PEDAGOGIK TADQIQOTLAR JURNALI *№ 3,Yanvar, 2025*
ISSN: 3060-4923, Impact Factor – 7,212 *worldly knowledge*
Index: google scholar, research gate, research bib, zenodo, open aire.
https://scholar.google.com/scholar?hl=ru&as_sdt=0%2C5&q=wosjournals.com&btnG
https://www.researchgate.net/search/publication?q=worldly%20knowledge
https://journalseeker.researchbib.com/view/issn/3060-4923

AXBOROTLARNI SHIFRLASH: NAZARIYASI VA AMALIYOTI

HAYITOVA ZEBINISO ILHOMOVNA

Romitan tuman 1-son politexnikumining

“Informatikav a axborot texnologiyalari ” fani o’qituvchisi

Kirish

Axborotlar zamonaviy jamiyatda eng muhim resurslardan biri bo‘lib, uning xavfsizligi, maxfiyligi va butunligini ta'minlash hayotiy ahamiyat kasb etadi. Axborotlarni shifrlash (kripografiya) usullari, o‘z navbatida, bu xavfsizlikni ta'minlashda asosiy vosita hisoblanadi. Shifrlash – bu axborotni ma'lum bir algoritm yordamida noaniq, tushunarsiz holatga keltirish jarayonidir, shu bilan birga faqat ma'lum shaxslar tomonidan axborotni qayta tiklash yoki o'qish imkonini beradi. Shifrlar yillar davomida taraqqiy etib, hozirda o‘ta murakkab va ishonchli tizimlarga aylangan.

Ushbu maqolada axborotlarni shifrlashning nazariyasi, usullari va zamonaviy texnologiyalarni tahlil qilamiz. Shuningdek, axborot xavfsizligini ta'minlashdagi asosiy masalalar va kriptoprotokollarning amaliy qo‘llanilishi ham muhokama qilinadi.

1. Shifrlaishning Nazariy Asoslari

Shifrlaishning asosiy maqsadi – axborotni muayyan shaklda kodlash, shunday qilib, uni shifrlash va dekodlashda faqat maxsus kalitlar yordamida amalga oshirish mumkin bo‘ladi. Kripografiya so‘zi yunoncha "kryptos" (maxfiy) va "grapho" (yozish) so‘zlaridan olingan, bu shifrlash jarayonining mohiyatini aks ettiradi.

Shifrlaish texnikalari ikki asosiy kategoriya bo‘yicha tasniflanadi: **simmetrik** va **asimmetrik** shifrlash.

- **Simmetrik (bir xil kalitli) shifrlash** – bu usulda ma'lumotlarni shifrlash va dekodlash uchun bir xil kalit ishlatiladi. Agar kalitni noma'lum shaxslar bilsa, shifrlangan axborotni o‘qish mumkin bo‘ladi. Bu turdagi shifrlash tizimlaridan eng mashhurlari DES (Data Encryption Standard) va AES (Advanced Encryption Standard) hisoblanadi. AES 128, 192, va 256 bitli kalitlar bilan ishlaydi va zamonaviy kriptografiyada keng qo‘llaniladi.

- **Asimmetrik (ochiq-yiqilishli) shifrlash** – bu usulda ikki xil kalit ishlatiladi: biri ochiq (public), ikkinchisi esa shaxsiy (private). Ochiq kalit umumiy maqsadlar uchun tarqatiladi, shaxsiy kalit esa faqat tegishli foydalanuvchida saqlanadi. Asimmetrik shifrlashning eng mashhur algoritmi RSA hisoblanadi, bu usulni ko‘plab internet xavfsizligi tizimlarida, jumladan, HTTPS protokollarida qo‘llashadi.

2. Shifrlaish Algoritmlari va Ularning Turlari

Zamonaviy kriptoalgoritmlar juda murakkab va ko‘p holatlarda matematik, statistik va algoritmik metodlarga asoslanadi. Quyida ularning ayrimlarini ko‘rib chiqamiz:

- **RSA (Rivest-Shamir-Adleman)** – bu asimmetrik shifrlash algoritmi 1978-yilda Ron Rivest, Adi Shamir va Leonard Adleman tomonidan ishlab chiqilgan. RSA algoritmi asosida ikkita kalit mavjud: ochiq va shaxsiy kalit. Bu algoritmning xavfsizligi katta sonli qarorlarning

ko‘paytmasini faktorizatsiya qilishning qiyinligi bilan bog‘liq. RSA ko‘plab xavfsiz tizimlarda, masalan, raqamli imzolarni yaratishda va elektron to‘lov tizimlarida qo‘llaniladi.

- **AES (Advanced Encryption Standard)** – AES simmetrik shifrlash algoritmi bo‘lib, asosan davlat xavfsizligi va tijorat sohasida ishlatiladi. AES 128, 192, va 256 bitli kalitlar bilan ishlaydi va yuqori darajadagi xavfsizlikni ta'minlaydi. AES algoritmi, shu bilan birga, mobil qurilmalar va bulutli xizmatlarda keng qo‘llaniladi.

- **ECC (Elliptic Curve Cryptography)** – bu asimmetrik shifrlash algoritmi elliptik egri chiziqlarga asoslanadi va RSA ga nisbatan kichikroq kalitlar bilan yuqori xavfsizlikni ta'minlaydi. ECC ko‘plab mobil qurilmalar va IoT (Internet of Things) tizimlarida qo‘llaniladi.

- **SHA (Secure Hash Algorithm)** – bu algoritm axborotni to‘liq va o‘zgarmas holatga keltiradi. SHA algoritmlari raqamli imzolarni yaratish va axborotlar yaxlitligini ta'minlashda ishlatiladi. SHA-2 va SHA-3 versiyalari eng mashhur variantlardir.

3. Kriptografiyaning Amaliy Qo‘llanilishi

Zamonaviy axborot texnologiyalari va internet xavfsizligini ta'minlashda kriptografiya muhim rol o‘ynaydi. Shifrlash texnologiyalarining eng keng tarqalgan qo‘llanilishi quyidagilarni o‘z ichiga oladi:

- **Internet Xavfsizligi**: Web-saytlar va internet xizmatlarining xavfsizligini ta'minlash uchun SSL/TLS protokollari qo‘llaniladi. Ushbu protokollar ma'lumotlarni uzatish paytida shifrlashni amalga oshiradi va foydalanuvchi va server o‘rtasidagi aloqani xavfsiz qiladi. HTTPS (Hypertext Transfer Protocol Secure) bu protokollarning keng qo‘llaniladigan shaklidir.

- **Elektron Imzolar**: Raqamli imzolar, asosan, asimmetrik shifrlash algoritmlari yordamida yaratiladi va hujjatlarning haqiqiyligini va yaxlitligini ta'minlaydi. Elektron imzolar ko‘plab huquqiy hujjatlar, shartnomalar va elektron to‘lov tizimlarida ishlatiladi.

- **Blokcheyn Texnologiyalari**: Blokcheyn texnologiyasi, shifrlash va raqamli imzolardan foydalangan holda, xavfsiz va o‘zgarishsiz tizimlarni yaratadi. Kriptoaktivlar, masalan, Bitcoin, o‘zining xavfsizlik va ishonchliligini blokcheyn asosida ta'minlaydi.

- **Mobil Qurilmalar va IoT**: Mobil telefonlar va IoT qurilmalarida axborot xavfsizligi uchun kriptografik texnologiyalar ishlatiladi. ECC algoritmi ko‘p hollarda mobil qurilmalarda qo‘llaniladi, chunki u kam resurslar sarflaydi va yuqori xavfsizlikni ta'minlaydi.

4. Kriptografiya Xavfsizligi va Hujumlar

Kriptografiya tizimlarining xavfsizligi har doim tajovuzkorlar tomonidan amalga oshiriladigan turli hujumlar bilan ta'sirlanishi mumkin. Ba'zi eng keng tarqalgan hujumlar quyidagilardir:

- **Brute-force hujumi**: Kalitning barcha mumkin bo‘lgan qiymatlarini sinash orqali tizimni buzish. Bu hujumni samarali amalga oshirish uchun kalit uzunligi katta bo‘lishi kerak.

- **Matn tahlili hujumi (Ciphertext attack)**: Shifrlangan matnning xususiyatlarini tahlil qilish orqali uni ochishga urinish. Ba'zi shifrlash algoritmlari, masalan, shifrlashning kuchli yodgorliklarga ega bo‘lishi kerak, bu esa hujumni qiyinlashtiradi.

- **Kuchli tomonlarni aniqlash**: Kriptografiya tizimlarini muntazam tahlil qilib, ular zaif tomonlarni aniqlash va ularni kuchaytirish muhimdir. Yangi yondashuvlar va algoritmlar doimiy ravishda ishlab chiqilmoqda.

Xulosa

Axborotlarni shifrlash bugungi kunda axborot xavfsizligini ta'minlashning asosiy vositalaridan biri hisoblanadi. Shifrlash texnologiyalari nafaqat internetda, balki moliya, tibbiyot, hukumat tizimlarida ham keng qo‘llaniladi. Kriptografiya doimiy ravishda rivojlanib bormoqda, va yangi texnologiyalar, masalan, kvant kriptografiyasi, bu sohaning kelajagini yangi bosqichga olib chiqishi mumkin. Shifrlaishning rivojlanishi va xavfsizlikni ta'minlashda yangi yondashuvlar kiritilishi axborotlarni himoya qilishda yana bir qadam oldinga siljish bo‘ladi.

FOYDALANILGAN ADABIYOTLAR

1. Муродов, О. Т. (2023). РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕМПЕРАТУРЫ И ВЛАЖНОСТИ В ПРОИЗВОДСТВЕННЫХ КОМНАТ. *GOLDEN BRAIN*, *1*(26), 91-95.
2. Murodov, O. T. R. (2023). INFORMATIKA DARSLARINI TASHKIL ETISHDA INNOVATSION USULLARDAN FOYDALANISH. *GOLDEN BRAIN*, *1*(32), 194-201.
3. Murodov, O. T. R. (2023). Zamonaviy ta’limda axborot texnologiyalari va ularni qo ‘llash usul va vositalari. *Educational Research in Universal Sciences*, *2*(11), 481-486.
4. Murodov, O. T. R. (2023). INFORMATIKA FANINI O ‘QITISHDA YANGI INNOVATSION USULLARDAN FOYDALANISH METODIKASI. *GOLDEN BRAIN*, *1*(34), 130-139
5. Torakulovich, M. O. (2024). Innovative information technologies and new methods and tools for their application in today's education. *Central Asian Journal Of Education and Innovation*, *3*(2-2), 83-92.
6. Muradov, O. (2024). Basic principles and rules of innovative pedagogical technologies in the educational process. *Models and methods in modern science*, *3*(1), 84-93.
7. Turakulovich, M. O. (2024). DEVELOPMENT AND INSTALLATION OF AN AUTOMATIC TEMPERATURE CONTROL SYSTEM IN ROOMS. *Methods of applying innovative and digital technologies in the educational system*, *1*(2), 72-77.
8. Muradov, O. (2024, January). Application of basic principles and rules of innovative pedagogical technologies to educational processes. In *Международная конференция академических наук* (Vol. 3, No. 1, pp. 46-55).
9. Murodov, O. (2024). DEVELOPMENT OF AN AUTOMATED PARAMETER CONTROL SYSTEM ROOMS AND WORKSHOPS BASED ON CLOUD TECHNOLOGIES. *Академические исследования в современной науке*, *3*(2), 16-27.
10. Muradov, O. (2024). APPLIED TO THE CURRENT TRAINING PROCESS REQUIREMENTS. *Инновационные исследования в науке*, *3*(1), 54-63.
11. Murodov, O. (2024). DEVELOPMENT AND INSTALLATION OF AN AUTOMATIC TEMPERATURE CONTROL SYSTEM IN ROOMS. *Solution of social problems in management and economy*, *3*(2), 91-94.
12. To’raqulovich, M. O. (2024). IMPROVING THE TEACHING PROCESS OF IT AND INFORMATION TECHNOLOGIES BASED ON AN INNOVATIVE APPROACH. *Multidisciplinary Journal of Science and Technology*, *4*(3), 851-859.
13. Murodov, O. (2023). INNOVATSION YONDASHUV ASOSIDA INFORMATIKA VA AXBOROT TEXNOLOGIYALARI FANINI O’QITISH JARAYONINI

TAKOMILLASHTIRISH. *Theoretical aspects in the formation of pedagogical sciences*, *3*(4), 77-81.

14. Murodov, O. (2024). TA'LIM TEXNOLOGIYALARINING ILMIY-NAZARIY ASOSLARI. *Science and innovation in the education system*, *3*(3), 155-160.

15. Murodov, O. (2024). DEVELOPMENT OF AN AUTOMATED SYSTEM FOR CONTROLLING TEMPERATURE AND HUMIDITY IN PRODUCTION ROOMS. *Development and innovations in science*, *3*(1), 84-93.

16. To'raqulovich, M. O. (2024). OLIY TA'LIM MUASSASALARIDA TA'LIMNING INNOVASION TEXNOLOGIYALARDAN FOYDALANISH. *PEDAGOG*, *7*(5), 627-635.

17. . Muradov, O. (2024, January). IN TEACHING INFORMATICS AND INFORMATION TECHNOLOGIES REQUIREMENTS. In *Международная конференция академических наук* (Vol. 3, No. 1, pp. 97-102).

18. To'raqulovich, M. O. (2024). OLIY TA'LIM MUASSASALARIDA AXBOROT KOMMUNIKASIYA TEXNOLOGIYALARI DARSLARINI TASHKIL ETISHDA ZAMONAVIY USULLARDAN FOYDALANISH. *PEDAGOG*, *7*(6), 63-74.