

for n qubits // Phys. Lett. A. – 1998. – Vol. 246, №1–2. – P. 1–6.

8. Cheddad A., Condell J., Curran K., Mc Kevitt P. Digital image steganography: Survey and analysis of current methods // Signal Process. – 2010. – Vol. 90, №3. – P. 727–752.

9. Özkaynak F. Brief review on application of nonlinear dynamics in image encryption // Nonlinear Dynam. – 2018. – Vol. 92, №2. – P. 305–313.

10. Sharma M., Choudhary V., Bhatia R., Malik S., Raina A., Khandelwal H. Leveraging the power of quantum computing for breaking RSA encryption // Cyber-Phys. Syst. – 2021. – Vol. 7, №2. – P. 73–92.

11. Zhang Y. Test and verification of AES used for image encryption // 3D Res. – 2018. – Vol. 9. – P. 1–27.

12. Pawar H.R., Harkut D.G. Classical and quantum cryptography for image encryption & decryption // Proc. 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE). – IEEE, 2018. – P. 1–4.

13. Dworkin M.J. Advanced Encryption Standard (AES) // Federal Information Processing Standards (FIPS)-197. – 2001.

14. Data Encryption Standard (DES) // Fed. Inf. Process. Stand. Publ. 112. – 1999. – P. 3.

15. Preneel B. Cryptographic hash functions // Eur. Trans. Telecommun. – 1994. – Vol. 5, №4. – P. 431–448.

16. Ullah S., Zheng J., Din N., Hussain M.T., Ullah F., Yousaf M. Elliptic curve cryptography; applications, challenges, recent advances, and future trends: A comprehensive survey // Comput. Sci. Rev. – 2023. – Vol. 47. – P. 100530.

17. Sharma P.L.G., Nayyar S., Harish A., Gupta M., Sharma K., Kumar A. ECC based novel color image encryption methodology using primitive polynomial // Multimedia Tools Appl. – 2024.

18. Shivaramakrishna D., Nagaratna M. A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and time-limited access control // Alex. Eng. J. – 2023. – Vol. 84. – P. 275–284.

19. Kumar S.S., Deepmala. A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm // Artif. Intell. Rev. – 2024.

20. Rahman R., Azad M.S., Hasan M.R., Emad S., Shubha U., Mahdy M. Enhancing the security of image transmission in quantum era: A chaos-assisted QKD approach using entanglement – 2023. – ArXiv:2311.18471.

GIDROMODULLI RAYONLASHTIRISH VA GRAF MODEL ASOSIDA SUV RESURSLARINI ADOLATLI LIMITLASH ALGORITMI

Qudaybergenov A.A.¹

¹PhD, dotsent, Mirzo Ulugʻbek nomidagi Oʻzbekiston Milliy universiteti doktoranti

adilbaygm@gmail.com

Qazimbetova M.M.²

²PhD, Berdax nomidagi Qoraqalpoq davlat universiteti doktoranti, Nukus, Oʻzbekiston

qazimbetovamuxabbad@gmail.com

Ispanova J.P.³

³Berdax nomidagi Qoraqalpoq davlat universiteti tayanch doktoranti, Nukus, Oʻzbekiston

paraxatovna1996@gmail.com

Annotatsiya: Ushbu ishda gidromodulli rayonlashtirish, kanal tarmogʻini graf koʻrinishida ifodalash va chiziqli dasturlash usulini birlashtirgan holda suv resurslarini adolatli limitlash algoritmi ishlab chiqildi. Taklif etilgan yondashuv fermerlar kesimida netto va brutto suv talabini hisoblash, tarmoqdagi oʻtkazuvchanlik va taqsimot cheklovlarini inobatga olish hamda cheklangan suv sharoitida suvni maqbul taqsimlash imkonini beradi. Olingan natijalar qondirilmagan talabni kamaytirish, nisbiy defitsitni

barqarorlashtirish va suv taqsimoti bo'yicha qaror qabul qilishni asoslashda ushbu algoritmnining amaliy ahamiyati yuqori ekanini ko'rsatdi.

Kalit so'zlar: gidromodulli rayonlashtirish, suv resurslarini limitlash, graf model, chiziqli dasturlash, adolatli taqsimlash, netto suv talabi, brutto suv talabi, irrigatsiya tarmog'i.

AN ALGORITHM FOR FAIR WATER RESOURCE LIMITING BASED ON HYDROMODULAR ZONING AND A GRAPH MODEL

Kudaybergenov A.A.¹, Kazimbetova M.M.², Ispanova J.P.³

¹PhD, Associate Professor, Doctoral Student of the National University of Uzbekistan named after Mirzo Ulugbek, Tashkent, Uzbekistan

²PhD, Doctoral Student of Berdakh Karakalpak State University, Nukus, Uzbekistan

³Basic Doctoral Student of Berdakh Karakalpak State University, Nukus, Uzbekistan

adilbaygm@gmail.com qazimbetovamuxabbad@gmail.com paraxatovna1996@gmail.com

Abstract: This paper develops an algorithm for fair water resource limiting by integrating hydromodular zoning, graph-based representation of a canal network, and linear programming. The proposed approach makes it possible to estimate net and gross water demand at the farmer level, account for conveyance and allocation constraints in the network, and achieve efficient water allocation under conditions of limited water availability. The obtained results demonstrate the high practical significance of

the algorithm for reducing unmet demand, stabilizing relative deficit, and supporting decision-making on water allocation.

Keywords: hydromodular zoning, water resource limiting, graph model, linear programming, fair allocation, net water demand, gross water demand, irrigation network.

АЛГОРИТМ СПРАВЕДЛИВОГО ЛИМИТИРОВАНИЯ ВОДНЫХ РЕСУРСОВ НА ОСНОВЕ ГИДРОМОДУЛЬНОГО РАЙОНИРОВАНИЯ И ГРАФОВОЙ МОДЕЛИ

Кудайбергенев А.А.¹

¹PhD, доцент, докторант Национального университета Узбекистана имени Мирзо Улугбека
adilbaygm@gmail.com

Казымбетова М. М.²

²PhD, докторант Каракалпакского государственного университета имени Бердаха,
Нукус, Узбекистан
qazimbetovamuxabbad@gmail.com

Испанова Ж.П.³

³Базовый докторант Каракалпакского государственного университета имени Бердаха,
Нукус, Узбекистан
paraxatovna1996@gmail.com

Аннотация: В данной работе разработан алгоритм справедливого лимитирования водных ресурсов, объединяющий гидромодульное районирование, представление канальной сети в виде графа и метод линейного программирования. Предложенный подход позволяет рассчитывать нетто- и брутто-потребность в воде в разрезе фермерских хозяйств, учитывать ограничения пропускной способности и распределения в сети, а также осуществлять рациональное распределение воды в условиях её ограниченности. Полученные результаты показали, что данный алгоритм имеет высокую практическую значимость для снижения неудовлетворённого спроса, стабилизации относительного дефицита и обоснования принятия решений по распределению воды.

Ключевые слова: гидромодульное районирование, лимитирование водных ресурсов, графовая модель, линейное программирование, справедливое распределение, нетто-потребность в

воде, брутто-потребность в воде, ирригационная сеть.

Kirish. Irrigatsiya tarmoqlarida suvni adolatli limitlash masalasi dolzarb hisoblanadi, chunki bunda suv talabini to'g'ri baholash, tarmoq topologiyasini hisobga olish, kanallar bo'ylab yo'qotishlarni inobatga olish hamda tanqislik sharoitida qabul qilinadigan qarorlarni o'zaro muvofiqlashtirish bir vaqtning o'zida talab etiladi. Mahalliy tadqiqotlarda magistral kanallarda suv taqsimotining matematik modellari [1], ochiq kanallarda optimal boshqaruv g'oyalari [2], gidromodulli rayonlashtirish asosida fermerlar dekadaviy netto talabini hisoblashning matematik modeli [3], ushbu talabni algoritmlashtirish masalalari [4] hamda graf hamda chiziqli dasturlash asosida dekadaviy limitlash modeli [5] ishlab chiqilgan. Xalqaro adabiyotlarda esa sug'orish suviga bo'lgan talabni iqlim o'zgarishi sharoitida baholash uchun gibrid bashorat modellari [6], kanal bo'ylab fazoviy-vaqtiy yo'qotishlarni rejalashtirish modeli tarkibiga kiritish [7], ko'p ierarxiyalik kanal tarmoqlarida ko'p maqsadli optimallashtirish [8], sug'orish taqsimot tarmoqlarini loyihalash uchun tugun-qirra modeli va aralash butun sonli yondashuvlar [9], kanalga asoslangan suv taqsimoti uchun ko'p davrli chiziqli dasturlash [10], suv ta'minoti noaniqligi sharoitida ikki bosqichli iqtisodiy modellar [11] shuningdek adolatli taqsimot uchun leksikografik minimaks tamoyili [12] taklif etilgan. Biroq ushbu yo'nalishlar ko'p hollarda alohida rivojlangan: bir qismi talabni hisoblaydi, boshqasi tarmoqni modellaydi, yana biri tanqislikda adolat mezonini shakllantiradi. Shu sabab gidromodulli rayonlashtirish, dekadaviy talab, graf tuzilma va adolatli limitlashni yagona hisoblash zanjirida birlashtirish amaliy boshqaruv nuqtai nazaridan muhim vazifa bo'lib qolmoqda.

Ushbu ishning maqsadi gidromodulli rayonlashtirish asosida shakllangan dekadaviy suv talabini kanal tarmog'ining graf modeli va chiziqli dasturlash apparati bilan bog'lab, suv tanqisligi sharoitida fermerlar kesimida adolatli limitlarni hisoblashga xizmat qiluvchi yagona matematik-algoritmik yondashuvni asoslashdan iborat.

Metodlar. Ushbu tadqiqotda magistral kanal tarmog'ida suv resurslarini adolatli limitlash masalasi gidromodulli rayonlashtirish, dekadalar bo'yicha suv talabini hisoblash, kanal tarmog'ini yo'naltirilgan graf ko'rinishida formallashtirish va chiziqli dasturlash asosida yechish ketma-ketligi orqali amalga oshirildi. Metodik yondashuv to'rt o'zaro bog'liq bosqichdan tashkil topdi: 1) fermerlar kesimida netto suv talabini aniqlash; 2) talabni tarmoq tugunlari bo'yicha agregatlash va brutto talabga o'tkazish; 3) kanal tarmog'i uchun graf model va quvvat cheklovlarini tuzish; 4) cheklangan limit sharoitida adolatli taqsimot yechimini olish.

1. Boshlang'ich ma'lumotlar va belgilanishlar

Hisoblashlarda fermerlar to'plami F , dekadalar to'plami D , kanal tarmog'ining tugunlari to'plami V va qirralari to'plami E qabul qilindi. Kanal tarmog'i $G = (V, E)$ yo'naltirilgan graf

ko'rinishida ifodalandi. Har bir fermer $f \in F$ uchun maydon A_f [ga], tegishli gidromodul rayon indeksi

$g(f)$, ekin turi $c(f)$ va rotatsiya indeksi $r(f)$ belgilandi.

Gidromodul rayon–ekin–rotatsiya kesimida dekadalik sug'orish normasi $V_{g,c,r,d}$ [m^3 /ga] parametr sifatida qabul qilindi. Zarur hollarda gidromodul $Q_{g,c,r}$ [$l/s \cdot ga$] qiymati orqali ham hisoblash mumkin bo'lib,

bu holda dekadalik hajm $V_{g,c,r,d}$ vaqt intervali va maydonga ko'paytirish orqali aniqlanadi.

2. Fermerlar kesimida dekadalar bo'yicha suv talabini hisoblash

Har bir fermer uchun dekadalar bo'yicha netto suv talabi maydon va dekadalik sug'orish normasi asosida hisoblandi. Bunda f fermerning d dekadadagi netto talabi quyidagi ifoda bilan aniqlandi:

$$R_{f,d} = A_f \cdot v_{g(f),c(f),r(f),d}, \quad f \in F, d \in D. \quad (1)$$

Fermerning yillik yoki vegetatsiya davri uchun jami netto talabi esa quyidagicha topildi:

$$R_f^{yr} = \sum_{d \in D} R_{f,d} \cdot \quad (2)$$

(1)-formula dekada kesimidagi asosiy talab parametrini, (2)-formula esa fermerning yig'indi mavsumiy talabini ifodalaydi. Keyingi hisoblashlarda aynan (1) formula bilan $R_{f,d}$ qiymatlari olingan limitlash modeli uchun bosh kirish parametri sifatida ishlatildi.

3. Kanal tarmog'ini graf model asosida formallashtirish

Suv yetkazib berish tarmog'i manba, magistral kanal, tarmoqlanish tugunlari, regulyatorlar va iste'mol nuqtalaridan tashkil topgan yo'naltirilgan graf sifatida qaraldi. Har bir qirra $e \in E$ uchun o'tkazuvchanlik chegarasi $C_{e,d}$ [m^3] va samaradorlik koeffitsienti $\eta_e \in (0,1]$ belgilandi.

Agar $\phi(f)=t$ funksiyasi f fermerni t terminal tugunga mos qo'ysa, u holda ushbu tugundagi agregatlangan netto talab quyidagicha hisoblandi:

$$N_{t,d} = \sum_{f: \phi(f)=t} R_{f,d} \cdot \quad (3)$$

Tarmoq bo'yicha yo'qotishlarni hisobga olish uchun terminal tugun talabini manbagacha brutto talabga o'tkazish amali bajarildi. Agar $path(s \rightarrow t)$ manbadan t tugungacha bo'lgan yo'lni bildirsa,

u

holda tegishli brutto talab quyidagicha yozildi:

$$B_{t,d} = \frac{N_{t,d}}{\prod_{\substack{a \\ a \in path(s \rightarrow t)}} \eta} \cdot \quad (4)$$

(3)-formula terminal tugundagi agregatlangan netto talabni, (4)-formula esa yo‘qotishlarni hisobga olgan holda manba darajasidagi brutto talabni aniqlaydi. Shu tarzda har bir qirrada qaysi fermerlar yoki terminallar oqimi o‘tishi belgilanib, keyingi LP cheklovlari uchun asos yaratildi.

4. Adolatli limitlashning chiziqli dasturlash modeli

Limitlash masalasida qaror o‘zgaruvchisi sifatida $x_{f,d}$ — f fermerga d dekadada ajratiladigan suv hajmi [m^3] qabul qilindi. Modelning asosiy maqsadi fermerlar o‘rtasidagi nisbiy defitsitning eng katta qiymatini kamaytirishdan iborat bo‘ldi. Buning uchun yordamchi θ o‘zgaruvchisi kiritilib, quyidagi minimaks qo‘yilishi qabul qilindi:

$\min \theta$ (5)

Bunda adolat sharti quyidagi cheklov bilan berildi:

$$1 - \frac{\sum_{d \in D} x_{f,d}}{\sum_{d \in D} R_{f,d}} \leq \theta, \quad f \in F. \quad (6)$$

Har bir fermer uchun ajratiladigan suv hajmi talabdan oshmasligi hamda manfiy bo‘lmasligi quyidagi shart bilan ta’minlandi:

$$0 \leq x_{f,d} \leq R_{f,d}, \quad f \in F, d \in D. \quad (7)$$

Manba yoki bosh taqsimlash nuqtasidagi mavjud limit L_d hisobga olinib, umumiy resurs cheklovi quyidagicha yozildi:

$$\sum_{f \in F} x_{f,d} \leq L_d, \quad d \in D. \quad (8)$$

Kanal tarmog‘idagi har bir qirra uchun o‘tkazuvchanlik cheklovi ham qo‘yildi. Agar $P(e)$ qirrasi orqali suv oladigan fermerlar to‘plami bo‘lsa, u holda:

$$\sum_{f \in P(e)} x_{f,d} \leq C_{e,d}, \quad e \in E, d \in D. \quad (9)$$

$f \in P(e)$

(5) maqsad funksiyasi, (6) adolat mezoni, (7) fermer darajasidagi cheklov, (8) umumiy resurs cheklovi va (9) tarmoq quvvati cheklovini ifodalaydi. Shu bois limitlash yechimi ham talablarga yaqinlikni, ham tarmoq imkoniyatlarini bir vaqtda hisobga oladi.

Taqsimot samaradorligini oshirish maqsadida ikki bosqichli yechim qo‘llanildi. Birinchi bosqichda (5)–(9) qo‘yilish orqali θ minimallashtirildi. Ikkinchi bosqichda topilgan θ^* qiymati saqlangan holda jami qondirilgan talab maksimallashtirildi:

$$\max \sum_{d \in D} \sum_{f \in F} x_{f,d} \quad (10)$$

Ikkinchi bosqichda (6)–(9) cheklovlar saqlanib qoladi, faqat (6)-formuladagi θ o'rniga θ^* qiymati qo'yiladi. Bu yondashuv avval adolatni ta'minlash, so'ng shu adolat darajasini buzmag holida jami ajratilgan suv hajmini oshirish imkonini beradi.

5. Hisoblash algoritmining amaliy ketma-ketligi

Hisoblash algoritmi quyidagi amaliy ketma-ketlikda bajarildi. Avvalo fermerlar, maydonlar, gidromodul rayonlar, ekinlar va dekadalik sug'orish normalari bo'yicha kirish jadvallari shakllantirildi. Keyin (1) va (2) formulalar asosida fermerlar kesimidagi suv talablari hisoblandi. Uchinchi bosqichda kanal tarmog'i $G = (V, E)$ grafi tuzilib, (3) va (4) formulalar orqali terminal va manba darajasidagi talablar

aniqlandi. To'rtinchi bosqichda (5)–(10) munosabatlar asosida chiziqli dasturlash masalasi shakllantirilib, standart LP yechuvchi yordamida yechim olindi. Yakunda har bir fermer bo'yicha ajratilgan suv hajmi, defitsit va defitsit ulushi hisoblanib, jadval va grafik ko'rinishida tahlil qilindi.

Taklif etilgan metodlar bloki keyinchalik tarmoqning haqiqiy ma'lumotlari bilan to'ldirilganda ham o'z strukturasi saqlab qoladi va limitlash masalasini axborot tizimi doirasida avtomatlashtirilgan hisoblashga moslashtirish imkonini beradi.

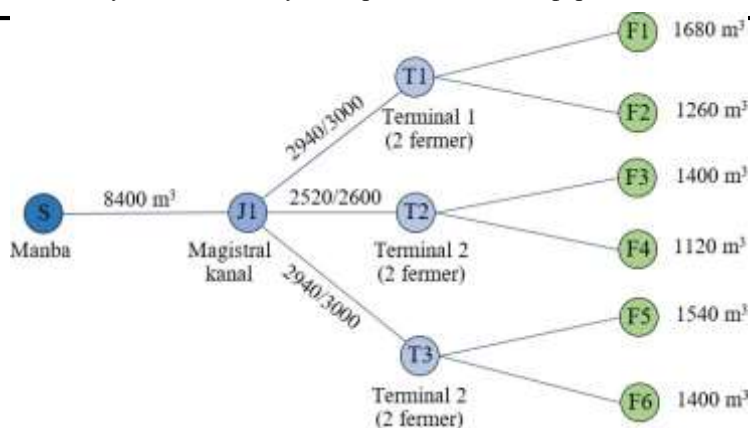
Natijalar. Taklif etilgan metodika (1)–(10) munosabatlar asosida 6 ta fermer, 3 ta terminal tugun va 1 ta manbadan tashkil topgan kanal tarmog'i uchun qo'llanildi. (1) va (2) formulalar bo'yicha hisoblash natijasida fermerlar kesimida jami netto suv talabi 12000 m³ ni tashkil qildi. (3) va (4) formulalar orqali yo'qotishlar hisobga olinganda manba darajasidagi jami brutto talab 14900 m³ ga teng ekani aniqlandi. Bu holat suv ta'minoti sharoiti cheklangan davrda taqsimotni adolat mezonini asosida tashkil etish zarurligini ko'rsatdi.

Birinchi bosqichda (5)–(9) qo'yilish yechilib, eng katta nisbiy defitsitning minimal qiymati $\theta^*=0.30$ ekani topildi. Demak, mavjud limit sharoitida har bir fermer uchun defitsit ulushining yuqori chegarasi 30 foizdan oshmasligi ta'minlandi. Ikkinchi bosqichda (10) maqsad funksiyasi qo'llanilib, $\theta^*=0.30$ qiymat saqlangan holda jami qondirilgan talab maksimallashtirildi va ajratilgan suvning yig'indi hajmi 8400 m³ ni tashkil qildi.

1-jadval. Fermerlar kesimida suv talablari va limitlash natijalari

Fermer	Terminal	Maydon, ga	Netto talab, m ³	Brutto talab, m ³	Ajratilgan suv, m ³	Defitsit, m ³	Defitsit, %
F1	T1	30	2400	3000	1680	720	30.0
F2	T1	20	1800	2400	1260	540	30.0
F3	T2	25	2000	2500	1400	600	30.0
F4	T2	20	1600	2000	1120	480	30.0
F5	T3	22	2200	2500	1540	660	30.0
F6	T3	25	2000	2500	1400	600	30.0
Jami	—	142	12000	14900	8400	3600	30.0

1-jadval ma'lumotlariga ko'ra, barcha fermerlar bo'yicha defitsit ulushi bir xil — 30.0 foizni tashkil qildi. Bu esa (6) formulada berilgan adolat sharti amalida ta'minlanganini ko'rsatadi. Shu bilan birga, ajratilgan suv hajmlari fermerlarning talab miqdoriga mutanosib taqsimlandi: eng katta ajratma F1 fermer uchun 1680 m³, eng kichik ajratma esa F4 fermer uchun 1120 m³ bo'ldi.



1-rasm. Kanal tarmog'ining graf modeli va ajratilgan oqimlar

1-rasmda keltirilgan tarmoq bo'yicha taqsimot natijalariga muvofiq magistral kanaldan T1, T2 va T3 terminallariga mos ravishda 2940/3000, 2520/2600 va 2940/3000 nisbatda suv uzatildi. Demak, (8) va

(9) cheklovlar bir vaqtning o'zida bajarildi: umumiy manba limiti 8400 m³ dan oshmadi va qirralar bo'yicha quvvat chegaralari buzilmadi. Olingan natijalar taklif etilgan algoritm suv yetishmovchiligi sharoitida ham adolatli taqsimotni hamda tarmoqning texnik cheklovlariga mos yechimni ta'minlashini ko'rsatadi.

Xulosa. Ushbu tadqiqotda gidromodulli rayonlashtirish, tarmoqni graf ko'rinishida ifodalash va chiziqli dasturlash usulini birlashtirgan holda suv resurslarini adolatli limitlash algoritmi taklif etildi. Ishlab chiqilgan yondashuv fermerlar kesimida netto va brutto suv talabini hisoblash, kanal tarmog'idagi cheklovlarni inobatga olish va mavjud limit sharoitida suvni maqbul taqsimlash imkonini berdi. Olingan natijalar taqsimot jarayonida qondirilmagan talabni kamaytirish, nisbiy defitsitni barqarorlashtirish va qaror qabul qilishni asoslashda mazkur algoritmning amaliy ahamiyati yuqori ekanini ko'rsatdi. Taklif etilgan yondashuvni real tarmoq ma'lumotlari asosida qo'llash suv boshqaruvi samaradorligini oshirishga xizmat qiladi.

Foydalanilgan adabiyotlar

- 1.Кудайбергенов А. А. Йирик магистрал каналларнинг сув ресурсларини тақсимлаш масаласининг математик моделларини ишлаб чиқиш // Фан ва жамият. 2023. № 2. С. 17–18.
- 2.Рахимов Ш. Х., Сейтов А. Ж., Кудайбергенов А. А. Оптимальное управление распределением воды в магистральных каналах ирригационных систем // Наука и общество. 2020. № 2. С. 8–10.
- 3.Qudaybergenov A. A. Gidromodulli tumanlashtirish asosida fermer xo'jaliklarining dekadaviy suv talabini hisoblashning matematik modeli // Muhammad Al-Xorazmiy avlodlari. 2025. T. 4, № 34. С. 175–178.
- 4.Qudaybergenov A. A. и др. Gidromodulli tumanlashtirish asosida fermer xo'jaliklarining dekadaviy suv talabini hisoblash algoritmi // "Raqamli iqtisodiyot sharoitidaiqtisodiyot,buxgalteriya hisobi va axborot texnologiyalarini rivojlantirishistiqbollari" mavzusida Xalqaro ilmiy konferensiya. Samarqand, 2026. С. 193–196.
- 5.Qudaybergenov A. A. и др. Irrigatsiya tarmoqlarida iste'molchilar uchun dekadaviy optimal suv limitlarini hisoblashning graf va chiziqli dasturlash modeli // "Raqamli iqtisodiyot sharoitidaiqtisodiyot,buxgalteriya hisobi va axborot texnologiyalarini rivojlantirishistiqbollari" mavzusida Xalqaro ilmiy konferensiya. Samarqand, 2026. С. 189–192.
- 6.Dang C. и др. IWRAM: A hybrid model for irrigation water demand forecasting to quantify the impacts of climate change // Agricultural Water Management. 2024. T. 291. С. 108643.
- 7.Liao X. и др. A novel irrigation canal scheduling model adaptable to the spatial-temporal variability of water conveyance loss // Agricultural Water Management. 2022. T. 274. С. 107961.
- 8.Delgoda D. и др. A novel generic optimization method for irrigation scheduling under multiple objectives and multiple hierarchical layers in a canal network // Advances in Water Resources. 2017. T.

9. Gonçalves G. M., Vaz Pato M. A three-phase procedure for designing an irrigation system's water distribution network // Annals of Operations Research. 2000. T. 94, № 1–4. С. 163–179.

10. N. A. Akhand, D. L. Larson, D. C. Slack. Canal Irrigation Allocation Planning Model // Transactions of the ASAE. 1995. T. 38, № 2. С. 545–550.

11. Marques G. F., Lund J. R., Howitt R. E. Modeling irrigated agricultural production and water use decisions under water supply uncertainty // Water Resources Research. 2005. T. 41, № 8. С. 2005WR004048.

12. Luss H., Smith D. R. Resource allocation among competing activities: a lexicographic minimax approach // Operations Research Letters. 1986. T. 5, № 5. С. 227–231.

ELLIPTIK EGRI CHIZIQ KRIPTOGRAFIYASI ASOSIDA KVANT KALIT ALMASHINUVI SXEMASINI MODELLASHTIRISH

¹ D.T. Muhamediyeva, ¹ Tagaev Farxad Abduvaxabovich

«Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash
muhandislari instituti» milliy tadqiqot universiteti

dilnoz134@rambler.ru

Annotatsiya: Ushbu maqolada Elliptik egri chiziq kriptografiyasi (ECC) asosida kalit almashinuvi jarayoni va uning kvant simulyatsiyasi Qiskit muhiti yordamida amalga oshiriladi. Elliptik egri chiziq ustida nuqta qo'shish va ko'paytirish amallari orqali Alice va Bob o'zlarining maxfiy va ochiq kalitlarini generatsiya qiladi. Shundan so'ng, ular o'zaro umumiy kalitni hisoblaydilar va ushbu kalit bir xil natijaga ega bo'lishi tekshiriladi. Maqolada kvant simulyatsiya bosqichi sifatida Hadamard va CNOT kvant darvozalari ishlatilgan bo'lib, ular orqali kvant holatlaridagi superpozitsiya va bog'liqlik (entanglement) jarayoni modellashtirilgan. Natijalar kvant hisoblashning ECC asosidagi xavfsiz kalit almashinuvi tizimlarini yanada takomillashtirish imkonini berishini ko'rsatadi.

Kalit so'zlar: Elliptik egri chiziq kriptografiyasi; kvant kalit almashinuvi; superpozitsiya; kvant simulyatsiyasi.

МОДЕЛИРОВАНИЕ СХЕМЫ КВАНТОВОГО ОБМЕНА КЛЮЧАМИ НА ОСНОВЕ КРИПТОГРАФИИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

¹Д.Т. Мухамедиева, ¹Тагаев Фархад Абдувахабович

Национальный исследовательский университет «Ташкентский институт инженеров
иригации и механизации сельского хозяйства»

dilnoz134@rambler.ru

Аннотация: В данной статье реализован процесс обмена ключами на основе криптографии на эллиптических кривых (ECC) и его квантовое моделирование с использованием среды Qiskit. Алиса и Боб генерируют свои секретный и открытый ключи, добавляя и умножая точки на эллиптической кривой. После этого они вычисляют общий ключ и проверяют, даёт ли этот ключ одинаковый результат. В статье квантовые вентили Адамара и CNOT используются в качестве этапов квантового моделирования, посредством которых моделируются процессы суперпозиции и запутывания в квантовых состояниях. Результаты показывают, что квантовые вычисления могут дополнительно улучшить безопасные системы обмена ключами на основе ECC.

Ключевые слова: эллиптическая кривая криптографии; квантовый обмен ключами; суперпозиция; квантовое моделирование.