UOT: 004.056**; JEL:** L86; O33

Simarə Ramazan qızı ƏHMƏDOVA
Azərbaycan Respublikasının Prezidenti yanında
Dövlət İdarəşilik Akademiyası, magistr
simareehmedova533@gmail.com

Pərviz Əhməd oğlu QURBANOV
Azərbaycan Respublikasının Prezidenti yanında
Dövlət İdarəşilik Akademiyası
“Dövlət idarəçiliyində informasiya texnologiyaları”
kafedrasının dosenti
İqdisad üzrə fəlsəfə doktoru
E-mail: parviz.gurban@gmail.com
https://doi.org/10.30546/4.71.73001.2025.002.0176

İNFORMASİYA MÜDAFİƏSİ TEXNOLOGİYASI

Xülasə

Tədqiqatın məqsədi – informasiya müdafiəsi texnologiyalarının (IMT) inkişaf perspektivlərini araşdırmaq, mövcud problemləri müəyyənləşdirmək və süni intellekt (AI), maşın öyrənməsi (MÖ) və blokçeyn texnologiyalarının kibertəhlükəsizlik sahəsində potensial tətbiqlərini qiymətləndirməkdir.

Tədqiqatın metodologiyası – Tədqiqatda analiz, sintez, müqayisə və ümumiləşdirmə metodlarından istifadə olunmuşdur. Eyni zamanda, IMT sahəsindəki mövcud elmi ədəbiyyatlar və praktik tədqiqatlar araşdırılaraq müqayisəli təhlillər aparılmışdır.

Tədqiqatın tətbiqi əhəmiyyəti – tədqiqatın nəticələri informasiya təhlükəsizliyi sahəsində fəaliyyət göstərən mütəxəssislər, dövlət qurumları və özəl şirkətlər üçün faydalı ola bilər. Xüsusilə, süni intellekt və maşın öyrənməsi əsaslı təhlükəsizlik tədbirlərinin tətbiqi ilə bağlı yeni yanaşmalar təqdim edilir.

Tədqiqatın nəticələri – Araşdırmanın nəticələrinə əsasən, mövcud IMT metodları bəzi kibertəhlükələrə qarşı qeyri-kafi qala bilər. Süni intellekt və maşın öyrənməsi əsaslı sistemlərin təhlükəsizlik sahəsində effektivliyi göstərilmiş və blokçeyn texnologiyasının informasiya təhlükəsizliyi üçün potensial istifadəsi təhlil edilmişdir.

Tədqiqatın orijinallığı və elmi yeniliyi – tədqiqat IMT sahəsində süni intellekt və blokçeyn texnologiyalarının gələcək tətbiq perspektivlərini sistemli şəkildə araşdıran məqalələrdən biridir. Yeni texnologiyaların kibertəhlükəsizliyə inteqrasiyası və onların effektivliyi ilə bağlı elmi əsaslandırmalar təqdim edilmişdir.

Açar sözlər: İnformasiya müdafiəsi texnologiyası, kibertəhlükəsizlik, məlumat sızıntıları, süni intellekt, kvant şifrələmə, texnoloji irəliləyişlər, potensial təhlükələr.

Giriş

Müasir dövrdə informasiya təhlükəsizliyi hər bir təşkilatın və müəssisənin fəaliyyətinin ayrılmaz hissəsinə çevrilmişdir. İnformasiyanın qorunması müəssisələr üçün təkcə texniki deyil, eyni zamanda hüquqi, maliyyə və təşkilati aspektləri əhatə edən vacib bir sahədir. Məlumat sızıntıları, kibertəhlükələr və digər risklər təşkilatların etibarlılığına, maliyyə göstəricilərinə və iş proseslərinin davamlılığına ciddi təsir edə bilər. Bu baxımdan, informasiya müdafiəsi müəssisələrin uğurlu və dayanıqlı fəaliyyət göstərməsi üçün vacib elementlərdən biridir.

İlk növbədə, informasiya təhlükəsizliyinin əsas istiqamətlərindən biri məlumatların təhlükəsizliyi və qorunmasıdır. Müasir texnologiyaların inkişafı və internetin geniş yayılması nəticəsində məlumatların icazəsiz əldə edilməsi və oğurlanması riski əhəmiyyətli dərəcədə artmışdır. İnformasiya müdafiəsi bu məlumatların gizliliyini qorumaq üçün mühüm rol oynayır. Şəxsi məlumatların

qorunması isə xüsusi qanunvericilik çərçivəsində tənzimlənir. Məsələn, GDPR kimi beynəlxalq tənzimləmələr istifadəçilərin şəxsi məlumatlarının təhlükəsiz saxlanılmasını və icazəsiz istifadəsinin qarşısının alınmasını tələb edir [7].

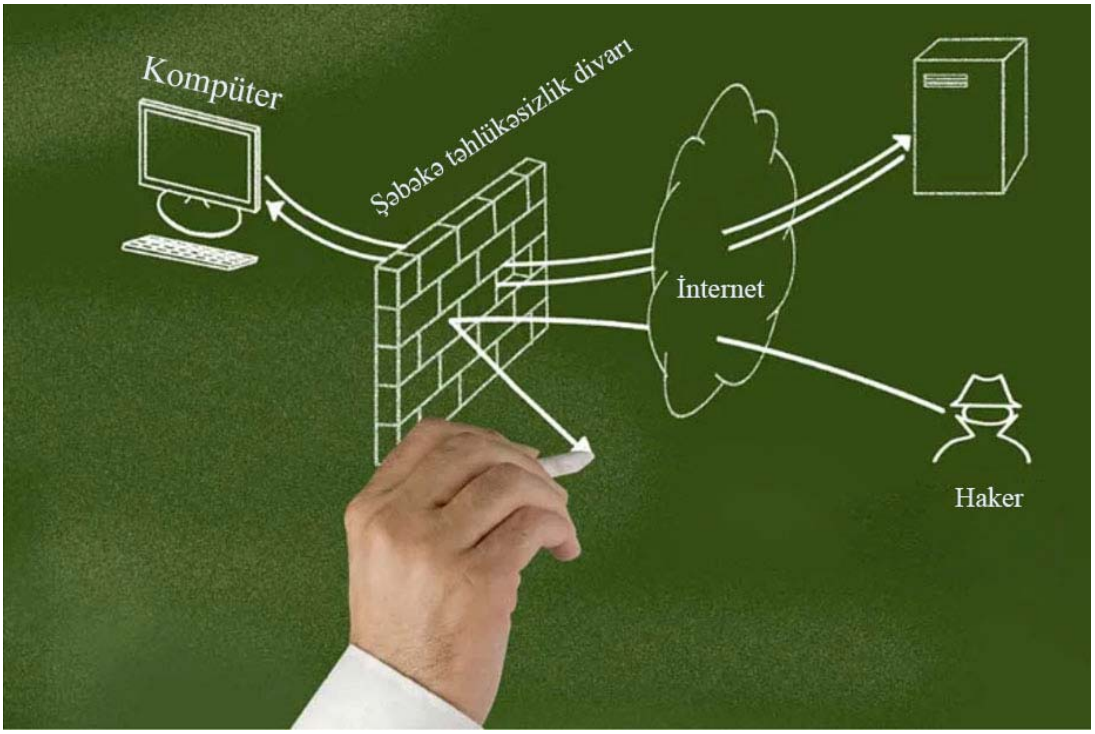
Digər mühüm aspekt müəssisələrin etibarlılığı və reputasiyasıdır. Güclü informasiya təhlükəsizliyi siyasəti tətbiq edən təşkilatlar müştərilər və tərəfdaşlar arasında etibarlılığını artırır. Məlumatların qorunmasına dair ciddi tədbirlər gördükləri bilinərsə, bu, şirkətə olan inamı yüksəldir və müştəri bazasının genişlənməsinə kömək edir [7]. Əksinə, məlumat sızıntıları və kibertəhlükələr təşkilatların nüfuzuna ciddi zərər vura bilər. Bu səbəbdən təhlükəsizlik tədbirlərinin düzgün planlaşdırılması və tətbiqi reputasiya risklərinin azalmasına töhfə verir.

İnformasiya təhlükəsizliyi həmçinin maliyyə və hüquqi risklərin idarə edilməsində mühüm rol oynayır. Kibertəhlükəsizlik hadisələri müəssisələr üçün böyük maliyyə itkilərinə səbəb ola bilər. Məlumat itkisi, sistemlərin fəaliyyətinin dayanması və bərpa işləri ciddi xərclər tələb edir. Güclü təhlükəsizlik tədbirləri bu kimi maliyyə zərərlərinin qarşısını almağa kömək edir [7]. Bundan əlavə, təhlükəsizlik pozuntuları hüquqi məsuliyyət yarada bilər. Təşkilatlar informasiya təhlükəsizliyi standartlarına əməl etmədikdə, hüquqi tənzimləyicilər tərəfindən cəzalandırıla bilərlər. Hüquqi təhlükələrin qarşısını almaq üçün təhlükəsizlik tələblərinə tam əməl olunmalı və beynəlxalq standartlara uyğun strategiyalar hazırlanmalıdır.

İş mühitində informasiya təhlükəsizliyi həm də iş proseslərinin davamlılığı və əməyin məhsuldarlığı üçün vacibdir. Məlumatların qorunması müəssisənin fəaliyyətinin fasiləsiz davam etməsinə imkan yaradır. Güclü təhlükəsizlik tədbirləri məlumat itkisi, kiberhücumlar və sistem xətalarının qarşısını almaqla iş proseslərinin sabitliyini təmin edir. Eyni zamanda, işçilərin təhlükəsiz mühitdə çalışması onların məhsuldarlığını artırır və daha rahat işləmələrinə şərait yaradır [7]. Müasir texnologiyaların inkişafı ilə texnoloji invaziyalara qarşı mübarizə də vacib məsələyə çevrilmişdir. Süni intellekt və kvant kompüterləri kimi yeni texnologiyalar kibertəhlükəsizlik sahəsinə ciddi təsir göstərir. Bu texnologiyalar mövcud təhlükəsizlik sistemlərinin sınaqdan keçirilməsinə və yeni təhlükəsizlik standartlarının yaradılmasına ehtiyac yaradır. İnformasiyanın qorunmasını təmin etmək üçün intensiv təhlükəsizlik tədbirləri bu yeni risklərə qarşı tətbiq edilməlidir.Bununla yanaşı, informasiya təhlükəsizliyində məlumatların idarə edilməsi və paylaşılması da mühüm əhəmiyyət daşıyır. Effektiv idarəetmə sistemləri müəssisələrin müştərilər və tərəfdaşlarla daha təhlükəsiz əlaqə saxlamasına kömək edir. Təşkilatlar öz məlumatlarını yalnız səlahiyyətli şəxslərlə paylaşmalı və icazəsiz girişlərin qarşısını almaq üçün ciddi təhlükəsizlik protokollarını tətbiq etməlidirlər.İnformasiya təhlükəsizliyinin təmin edilməsində kibertəhlükəsizlik mədəniyyətinin formalaşdırılması vacib rol oynayır. Bu istiqamətdə təşkilatlar daxilində təhlükəsizlik təlimləri və maarifləndirmə proqramları həyata keçirilməlidir. İşçilərin kibertəhlükələr və təhlükəsizlik tədbirləri haqqında məlumatlandırılması onların daha diqqətli olmasına və potensial təhlükələrə qarşı daha hazırlıqlı olmasına şərait yaradır. Bundan əlavə, təhlükəsizlik sahəsində beynəlxalq və yerli standartların tətbiqi təşkilat daxilində təhlükəsizlik mədəniyyətinin möhkəmlənməsinə kömək edir. Bütün bu amillər nəzərə alındıqda, informasiya müdafiəsi müasir dövrdə müəssisələrin uğurla fəaliyyət göstərməsi üçün əvəzolunmaz elementdir. Bu sahədə güclü və etibarlı təhlükəsizlik tədbirlərinin tətbiqi həm texniki, həm də təşkilati aspektlərdə uzunmüddətli faydalar təmin edir. Məlumatların qorunması strategiyalarının davamlı olaraq yenilənməsi və təkmilləşdirilməsi informasiya təhlükəsizliyi sahəsində səmərəli nəticələr əldə etməyə imkan yaradır. Güclü informasiya təhlükəsizliyi tədbirləri yalnız məlumatların qorunmasını deyil, həm də müəssisələrin gələcək uğurunu və dayanıqlılığını təmin edir.

İnformasiya təhlükəsizliyində çətinliklər və təhlükələr

Müasir dövrdə informasiya təhlükəsizliyinin təmin edilməsi getdikcə daha mürəkkəb və çətin bir prosesə çevrilir. Texnologiyaların inkişafı ilə yanaşı, kibertəhlükələr və məlumat sızmalarının miqyası da artır. Yeni hücum üsulları və zəifliklər ortaya çıxır və bu vəziyyət təşkilatları daha effektiv təhlükəsizlik strategiyaları tətbiq etməyə məcbur edir. İnformasiya təhlükəsizliyində mövcud olan əsas çətinliklər və təhlükələr müxtəlif aspektlərdən təhlil edilə bilər.



Şəkil 1. İnformasiya təhlükəsizliyi

İlk növbədə, kibertəhlükələr informasiya təhlükəsizliyinin ən geniş yayılmış problemlərindən biridir. Kibertəhlükələr əsasən sistemlərə və məlumat bazalarına hücum edərək, onları zədələmək və ya məhv etmək məqsədi güdür. Bu təhlükələrin ən çox rast gəlinən növlərindən biri zərərli proqramlardır (malware). Bunlara viruslar, Troya atları və kəlbətinlər (worms) daxildir. Bu cür proqram təminatları istifadəçilərin məlumatlarını oğurlaya, sistemləri sıradan çıxara və ya şifrələyə bilər. Fidyə hücumları (ransomware) isə məlumatların şifrələnərək istifadəçidən fidyə tələb edilməsi yolu ilə həyata keçirilir. Məsələn, WannaCry və CryptoLocker kimi fidyə proqramları ciddi təhlükələr yaradır [6].

Bundan əlavə, kibertəhlükəsizlik hücumları da geniş yayılmış təhdidlər sırasındadır. Məsələn, phishing hücumları saxta mesajlar vasitəsilə istifadəçiləri aldadaraq onların məxfi məlumatlarını ələ keçirməyə çalışır. Daha hədəfli və spesifik hücumlar olan spear-phishing metodları isə xüsusi olaraq müəyyən şəxslərə və təşkilatlara qarşı yönəldilir. DDoS (Distributed Denial of Service) hücumları isə sistemləri və şəbəkələri həddindən artıq yükləyərək onların fəaliyyətini dayandırmağa çalışır. Xüsusilə zero-day hücumları, yəni hələ aşkar edilməmiş və ya düzəldilməmiş təhlükəsizlik zəifliklərini hədəf alan hücumlar, ən təsirli və təhlükəli metodlardan biri hesab edilir [9].

Məlumat sızmaları da informasiya təhlükəsizliyinin əsas problemlərindən biridir. Bu, məxfi məlumatların icazəsiz şəxslər tərəfindən əldə olunması ilə bağlıdır və müxtəlif səbəblərlə baş verə bilər. Sosial mühəndislik üsulları insanların aldanaraq öz məxfi məlumatlarını açıqlaması ilə nəticələnir. Bu üsullar arasında phishing və pretexting (saxta pretekst vasitəsilə məlumat əldə edilməsi) geniş yayılıb. Digər mühüm təhlükə insider riskləridir. Şirkət daxilində çalışan şəxslər bəzən qəsdən və ya bilmədən məlumatların sızmasına səbəb ola bilirlər. Bu, işçilər, partnyorlar və ya digər əlaqəli şəxslər tərəfindən həyata keçirilə bilər [2].

Məlumat sızmalarına səbəb olan digər amil isə texnoloji zəifliklərdir. Köhnəlmiş və ya düzgün qorunmayan proqram təminatları və sistemlər bu cür sızıntılara gətirib çıxara bilər. Proqramların vaxtında yenilənməməsi və ya lazımi təhlükəsizlik tədbirlərinin görülməməsi kiberhücumçular üçün asan hədəf yaradır.

İnformasiya təhlükəsizliyində əhəmiyyətli rol oynayan digər amil isə infrastruktur zəifliklərdir. Buraya şəbəkə və fiziki təhlükəsizliklə bağlı problemlər daxildir. Şəbəkə hücumları, sistemlərdəki

zəifliklərdən istifadə edərək məlumatların ötürülməsinə müdaxilə etməyi hədəfləyir. Fiziki təhlükəsizlik problemləri isə server otaqlarına və ya digər kritik məlumat mərkəzlərinə icazəsiz girişin olması nəticəsində meydana çıxır. Sistemlərin təhlükəsiz saxlanmaması və fiziki girişlərin kifayət qədər nəzarət altında olmaması ciddi risklər yarada bilər.

Digər bir vacib məsələ isə məlumatın qorunması və idarə edilməsi problemləridir. Müəyyən təşkilatlarda məlumat idarəetmə siyasətinin olmaması və ya düzgün tətbiq edilməməsi ciddi təhlükəsizlik boşluqları yaradır. Qanunvericilik və tənzimləmə uyğunluğunun pozulması da məlumat təhlükəsizliyi üçün əsas problemlərdən biridir. Məsələn, GDPR və digər regional qanunlar məlumatların qorunmasına dair ciddi tələblər müəyyən edir. Bu qanunlara əməl edilmədiyi təqdirdə, təşkilatlar ciddi hüquqi və maliyyə cəzalarına məruz qala bilərlər [9].

İnformasiya təhlükəsizliyi sahəsində qarşıya çıxan yeni və mürəkkəb təhlükələrdən biri də yüksək texnoloji təhlükələrdir. Süni intellekt və maşın öyrənmə texnologiyaları kibertəhlükəsizlikdə yeni imkanlar yaratsa da, eyni zamanda kiberhücumçular üçün də yeni metodlar təqdim edir. Məsələn, süni intellektlə daha inkişaf etmiş phishing hücumları həyata keçirmək mümkündür. Bununla yanaşı, kvant kompüterlərinin inkişafı mövcud şifrələmə metodlarını köhnəldə bilər. Kvant texnologiyalarının gücü sayəsində bugünkü şifrələmə sistemlərinin bir çoxu gələcəkdə təhlükəsizliyini itirə bilər [5].

İnformasiya təhlükəsizliyində digər bir mühüm məsələ isə zəif proqram təminatı və tətbiqlərdir. Köhnəlmiş və ya kifayət qədər qorunmayan proqram təminatları məlumatların oğurlanmasına və sistemlərin sıradan çıxmasına səbəb ola bilər. Müasir dövrdə təşkilatlar üçün informasiya təhlükəsizliyinin təmin olunması yalnız texniki tədbirlərdən ibarət deyil, eyni zamanda sistemlərin daim yenilənməsini və optimallaşdırılmasını da tələb edir.

Bütün bu çətinliklər və təhlükələr nəzərə alınaraq, informasiya təhlükəsizliyi sahəsində müasir və innovativ tədbirlərin tətbiq edilməsi vacibdir. Təhlükəsizlik strategiyaları təkcə texnoloji deyil, həm də insan faktorunu nəzərə alaraq hazırlanmalıdır. Bunun üçün mütəmadi olaraq işçilər üçün təhlükəsizlik təlimləri keçirilməli, təhlükəsizlik protokolları gücləndirilməli və ən müasir texnologiyalar tətbiq edilməlidir. Ancaq bu halda kibertəhlükələrə qarşı effektiv müdafiə tədbirləri həyata keçirmək mümkün olacaqdır [8].



Şəkil 2. Kiber təhlükələr

İnformasiya müdafiəsi sahəsində əsas amillər

İnformasiya təhlükəsizliyinin ən vacib aspektlərindən biri məlumatların qorunmasını təmin etmək üçün istifadə edilən şifrələmə metodlarıdır. Şifrələmə, məlumatları yalnız səlahiyyətli şəxslər tərəfindən oxuna bilən hala gətirmək üçün istifadə edilən texnologiyadır. Müasir dövrdə informasiya təhlükəsizliyinin təmin olunması üçün müxtəlif şifrələmə metodlarından istifadə

olunur. Bu metodlar müxtəlif tətbiq sahələrinə uyğun olaraq fərqlənir və bir neçə əsas kateqoriyaya bölünür.

Simmetrik Şifrələmə

Simmetrik şifrələmə metodları şifrələmə və deşifrələmə üçün eyni açardan istifadə edir. Bu metod yüksək sürətli işləmə imkanına malikdir və böyük həcmli məlumatların qorunması üçün istifadə edilir. Ən geniş yayılmış simmetrik şifrələmə alqoritmlərindən biri AES (Advanced Encryption Standard) hesab olunur.

AES-in əsas xüsusiyyətləri onun 128, 192 və 256 bitlik açar uzunluqlarını dəstəkləməsi və yüksək təhlükəsizlik səviyyəsi təmin etməsidir. Bu şifrələmə metodu sürətli işləmə qabiliyyətinə və geniş istifadə sahəsinə malikdir. Eyni zamanda, ABŞ Milli Standartlar və Texnologiyalar İnstitutu (NIST) tərəfindən təsdiqlənmişdir və maliyyə, dövlət və texnoloji sektorlar da daxil olmaqla bir çox sahədə tətbiq edilir [1].

Simmetrik şifrələmə metodlarından biri də 3DES (Triple Data Encryption Standard) alqoritmidir. 3DES klassik DES (Data Encryption Standard) metodunun üçqat tətbiq olunmuş versiyasıdır və bu səbəbdən daha güclü təhlükəsizlik təmin edir. Lakin, AES ilə müqayisədə 3DES daha aşağı performansa malikdir, çünki məlumatlar üç dəfə şifrələnir və bu da daha çox hesablama gücü tələb edir. Buna görə bəzi müasir tətbiqlərdə 3DES artıq köhnəlmiş hesab olunur [1].

Asimmetrik Şifrələmə

Asimmetrik şifrələmə metodlarında məlumatların şifrələnməsi və deşifrələnməsi üçün iki fərqli açar istifadə olunur: ictimai açar (public key) və gizli açar (private key). Bu metodun əsas üstünlüyü odur ki, şifrələmə üçün istifadə edilən açar məlumatın deşifrələnməsi üçün istifadə edilmir. Asimmetrik şifrələmə xüsusilə məlumat mübadiləsi və rəqəmsal imzalar üçün geniş istifadə olunur.

Ən populyar asimmetrik şifrələmə metodlarından biri RSA (Rivest-Shamir-Adleman) alqoritmidir. RSA böyük ədədlərin faktorizasiyası prinsipi üzərində qurulmuşdur və bu, onun yüksək təhlükəsizlik səviyyəsini təmin edir. RSA metodu geniş istifadə olunsa da, uzun açar uzunluqları tələb etdiyinə görə bəzi tətbiqlərdə yavaş işləyə bilər [1].

Asimmetrik şifrələmənin başqa bir effektiv növü ECC (Elliptic Curve Cryptography) texnologiyasıdır. ECC eliptik əyrilər üzərində işləyən bir şifrələmə metodudur və daha qısa açarlardan istifadə etməklə RSA ilə müqayisədə daha güclü təhlükəsizlik təmin edə bilər. ECC-nin əsas üstünlüklərindən biri mobil və resurs məhdudiyyəti olan sistemlər üçün daha effektiv olmasıdır [1].

Hash Funksiyaları

Hash funksiyaları məlumatların sabit uzunluqda xülasəsini yaratmaq üçün istifadə olunur. Hash alqoritmləri əsasən məlumatların bütövlüyünü qorumaq və dəyişdirilmədiyini təsdiqləmək üçün tətbiq edilir.

Müasir hash alqoritmlərindən biri SHA-256 (Secure Hash Algorithm 256-bit) texnologiyasıdır. SHA-256 məlumatların 256-bitlik xülasəsini yaradır və yüksək təhlükəsizlik təmin edir. Bu alqoritm, xüsusilə blokçeyn texnologiyasında və rəqəmsal sertifikatların yaradılmasında geniş istifadə edilir [4].

Daha yeni və inkişaf etmiş hash funksiyası SHA-3 (Secure Hash Algorithm 3) isə SHA-2 alqoritminin davamı olaraq FIPS PUB 202 standartı ilə təsdiqlənmişdir. SHA-3 müasir təhlükəsizlik tələblərinə uyğunlaşdırılmış yeni nəsil hash funksiyasıdır və əlavə təhlükəsizlik xüsusiyyətləri təqdim edir [4].

Hibrid Şifrələmə

Hibrid şifrələmə metodları simmetrik və asimmetrik şifrələmə metodlarının kombinasiyasına əsaslanır. Bu yanaşma məlumat mübadiləsini daha sürətli və təhlükəsiz etmək üçün istifadə edilir.

Müasir internet təhlükəsizliyində TLS/SSL (Transport Layer Security / Secure Sockets Layer) protokolları hibrid şifrələmənin ən çox istifadə olunan nümunələrindən biridir. TLS və SSL veb brauzerlər və serverlər arasında təhlükəsiz əlaqəni təmin etmək üçün istifadə edilir. Bu protokollar

simmetrik, asimmetrik və hash metodlarını birləşdirərək məlumatların qorunmasını təmin edir [3].

Nəticə

İnformasiya təhlükəsizliyinin əsas təminatçılarından biri şifrələmə metodlarının effektiv istifadəsidir. Müasir dövrdə simmetrik şifrələmə (AES, 3DES), asimmetrik şifrələmə (RSA, ECC), hash funksiyaları (SHA-256, SHA-3) və hibrid şifrələmə metodları (TLS/SSL) kimi texnologiyalar geniş şəkildə tətbiq olunur. Hər bir metodun özünəməxsus üstünlükləri və çatışmazlıqları vardır.

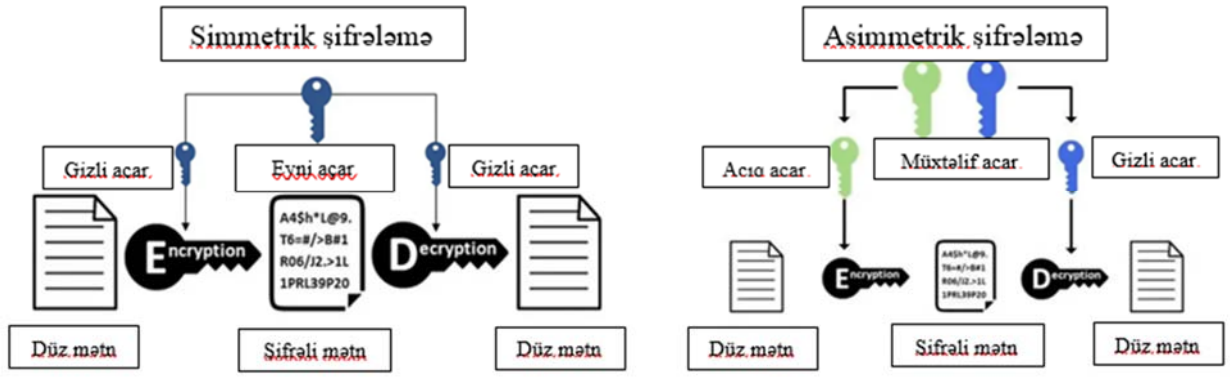
Simmetrik şifrələmə yüksək sürət və güclü təhlükəsizlik təmin etsə də, açarların təhlükəsiz idarə edilməsi problemi yaradır.

Asimmetrik şifrələmə daha yüksək təhlükəsizlik təqdim etsə də, performans baxımından daha çox resurs tələb edir.

Hash funksiyaları məlumatların bütövlüyünü qorumaq üçün istifadə olunur, lakin məlumatların məxfiliyini təmin etmir.

Hibrid şifrələmə metodları, xüsusilə TLS/SSL texnologiyaları, müxtəlif şifrələmə metodlarını birləşdirərək internet üzərindən məlumat mübadiləsini təhlükəsiz şəkildə həyata keçirməyə imkan yaradır.

Günümüzdə kibertəhlükələr və informasiya sızmaları artdıqca, şifrələmə metodları da inkişaf etdirilməli və daim yenilənməlidir. Bu texnologiyaların tətbiqi məlumat təhlükəsizliyini artırmaq, kibertəhlükələrin qarşısını almaq və məxfi informasiyanı qorumaq üçün vacib addımlardan biridir. Hər bir təşkilat və fərdi istifadəçi məlumatlarının təhlükəsizliyini qorumaq üçün ən müasir şifrələmə texnologiyalarından istifadə etməli və təhlükəsizlik siyasətlərini daim yeniləməlidir.



İnformasiya təhlükəsizliyi müasir dövrdə müəssisələrin və fərdi istifadəçilərin məlumatlarının qorunmasında kritik rol oynayır. Kibertəhlükələr, o cümlədən zərərli proqramlar, fidya hücumları və zero-day hücumları, məlumatların təhlükəsizliyini ciddi şəkildə təhdid edir. Məlumat sızmaları, sosial mühəndislik, insider təhlükələr və texnoloji zəifliklər məlumatların icazəsiz şəxslər tərəfindən əldə olunmasına səbəb olur. Müasir şifrələmə metodları, simmetrik (AES, 3DES) və asimmetrik (RSA, ECC) texnologiyalarla məlumatların qorunmasını təmin edir. Şifrələmə metodlarının effektivliyi məlumatların məxfiliyini və bütövlüyünü qoruyur, lakin hər metodun öz müsbət və mənfi tərəfləri vardır. Simmetrik şifrələmə sürətli və güclü təhlükəsizlik təmin etsə də, açar idarəetmə problemləri yarada bilər. Asimmetrik şifrələmə isə daha uzunmüddətli təhlükəsizlik təmin edir, amma daha yüksək hesablama gücü tələb edir. Hash funksiyaları məlumatların bütövlüyünü təsdiqləyir, lakin məlumatların gizliliyini təmin etmir. Hibrid şifrələmə metodları, məsələn, TLS/SSL, müxtəlif təhlükəsizlik texnologiyalarını birləşdirərək geniş miqyaslı mühafizə təmin edir. Təhlükəsizlik tədbirləri daim yenilənməli və inkişaf etdirilməlidir, çünki kibertəhlükələr və texnologiyalar sürətlə dəyişir. İnsider təhlükələr və texnoloji zəifliklər, müvafiq təhlükəsizlik tədbirləri olmadan ciddi risklər yarada bilər. Eyni zamanda, hüquqi və tənzimləyici tələblərə

uyğunluq məlumatların qorunması üçün əsasdır. Məlumatların qorunması yalnız texnologiya ilə deyil, həm də insan faktoruyla bağlıdır. Təhlükəsizlik mədəniyyətinin formalaşdırılması, müntəzəm təlimlər və təhlükəsizlik siyasətləri müvəffəqiyyətli məlumat qorunması üçün vacibdir. Müasir təhlükəsizlik texnologiyalarının effektivliyi məlumatların qorunmasını daha təhlükəsiz və etibarlı edir. Yenilikçi şifrələmə metodlarının tətbiqi məlumatların mühafizəsini daha da gücləndirir. Təhlükəsizlik sahəsindəki inkişaflar, həmçinin yeni risklər və çətinliklər ilə mübarizəyə kömək edir. Məlumat təhlükəsizliyini təmin etmək həm fərdi istifadəçilər, həm də müəssisələr üçün davamlı bir prosesdir.

ƏDƏBİYYAT

1. https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking
2. National Institute of Standards and Technology (NIST). (2022). Framework for Improving Critical Infrastructure Cybersecurity. NIST. https://www.nist.gov/cyberframework
3. Əliquliyev R.M., İmamverdiyev Y.N.. Kriptoqrafiyanın əsasları, Bakı 2006, səh 71-72.
4. Uma Dixit.Cryptography — Security in E-Banking. IOSR Journal of Business and Management (IOSR-JBM).
5. Gartner, Inc. (2023). Hype Cycle for Cybersecurity, 2023. Gartner
6. https://www.linkedin.com/advice/3/how-can-you-secure-financial-transactions#how-does-cryptography-secure-financial-transactions
7. Chen, T., & Liu, J. (2018). Cybersecurity and Privacy: A Survey on Recent Advances and Emerging Challenges. İn: Proceedings of the IEEE International Conference on Computer Communications, 1-8. IEEE.
8. https://www.devglan.com/online-tools/text-encryption-decryption
9. https://openvpn.net/solutions/industries/finance/

Симара Рамазан Ахмедова
simareehmedova533@gmail.com

Пярвиз Ахмед Курбанов
Доцент кафедры «Информационные технологии в государственном управлении»
Академия государственного управления при Президенте Азербайджанской Республики
Доктор философии по экономике
E-mail: parviz.gurban@gmail.com

Технология защиты информации

Резюме

Цель исследования:Цель данного исследования – изучить перспективы развития технологий защиты информации (ТЗИ), определить существующие проблемы и оценить потенциальные применения искусственного интеллекта (ИИ), машинного обучения (МО) и технологии блокчейн в области кибербезопасности.

Методология исследования:В исследовании использованы методы анализа, синтеза, сравнения и обобщения. Кроме того, был проведен сравнительный анализ существующей научной литературы и практических исследований в области ТЗИ.

Практическая значимость исследования:Результаты данного исследования могут быть полезны специалистам в области информационной безопасности, государственным учреждениям и частным компаниям. В частности, представлены новые подходы к

внедрению мер безопасности на основе ИИ и МО.

Результаты исследования:Результаты исследования показывают, что существующие методы ТЗИ могут оказаться недостаточными против некоторых киберугроз. Продемонстрирована эффективность систем на основе ИИ и МО в сфере кибербезопасности, а также проанализировано потенциальное использование технологии блокчейн для защиты информации.

Оригинальность и научная новизна исследования:Данное исследование является одним из немногих системных анализов, изучающих перспективы применения ИИ и блокчейн-технологий в сфере ТЗИ. Представлены научные обоснования интеграции новых технологий в кибербезопасность и их эффективности.

Ключевые слова: Технологии защиты информации, кибербезопасность, утечки данных, искусственный интеллект, квантовое шифрование, технологические достижения, потенциальные угрозы.

Simara Ramazan Ahmadova
simareehmedova533@gmail.com

Pərviz Ahmad Qurbanov
Associate Professor at the Department of "
Information Technologies in Public Administration"
Academy of Public Administration under the
President of the Republic of Azerbaijan
Doctor of Philosophy in Economic
E-mail: parviz.gurban@gmail.com

Information Protection Technolog

Summary

Research Objective: The aim of this research is to explore the development prospects of information protection technologies (IPT), identify existing challenges, and evaluate the potential applications of artificial intelligence (AI), machine learning (ML), and blockchain technologies in the field of cybersecurity.

Research Methodology: The study employs analysis, synthesis, comparison, and generalization methods. Additionally, existing scientific literature and practical studies in the field of IPT have been examined to conduct comparative analyses.

Practical Significance of the Research:The findings of this research may be beneficial for specialists in information security, government agencies, and private companies. In particular, new approaches to the implementation of AI- and ML-based security measures are introduced.

Research Findings:The results of the study indicate that existing IPT methods may be insufficient against certain cyber threats. The effectiveness of AI- and ML-based systems in the field of cybersecurity has been demonstrated, and the potential use of blockchain technology for information security has been analyzed.

Originality and Scientific Novelty of the Research:This study is one of the few systematic analyses exploring the future applications of AI and blockchain technologies in the IPT field. Scientific justifications have been provided regarding the integration of new technologies into cybersecurity and their effectiveness.

Keywords: Information protection technology, cybersecurity, data leaks, artificial intelligence, quantum encryption, technological advancements, potential threats.