MA’LUMOTLARNI SHIRFLASH TENALOGIYALARI VA XAVFSIZLIK STANDARTLARI

Umarov Bekzod Azizovich
Farg’ona davlat unversiteti o‘qituvchi
ubaumarov@mail.ru
Rahmatov Ziyodullo Rustamjon o‘g‘li
Farg‘ona davlat universiteti talabasi
zrahmatov921@gmail.com

Annotatsiya: *Ushbu maqola ma’lumotlarni shifrlash texnologiyalari va xavfsizlik standartlarining ahamiyati, qo‘llanilishi hamda zamonaviy dunyodagi o‘rni haqida batafsil ma’lumot beradi. Shifrlash texnologiyalari orqali ma’lumotlarni himoya qilish, ularning maxfiyligini saqlash va ruxsatsiz kirishlardan xavfsizligini ta’minlash imkonini beradi. Shuningdek, maqolada shifrlash algoritmlari, ularning turlari, ma’lumotlar xavfsizligini ta’minlashdagi o‘rni va xalqaro standartlarning ahamiyati ko‘rib chiqilgan.*

Maqolada zamonaviy shifrlash texnologiyalarining rivojlanishi, ulardan foydalanishning huquqiy va texnik jihatlari, shuningdek, kriptografiyaning kelajakdagi istiqbollari haqida ma’lumot berilgan. Shu bilan birga, ma’lumotlarni shifrlashning amaliy qo‘llanilishi va axborot xavfsizligini ta’minlashdagi muhim jihatlar yoritilgan.

Kalit so‘zlar: *Shifrlash, kriptografiya, xavfsizlik standartlari, ma’lumotlarni himoya qilish, algoritmlar, maxfiylik, axborot xavfsizligi.*

Аннотоция: *статья предоставляет подробную информацию о значении технологий шифрования данных и стандартах безопасности, их применении и месте в современном мире. Технологии шифрования обеспечивают защиту данных, сохранение их конфиденциальности и защиту от несанкционированного доступа. Также в статье рассматриваются алгоритмы шифрования, их виды, роль в обеспечении безопасности данных и значение международных стандартов.*

В статье также представлены данные о развитии современных технологий шифрования, правовых и технических аспектах их использования, а также перспективах криптографии в будущем. Важное внимание уделяется практическому применению шифрования данных и аспектам обеспечения информационной безопасности.

Ключевые слова: *Шифрование, криптография, стандарты безопасности, защита данных, алгоритмы, конфиденциальность, информационная безопасность.*

Annotation: *This article provides detailed information on the importance of data encryption technologies and security standards, their application, and their place in the modern world. Encryption technologies allow for the protection of data, preservation of their confidentiality, and prevention of unauthorized access. The article also covers*

encryption algorithms, their types, their role in ensuring data security, and the importance of international standards.

The article presents information on the development of modern encryption technologies, the legal and technical aspects of their use, and the future prospects of cryptography. Moreover, the practical application of data encryption and key aspects of ensuring information security are highlighted.

Keywords: *Encryption, cryptography, security standards, data protection, algorithms, confidentiality, information security.*

Kirish

Global axborot makonining rivojlanishi natijasida ma’lumotlarni himoya qilish masalasi dolzarb muammolardan biriga aylandi. Kompaniyalar, davlat muassasalari va jismoniy shaxslar tomonidan foydalanilayotgan ma’lumotlarning maxfiyligi va butunligini ta’minlash uchun zamonaviy shifrlash texnologiyalaridan foydalanish zarur bo‘lib bormoqda. Ma’lumotlarni shifrlash texnologiyalari har qanday tashqi tajovuz va ruxsatsiz kirishlarga qarshi samarali himoya vositasi hisoblanadi.

Shifrlash texnologiyasi ma’lumotlarni o‘qilmaydigan shaklga aylantirishga imkon beradi. Ushbu jarayon shifrlash algoritmlari yordamida amalga oshiriladi va shifrlangan ma’lumotlarni faqat tegishli kalit yordamida qayta tiklash mumkin. Zamonaviy kriptografiya texnologiyalari ma’lumotlarning xavfsizligini ta’minlash bilan birga, ulardan qonuniy foydalanish uchun huquqiy asoslarni ham shakllantiradi.

Shifrlash texnologiyalarining qo‘llanilishi

1. Tarmoq xavfsizligi

Shifrlash texnologiyalari tarmoq xavfsizligini ta’minlashda asosiy rol o‘ynaydi. Internet orqali uzatiladigan ma’lumotlarni shifrlash orqali ularning maxfiyligini va ruxsatsiz kirishdan himoyalanishini ta’minlash mumkin.

Masalan:

• TLS/SSL protokollari: Veb-saytlar va foydalanuvchilar o‘rtasida uzatiladigan ma’lumotlarni shifrlash orqali xavfsizlikni oshiradi.

• VPN texnologiyalari: Tarmoqda uzatilayotgan ma’lumotlarning maxfiyligini ta’minlaydi va ruxsatsiz kuzatuvlarning oldini oladi.

2. Elektron pochta xavfsizligi

Elektron pochta orqali yuboriladigan xabarlarning mazmunini shifrlash ularni begona shaxslar tomonidan o‘qilishidan himoya qiladi. Zamonaviy elektron pochta tizimlarida PGP (Pretty Good Privacy) va S/MIME kabi shifrlash texnologiyalaridan keng foydalaniladi.

3. Ma’lumotlarni saqlash xavfsizligi

Shifrlash texnologiyalari orqali foydalanuvchi ma’lumotlari qattiq disklar, bulutli xizmatlar yoki boshqa saqlash vositalarida himoya qilinadi. Bu texnologiya ma’lumotlar

o‘g‘irlanishi yoki yo‘qotilishining oldini olishda katta ahamiyatga ega. Masalan, AES (Advanced Encryption Standard) algoritmi ma’lumotlarni xavfsiz shifrlashda keng qo‘llaniladi.

4. Moliyaviy operatsiyalar xavfsizligi

Onlayn to‘lovlar va bank operatsiyalarida shifrlash texnologiyalari muhim o‘rin tutadi. Har bir tranzaksiya xavfsizligini ta’minlash uchun RSA va ECC (Elliptic Curve Cryptography) kabi shifrlash algoritmlari qo‘llaniladi.

Xavfsizlik standartlari

1. Xalqaro standartlar

Xavfsizlikni ta’minlash maqsadida xalqaro miqyosda bir qator standartlar ishlab chiqilgan:

- ISO/IEC 27001: Axborot xavfsizligini boshqarish tizimining xalqaro standarti.

- NIST (National Institute of Standards and Technology): Kriptografik algoritmlar va xavfsizlik bo‘yicha tavsiyalar beradi.

2. Regional standartlar

Ba’zi davlatlarda ma’lumotlar xavfsizligini ta’minlash uchun maxsus standartlar qabul qilingan. Masalan:

- GDPR (General Data Protection Regulation): Yevropa Ittifoqida ma’lumotlarni himoya qilish bo‘yicha qoidalarni belgilaydi.
- HIPAA (Health Insurance Portability and Accountability Act): AQShda tibbiy ma’lumotlar xavfsizligini ta’minlash uchun ishlatiladi

3. Kriptografik algoritmlar standarti

Hozirda eng ishonchli algoritmlar quyidagilardan iborat:

- AES (Advanced Encryption Standard): Ma’lumotlarni yuqori darajada shifrlash imkonini beradi.
- RSA (Rivest-Shamir-Adleman): Asimmetrik shifrlashda keng qo‘llaniladi.
- SHA (Secure Hash Algorithm): Ma’lumotlarning yaxlitligini tekshirish uchun ishlatiladi.

Shifrlash texnologiyalarining afzalliklari

Afzalliklar	Tavsif
Maxfiylikni ta’minlash	Ma’lumotlarni begona shaxslardan himoya qilish imkonini beradi.

Ma’lumot yaxlitligi	Ma’lumotlarga ruxsatsiz o‘zgartirishlarning oldini oladi.
Ishonchlilik	Tarmoq orqali uzatilayotgan ma’lumotlarning xavfsizligini ta’minlaydi.
Keng qo‘llanilish	Moliyaviy tizimlardan boshlab, tibbiyotgacha turli sohalarda ishlatiladi.

Kelajakdagi istiqbollar

Shifrlash texnologiyalari va xavfsizlik standartlari tez sur‘atlar bilan rivojlanmoqda. Kelajakda quyidagi yo‘nalishlarda sezilarli o‘zgarishlar kutilmoqda:

- Kvant kriptografiyasi: Kvant kompyuterlarining paydo bo‘lishi bilan yangi xavfsizlik texnologiyalarini ishlab chiqish zarur bo‘ladi.
- Blokcheyn texnologiyalari: Ma’lumotlar xavfsizligini oshirish va tranzaksiyalarni shaffof qilish

Xulosa:

Ushbu maqolada ma’lumotlarni himoya qilishda shifrlash texnologiyalarining roli, ularning turlari va xavfsizlikni ta’minlashdagi ahamiyati batafsil yoritildi. Shifrlash texnologiyalari ma’lumotlarning maxfiyligini saqlash va ruxsatsiz kirishlardan himoya qilishda muhim vosita hisoblanadi. Tarmoq xavfsizligi, elektron pochta xavfsizligi, ma’lumotlarni saqlash va moliyaviy operatsiyalar kabi sohalarda shifrlash texnologiyalarining qo‘llanilishi keng tarqalgan. Shuningdek, xalqaro va regional xavfsizlik standartlari hamda kriptografik algoritmlar xavfsizlikni ta’minlashdagi o‘rni haqida ma’lumot berildi. Maqola, kelajakda kvant kriptografiyasi va blokcheyn texnologiyalarining rivojlanishi bilan xavfsizlikning yangi yo‘nalishlarini keltirib chiqarishi kutilayotganini ta’kidladi.

FOYDALANILGAN ADABIYOTLAR:

1. ISO/IEC 27001: Axborot xavfsizligini boshqarish tizimining xalqaro standarti.
2. National Institute of Standards and Technology (NIST): Kriptografik algoritmlar va xavfsizlik bo‘yicha tavsiyalar.
3. GDPR (General Data Protection Regulation): Yevropa Ittifoqi ma’lumotlarni himoya qilish bo‘yicha qoidalar.
4. HIPAA (Health Insurance Portability and Accountability Act): AQShda tibbiy ma’lumotlar xavfsizligini ta’minlash uchun standart.
5. AES (Advanced Encryption Standard): Ma’lumotlarni yuqori darajada shifrlash imkonini beradi.
6. RSA (Rivest-Shamir-Adleman): Asimmetrik shifrlashda keng qo‘llaniladigan algoritm.
7. SHA (Secure Hash Algorithm): Ma’lumotlarning yaxlitligini tekshirish uchun ishlatiladi.