключи сеанса и не имеет возможности обмена паролями. Таким образом, указанные в диссертационной работе недостатки устранены двумя разными подходами. Первый - изменить протокол, предоставляемый W.S.Ku, а второй - выразить его в форме протокола SAS-2 (Simple and Secure). В первом подходе в процессе регистрации вводится дополнительная случайная величина K_N. Этап входа показан на рисунке 7.

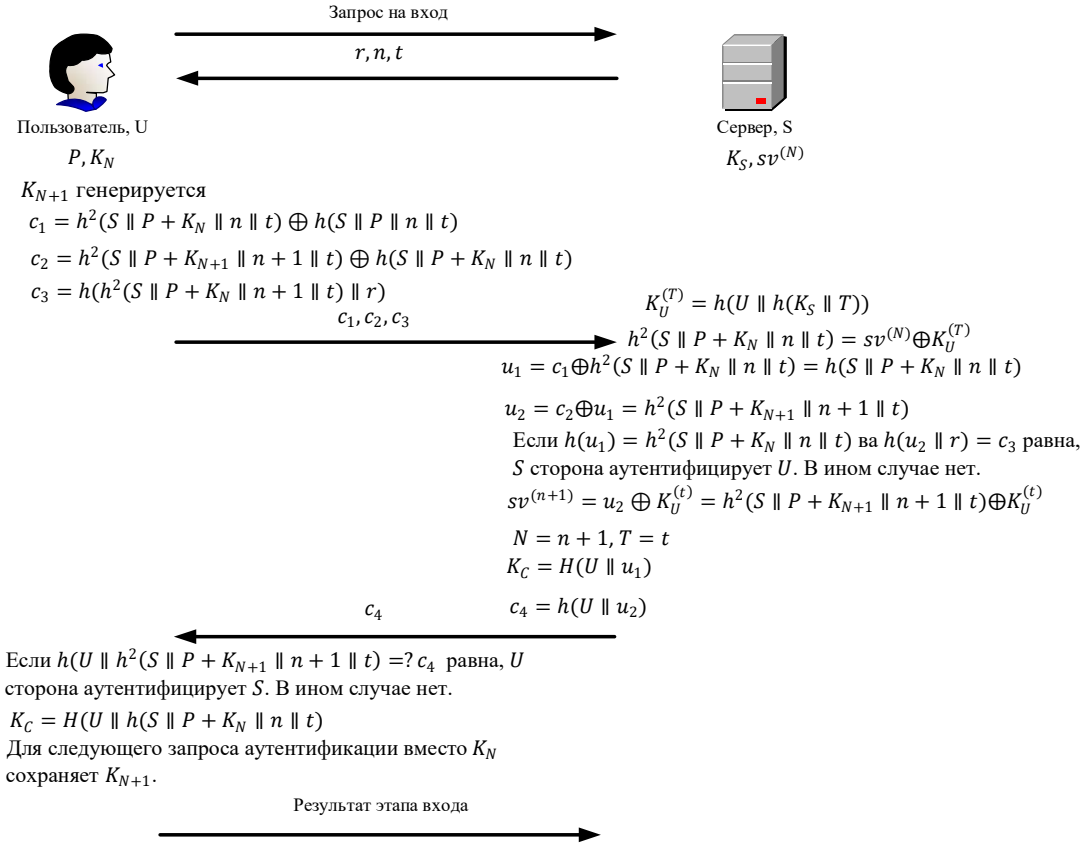
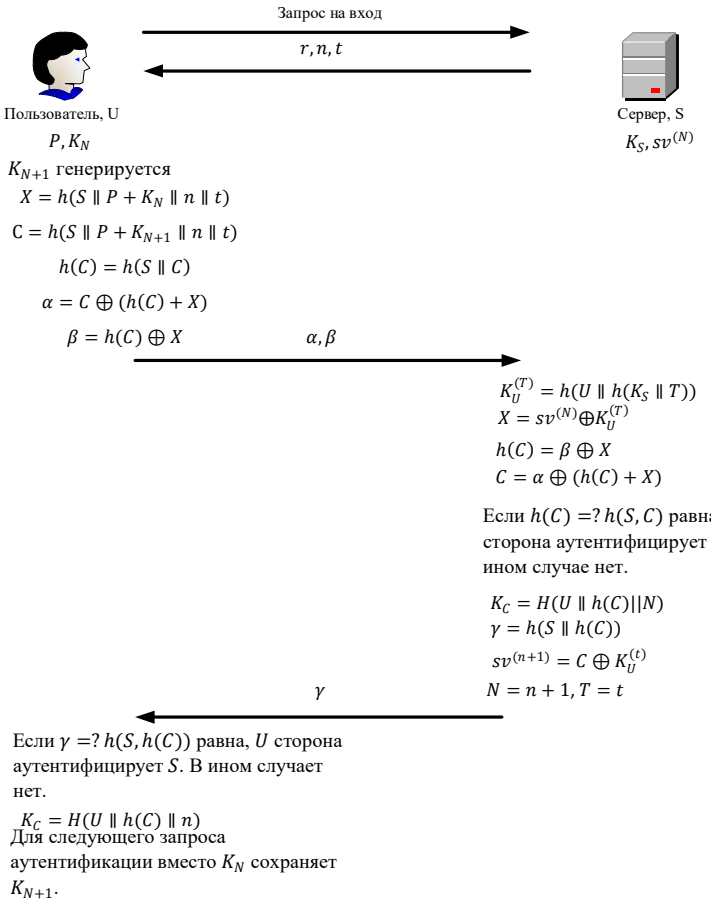


Рис.7. Этап входа модификациоронного метода W.C.Ku

При этом функция $h()$ - это односторонне стойкая хеш-функция, результат которой указывает количество хешированый. N - целое число,

начиная с 1 для регистрации U и увеличивающееся с каждым процессом аутентификации. Надежный пароль P пользователя U. K_S - секретный ключ сервера S. T - метка времени, указывающая время, когда пользователь U был зарегистрирован или повторно переведен. $\oplus$- знак операции XOR и || - символ представляет операцию слияния.



8-расм. SAS-2 кўринишидаги W.C.Ku усулининг кириш босқичи

Форма метода W.C.Ku в виде протокола SAS-2 также включает вышеупомянутые недостатки, и его этап входа показана на рисунке 8.

Обе улучшенные версии протокола, разработанный W.C.Ku, предлагают двустороннюю аутентификацию и возможность совместного использования сеансового ключа.

Кроме того, возможность смены пароля еще больше расширяет возможности использования протокола на практике. Анализ безопасности и вычислительной эффективности этих двух представлений представлен в следующем разделе.

В четвертой главе диссертации по названию «**Анализ и практическое применение протоколов аутентификации»**, приведенные информации посвящены к анализу и к практическому применению вышеприведённых протоколов аутентификации, основанные на одноразовые пароли.

Анализ усовершенствованного алгоритма TOTP / HOTP показал, что он предотвращает такие атаки, как кража QR-кода и «кража мобильного устройства». Было обнаружено, что метод аутентификации, основанный на отправке OTP через SMS, устойчив к таким атакам, как перехват SMS-сообщений, атаки вслушивания и овладения, атакам грубой силы, направленным на захват сгенерированного OTP, атакам, направленные на нахождения распределенного ключа и атакам с подделкой SIM (Subscriber Identification Module) -карт.

Используя метод аутентификации на основе одноразового пароля, было выявлено, что данный метод аутентификации оказался устойчивым к повторяющим атакам, атакам фальсификации, атакам человек в середине, атаки, направленные на нахождение распределенного ключа.

При анализе модифицированных версий метода W.C.Ku по отношению к существующим, были выбраны следующие факторы: (1) атака «отказ в обслуживании», (2) атака «фальсификация», (3) атака «человек в середине», (4) атака с повторением, (5) «предполагаемая» атака, (6) атака «украденный верификатор» и (7) наличие двусторонней аутентификации. Кроме того, было уделено внимание количеству операций на стороне сервера и клиента и размеру данных, передаваемых между ними, чтобы оценить эффективность протоколов. Результаты анализа 7 выбранных факторов и требований к эффективности показаны на рисунке 9. Результаты анализа показали, что улучшенные методы соответствовали всем выбранным требованиям и показали высокие результаты эффективности.

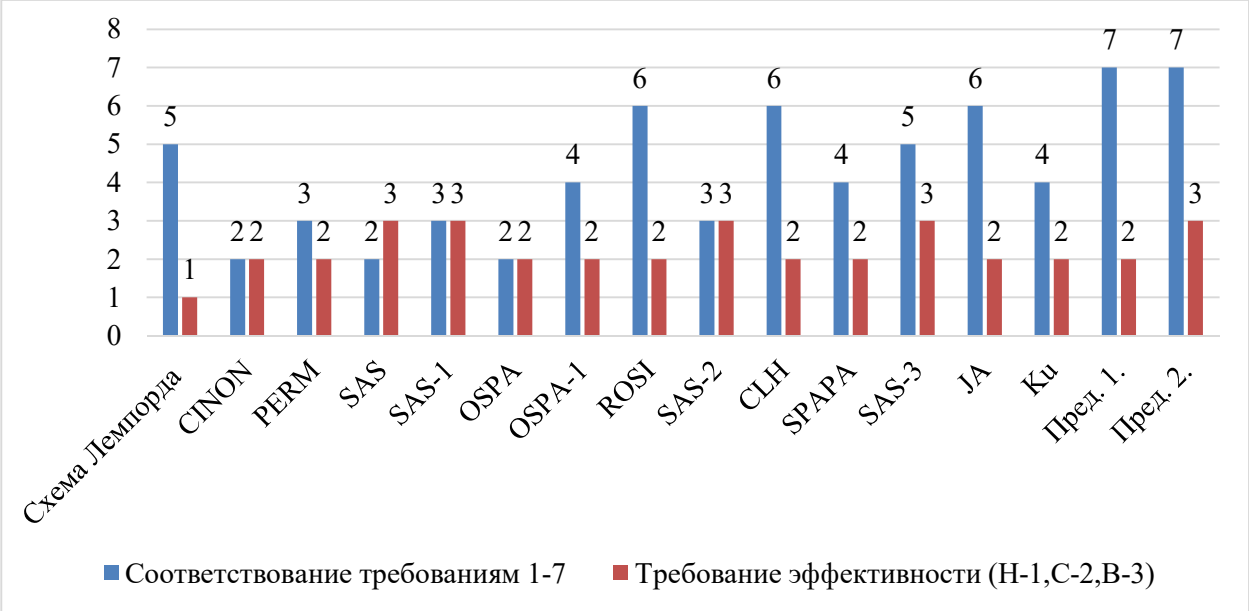


Рис.9. Анализ существующих и усовершенствованных алгоритмов

Два улучшенных метода показали среднюю и высокую эффективность соответственно, которые более подробно обсуждаются в таблице 3.

Таблица 3

Анализ усовершенстованных методов аутентификации, основанные на одноразовые пароли по фактору эффективности

	В сервер		**У пользователя**		**Пользователь→ Сервер**	
	Число хэширований (раза)	Храняемые данные	Число хэширований (раза)	Храняемые данные	Количество передач	Объем передаваемой информации
Пред. 1.	4 ($mutual$ 6)	$sv^{(N)}, T, N, K_S$	6 ($mutual$ 7)	K_N	1	$L(log.req) + 3L(H)$
Пред. 2.	3 ($mutual$ 6)	$sv^{(N)}, T, N, K_S$	3 ($mutual$ 4)	K_N	1	$L(ID) + 2L(H)$

Было обнаружено, что добавление нового случайного значения к протоколу W.C.Ku на основе одноразовых паролей гарантирует его устойчивость к существующим атакам повторения и атакам с предположением пароля. Кроме того, модифицированный метод обеспечивает

двустороннюю аутентификацию и возможность обмена паролями в нем, что повышает уровень удобства использования протокола.

ЗАКЛЮЧЕНИЕ

Приведены следующие выводы в результате проведенных исследований по диссертационной работе на тему «Методы и алгоритмы аутентификации на основе генераторов псевдослучайных чисел»:

1. Разработан генератор псевдослучайных чисел на основе стойких алгоритмов симметричного блочного шифрования. Разработанный генератор псевдослучайных чисел показал высокую степень случайности.
2. Разработан метод и алгоримт генерации одноразовых паролей на основе предложенных генераторов псевдослучайных чисел с использованием свойства иррациональных чисел. Разработанный генератор позволил сгенерировать пароли длиной 6 разряда с показателем полного неповторения 85,4%.
3. Метод и алгоритм аутентификации, разработанный на основе алгоритма TOTP / HOTP, были улучшены за счет безопасной передачи и безопасного хранения распределенных ключей. Усовершенствованный метод позволил повысить устойчивость к атакам с использованием различных вредоносных программ.
4. Усовершенствован способ передачи одноразового пароля в SMS-сообщении с помощью шифрования. Усовершенствованный метод позволил защитить от несанкционированного перехвата и угроз, исходящих от уязвимостей в протоколе SS7.
5. Разработан метод и алгоритм аутентификации, основанный на передаче одноразового пароля путем представления его в виде QR-кода. Разработанный метод позволил предотвратить атаки на методы аутентификации с использованием одноразового пароля и легкость в использовании.
6. Протокол аутентификации на основе одноразового пароля, предоставляемый W.C.Ku, был улучшен за счет введения нового случайного значения и возможности двусторонней аутентификации. Усовершенствованный метод позволил предотвратить атаку повторения и атаку предполоежения пароля, которые существуют в практике.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.13/30.12.2019.T.07.01 AT TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

ARZIYEVA JAMILA TILEUBAEVNA

AUTHENTICATION METHODS AND ALGORITHMS BASED ON PSEUDO RANDOM NUMBER GENERATION

05.01.05 – Methods and systems of information protection. Information Security

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

Tashkent-2020

The theme of doctor of philosophy (PhD) on technical sciences was registered at the Supreme attestation commission at the Cabinet of Ministers of the Republic of Uzbekistan under number B2019.1.PhD/T996.

The dissertation has been prepared at Tashkent University of Information Techologies.

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

Scientific adviser:	**Karimov Madjit Malikovich** doctor of technical sciences, professor
Official opponents	**Ganiev Salim Karimovich** doctor of technical sciences, professor
	Juraev Gayrat Umarovich doctor of physical-mathematical sciences, docent
Leading organization:	**Scientific-Engineering and Marketing researches Center «UNICON.UZ»**

The defense will take place «08» october 2020 at 16 00 the meeting of Scientific council No. DSc.13/30.12.2019.T.07.01 at Tashkent University of Information Technologies (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52, 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 No2620). (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

Abstract of dissertation sent out on «25» september 2020 y.
(mailing report No. 14 on «24» august 2020 y.).

R.Kh. Khamdamov
Chairman of the scientific council awarding scientific degrees, Doctor of Technical Sciences, Professor

F.M. Nuraliev
Scientific secretary of scientific council awarding scientific degrees, Doctor of Technical Sciences, Docent

S.K. Ganiev
Chairman of the academic seminar under the scientific council awarding scientific degrees, Doctor of Technical Sciences, Professor

INTRODUCTION (abstract of PhD thesis)

The purpose of the research work is to develop effective, secure strong authentication methods and algorithms based on a pseudo-random number generator with a high degree of randomness.

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

The scientific novelty of the research work:

a pseudo-random number generator was developed, subject to the high degree of randomness of one-time passwords;

a method and algorithm for generating one-time passwords was developed, which has a high degree of uniqueness using the properties of irrational numbers;

an authentication methods based on the TOTP / HOTP algorithm and one-time passwords sent in SMS messages was improved to eliminate existing security problems;

an authentication method and algorithm based on the transmission of one-time passwords in the form of a QR code was developed;

an one-time password based authentication protocol was improved, subject to the impossibility of mutual authentication and distribution of the session key.

Implementation of the research results. Based on the results on the implementation of method of one-time password generation, authentication methods, algorithms and software based on it:

a software for generating one-time passwords with a high degree of randomness and non-repetition was implemented in the activities of State Tax Inspection of Nukus district of the State Tax Administration of the Republic of Karakalpakstan (Certificate No. 33-8/3105 as of June 9, 2020 the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan). As a result of scientific research, the software that generates only numeric one time password with six digit length, gives a 36,865% complete non-repetition rate;

“Secure SMS Authenticator” and “Secure OTP Authenticator” software for user authentication based on the use of one-time passwords as a secondary factor, was implemented in the activities of Republic of Karakalpakstan Branch of “Microcreditbank” (Certificate No. 33-8/3105 as of June 9, 2020 the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan). Because of scientific research, using this software in mobile bank services gives opportunities of preventing attacks, like, stealing a QR code, stealing a mobile device and intercepting an SMS message, without causing inconvenience to users.

The outline of the dissertation. The dissertation consists of an Introduction, four Chapters, Conclusion, a list of References and Appendices. The volume of the dissertation is 119 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

1. Tashev K.A., Khudoykulov Z.T., Arziyeva J.T., Improvement of a Security Enhanced One-time Mutual Authentication and Key Agreement Scheme // International Journal of Innovative Technology and Exploring Engineering (IJITEE), - India, 2019, Volume 8, Issue 12, -P. 5031-5036 (№3; Scopus; IF=0.3).

2. Karimov M.M., Khudoykulov Z.T., Arziyeva J.T., A Method of Efficient OTP Generation Using Pseudorandom Number Generators // 2019 International conference on information science and communications technologies applications, trends and opportunities (ICISCT), -Tashkent, 2019. –P. 1-4, (05.00.00; 30.09.2019 №269/8-сон раёсат қарори).

3. Каримов М.М., Худойқулов З.Т., Арзиева Ж.Т., Анализ метода аутентификации на основе одноразовых паролей // Муҳаммад ал-Хоразмий авлодлари. –Ташкент, 2019, №4(10)/2019. –P. 3-6, (05.00.00; №10).

4. Каримов М.М., Худойқулов З.Т., Арзиева Ж.Т., Атаки направленные на методы аутентификации по паролю // Муҳаммад ал-Хоразмий авлодлари. – Ташкент, 2019, №4(10)/2019. –P. 156-159, (05.00.00; №10).

5. Худойқулов З.Т., Арзиева Ж.Т., Ортиқбоев А.М., Бир мартали парол генераторларининг таҳлили // Ахборотқоммуникациялар: Тармоқлар, Технологиялар, Ечимлар. –Ташкент, 2019, №3(51)/2019. –P. 48-55, (05.00.00; №2).

6. Karimov M.M., Tashev K.A., Arziyeva J.T., Abdurakhmonov A.A., Imamaliyev A.T., About one of the authentication methods // TUIT BULLETIN. – Tashkent, 2013, №3/2013. –P. 5-12, (05.00.00; №31).

7. Ташев К.А., Абдурахмонов А.А., Имамалиев А.А., Арзиева Ж.Т., Парол генераторининг аппарат воситасини яратиш муаммоси // TATU xabarlari. – Тошкент, 2013, №3/2013. –P. 19-24, (05.00.00; №31).

8. Арзиева Ж.Т., Об одном способе применения генераторов паролей в задачах аутентификации пользователей // TATU xabarlari. –Тошкент, 2012, №2/2012. –P. 23-27, (05.00.00; №31).

9. Karimov M.M., Tashev K.A., Kim S.S., Ishmuratov A.R., Arzieva J.T., The authentication method based on the random number generator // International Journal of Ubiquitous Computing and Internationalization. – 2011, Vol.3, No.2, -P. 35-40.

10. Арзиева Ж.Т., Генераторы псевдослучайных последовательностей и стохастические алгоритмы в задачах защиты информации // Научно-теоритический журнал “Вопросы науки и образования”. – Москва, 2018, №26(38), -С.20-21.

11. Karimov M.M., Tashev K.A., Kim S.S., Ishmuratov A.R., Arzieva J.T., The authentication method based on the random number generator // International Journal of Ubiquitous Computing and Internationalization. – 2011, Vol.3, No.2, -P. 35-40.

12. Каримов М.М., Арзиева Ж.Т., Метод аутентификации объектов инфо-коммуникационных систем// ILMIY xabarnoma. –Тошкент, 2011, №4/2011. –P. 17-18.

13. Utewliev N., Arzieva J.T., Direct search methods to solve stochastic optimization problem // International conference on IT Promotion in Asia 2009, -Tashkent, 2009, -P. 101-105.

14. Арзиева Ж.Т., Шыхыев Р.М., Аутентификация в системах с разделением времени // Актуальные проблемы прикладной математики и информационных технологий – Аль – Хорезми 2016, -Бухара, Узбекистан, 2016, -P. 147-149.

15. Каримов М.М., Арзиева Ж.Т., Абдурахмонов А.А., Способ двухсторонней аутентификации в инфокоммуникационных системах // Республиканский семинар: «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения», -Ташкент, 2011, -С. 37-38.

16. Арзиева Ж.Т., Об одном методе удостоверения подлинности пользователей в инфокоммуникационных системах // Республиканский семинар: Информационные технологии и проблемы телекоммуникаций. – Ташкент, 2012, -С. 196-197.

17. Ташев К.А., Арзиева Ж.Т., Насруллаев Н.Б., Анализ протокола аутентификации объектов инфокоммуникационных системах // Международная конференция “Актуальные проблемы развития инфокоммуникаций и информационно общества”. – Ташкент, 2012, -С. 718-723.

18. Арзиева Ж.Т., Утепбергенова Г., Тестирование получаемых псевдослучайных чисел в системах аутентификации // Математик физика ва замонавий анализнинг турдош масалалари республика илмий-амалий анжумани. – Бухоро, 2015, -P. 317-318.

19. Арзиева Ж.Т., Арзиев А.Т., Разработка клиентской модули системы аутентификации на основе одноразовых паролей для инфокоммуникационных систем // Республика илмий-назарий анжуман: “Фан ва тарбиянинг долзарб масалалари”. – Нукус, 2019, -С.341-343.

20. Арзиева Ж.Т., Паролга асосланган аутентификация усулларининг хавфсизлигини таъминлашда инсон омили // Республика илмий-амалий анжумани: Ахборот-коммуникация технологияларини ривожлантириш шароитида инновациялар. – Қарши, 2019, -P. 363-365.

21. Арзиева Ж.Т., Аутентификация усулларининг таҳлили // Республика илмий-техник анжумани: “Ахборот-коммуникация

технологиялари ва телекоммуникацияларнинг замонавий муаммолари ва ечимлари”. – Фарғона, 2019, -Р. 343-345.

22. Арзиева Ж.Т., OTP асосида бир йўналишли аутентификация протоколларининг таҳлили // Республика илмий-техник конференция: “Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги муаммолари”. – Тошкент, 2019, -Р.63-67.

23. Каримов М.М., Арзиева Ж.Т., Бир мартали паролларга асосланган аутентификацияда мавжуд муаммолар // Республика илмий-техника анжумани: ”Иқтисодиётнинг тармоқларини инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти”. –Тошкент, 2019, -Р. 190-192.

24. Ташев К.А., Худойқулов З.Т, Арзиева Ж.Т., Арзиев А.Т., Ёриқулов М., Рустамова С.Р. “Secure SMS Authenticator” // Дастурга гувоҳнома № DGU 07387, 23.12.2019.

25. Ташев К.А., Худойқулов З.Т, Арзиева Ж.Т., Арзиев А.Т., Ёриқулов М., Рустамова С.Р. “Secure OTP Authenticator” // Дастурга гувоҳнома № DGU 07386, 23.12.2019.

26. Худойқулов З.Т, Арзиева Ж.Т., Арзиев А.Т., Ёриқулов М. “Secure OTP Reader” // Дастурга гувоҳнома № DGU 07388, 23.12.2019.

Автореферат «Муҳаммад ал-Хоразмий авлодлари» илмий журнали таҳририятида таҳрирдан ўтказилди ва ўзбек, рус ва инглиз тилларидаги матнларини мослиги текширилди.