DOI: https://doi.org/10.36719/2789-6919/45/132-135

Günay Şahbazova
Odlar Yurdu Universiteti
magistrant
https://orcid.org/0009-0006-7907-7044
gunay.shahbazova20@gmail.com

İnformasiya təhlükəsizliyi və kodlaşdırma üsullarının təhlili

Xülasə

Bu məqalədə informasiya təhlükəsizliyi və kodlaşdırma üsullarının təhlili aparılmışdır. Rəqəmsal məlumatların artması ilə yanaşı bu məlumatların icazəsiz əldə olunması, dəyişdirilməsi və ya silinməsi kimi təhdidlər də çoxalır. İnformasiya təhlükəsizliyinin əsas prinsipləri olan məxfilik, bütövlük və əlçatanlıq çərçivəsində müxtəlif şifrələmə texnologiyaları simmetrik və asimmetrik şifrələmə, hash funksiyaları, blokçeyn və kvant kriptoqrafiyası kimi yanaşmalar təhlil edilmişdir.

Müasir dövrdə bu texnologiyalar yalnız fərdi deyil, həm də təşkilati və milli təhlükəsizliyi təmin etmək üçün əsas vasitə kimi çıxış edir. Ənənəvi metodların zəifliyi müasir kriptoqrafik sistemlərin zəruriliyini ortaya qoyur. Təhlillər göstərir ki, təhlükəsizlik yalnız texnologiya ilə deyil, həm də idarəetmə, hüquqi çərçivə və insan faktorunun nəzərə alınması ilə təmin oluna bilər. Məqalədə həmçinin, informasiya təhlükəsizliyi sahəsindəki problemlər, müasir yanaşmalar və tətbiq olunan metodların müqayisəsi verilmiş, nəticə və təkliflər bölməsində isə mövcud problemlərin həlli yolları üzrə konkret addımlar göstərilmişdir.

Açar sözlər: *informasiya təhlükəsizliyi, şifrələmə, kodlaşdırma, blokçeyn, kvant kriptoqrafiyası*

Gunay Shahbazova
Odlar Yurdu University
Master student
https://orcid.org/0009-0006-7907-7044
gunay.shahbazova20@gmail.com

Analysis of Information Security and Coding Methods

Abstract

This paper analyzes information security and encryption methods. With the increasing volume of digital data, the threats of unauthorized access, modification, or deletion of this data are also growing. The key principles of information security, such as confidentiality, integrity, and availability, are discussed in the context of various encryption technologies – symmetric and asymmetric encryption, hash functions, blockchain, and quantum cryptography. In the modern era, these technologies serve as fundamental tools for ensuring not only personal but also organizational and national security. The weaknesses of traditional methods highlight the necessity of contemporary cryptographic systems. The analysis reveals that security cannot solely rely on technology; it must also incorporate management, legal frameworks, and human factors. The paper also compares modern approaches and applied methods, and in the conclusion and recommendations section, it outlines specific measures for addressing existing challenges.

Keywords: *information security, encryption, coding, blockchain, quantum cryptography*

Giriş

Texnologiyalardakı sürətli işlənmə və qloballaşma prosesi insanlıq tarixində informasiyanın əhəmiyyətini daha da artırmışdır. Bu baxımdan, informasiyanın qorunması və onun əlavə olunmamış, özgə tərəflərə çatmayan formada saxlanması informasiya təhlükəsizliyinin əsas predmetidir (Stallings,

Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0)

2017, s.24). Rəqəmsal məlumatların istifadə sahələri artdıqca, bu informasiyanı qorumaq üçün yeni metodlara və texnologiyalara ehtiyac duyulur.

Klassik fiziki təhlükəsizlik münasibətlərinin yerini virtual qoruma sistemləri tutur. Artıq korporativ sistemlər, müəssisələr, banklar, tibb və hüquq müdafiə sistemləri kimi mühüm sahələrdə informasiya təhlükəsizliyi əsas prioritetdir (Andress, 2014, s. 9).

İnformasiya təhlükəsizliyi anlayışı:

İnformasiya təhlükəsizliyi (IT) - verilənlərin icazəsiz əlçatanlığından, dəyişdirilməsindən və ya silinməsindən qorunmasını təmin edir (Shhitman, Mattord, 2011, s.38). Beynəlxalq standartlara (məs. ISO/IEC 27001) əsasən, bu sahənin idarə olunması təşkilati siyasətlər, texniki alətlər və prosedurlar vasitəsilə reallaşır.

CIA Triadası:

- Məxfilik (Confidentiality) – məlumatın yalnız icazəli şəxslər tərəfindən görülməsi;
- Bütövlük (Integrity) – verilənlərin icazəsiz dəyişdirilməsinin qarşısını almaq;
- Əlçatanlıq (Availability) – informasiyanın zəruri vaxtda istifadəyə hazır olması (Peltier, 2016, s.45).

Təhdid növləri:

- Zərərli proqramlar (viruslar, trojanlar)
- Fiçinq və sosial mühəndislik
- Xakerlik əməliyyatları
- Ransomware hücumları
- Sistem çökmələri və DDoS hücumları (Cole, 2020, s. 101-102).

Tədqiqat

İnformasiya təhlükəsizliyinin təmin olunması üçün müxtəlif şifrələmə metodları istifadə olunur. Bu tədqiqatda, simmetrik və asimmetrik şifrələmə metodlarının, blokçeyn və kvant kriptoqrafiyasının təhlükəsizlik baxımından effektivliyi təhlil edilmişdir. Məqsəd, bu metodların necə işlədiyini, hansı təhlükəsizlik risklərini aradan qaldırdığını və hansı sahələrdə daha effektiv olduğunu araşdırmaqdır.

Tədqiqatın məqsədi:

- Şifrələmə metodlarının təhlükəsizlik təminatını necə artırdığına dair ümumi qiymətləndirmə aparmaq.
- Hər bir şifrələmə metodunun zəif və güclü tərəflərini müəyyən etmək.
- Hər bir texnologiyanın real həyatda hansı vəziyyətlərdə daha uyğun olduğunu analiz etmək.

Ənənəvi metodlar. Sezar, Atbash, Vigenere kimi klassik şifrələmə texnikaları tarix boyu gizli məlumatları qorumaq üçün istifadə olunmuşdur (Kahn, 1996, s. 87). Müasir texnologiyalar bu metodları asanlıqla qırır, buna görə də daha kompleks sistemlər yaradılıb.

Simmetrik şifrələmə. AES (Advanced Encryption Standard) bu kateqoriyada ən çox tətbiq olunan sistemdir. Bu sistem sürətli emal imkanları və yüksək təhlükəsizlik dərəcəsinə malikdir (Daemen, Rijmen, 2002, s. 50).

Asimmetrik şifrələmə. RSA, ECC kimi texnologiyalar informasiya mübadiləsində məxfi açarların paylanmasında çox effektivdir (Diffie, Hellman, 1976, s.663). Məsələn, PGP texnologiyası bu prinsipə əsaslanır (Zimmermann, 1995, s.18).

Hash funksiyaları. SHA-256 kriptoqrafik hash funksiyası blokçeyn texnologiyalarında əsas rol oynayır. Bu, əlavə olaraq parol qorunması, sənəd təsdiqi və s. üsullarda da istifadə olunur (Eastlake, Jones, 2001).

Kriptoanaliz. Kodların qırılmasını təhlil edən sahədir. Brute Force, Dictionary Attack və Side-channel attack kimi metodlar istinad edilən təhdid metodlarındandır (Schneier, 1996, s.314).

Müasir texnologiyalar və tətbiqlər. Blokçeyn. Blokçeyn texnologiyası mühasibat, maliyyə, rəqəmsal identifikasiya kimi sahələrdə inqilabi rola malikdir. Hər bir blok hash kodla təsdiq edilir və bu dəyişdirilməni mümkünsüz edir (Nakamoto, 2008, s.3).

Ucdan-uca şifrələmə. Signal, WhatsApp, Telegram kimi mesajlaşma sistemləri tərəflər arasında məlumatı şifrələyir ki, arada olan tərəflər (serverlər də daxil olmaqla) bu məlumatı oxuya bilməsin (Marlinspike, 2013, s.2).

Kəmiyyət (quantum) kriptoqrafiyası. Quantum mexanikasının prinsiplərinə əsaslanan bu yanaşma, kənardan gözlənilmə halları da daxil olmaqla, maksimum təhlükəsizlik təmin edir (Bennett ,Brassard, 1984, s.175).

Təhlil və müqayisə. Kodlaşdırma texnologiyalarını effektivlik, performans, məxfilik və istifadə rahatlığı baxımından müqayisə etdikdə, ən ideal yanaşma bu texnikaların hibrid formada istifadəsidir (Menezes, 1996, s.215-218). Məsələn, SSL/TLS protokolları simmetrik şifrələmənin sürətini asimmetrik metodlarla birləşdirir (Tripathi, Singh, Antonio, Jara, s. 287-292).

Nəticə

Kodlaşdırma və şifrələmə üsullarının təhlili göstərir ki, informasiya təhlükəsizliyinin təminində bu texnologiyalar həlledici əhəmiyyət daşıyır. Ənənəvi şifrələmə metodlarından tutmuş blokçeyn və kvant kriptoqrafiyası kimi yeni texnologiyalara qədər geniş spektrdə həll yolları mövcuddur. İnformasiyanın qorunması təkcə texniki məsələ deyil, həm də hüquqi, sosial və təşkilati aspektləri əhatə edən kompleks bir problemdir (Shhitman, Mattord, 2011, s. 95).

Məlumatların oğurlanması və ya zərərli müdaxilələr yalnız fərdi deyil, korporativ və milli təhlükəsizlik üçün də ciddi risk yaradır. Bu səbəbdən, təhlükəsizliyin təmin edilməsi üçün yalnız texnologiyaya deyil, həm də insan resurslarına, idarəetmə modellərinə və hüquqi tənzimləmələrə kompleks yanaşmaq vacibdir (Peltier, 2016, s. 112).

Təkliflər:

- Qanunvericilik çərçivəsinin gücləndirilməsi: Rəqəmsal məlumatların qorunması ilə bağlı milli qanunvericilik beynəlxalq standartlara uyğun şəkildə inkişaf etdirilməlidir (Tipton, Krause, 2007, s. 53).
- Məxfi məlumatların təbəqələşdirilməsi: Təşkilatlar informasiyanı əhəmiyyətinə görə dərəcələndirməli və uyğun qoruma mexanizmləri seçməlidirlər (Andress, 2014, s. 63).
- Kadr potensialının artırılması: İnformasiya təhlükəsizliyi mütəxəssislərinin hazırlanması üçün universitetlərdə müvafiq ixtisaslar artırılmalı, dövlət və özəl qurumlar bu sahəyə investisiya qoymalıdır (Stallings, 2017, s. 307).
- Mütəmadi təhlükəsizlik auditi:Təşkilatlarda dövri şəkildə kibertəhlükəsizlik auditi həyata keçirilməli, zəif cəhətlər aşkarlanmalı və dərhal tədbirlər görülməlidir (Shhitman, Mattord, 2011, s.221).
- Maarifləndirmə kampaniyaları: İstifadəçilər üçün məlumat təhlükəsizliyi ilə bağlı təlimlər keçirilməli və fərdi səviyyədə şüurluluq artırılmalıdır. Statistikalar göstərir ki, məlumat sızmalarının əksəriyyəti insan səhvlərindən qaynaqlanır (Cole, 2020, s.141).
- Texnoloji yeniliklərin tətbiqi: Kəmiyyət kriptoqrafiyası, süni intellekt əsaslı təhlil sistemləri və avtomatlaşdırılmış təhlükəsizlik platformaları mərhələli şəkildə tətbiq olunmalıdır (Bennett, Brassard, 1984, s.176).
- Təhlükəsizlik siyasətləri və cavab mexanizmləri: Təşkilatlar üçün insidentlərə cavab planı (incident response plan) hazırlanmalı və test edilməlidir. Bu planlar mümkün hücumlara operativ cavab verməyə və informasiya sızmalarının qarşısını almağa imkan verir (Peltier, 2016, s.121).
- Hibrid şifrələmə texnikalarının geniş tətbiqi: Simmetrik və asimmetrik üsulların birləşdirildiyi sistemlər həm təhlükəsizlik, həm də performans baxımından optimal nəticələr verir (Tripathi, Singh, Antonio, 2017. s.290-291).

Bu tədbirlərin həyata keçirilməsi rəqəmsal mühitdə fəaliyyət göstərən bütün iştirakçılar üçün təhlükəsiz və etibarlı informasiya ekosistemi yaradacaqdır.

Ədəbiyyat

1. Andress, J. (2014). *The Basics of Information Security*. Syngress.
2. Bennett, C.H., Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*.
3. Cole, E., Krutz, R.L., Conley, J.Sh. (2020). *Network Security Bible*. Shiley.

4. Daemen, J., Rijmen, V. (2002). *The Design of Rijndael: AES – The Advanced Encryption Standard*. Springer.
5. Diffie, Sh., Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*.
6. Eastlake, D., Jones, P. (2001). *US Secure Hash Algorithm 1 (SHA1)*, RFC 3174.
7. Kahn, D. (1996). *The Codebreakers*. Scribner.
8. Marlinspike, M. (2013). *Signal Protocol Documentation*. Open Whisper Systems.
9. Menezes, A.J., Van, P.C., Vanstone, S.A. (1996). *Handbook of Applied Cryptography*. CRC Press.
10. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
11. Peltier, T.R. (2016). *Information Security Policies, Procedures, and Standards*. Auerbach.
12. Schneier, B. (1996). *Applied Cryptography*. Shiley.
13. Stallings, Sh. (2017). *Cryptography and Network Security*. Pearson.
14. Shhitman, M.E., Mattord, H.J. (2011). *Principles of Information Security*. Cengage Learning.
15. Tripathi, G., Singh, D., Antonio, J. (2017). A Comparative Study of Encryption Algorithms for Secure Data Communication in Smart Cities. *International Journal of Distributed Sensor Networks*, pp. 287-292.
16. Tipton, H.F., Krause, M. (2007). *Information Security Management Handbook*. Auerbach
17. Zimmermann, P. (1995). *The Official PGP User's Guide*. MIT.

Daxil oldu: 09.02.2025
Qəbul edildi: 14.05.2025