




# PROCEEDINGS

**II International Conference on**

## INFORMATION SECURITY: PROBLEMS AND PROSPECTS

**November 25, 2022**

**BAKU | AZERBAIJAN**

## CONFERENCE CHAIRS

**Saadat Aliyeva,** Rector, Azerbaijan University, Azerbaijan
**Igor Ruban,** Acting Rector, Kharkov National University of Radioelectronics, Ukraine
**Fuzuli Salahov**, Rector, Military Institute named after H.A. Aliyev

## ORGANIZING COMMITTEE

**Yusif Gasimov** (co-chair), Azerbaijan University, Azerbaijan
**Murad Omorov** (co-chair), Kharkiv National University of Radioelectronics, Ukraine

**Ali Abbasov**, Institute of Control Systems, ANAS
**Ramiz Alguliyev**, Institute of Information Technologies, ANAS
**Ivan Antipov**, Kharkov National University of Radioelectronics, Ukraine
**Carlo Cattani,** University of Tuscia, Italy
**Arzu Guliyev**, Azerbaijan State Pedagogical University, Azerbaijan
**Latifa Agamaliyeva**, Azerbaijan University
**Yuriy Lykov**, Kharkov National University of Radioelectronics, Ukraine
**Urfat Nuriyev**, Ege University, Turkiye
**Sharif Guseynov**, University of Liepaja, Latvia
**Denis Gorelov**, Kharkov National University of Radioelectronics, Ukraine
**Anvar Hazarkhanov**, Military Institute named after H.A. Aliyev, Azerbaijan
**Alakbar Aliyev**, Baku State University, Azerbaijan
**Gennadi Khalimov**, Kharkov National University of Radioelectronics, Ukraine
**Elvin Azizbayov**, Academy of Public Administration under the President of the Republic of Azerbaijan
**Victor Ruzhentsev**, Kharkov National University of Radioelectronics, Ukraine
**Abzeddin Adamov**, ADA University, Azerbaijan
**Alexander Severinov**, Kharkov National University of Radioelectronics, Ukraine
**Kamaləddin Ramazanov**, National Aviation Academy, Azerbaijan
**Yevgeniy Kotukh**, Kharkov National University of Radioelectronics, Ukraine
**Marina Yevdekimenko**, Kharkov National University of Radioelectronics, Ukraine
**Ramid Huseynov**, Military Institute named after H.A. Aliyev, Azerbaijan
**Asif Pashayev,** Azerbaijan University, Azerbaijan
**Tamara Radivilova**, Kharkov National University of Radioelectronics, Ukraine
**Yadigar Imamverdiyev**, Azerbaijan Technical University, Azerbaijan
**Aleksander Fedushin**, Kharkov National University of Radioelectronics, Ukraine
**Etibar Seyidzadeh**, Baku Engineering University, Azerbaijan
**Alexsander Lemeshko**, Kharkov National University of Radioelectronics, Ukraine
**Vagif Gasimov**, Azerbaijan Technical University, Azerbaijan
**Anatoly Oleynikov**, Kharkov National University of Radioelectronics, Ukraine
**Bahram Azizov**, Azerbaijan University, Azerbaijan
**Olexsandra Yeremenko**, Kharkov National University of Radioelectronics, Ukraine

## CONTENTS

# PLENARY TALKS

## CYBER SECURITY EDUCATION: CHALLENGES AND PROSPECTS

**Murad Omarov, Maryna Yevdokymenko**
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
e-mail: murad.omarov@nure.ua, marina.ievdokymenko@nure.ua

Today there is a rapid growth of cyber attacks. For example, between 2020 and the second quarter of 2022, there were over 600 million attacks [1], and according to McAfee and CSIS [2, 3], global damage from hacking attacks, including malware, password, phishing, DDoS, SQL injection attacks, etc., exceeded $600 billion per year. That is why the development of cybersecurity, especially in the context of accelerated global digitalization, is of vital importance for every state, business and individual.

For example, the EU is developing a set of European cybersecurity standards aimed at deterring and responding to cyber attacks that pose an external threat to the EU and its partner states. The European Cyber Security Organization (ECSO) and the European Union Cyber Security Agency (ENISA) are leading organizations providing security best practices to businesses, companies and individuals. Today, Europe has many regulations and directives [4-6] aimed at enhancing the cyber resilience of the Union and its member states to multifaceted and ever-changing hybrid threats, as well as increasing cooperation on detecting, preventing and countering them. The European Union works with Ukraine as an eastern neighbor to promote peace, stability and economic prosperity throughout the region.

Ukraine's main cyber security priorities are the creation of a secure cyberspace, protection of the rights, freedoms and legitimate interests of Ukrainians in cyberspace, as well as European and Euro-Atlantic integration in the sphere of cyber security. Thus, on August 26, 2021, the Cyber Security Strategy of Ukraine was approved, which is based on the provisions of the Constitution of Ukraine, the laws of Ukraine "On National Security of Ukraine" and "On the Basic Principles of Cyber Security of Ukraine," the Convention for the Protection of Human Rights and Fundamental Freedoms, the Convention on Cybercrime, the National Security Strategy of Ukraine [7-9].

The priorities of cybersecurity of Ukraine are:

- strengthening the national cybersecurity system to neutralize intelligence on the Internet, armed aggression against Ukraine in cyberspace, minimizing the threats of cybercrime and cyberterrorism;

- rapid adaptation to internal and external threats in cyberspace, maintain cyber security of critical information infrastructure facilities;

- organization of European and Euro-Atlantic integration in the sphere of cyber security

At the same time, the main constraint on the implementation of the Cyber Security Strategy to create a secure cyberspace is an acute shortage of specialists in this field. Indeed, today most private

companies and government agencies are experiencing a shortage of information security personnel: enterprises lack or have no management level specialists or engineers who can administer security tools or ensure the operation of Security Operation Centers (SOC).

In this regard, universities face an important and difficult task – to provide qualified specialists for the needs of the labor market. The challenge is the need to constantly update curricula and disciplines to keep up with new technologies and emerging attacks. In this regard, after analyzing the best practices of universities [10–12] that are among the top 100 in the world, the main directions of university development for the quality training of future cybersecurity specialists were formulated as shown in figure 1.

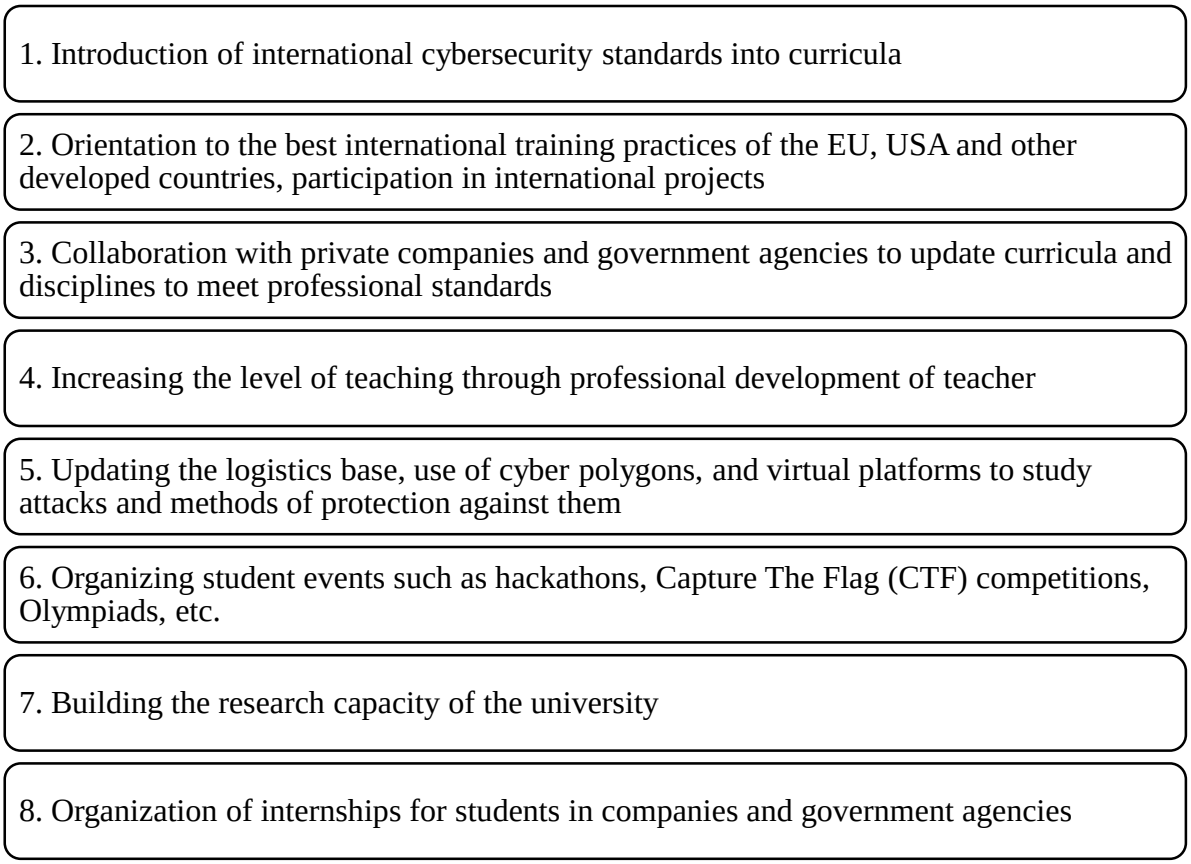



**Fig.1**. Key areas of university development in the field of cyber security

The development of these areas will not only prepare professionals in cybersecurity, but will also increase the competitiveness and ranking of universities both in Ukraine and abroad.

Nowadays more than 50 universities in Ukraine train cybersecurity specialists. Every year over 2,000 cybersecurity specialists graduate from universities at the bachelor's and master's levels. At the same time, the need for information security specialists is still growing and there is a shortage of these specialists. According to forecasts by leading IT companies in Ukraine, the demand for cyber security specialists in 2023 will increase by 8-10%, and will increase as digital services and products emerge.

**Keywords**: Cybersecurity Strategy, Cybersecurity Education, Labor Market, Practice-Oriented Training

## References


1. ENISA Threat Landscape 2022. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
2. Analytical report. https://www.csis.org/topics/cybersecurity-and-technology/cybersecurity
3. The McAfee Mobile Threat Report 2022 https://www.mcafee.com/en-us/resources/reports-and-guides.html
4. NIS Directive. https://digital-strategy.ec.europa.eu/en/policies/nis-directive
5. The EU Cybersecurity Act https: //digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
6. The EU Cybersecurity Strategy https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
7. Information security strategy: Decree of the President of Ukraine dated 12.28.21 № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069
8. Cyber Security Strategy of Ukraine: Decree of the President of Ukraine dated 08.26.21 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12
9. Constitution of Ukraine. https://zakon.rada.gov.ua/laws/show/254
10. Yonemura K. et al. (2021). Cybersecurity Teaching Expert Development Project by KOSEN Security Educational Community, 2021 IEEE Global Engineering Education Conference (EDUCON), 2021, pp. 468-477, doi: 10.1109/EDUCON46332.2021.9453958.
11. Ivanova S., Georgiev G., (2019). Using modern web frameworks when developing an education application: a practical approach, *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2019, pp. 1485-1491, doi: 10.23919/MIPRO.2019.8756914.
12. Trifonov R., Nakov O., Manolov S., Tsochev G., Pavlova G., (2020). Possibilities for Improving the Quality of Cyber Security Education through Application of Artificial Intelligence Methods, 2020 International Conference Automatics and Informatics (ICAI), 2020, pp. 1-4, doi: 10.1109/ICAI50593.2020.9311333.
13. Kuzminykh, M. Yevdokymenko, O. Yeremenko, O. Lemeshko. (2021). Increasing Teacher Competence in Cybersecurity using the EU Security Frameworks. I.J. Modern Education and Computer Science, 2021, 6, p. 60-68. DOI: 10.5815/ijmecs.2021.06.06

# SÜNİ İNTELLEKTİN İNFORMASİYA TƏHLÜKƏSİZLİYİNDƏ TƏTBİQİ: PROBLEMLƏR VƏ PERSPEKTİVLƏR

**Əli Abbasov**
Elm və Təhsil Nazirliyi, İdarəetmə Sistemləri İnstitutu, Bakı, Azərbaycan

3-cü sənaye inqilabı kompüter və İT texnologiyaların, 4-cü sənaye inqilabı isə Süni İntellekt (Sİ), nano və biotexnologiyalar, 5G telekommunikasiya və Əşyalar İnterneti (İoT), insansız idarə olunan hərəkət vasitələri və iqtisadi sahələrin sürətli avtomatlaşdırılması və rəqəmsallaşdırılması və informasiya cəmiyyətinin inkişafı informasiya və kibertəhlükəsizlik problemlərini ön plana çıxarır və qlobal miqyasda həllini tələb edir.

Qlobal İnformasiya Texnologiyaları (İT) sənayesinin həcmi 2022-ci ildə təxminən 5.3 trl. ABŞ dolları olması və 5% birləşmiş (compound) orta illik artım tempi ilə inkişaf edəcəyi gözlənilir. Cybersecurity Ventures-in proqnozlarına görə kiber cinayətlərin həcmi ildə 15% artaraq 2015-ci ildə olan 3 trl. dollardan 2025-ci ildə 10.5 trl. dollara çatacağı gözlənilir. Bu rəqəm bir il ərzində təbii fəkakətlərin vurduğu zərərdən eksponensial olaraq böyükdür və bütün qanunsuz narkotiklərin qlobal ticarətindən daha "gəlirli" olacağı gözlənilir.

Bu gün rəqəmsal mühitlə bağlı olan insanlar, hətta mütəxəssislər də informasiya təhlükəsizliyi ilə kibertəhlükəsizliyi terminlərini dəqiqləşdirməkdə çətinlik çəkirlər və adətən eyniləşdirirlər. Bu halda fikrimizcə, hesab edirik ki, informasiya təhlükəsizliyi kibertəhlükəsizlikdən daha geniş anlayışdır və kibertəhlükəsizliyə informasiya təhlükəsizliyinin bir hissəsi kimi baxmaq olar. Yaranan fərq ondan ibarətdir ki, informasiya təhlükəsizliyi dedikdə həmçinin informasiya kontentinin kiberhücumlar vasitəsi ilə məlumatların mahiyyətinin dəyişdirilməsi, düzgünlüyünə xətər gətirilməsi, əlavə məlumatların və yalan məlumatların daxil edilməsi və beləliklə kontentin dəyişdirilməsi, feyknyusların əlavə edilməsi nəzərdə tutulur. Bu halda yeni yanaşma, yeni metodların tətbiqinin zəruriliyi yaranır.

Süni intellekt (Sİ) informasiya yaxud kibertəhlükəsizliyin qorunmasında üç əsas istiqamətdə hallanır:

- rəqəmsal resurslar, şəbəkə və bulud infrastruktur və tətbiqlərin qorunması;
- kiber cinayətləri həyata keçirən haker potensialının intellektual gücləndirilməsi;
- Sİ sistemlərinin özlərindən doğan təhlükələrin yaranması.

Bu təhlükələrin reallaşması və onlara qarşı mübarizədə Sİ-in tətbiqində aşağıdakı metodlardan istifadə olunur:

- neyron şəbəkələri, böyük verilənlər və dərin öyrənmə;
- Sİ analitikası;
- intellektual qərar qəbuletmə.

Kiberhücumlardan heç bir ölkə, heç bir təşkilat, kiçik biznesdən tutmuş dövlət orqanları və nəhəng şirkətlərə qədər heç biri, hətta adi insanlara qədər heç kim sığorta olunmamışdır. İdarəetmə Sistemləri İnstitutunun əsas fəaliyyət istiqaməti mürəkkəb dinamik obyektlərin, texnoloji proseslərin idarə olunması və qərar qəbuletmə, idarəetmənin optimallaşdırılması, avtomatlaşdırılması və Sİ-in tədqiqi və tətbiqi məsələlərinin həllinə yönəlmişdir. İnformasiya təhlükəsizliyi birbaşa bizim tədqiqat obyektimiz olmasa da kontrakt və əməkdaşlıq çərçivəsində institut tərəfindən işlənib hazırlanan sistemlərdə və onların tətbiqində informasiya təhlükəsizlik məsələləri ilə qarşılaşırıq və onların həlli ilə məşqul oluruq. Həmçinin İnstitutun tədqiqat işləri çərçivəsində təbii dillərin emalı (NLP) texnologiyaları, Sİ-in tətbiqi ilə Azərbaycan dilinin kompüter emal sistemi işlənib hazırlanmışdır və qismən kommersiallaşdırılmışdır.

Bu gün sürətli rəqəmsal transformasiya bütün sahələrə və mürəkkəb sistemlərə müdaxilə edir ki, kibertəhlükəsizlik ön plana çıxarılır. İdarəetmənin diqqət mərkəzində mürəkkəb dinamik obyektlərin, o cümlədən böyük həcmli və paylanmış sənaye komplekslərinin, kritik infrastrukturun, aviasiya və aerokosmik sistemlərin, atom elektrik stansiyaları, qlobal rabitə və nəqliyyat sistemləri və s. qeyri-müəyyənlik amilləri, dəyişən mühit və yüksək təhlükəsizlik tələbləri şəraitində işləmələri müasir idarəetmə və monitorinq siistemlərinin qurulmasında tamamilə yeni yanaşmalar tələb edir.

Müasir sənaye idarəetmə sistemləri (SİS) əsasən SCADA - (Supervisory Control And Data Acquisition) idarəetmə obyektləri haqqında informasiyanın toplanması, işlənməsi, təsvir edilməsi və arxivləşdirilməsi sistemi üzərində qurulur və artıq qlobal standarta çevrilmişdir. İdarəetmə Sistemləri İnstitutunun Xüsusi Konstruktor Bürosunda SCADA konsepsiyasına əsaslanan proqram-texniki sistemi işlənib hazırlanmış və artıq bir neçə sənaye obyektlərində tətbiq edilmişdir. Son zamanlar Sənaye Əşyalar İnternetin (Industrial Internet of Things - IIoT) yayılması ilə əlaqədar SİS-in kibertəhlükələrə qarşı həssaslığı artır. Müasir sənaye sistemləri, əsasən neft, qaz, kommunal və enerji şəbəkələri uzaq məsafələrə paylanır və sistemin normal işləməsi üçün TCP/İP protokollarından istifadə olunur ki, bunlar da kiberhücumlara məruz qala bilirlər.

Texnoloji prizmadan baxsaq görərik ki, bu gün və yaxın gələcəkdə əsas və qorxulu kibertəhlükə 5G şəbəkələri üzərində qurulan IoT sistemləri mühitində olacaqdır ki, bu da birbaşa SİS-lərə təhlükə yaradır.

Təbii ki, İnternet üzərindən hücumların qarşısının alınması üçün mütəmadi olaraq təhlükəsizlik üçün nəzərdə tutulmuş protokolların üzərində təkmilləşdirmə işləri aparılır. Lakin bu dəyişikliklər ondan xəbər verir ki, hakerlər dayanmadan protokolları analiz edir və sonda yenə də hücum üçün yol tapırlar. Deməli, nə qədər dəyişiklik olsa da təhlükəsizliyi ideal səviyyədə təmin etmək mümkün deyil. Nəticə etibarı ilə qeyd etmək olar ki, SİS-lər təhlükəsizliyini İnternet üzərindən cloud ilə əlaqələndirilməsində müxtəlif şifrələmə metodları kifayət etmir.

Son zamanlar süni intellekt metodlarının tətbiqi ilə kiberhücumların qarşısının alınmasında xəbərdarlıq sistemlərinin olunması perspektiv və effektiv sayılır. İdarəetmə Sistemləri İnstitutunda innovativ özəl şirkətlərlə əməkdaşlıq çərçivəsində təbii dilin emalı, o cümlədən Azərbaycan dili üçün istiqamətində müəyyən nəticələr alınmışdır. Qurulmuş süni neyron şəbəkələrində dərin öyrənmə və Böyük Verilənlər (Big Data) metodlarının köməyi ilə hadisələrin proqnozlaşdırılması məsələlərinin

üzərində geniş tədqiqat işləri aparılır ki, nəticələrin tətbiq istiqamətlərindən biri də kiberhücumlardan qorunmaq üçün xəbərdarlıq sisteminin yaradılması ola bilər.

Azərbaycanda bu gün neft, qaz, elektrik şəbəkələri geniş yayılmış, su resurslarının idarə olunması, kommunal sistemlər, bütün bu sahələrdə idarəetmənin avtomatlaşdırılması sürətlə həyata keçirilir. Son zamanlar ölkəmizdə, xüsusən işğaldan azad olunmuş ərazilərdə IoT platformasında ağıllı kənd və şəhərlərin salınması dövlət dəstəyi altında həyata keçirilməsi planlaşdırılır. Bütün bu qeyd olunanlar SİS-nin kibertəhlükəsizliyin təmin olunmasının bizim üçün nə qədər vacib olduğunu bir daha təsdiqləyir.

Əşyalar İnterneti (IoT) cihazlarının qeyri-standart istehsalını və IoT cihazları vasitəsi ilə axan məlumat ehtiyatını nəzərə alsaq, biz daim kiberhücumlara məruz qalırıq. Zəifliklər, kiberhücumlar, məlumat oğurluğu, təzyiqlər və IoT cihazlarından istifadə nəticəsində yaranan digər risklər IoT təhlükəsizlik həllərinə ehtiyacı daha da artırır. Əgər nəzərə alsaq ki, bu gün dünyada IoT cihazlarının sayı təxminən 14 milyard və 2030-cu ilə 29 milyarda çatmağı gözlənilir IoT təhlükəsizliyinin qorunmasının nə qədər vacib olduğunu təsəvvür edə bilərik.

Kiber və informasiya təhlükəsizliyinin qorunmasında Sİ-in tətbiqi ilə yaradılan modullar növləri arasında antivirus proqramları, məlumat itgisinin qarşısının alınması, fırıldaqçılığın qarşısının alınması/anti-fırıldaqçılıq, şəxsiyyət və girişin idarə edilməsi, müdaxilənin aşkarlanması/qarşısının alınması sistemi, risk və uyğunluğun idarə edilməsi daha sürətlə yayılmaqdadır. Kiberhücumların artması Sİ-ə əsaslanan təhlükəsizlik məhsulları bazarında artımın yüksəlməsinə kömək edir. Sİ-ə əsaslanan təhlükəsizlik məhsulları qlobal bazarının həcmi ötən il 14.9 milyard dollardan 2030-cu ilə 133.8 milyard dollara çatacağı təxmin edilir. Hakerlər də bundan istifadə edirlər: Məsələn, Sİ ilə yaradılan fişing e-poçtlarının açılma sürəti adi qaydada hazırlanmış fişing e-poçtlarından daha yüksəkdir.

Süni İntellektin kiber və informasiya təhlükəsizliyində rolundan danışarkən adətən iki əsas aspektə baxılmalıdır: Sİ-nin köməyi ilə rəqəmsal hücumlara qarşı mübarizə və Sİ-nin özünün yaratdığı təhlükələr. Bu gün Sİ-nin informasiya təhlükəsizliyində ən yeni tətbiqi müxtəlif formatlarda saxlanılan və göndərilən məlumat toplusunda informasiyanın dəyişdirilməsi və həqiqətə uyğun olmaması (misinformation and disinformation), feyknyuslar və s. faktların mənasının araşdırılması və müvafiq təhlükəsizliyin təmin olunmasına yönəlmişdir. Bu kateqoriyalardan olan məlumatlara, həmçinin həqiqəti əks etdirməyən, şantaj və digər məqsədlərlə qəsdən hazırlanan, şəkil, video və audio məlumatlar da daxildir. Burada ən perspektivli görünən metodlardan Təbii Dillərin Emalı (NLP) texnologiyalarıdır ki, bu da kompüter və insan dili arasındakı qarşılıqlı əlaqə ilə, xüsusən də böyük həcmdə təbii dil məlumatlarını emal və təhlil etmək, yəni dilin tərcüməsi, başa düşülməsi, səsdən yazıya, yazıdan səsə çevrilməsi və mətnlərin sintezi və s. ilə məşqul olan dilçiliyin, kompüter elminin və Sİ-nin bir altsahəsidir. Dərin neyron şəbəkələrinə əsaslanan semantik vektorlar üzərində qurulan NLP sistemləri, məsələn Siri, Alexa və Corona kimi ağıllı köməkçilər, dilin kvant modeli əsasında qurulan Grover axtarış modulu kimi yeni sistemlərin tətbiqi NLP texnologiyaların informasiya təhlükəsizliyində istifadəsini yeni səviyyələrə çıxarır. Lakin bu sistemlərin tətbiqinin faydalılıq dərəcəsi dillərdən asılıdır, yəni ingilis dili kontenti üçün alınan nəticə Azərbaycan dili üçün

alınmır. Ümumiyyətlə dillərin linqvistik xarakteristikalarının fərqlənməsi hər dil üçün öz NLP sisteminin yaradılmasını tələb edir. Azərbaycan dili üçün də ölkəmizdə NLP texnologiyaları inkişaf etdirilir və DİLMANC layihəsi çoxlarımıza tanışdır. İdarəetmə Sistemləri İnstitutu ilə Robotroniks startup şirkətinin əməkdaşlığı çərçivəsində yaradılan yeni Azərbaycan dilli asistent buna misaldır. Asistent 10 min saatdan ibarət nitq (səs), 300 mln. cümlədən və təxminən 1 mld. söz formalarından, 1 mln. tələffüz korpuslarından ibarətdir. Asistent müasir NLP sistemlərinin həyata keçirdiyi nitqin tanınması, başa düşülməsi, dilin tərcüməsi, mətnin səsləndirilməsi kimi funksiyalarla yanaşı müxtəlif mənalı mətnlərin generasiyasını da həyata keçirə bilir ki, bu da Azərbaycan dilində yaradılan feyknyusların, həqiqətə uyğun olmayan xəbərlərin rəqəmsal mediada avtomatik tapılmasını və ləğv edilməsini təmin edə bilər. NLP texnologiyaların yaratdığı son funksiya – mətnlərin avtomatik generasiyası yuxarıda qeyd etdiyimiz Sİ-in özünün törətdiyi təhlükələri, kiberhücumları yaxud feyknyusları törətməyə kömək edə bilər, yəni bu halda Sİ özü hakerə çevrilə bilər. Nəzərə alsaq ki, son tendensiyalar və gələcək inkişaf xəttləri Sİ əsasında qurulan obyektlərin idarəetmə sistemlərinin avtonom qərar qəbuletmə mexanizminə meyilliyi artmaqda davam edir, məsələnin informasiya təhlükəsizliyində nə qədər vacib olduğunu hiss etməmək mümkün deyil. İdarə olunan obyektlərin sırasına xüsusi təyinatlı pilotsuz uçuş aparatları, sualtı və quruda hərəkət edən robot-maşınları, kritik infrastruktur obyektləri və s. daxil olduğunu təsəvvür edəndə Sİ-in bu imkanı bizi, özümüzü Sİ-sistemlərindən ehtiyatlı olmağa çağırır.

## SECURITY-BASED ROUTING MODELS WITH TRAFFIC ENGINEERING SUPPORT

**Oleksandr Lemeshko, Oleksandra Yeremenko, Maryna Yevdokymenko,**
**Volodymyr Porokhniak**
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
e-mail: oleksandr.lemeshko@nure.ua, oleksandra.yeremenko@nure.ua, marina.ievdokymenko@nure.ua, volodymyr.porokhniak@nure.ua

In today's world, information and communication networks (ICNs) are complicated, specialized systems that constantly operate under various disruptive influences. Moreover, network attacks organized at different OSI model layers are increasingly becoming major [1, 2]. The aim of such cyber intrusions is frequently not only to take possession of confidential information circulating in the network but also to provoke the overloading of individual devices and critical parts of the network, causing a denial of service. Based on [5, 7-8], fault-tolerant routing is vital in resilience solutions for information systems. First Hop Redundancy Protocols (FHRP), Fast ReRoute (FRR), and fault-tolerant routing protocols can prevent and effectively counteract network equipment failures.

In the current environment, ICN edge routers, whose interfaces act as default gateways to connected access networks, must be subject to enhanced protection against failure. Overloading or

compromising edge devices can lead to complete blockage of access networks and/or compromise the security level of information transmitted to or from them. Therefore, FHRP class protocols are constantly evolving, and GLBP (Gateway Load Balancing Protocol) has replaced the low-functioning VRRP (Virtual Router Redundancy Protocol) protocol. Unlike most other FHRP class protocols, GLBP allows load balancing based, for example, on operational reliability and Quality of Service (QoS) metrics. Many papers [3, 6] are devoted to this line of research, proposing solutions represented by mathematical flow-based models and load-balanced fault-tolerant routing optimization techniques aimed at ensuring the efficient use of network resources [3, 5].

A relevant area of research on extending the functionality of FHRP class protocols is ensuring network security parameters' accountability while proactively providing fault-tolerant edge routers. Such an effect can be achieved by developing new mathematical models and methods for fault-tolerant routing and load balancing between edge routers that include virtual default gateways, considering the number of vulnerabilities detected on them and the probability of exploitation [4, 9].

This work considers the problem of proactively improving network resilience by connecting access networks simultaneously to multiple edge routers with support for load balancing between them. Such an approach reduces packet loss when one or more routers fail, with interfaces that create virtual default gateways using FHRPs. Since a security breach of an edge router can trigger the compromise of all information coming to it from access networks, it is proposed to consider the network security level of such routers when load balancing between virtual gateway interfaces.

For the research, the basis was the flow-based routing model, augmented by Traffic Engineering, extended to implement fault-tolerant routing [3]. Thus, two load-balancing models have been proposed and investigated for their effectiveness with respect to the security level of the edge routers. Both models use information security risk to estimate the security level of edge routers. The first model, the Security Aware Traffic Engineering (SATE) model, which is an extension of the approach described in [3, 4], provides load balancing inversely proportional to the information security risk values of the edge routers. The second model, Security Metrics Traffic Engineering (SecMetrTE) model, is based on a modified optimality criterion. Here, in addition to an upper bound of the network links utilization, it is proposed to minimize the degree of using the access lines to border routers under the metrics values formed from their information security risks.

A study and comparative analysis of the proposed balancing models and Traffic Engineering model found that the implementation of the SATE model could lead to some increase (on average from 2 to 20%) in the upper bound of the network links utilization. This effect was particularly evident when using edge routers with very different information security risk values. Therefore, the SecMetrTE model that provides the same upper bound of the links utilization for all the studied reference data variants compared with the TE model can be recommended.

The GLBP fault-tolerant routing protocol can be used to implement the practical part of the proposed solutions. Its functionality enables simultaneous load balancing between several edge routers performing AVF (Active Virtual Forwarder) tasks. In this case, in the weighted load balancing mode, using weighting factors selected according to SATE or SecMetrTE model calculation results,

the necessary load balancing order can be set considering the edge's routers network security level, namely their information security risks.

To further improve the results proposed in this work, it is suggested to extend the network security indicators considered in ICN load balancing and to use the link and network utilization and direct QoS indicators to estimate the QoS level. Separately, the need for further application of dynamic mathematical models that adequately describe the load-balancing process and the change in the network state over time is worth noting.

**Keywords:** Network Security, Information Security Risk, Infocommunication Network, Traffic Engineering.

## References

1. Kiser, Q. (2020). Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats. Kindle Edition.
2. Lemeshko, O., Papan, J., Yeremenko, O., Yevdokymenko, M., Segec, P. (2021). Research and Development of Delay-Sensitive Routing Tensor Model in IoT Core Networks. Sensors 21(11), 3934, 1-23 https://doi.org/10.3390/s21113934
3. Lemeshko, O., Yeremenko, O., Mersni, A., Yevdokymenko, M. (2021). Resilience Aware Traffic Engineering FHRP Solution. In: 2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) Proceedings. IEEE, pp. 1-5. https://doi.org/10.1109/UkrMiCo52950.2021.9716677
4. Lemeshko, O., Yeremenko, O., Yevdokymenko, M. (2022). Models and Methods of Secure Routing and Load Balancing in Infocommunication Networks. In: Oliynykov, R., Kuznetsov, O., Lemeshko, O., Radivilova, T. (eds) Information Security Technologies in the Decentralized Distributed Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 115. Springer, Cham. https://doi.org/10.1007/978-3-030-95161-0_10
5. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Hailan, A.M., Mersni, A. (2019). Cyber resilience approach based on traffic engineering fast reroute with policing. In: 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) Proceedings, vol. 1, pp. 117-122. IEEE. https://doi.org/10.1109/IDAACS.2019.8924294
6. Rahman, Z.U., Mukhtar, S., Khan, S., Khan, R., Ullah, Z., Rashid, R., Ahmad, W. (2017). Performance Evaluation of First HOP Redundancy Protocols (HSRP, VRRP & GLBP). J. Appl. Environ. Biol. Sci, **7**(3), 268-278.
7. Rak, J. (Ed.), Hutchison, D. (Ed.). (2020). Guide to Disaster-Resilient Communication Networks (Computer Communications and Networks) 1st ed. 2020 Edition. Springer.
8. Yeremenko, O., Lemeshko, O., Persikov, A. (2018). Secure routing in reliable networks: proactive and reactive approach. In: Shakhovska, N., Stepashko, V. (eds.) CSIT 2017. AISC, vol. 689, pp. 631–655. Springer, Cham. https://doi.org/10.1007/978-3-319-70581-1_44

9. Yevdokymenko, M., Yeremenko, O., Shapovalova, A., Shapoval, M., Porokhniak, V., Rogovaya, N. (2021). Investigation of the Secure Paths Set Calculation Approach Based on Vulnerability Assessment. In: Modern Machine Learning Technologies and Data Science Workshop. Proc. 3rd International Workshop (MoMLeT&DS 2021), 2917, 207-217.

## İNFORMASİYA TƏHLÜKƏSİZLİYİ: MÜASİR VƏZİYYƏT VƏ ELMİ TƏDQİQAT İSTİQAMƏTLƏRİ

**Vaqif Qasımov**
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

İnformasiya təhlükəsizliyi – informasiyanın və ya informasiyanı saxlayan infrastrukturun onun sahiblərinə və istifadəçilərinə ziyan vuran təbii və süni xarakterli təsirlərdən qorunmasıdır. Burada, ümumi halda informasiyanın məxfiliyinin, bütövlüyünün və əlyetərliyinin təmin edilməsi nəzərdə tutulur. Qeyd edilməlidir ki, informasiya təhlükəsizliyi və kibertəhlükəsizlik anlayışları eyniləşdirilməməlidir. Belə ki, kibertəhlükəsizlik – kiberfəzanın bütün komponentlərinin mümkün təhlükələrdən və arzu olunmaz nəticələrə gətirib çıxaran təsirlərdən qounmasıdır.

İnformasiya təhlükəsizliyi problemi informasiya mühitində dövlətin, cəmiyyətin, fiziki və hüquqi şəxslərin maraqlarının qorunmasını özündə ehtiva edir. Belə problemlərə bütün kritik infrastrukturlarda, o cümlədən müdafiə və hərb sənayesi, atom və kosmik sənaye, iqtisadiyyat, maliyyə və bank sektoru, nəqliyyat və logistika, informasiya texnologiyaları və rabitə, siyasi idarəetmə, sosial-ictimai sfera, səhiyyə və həyat təhlükəsizliyi, ekologiya, elm və təhsil sahələrində rast gəlinir. Ona görə də belə təhlükələrin qarşısının alınması üçün dövlətlər, təşkilatlar, hüquqi və fiziki şəxslər səviyyəsində tədbirlərin görülməsinə zərurət vardır. İnformasiya təhlükəsizliyi sahəsində son illərdə respublikamızda da böyük işlər görülür. Ölkə başçısının fərman və sərəncamları ilə bir sıra yeni strukturlar yaradılmış və normativ hüquqi aktlar təsdiq edilmişdir.

Bu istiqamətdə həllini gözləyən məsələlərdən biri də kadrların, yüksəkixtisaslı mütəxəssislərin hazırlanmasıdır. 2022-ci ildə Azərbaycan Respublikası Elm və Təhsil Nazirliyinin əmrinə əsasən, "İnformasiya təhlükəsizliyi" ixtisasının beynəlxalq tələblərə cavab verən yeni standartı işlənib hazırlanmışdır. Cari tədris ilindən, demək olar ki, bütün universitetlərdə informasiya təhlükəsizliyi ixtisası üzrə kadr hazırlığına həyata keçirilir. AzTU-da da bu sahəyə xüsusi diqqət verilir. Belə ki, universitetdə Kibertəhlükəsilik institutu və eyni adlı kafedra yaradılmışdır.

Təbii ki, yeni texnologiyaların inkişafı şəraitində informasiya təhlükəsizliyi problemini tələb olunan səviyyədə və vaxtında həll edə bilmək üçün müvafiq sahədə məqsədyönlü elmi tədqiqatların aparılması vacibdir. Bu istiqamətdə son dövrlərdə tərəfimizdən çoxlu sayda elmi tədqiqat işləri həyata keçirilir. Belə ki, informasiya təhlükəsizliyi sisteminin yaradılması, DNT və fraktal əsaslı, xaotik çevirmə funksiyasına və molekulların xaotik hərəkətinə əsalanan kriptoqrafik sistemlərin, yeni açar mübadiləsi protokolunun işlənməsi, təsvirlərdə və mətnlərdə, eləcə də internet üzərindən

steqanoanalizə davamlı gizli informasiya ötürmə kanallarının yaradılması, ağıllı şəhərlərdə enerji təminatı sisteminin təhlükəsizliyinin təmin edilməsi, sosial şəbəkələrdə anomaliyaların aşkarlanması, bulud və IoT mühitlərində informasiya təhlükəsizli, kriptovalyuta və blokçeyn texnologiyaları, onların təhlükəsizliyi və rəqəmsal iqtisadiyyata təsiri və s. istiqamətlərdə elmi tədqiqatlar aparılır, alınmış nəticələr nüfuzlu elmi jurnallarda dərc olunur, beynəlxalq konfranslarda məruzə edilir.

# SECTION TALKS

## ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ SIEM СИСТЕМ

**Джейхун Алиев, Байрамали Назаров, Ибрагим Ибрагимли**
Харьковский Национальный Университет Радиоэлектроники. Харьков, Украина
e-mail: jeyhun.aliyev@nure.ua, bayram.nazarov@nure.ua, ibrahimli.ibrahim210@gmail.com

**Аннотация.** Сегодня центры обработки данных должны соответствовать определенным законам или стандартам, уметь защищаться от рисков, заблаговременно обнаруживать подозрительные ситуации, который хранит журналы событий безопасности, системы или приложений для предоставления доказательств в случаях SIEM (Security), что означает информационная безопасность и управление инцидентами. Они используют решения для управления информацией и событиями.

В неуправляемых SIEM-решениях большое количество промахов логов, возникают ложные срабатывания, такие риски, как игнорирование киберугроз. Центры обработки данных, которые спроектированы неправильно, и не используются правильные продукты безопасности, становится уязвимым для угроз. Цель статьи рассмотреть вопрос по обеспечения информационной безопасности посредством SIEM.

**Введение.** С развитием компьютерных коммуникаций и сетевых технологий увеличилось разнообразие кибератак и возникли различные проблемы безопасности. Эти проблемы еще больше повысили важность концепции информационной безопасности. Для обеспечения безопасности информации учреждения используют различные продукты безопасности. Целью продуктов безопасности, используемых в учреждениях, является обеспечение конфиденциальности информации от несанкционированного доступа во время ее обработки, транспортировки или хранения, защита ее целостности от искажения, модификации или удаления, своевременный доступ к желаемой информации и обеспечить доступность для полного использования этой информации. Безопасность, сетевые устройства, системы и приложения записывают доступ пользователей, события системы и безопасности для обнаружения киберугроз, отслеживания изменений неправильной конфигурации, изучения системных сбоев и их записи в целях соблюдения некоторых законов и стандартов. Из-за растущего разнообразия кибератак на сегодняшний день недостаточно вести только эти записи. Необходимо анализировать эти записи событий (логи), чтобы иметь возможность бороться с киберсобытиями, обнаруживать подозрительные события в системах и принимать меры предосторожности до киберсобытия. Критические центры обработки данных содержат множество защитных, сетевых и прикладных устройств для хранения, обработки и защиты

критически важных данных. Эти устройства производят логи, что означает большое количество логов каждый день [1]. Если эти логи не собираются в центральной точке, ими будет очень сложно управлять, и это продлит время решения проблемы. Одного сбора логов недостаточно. Также необходимо анализировать логи из каждого источника в таких случаях, как обнаружение перед атакой и решение системных проблем. С помощью SIEM, что означает «Информационная безопасность и управление событиями», можно получить целостное представление о подходе к информационной безопасности, когда обнаруживается угроза, путем сбора и анализа ежедневных данных из нескольких источников.

**Хранение логов.** Необходим способ хранения логов, чтобы иметь возможность работать с логами, поступающими в SIEM, и делать запросы между прошлыми событиями. Логи хранятся в реальном времени и архивируются. Логи в реальном времени, поиск среди событий, произошедших за определенный период времени, отслеживание на экране мониторинга. Это события, сохраненные для записи, корреляции и записи аварийных сигналов. Время поддержания активности каждого производителя SIEM отличается. В то время как некоторые производители хранят логи в течение 1 месяца, некоторые решения SIEM могут хранить их в течение 2 лет. Эта ситуация полностью связана с ресурсом, выделенным в проекте SIEM, и возможностями продукта. По истечении периода поддержания активности логи архивируются. Архивные логи могут различаться в зависимости от законов и стандартов, а также в зависимости от выделенного источника. Архивные логи важны не только для соблюдения законов и стандартов, но и для просмотра прошлых событий. Как долго логи будут оставаться в архиве, зависит от размера диска и законов и стандартов, которые необходимо соблюдать

**Мониторинг.** Завершающим этапом в компонентах SIEM является способ взаимодействия с логами, хранящимися в SIEM. После того, как у вас есть все логи в SIEM и обработаны события, возникает необходимость в способе сделать что-то полезное с этой информацией. В противном случае логи будут храниться только в SIEM для целей хранения. SIEM должна иметь интерфейсную консоль, которая может быть веб-интерфейсом или приложением и должна быть установлена на рабочей станции. Оба интерфейса должны позволять пользователям взаимодействовать с данными, хранящимися в SIEM. Эта консоль будет использоваться для управления SIEM, будь то веб-интерфейс или приложение. Этот интерфейс в реальной реализации SIEM придаст обработчикам событий или системным инженерам уникальный взгляд на среду SIEM.

**Управления логов** — это лог событий, который происходит на всех системных и сетевых устройствах. Каждый из этих логов состоит из записи лога, и все эти записи содержат определенное событие. Наиболее важными из них являются логи безопасности. Многие логи в организации связаны с компьютерной безопасностью. По данным института SANS, логи используются специалистами по безопасности для записи данных о том, кто, что, когда, где и почему произошло событие для конкретного устройства или приложения. этот компьютер Программное обеспечение безопасности, такое как логи безопасности, антивирусное

программное обеспечение, брандмауэры и системы обнаружения и предотвращения вторжений, состоит из операционных систем и приложений на серверах, рабочих станциях и сетевом оборудовании. Основные рабочие процессы управления логами обычно включают в себя настройку ресурсов логов, выполнение анализа логов, инициирование ответов на выявленные события и управление долговременным хранением. Кроме того, управление логами включает в себя поддержание конфиденциальности, целостности и доступности логов. Вот некоторые аспекты управления логами:

- Сбор логов в центральной точке
- Хранение логов • Обеспечение быстрого доступа и отображения данных • Поддержка нескольких форматов логов
- Выполнение анализа данных
- Хранение записей
- Архивирование и восстановление архивных логов
- Доступ к восстановлению данных на уровне полномочий и отношений
- Обеспечение целостности данных. Помимо указанных выше целей, хранение и безопасность логов осуществляется в соответствии с определенными законами и стандартами [2].

**Обеспечение информационной безопасности цод и эффективного управления SIEM.** В центрах обработки данных происходит сбор, хранение, обработка и распределение больших объемов данных по конкретным точкам. Эти центры объединяют системы, приложения, сети и устройства безопасности под одной крышей для удовлетворения различных услуг и потребностей. Сегодня, помимо некоторых государственных, образовательных и финансовых учреждений, дата-центрами являются и компании, предоставляющие онлайн-услуги, такие как Google и Яндекс. предлагает услуги в. С SIEM он направлен на предоставление таких преимуществ, как анализ критических событий, обнаружение подозрительных ситуаций и обнаружение перед атакой, а также определение основной причины проблемы благодаря логам, собранным из систем, приложений, сеть и устройства безопасности в центре обработки данных. Каждый шаг процесса проекта SIEM с самого начала имеет решающее значение. В конце неправильно сконфигурированного процесса и плохо управляемого этапа планирования могут возникнуть такие проблемы, как проблемы с производительностью, стек логов, ведение логов и трудности с анализом событий. Планирование очень важно при инициировании проекта SIEM для центров обработки данных. Расчет ресурсов и мощностей, необходимых для создания системы, играет решающую роль на этапе планирования в этом направлении [3].

**Ключевые слова:** киберугроза, лог, SIEM, SEM.

**Литература**

1. Cyberdefenses INC., 2019, What Is SIEM And How To Choose The Right Tool, https://cyberdefenses.com/what-is-siem-and-how-to-choose-the-right-tool/
2. Миллер Д., Харрис С., Харпер А., ВанДайк С. и Бласк С., 2011 г., Реализация информации о безопасности и управления событиями, McGraw-Hill Компании, Соединенные Штаты Америки, ISBN: 978-0-07-170108-2.
3. Exabeam, 2019, Log Aggregation, Processing and Analysis for Security, https://www.exabeam.com/siem-guide/events-and-logs/

**Information security based on SIEM systems**

Nowadays, data centers must comply with certain laws or standards, be able to protect themselves from risks, detect suspicious situations in advance, which stores security event logs, systems or applications to provide evidence in cases of SIEM (Security), which means information security and incident management. They use information and event management solutions.

There are a large number of log misses, false positives, risks such as ignoring cyber threats in unmanaged SIEM solutions. Data centers that are not designed correctly and that the right security products are not used become vulnerable to threats. The purpose of thesis, the issue of ensuring information security through SIEM.

## ANALIZING PROTOCOLS FOR LAYER THREE NETWORK AND WAYS TO COMBAT THEM

**Jeyhun Aliyev**
Kharkov National University of Radioelectronics, Kharkov, Ukraine
e-mail: jeyhun.aliyev@nure.ua

**Abstract.** The purpose of thesis, analyze three redundancy protocols at the FHRP (First Hop Redundancy Protocol), IP layer (Layer 3). This work focuses on the differences between the three protocols and how they work used to keep the network running. A crucial component of any company local area or data center network is high availability. Different protocols are used by organizations to guard against single points of failure in their networks. The First Hop Redundancy Protocol (FHRP), one of these protocols, presents a virtual default gateway to the company's network in order to offer a network uptime of almost 100 percent. To avoid network failure at a default gateway, FHRP is employed which is accomplished by establishing numerous routers with the same IP address and Mac address, giving the hosts in a Local Area Network the impression that there is only one virtual router (LAN). All hosts in that network or subnet have the virtual router's IP address set as their default gateway. At the same time, the applications, types and observable attacks of FHRP will be examined.

**Introduction.** Due to the fact that it enables connectivity to distant locations, the default-gateway is an essential component of every local area network. First-hop redundancy protocols

(FHRP) ensure that the default gateway operates continuously, hence enhancing the high availability of the network and its constituent parts. The employment of a variety of strategies during the pre-deployment phase is beneficial for the design of complicated mission-critical networks. The configuration of network devices, major issues with the network design, and potential performance bottlenecks can all be revealed through network simulation. The implementation of the high availability mechanism is necessary for network infrastructure that is anticipated to offer continuous services. In this paper, we focus on the operation theory and implementation design of HSRP, VRRP, GLBP in detailed form, our findings also outline possible attacks by following prevention ways to mitigate the impact [1, 2].

**Hot Standby Router Protocol (HSRP). Attacks on HSRP.** This protocol's functioning methodology is highly effective since various routers inside the HSRP domain would connect with the main live router, that would be in charge of regulating all live inbound and outbound traffic. Similar to this, the backup routers would always be in contact with the primary router through the multicast address 224.0.0.2 (the multicast address for routers, used for HSRP “hello” packets) so that they could identify any problems or outages with the primary router as soon as possible [3]. If the primary router fails, the backup routers will immediately take over. However, there won't be any kind of delay for the end users because the same procedure of choosing a standby router will be repeated and a new backup will be picked [4].

In the illustration below, N2 represents a computer or other sender device that will transmit data to N1, the destination. On the routers R1 and R2, the HSRP protocol is configured. We add Virtual IP address as a default gateway since the source device has to make note of the gateway. If R1 is set to have the greatest priority, traffic will first travel to R1, then to R3, and last to N1 through the switch. However, if the R1 router goes down for whatever reason, the R2 router will be able to step in and handle the duties, and messages will be sent through R2. As long as preemption is not turned off in the router's setup mode, the second router in HSRP cannot assume the first router's responsibilities. Once preemption is enabled, traffic can be forwarded. Since R1 has a high priority in this situation, it will be our active router, and R2 will be our backup router. Load balancing is not done automatically by HSRP [5].

Moreover, the ICMP redirection is automatically enabled when the interfaces are set up to function with HSRP. An important Layer 3 protocol called ICMP is used to examine the end-to-end connection and find any faults along the way. Additionally, it provides us with a variety of IP processing statistics and diagnostic data. HSRP also filters outgoing ICMP redirection signals, which includes switching to a virtual HSRP IP address instead of the subsequent hop IP address [6].
Some of HSRP's limitations would be apparent if its fundamental functions were taken into account. Basically, any HSRP-capable device has the ability to announce a high priority value and take over as the active router. The device might be a genuine router or a malicious actor attempting to launch a man-in-the-middle (MITM) or denial-of-service (DoS) attack.

Furthermore, routers that support HSRP communicate among themselves via multicast messages to advertise the priority levels. The participating routers identify which of them is the

default active router by exchanging these messages. Since the default priority level is normally 100, the default active router will be the one of the participating routers with priority level 101. Every three seconds, all HSRP-compliant routers broadcast a "hello" message via multicast. The standby router with the next-highest priority will take over as the active router if the default active router is unable to transmit a "hello" message. This design vulnerability makes it feasible for an attacker to interfere with network traffic if they are on the same network segment as the HSRP routers. RFC2281 provides the clearest summary of the vulnerability:

- “This protocol does not provide security. The authentication field found within the message is useful for preventing misconfiguration. The protocol is easily subverted by an active intruder on the LAN. This can result in a packet black hole and a denial-of-service attack. It is difficult to subvert the protocol from outside the LAN as most routers will not forward packets addressed to the all-routers multicast address (224.0.0.2).”

**Virtual Router Redundancy Protocol (VRRP).** VRRP has many significant features which are being open standard, using RFC 3768, VIP which stands for Virtual IP can be utilized as physical IP in case of necessity, consisting of one master and many other backup routers, its IP address used for multicast is 224.0.0.18.

**Attacks on VRRP.** Poorly built VRRP setups are prone to compromise, which opens up a number of attack opportunities. Two web servers, two Cisco routers, and a user PC will all be included in a case study describing one of the assault scenarios. Try sending traffic to one server through the first router initially. Then play out a scenario in which one router has a power outage. As a result, following a VRRP failover, the user PC will now route traffic to the internet through a second router. The attack in this instance may take place if a hacker discovers a VRRP router that is not properly configured and tries to intercept communications. To find out if VRRP is active on the local subnet, try utilizing Cisco's "display VRRP all" feature after using the "tcpdump -I eth0 proto VRRP -v" command. If so, use TCPDUMP once again to record VRRP messages. Use the commands route, VRRPD -h, show vrrp all, and show VRRP short - to gather the required data before launching the assault. The attacker is now receiving user PC traffic flow that was previously bound for the Internet.

**Gateway Load Balancing Protocol (GLBP).** Gateway Load Balancing Protocol, or GLBP, is used to build a virtual gateway that hosts can use. It offers redundancy like other First Hops and functions similarly to HSRP and VRRP. It is a Cisco-exclusive proprietary protocol that is capable of carrying out both tasks. Using a single virtual IP address and many virtual Mac addresses, it offers load balancing over a number of routers. The fact that GLBP may perform load balancing without utilizing the group setup like HSRP/VRRP do is one of its main differences [7].

**Attacks on GLBP.** One of the attacks is GLBP Hijacking. This network attack uses a malicious GLBP packet with the highest priority value to force your device to act as the master router. A successful exploitation results in an MITM attack, which allows you to intercept network traffic, reroute it, or launch a denial-of-service attack. Building the GLBP package with the highest priority value of 255 and directing it to the local network is sufficient. Another one is GLBP Injection. If the GLBP protocol is not implemented in Scapy, it can still perform GLBP injection using Loki, a

specialized packet injector that permits attacks on L2 and L3 protocols. We can obtain the AVG role by injecting a malicious GLBP packet with a value of 255. We now have the chance to intercept traffic as a result. By examining GLBP traffic, such as Information about the GW2 router (AVF) and Information about the router GW1, all the essential data (AVG) can be gathered. Next one is carrying out an attack on the GLDP domain and intercepting the traffic. We can carry out the attacks this way: Loki is also implemented in this attack. The interface needs to be set to promiscuous mode so that traffic can be routed. We choose the GW1 router and choose the Get IP option to begin the injection. Following the injection, we must use the value of the virtual IP address to construct a secondary IP address on our network interface. Moreover, we define a 24-bit mask. Set up a SNAT rule in order to see both incoming and outgoing traffic (MASQUERADING). Now we must delete the default route from our computer and add a new one that will use the previous AVG router. The GW1 router will continue to be able to route traffic even after we have disabled the AVG role from it. We can now intercept sensitive data from network traffic now that we have become man-in-the-middle [8, 9].

**Conclusion.** In this paper, three commonly utilized Fast Hop Redundancy Protocols (FHRP)-Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol were explained in detailed form. Our goal was to provide our research findings about implementation of protocols, observed attacks in FHRP and crucial ways of mitigation their impact. Results of the research show that FHRP offers a constant network connection when a router malfunctions. It stops a malicious switch from taking over as the root by enabling an access port to switch from the receiving state to the forwarding state instantly. After the in-depth analysis of the research, we have come to the conclusion that the redundancy protocol made the topology more reliable and redundant, also possible attacks can be prevented by implementing appropriate prevention types, successfully.

**Keywords:** FHRP, HSRP, VRRP, GLBP.

## References

1. http://www.og150.com/assets/VRRP%20(Virtual%20Router%20Redundancy%20Protocol)%20Attack.pdf
2. https://louwrentius.com/configuring-attacking-and-securing-vrrp-on-linux.html
3. https://networklessons.com/cisco/ccie-routing-switching/glbp-gateway-load-balancing-protocol
4. https://prog.world/glbp-nightmare-how-to-attack-the-glbp-protocol-and-intercept-traffic-within-the-network/
5. https://www.beyondsecurity.com/dynamic-fuzzing-testing-virtual-router-redundancy-protocol-vrrp
6. https://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html
7. Juha R. (2005). Router Redundancy and Scalability Using Clustering.
8. Li, T., Cole, B., Morton, P., & Li, D. (1998). RFC2281: Cisco Hot Standby Router Protocol (HSRP).

9. Priyanka, D. Shilpi, S. H., & Aabha, S. (2013). Review of First Hop Redundancy Protocol and Their Functionalities.

## BANK OFİSİNİN DAYANIQLI İŞİNİN TƏŞKİLİNDƏ SİMULYASİYA EKSPERİMENTİ

**Bəhrəm Əzizov[1], Arzu Quliyev[2], Valeh İbrahimli[1]**
[1]Azərbaycan Universiteti, Bakı, Azərbaycan
[2]Azərbaycan Dövlət Pedaqoji Universiteti, Bakı, Azərbaycan
e-mail: Bahram.azizov@au.edu.az, quliyev.arzu.68@mail.ru

Müasir informasiya texnologiyaları idarə edilməsi qeyri-müəyyən şərtlər daxilində qərar qəbul etmələrdən asılı olan mürəkkəb sistemlərin özünü aparmasini tədqiq etmə imkanını artırmışdır.

İdarəetmə ilə bağlı olan mürəkkəb məsələləriin ümumi analitik həllinin tapılması üçün riyazi apparatın gücü kifayət qədər olmadığından mürəkkəb sistemlərin özünü aparmasının tədqiqi və qeyri-müəyyən şərtlər daxilində qərar qəbul etmələrdə alternativ yanaşma kimi paraktik məsələlərin həllində güclü vasitələrdə biri olan imitasiya modellərindən istifadə edilir [1, 2, 3].

***İmitasiya*** termini kimi real sistem üzərində uyğun təcrübələr aparmaq əvəzinə model üzərində erksperiment aparma prosesi işarə edilir. Çox variantlı hesablama erksperimentlərinin aparılması müəyyən keyfiyyət qanuna uyğunluqlarının aşkar edilməsinə və müəyyən ümumiləşmələrin çıxarılmasına imkan verir.

İmitasiya modelləşdirilməsi qeyri-müəyyənlik şərtləri daxilində zamana görə dəyişən dinamik sistemlərin özünü aparmasını tədqiq edən metodologiyadır. İmitasiya modeli tədqiq olunan prosesin zaman, fəza və məntiqi aspektlərini göstərir, dıgər modellərdə isə adətən bunıarda biri iştirak edir. Beləliklə imitasiya modelləşdirilməsi qeyri-müəyyənlik şərtləri daxilində qərar qəbul etmə üçün universl yanaşmadır.

İmitasiya modelləşdirilməsi dedikdə sistemin komputer üçün işlənmiş modeli və real sistem və ya obyekt əvəzinə proqrammla təcrübələrin aparılması başa düşülür. İmitasiya modelləşdirilməsi səbəb əlaqələrini, nəticələri, qeyri xəttiliyi, stoxastik dəyişənləri nəzərə almaqla sistemin analitik modelini qurmaq mümkün olmadıqda və həmçinin sistemin zaman kəsimində özünü aparmasını imitasiya etnək və daxiii və xarici şərtlərin dəyişilməsi ilə əlaqədar müxtəlif mümkün vəzityyətləırin inkişafına baxmaq zəruriyyəti yaranır.

AnyLogic imitasiya moddeləşdirilməsinin müasir nəslinin peşəkar alətləri informasiya texnologiyaları sahəsinin müasir konsepsiyalarına və qibrit sistemlər və obyekt yönümlü modelləşdirmənin tədqiqatının nəticələrinə əsasən işlənib hazırlanmışdır.

Tədqiqatçı AnyLogic-də müxtəlif səviyyəli abstraksiyalardan, müxtəlif stil və konsepsiyalardan müvəffəqiyyətlə istifadə edə, həmçinin eyni modelin yaradılmasında qeyd edilənlərin qarışığından da yararlana bilər.

Müasir dövrdə sistemin təsviri üçün bizness modelləşdirilməsində üç yanaşma (üsul) üstünlük təşkil edir. AnyLogic modelləşdirməyə müxtəlif yanaşmalrın köməyi ilə imitasiya modelinin yaradılmasına imkan verir [7]:

– sistem dinamikası;

– diskret hadisələrin modelləşdirilməsi;

– agent modelləşdirilməsi.


**Şəkil 1**. Simulyasiya modelləşdirilməsinin növləri

**Bank fəalıyyətının ımıtasıya modelı**

***Modelləşdirilən obyektin təsviri***

Məqalədə praktik iş variantlarından birinə baxılır:

Bankın modeli- Diskret hadisələrin modelləşdirilməsi (proses yönümlü) yanaşmadır.

İşin gedişində sistemin tam hüquqlu imitasiya modeli işlənəcəkdir.

Təklif olunan praktik işdə müştərilərə tez və effektiv xidmət etməyə imkan verən bankomat və menecerlər masası, bank kassirləri olan bank şöbəsi üçün sadə kütləvi xidmət sisteminin modelinin həyata keçirilməsi nəzərdə tutulur. Müştərilər nağd pulla əməliyyatları bankomat, kreditlərin sənədləşdirilməsi və hesaba ödəmələr kimi daha mürəkkəb əməliyyatları isə menecerlər və kassirlər vasitəsi ilə yerinə yetirirlər.

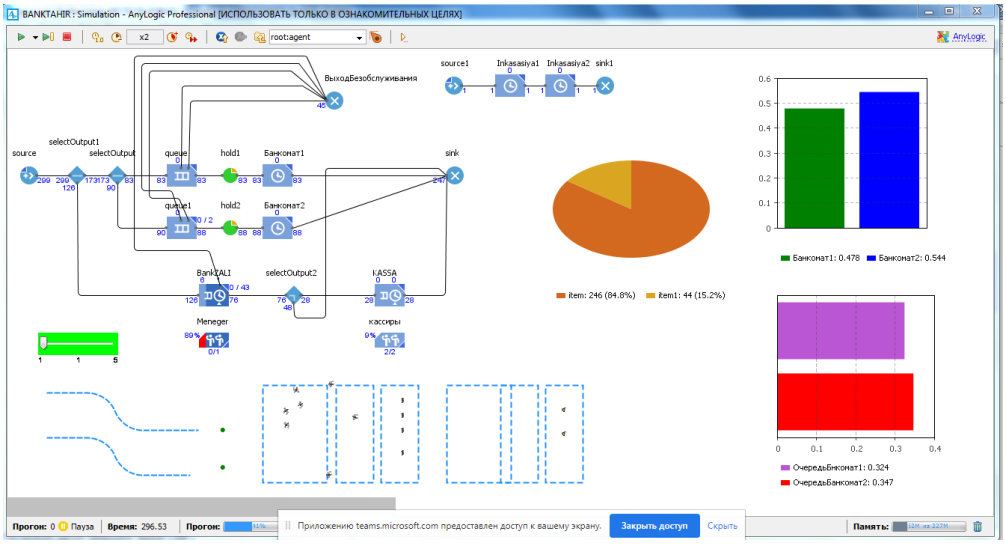
Görüləcək işin məqsədi müştərilərdən ibarət olan növbələrin modelləşdirilməsi və bank əməkdaşlarının və bank şöbəsi avadanlıqlarının iş rejiminin optimallaşdırılmasıdır.

Təqdim olunan işdə diskret hadisəli mürəkkəb modelin əyani və tez yaradılmasına kömək edən AnyLogic paketinin modelləşdirmə kitabxanasının sadə obyektlərinə baxılacaqdır.

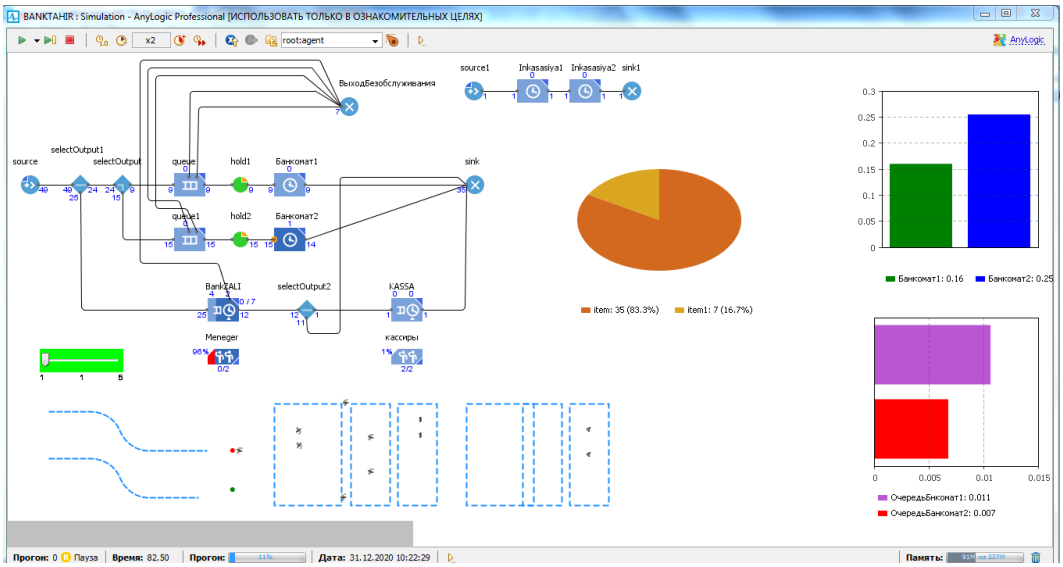
***Təcrübi hesablamalar***

İşləyən menecer və kassaların sayı müştərilərin sayından asılıdır. Bu modelin verilənlərinin köməyi ilə bankın işini optimallaşdırmaq olar. Bunun üçün modelin işinin bir neçə sumulyasiyasını həyata keçirmək lazımdır.

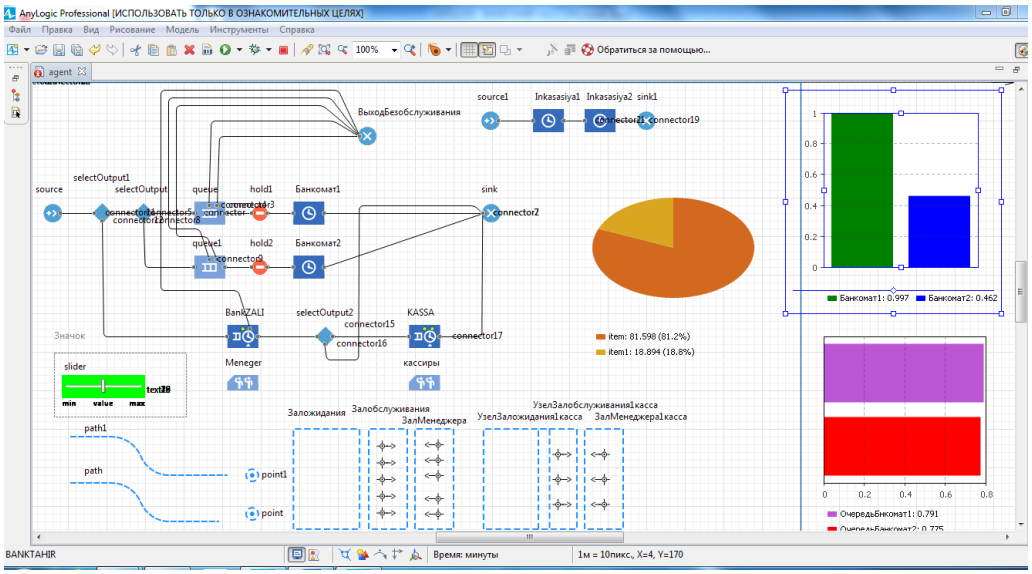
Təcrübi hesablamaların nəticəsində bank rəhbərliyinin nöqteyi nəzərindən ən yaxşı variantı seçmək olar. Təsvir olunan üsul müasir informasiya texnologiyaları vasitəsi ilə bank ofisinin ahəng və təhlükəsiz işinin yaxşılaşdirilmasına kömək edir. Bundan əlavə həm də göstərilir ki, təcrübə prosesində imitasiya modelləşdirilməsinin tətbiqi tədqiqatcının, real vaxt rejimində ilkin verilənləri operativ dəyişmək imkanı vasitəsi ilə onu daha əyani edir. Verilən üsul öyrənilən obyektin fəaliyyət texnologiyasını daha yaxşı başa düşülməsinə imkan verir.




**Şəkil 2.** 1 saylı təcrübi hesablamanın nəticələri




**Şəkil 3**. 2 saylı təcrübi hesablamanın nəticələri




**Şəkil 4.** 3 saylı təcrübi hesablamanın nəticələri

**Açar sözlər:** informasiya texnologiyaları, imitasiya, simulyasiya modeli, modeləşdidilən sistem.

## Ədəbiyyat

1. Бир С. Кибернетика и управление производством: пер. с англ. М.: Наука, 1985, 391с.
2. Шеннон Р. Имитационное моделирование систем – искусство и наука: пер. с англ. М.: Мир, 1978. 418 с.
3. Нейлор Т. Машинные имитационные эксперименты с моделями экономических систем: пер. с англ. М.: Мир, 1975, 500 с.
4. Борщев А.В. Практическое агентное моделирование и его место в арсенале аналитика. Exponenta Pro, 2008. № 3–4. URL: http://www.xjtek.ru/anylogic/articles/

# IMAGE-BASED MALWARE DETECTION METHOD

**Elshan Baghirov**
Institute of Information Technology of ANAS, Baku, Azerbaijan
e-mail: elsenbagirov1995@gmail.com

**Abstract.** According to international statistics, malware is one of the most critical threats to computer security today. In this study, identification methods based on images used to identify malicious programs were analyzed. The used datasets, ways of converting the malware file into images, and classification methods, in short, all stages from the assembler file to the identification stage were analyzed. The advantages and disadvantages of the approaches are comparatively analyzed.

**Introductıon.** Typically, malware is an umbrella name for several malicious software, including viruses, rootkits, backdoors, ransomware, worms, trojans, spyware, etc. The amount of new malware has been continuously growing, and its threats are increasing rapidly [1]. Today, the problem of detecting malware has become more difficult due to the high availability of attack methods, as well as anti-virus evasion instructions, over the Internet. Developing new types of detection methods and thereby protecting computer systems from malicious programs has always been of interest to scientific researchers, individuals, and organizations. Although the scientific research conducted in the direction of increasing the detection accuracy of malicious programs is rich due to its diversity, the need for improving the conducted research is always relevant.

Detection of new types of malware is a crucial problem since malware authors are able to bypass antivirus techniques using obfuscation methods like metamorphism, polymorphism, and packing techniques [2]. When obfuscation methods are applied to malware their signature are refreshed and it becomes difficult to identify by traditional methods. Knowing the advantages and disadvantages of static and dynamic analysis, there is a need to develop new advanced methods [3]. Recently, the application of image-based detection methods on malware is expanding in the literature. In this paper, related works with malware identification using image-based methods are analyzed and classified according to their image converting methods, classification methods, used datasets, and feature extraction methods.

**Related works.** Related works to this work have not been found extensively in the literature. Sang Ni et al. [1] analyzed static, dynamic, visualization, and other methods for malware detection shortly and showed that Self Organizing Maps, treemaps, gray-scale images, and local sensitive hashes are used for visualizing malware images. The authors also offered a new method for visualization and identification of malware called the MSCS algorithm. Abdullah Sh. et al [4] analyzed related research and showed that authors implemented a framework for the visualization and identification of malware using image processing techniques. Also converting malware into the gray-scale image and applying a histogram similarity metric to study similarity, applying a clustering-

based machine learning algorithm to discover new malware, and using image texture-based features for extraction methods are analyzed. Hamad N. [5] et al. concluded existing solutions and showed that converting malware to gray-scale image and generating entropy graphs from images, malware texture analysis, GIST descriptor, content-based image retrieval (CBIR) method for extracting local binary features, and using Local Sensitive Hashing algorithm and other works have been done by authors. Ahmed B. [6] et al. classified and analyzed works in two groups: traditional machine learning works and methods based on deep learning. Prajapati P. et al [7] discussed the first image-based analysis work, transfer learning. Mazhar J.A. et al [8] approved that transfer learning using ResNet-50 and GIST features, ResNet and GoogleNet, VGG16 and ResNet-50, a CNN-LSTM hybrid model, MalFCS that visualizes malware binaries as entropy graphs based on structural entropy, an IOT based hybrid visualization technique, genetic algorithms, a combination of the first-order and grey-level co-occurrence matrix are used in literature.

**Malware ıdentıfıcatıon steps.** Common image-based malware detection methods in the literature are mainly divided into four steps:

- Disassembling executable malware files;
- Feature extraction;
- Generating malware images;
- Classifying images.

PE (portable executable) file format is a data structure that captures valuable information in Windows OS. First of all, to extract the necessary features from the PE file, it must be disassembled using tools like PE viewer, IDA Pro, and Capstone [1]. The binary malware sample files are disassembled and divided into basic blocks, using IDA Pro or OllyDbg in [9].

After getting the disassembled file, the next step is the extraction of useful features. Sang N. et al [1] used opcode as a feature extracted from the code section of the PE file for the MCSC algorithm. Young-Man Kwon [3] used n-gram opcode as a feature in the MCSP algorithm. KyoungSoo Han et al. [9] extracted opcode sequences from executables for visualizing malware images. The major block selection method is applied when extracting opcodes from disassembled files [1,9]. Nataraj et al. [10] used GIST image features and extracted image texture for similarity checking. Kancherla et al [9] extracted three different sets of features intensity-based, wavelet-based, and Gabor-based features from images.

In the MCSC algorithm [1], the opcode sequence is described as a document and each opcode is the keyword referred to in the SimHash algorithm. Each malware code is encoded into a binary SimHash value with the same length and each SimHash value is converted to a pixel value as 0 to 0 pixel and 1 to 255 pixel. After arranging n pixel dots in a matrix, SimHash values are converted to a grayscale image [1, 3, 9].

Used datasets in the literature are generalized in table 1.

| Ref. | Dataset name | Sample size |
|---|---|---|
| [1, 3, 11,12] | Malware Classification Challenge by Microsoft on Kaggle | 10 868 with 9 labels |
| [13] | Offensive Computing / Windows OS | 27 000 (15k malware, 12k benign) (30% test) |
| [9] | Windows OS | 290 (16 labels) + 560 (14 labels) |
| [10] | Anubis analysis system | 9458 with 25 labels (1713 for the test) |
| [4] | SARVAM dataset | 9339 with 25 labels (33.33% test) |
| [5] | Malimg, Malheur, Virushare, Microsoft Kaggle | 9339(25), 3131(24), 2630(11), 3237 with 20% test |
| [7] | Winwebsec, Zeroaccess, Zbot, Malicia | 500000 with 20 labels |
| [6, 8, 14] | Malimg | 9389 with 25 labels |
| [15] | VX Heavens | 1000 with 50 labels |

**Conclusıon.** In this work published papers on the detection of malicious programs based on images were analyzed. The methods used in different steps of malware identification were systematized.

**Keywords**: malware, image, static method, dynamic method, malware visualization, simhash algorithm.

## References

1. Ni S., Qian Q., Zhang R. Malware Identification Using Visualization Images and Deep Learning, Computers & Security, vol 77, 2018, pp. 871-885.
2. Baghirov E., Techniques of Malware Detection: Research Review, 2021 IEEE 15th International Conference on Application of Information and Communication Technologies (AICT), 2021, pp. 1-6.
3. Kwon Y., An J., Lim M., et al, Malware Classification Using Simhash Encoding and PCA (MCSP), Symmetry-Adapted Machine Learning for Information Security, vol 12, No 5, 2020.
4. Abdullah Sh., Essa A. and James H. Empirical Analysis of Learning-based Malware Detection Methods using Image Visualization. International Journal of Advanced Computer Science and Applications(IJACSA), 13(4), 2022.
5. Naeem, H., Guo, B., Naeem, M. R., Ullah, F., Aldabbas, H., & Javed, M. S. (2019). Identification of malicious code variants based on image visualization. Computers & Electrical Engineering, 76, 225-237.
6. Bensaoud, A., Abudawaood, N., & Kalita, J. (2020). Classifying malware images with convolutional neural network models. International Journal of Network Security, 22(6), 1022-1031.
7. Prajapati, P., & Stamp, M. (2021). An empirical analysis of image-based learning techniques for malware classification. In Malware Analysis Using Artificial Intelligence and Deep Learning (pp. 411-435). Springer, Cham.

8. Awan M.J., Masood O.A., Mohammed M.A., Yasin A., Zain A.M., Damaševičius R., Abdulkareem, K.H. Image-Based Malware Classification Using VGG19 Network and Spatial Convolutional Attention. Electronics 2021, 10, 2444.
9. Kyoung Soo Han, BooJoong Kang, Eul Gyu, Malware Analysis Using Visualized Image Matrices, The Scientific World Journal, vol. 2014, Article ID 132713, 15 pages, 2014.
10. Nataraj L., Karthikeyan S., Jacob G., Manjunath B. S. (2011). Malware images: visualization and automatic classification. In Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec '11). Association for Computing Machinery, New York, NY, USA, Article 4, 1–7.
11. Ren Z., Chen G. & Lu W. Malware visualization methods based on deep convolution neural networks. Multimed Tools Appl., 79, 10975–10993 (2020).
12. Kancherla, K., Mukkamala, S. (2013). Image visualization-based malware detection. 2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 40-44.
13. Lin W.-C. Yeh Y.-R. Efficient Malware Classification by Binary Sequences with One-Dimensional Convolutional Neural Networks. Mathematics, 2022, 10, 608.
14. El-Shafai W., Almomani I. AlKhayer A. Visualized Malware Multi-Classification Framework Using Fine-Tuned CNN-Based Transfer Learning Models. Appl. Sci., 2021, 11, 6446.
15. Han K.S., Lim J.H., Kang B. et al. Malware analysis using visualized images and entropy graphs. Int. J. Inf. Security, 14, 1–14 (2015).

## MALLARIN ICAZƏSIZ ÇIXARILMASINDAN QORUNMAQ ÜÇÜN MÜASIR AVADANLIQLARIN İMKANLARI

**Nizami Cəfərov, Vəfa Fərhadlı**
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
e-mail: nizami_cd@mail.ru, vafaf18105@gmail.com

Oğurluğa qarşı sistemlər kommersiya avadanlıqlarının nisbətən yeni növüdür. Son onillikdə mağazaların özünəxidmət sisteminə keçməsi və yeni iri pərakəndə satış şəbəkələrinin açılması ilə əlaqədar geniş yayılıb.

Müasir mağaza stasionar bina və ya onun ticarət üçün xüsusi təchiz olunmuş bir hissəsidir, orada (anbarda və ticarət mərtəbəsində) çoxlu sayda mal var. Daxili İşlər Nazirliyinin və mağazaların statistikasına görə, onlar hər ay həm ziyarətçilər, həm də işçilər tərəfindən oğurluqdan xeyli itki ilə üzləşirlər. Faiz ifadəsində oğurluq və oğurluqdan itkilər formatından asılı olaraq mağaza dövriyyəsinin orta hesabla 0,5%-dən 5%-ə qədərdir. Bundan əlavə, adətən texniki nasazlıqlar və ya yanğınla ehtiyatsız davranma nəticəsində baş verən yanğın kimi fors-major hallar böyük itkilər gətirir. Buna görə də mağaza təhlükəsizliyi məsələləri xüsusi diqqət və kompleks yanaşma tələb edir. Kompleks yanaşma isə aşağıdakılardan ibarətdir [1, s. 10].

1. Mühafizə üsuluna görə: vizual müşahidə; elektron siqnal sistemləri; siqnalizasiya sistemləri; izləmə sistemləri);

2. Fəaliyyət prinsipinə görə: akustomaqnit; elektromaqnit; radiotezlik; radio maqnit;

3. İstifadə olunan sensorların növünə görə: deaktivləşdirilmiş - birdəfəlik; qeyri-aktivləşdirilmiş - təkrar istifadə edilə bilər; checklink - boya ilə;

4. Quraşdırma yerinə uyğun olaraq: mağazanın çıxışında; masanın ortasındakı xəzinə terminallarında; deaktivasiya ilə çıxışda;

5. Məhsul qrupu üzrə: nişanlarının bərkidilməsi mümkün olan geyim, ayaqqabı və analoji mallar üçün; qida məhsulları, kitablar üçün audio və video kasetlər;

6. Malların oğurlandığı yerə görə: piştaxtalardan oğurluqdan; paltardəyişmə otaqlarından paltar oğurluğundan.

Obyektin mühafizəsi üçün ən çox istifadə edilən dörd üsul:

1) vizual müşahidə - alıcılar üçün ticarət zalında satıcılar baxır, çıxışda və kassalarda mühafizəçilər növbə çəkir;

2) elektron siqnal sistemləri - hər bir mal vahidinə sensorların qoşulduğu, zaldan çıxışda antenaların və xəbərdarlıq sistemlərinin quraşdırıldığı məşhur qorunma üsulu, sensor yaxınlaşdıqda işə salınır;

3) həyəcan siqnalı sistemləri - onlar satıcıya malın pəncərədən çıxarıldığını, butiklərdə, zərgərlik, əntiq əşyaları, parfümeriya və saat mağazalarında istifadə edildiyini bildirirlər;

4) izləmə sistemləri (video kameralar) - müşahidə və videoçəkiliş üçün cihazlar, diametri təxminən 1 mm olan obyektivli kameralar və baxış bucağı 60-85°, nəzarət zaldan kənarda operator tərəfindən həyata keçirilir.

Sensorlar üç qrupa bölünür: deaktivləşdirilmiş (tək istifadə), qeyri-aktivləşdirilmiş (sərt təkrar istifadə edilə bilən); checklink (məhsulda iz buraxaraq boya ilə vurur) [2, s. 34].

**Mağazaların satış sahələrinin oğurluğa qarşı müasir avadanlıqları.** Özünə xidmət mağazalarında istifadə olunan oğurluğa qarşı sistemlər arasında bir neçə texnologiya fərqlənir:

- radio tezliyi;
- kustomaqnit;
- lektromaqnit;
- radiomaqnit.

Onların hamısı çox geniş tətbiq sahəsinə malikdir, lakin hər bir halda mağaza üçün hansı növ avadanlıqların optimal olduğunu müəyyən etmək üçün bir sıra parametrləri təhlil etmək lazımdır - axı, hər bir sistem növü vəif və güclü tərəfə malikdir. Beləliklə, adətən belə bir sistemi seçərkən qiymətə əlavə olaraq aşağıdakı xüsusiyyətləri nəzərə almaq lazımdır:

- qoruyucu etiketin və sensorların müxtəlif növ mallarla uyğunluğu;
- təkrar istifadə edilə bilən sensorlardan istifadə ehtiyacı;
- qorunan keçidin eni və ya xəzinə aparatlarının keçidlərin sayı;
- sistemlərin quraşdırılması yerində müdaxilə səviyyəsi;
- oğurluğa qarşı sistemin və deaktivatorların qiyməti;

- əməliyyatda olan oğurluğa qarşı sistemin etibarlılığı;
- qoruyucu etiketin darvazadan keçirilməsi zamanı işləmə əmsalı;
- yanlış pozitivlərin olması;
- istehlak materiallarının dəyəri (birdəfəlik qoruyucu etiketlər).

**Radiotezlik sistemləri.** Bu, ixtira oğurluğa qarşı yaradılmış ilk texnologiyadır. Müasir radiotezlik sistemlərindən əvvəl yaradılan qurğunun ixtirası sovet tədqiqatçısı Lev Termenə (əsl soyadı Theremin) aid edilir. 1946-cı ildə konstruktor təsadüfi radio dalğalarına audio məlumat verə bilən passiv ötürücü ("böcək") yaratmışdır. Qərbdə "yaddaşlı passiv radioötürücü" üçün ilk patent ABŞ-da mühəndis Mario Cardulloya verilmişdir.

Oğurluğa qarşı radiotezlikli sistemlər başqalarına zərərli təsir göstərmir və istifadəsi asandır. Radiotezliyin tanınması metodu elektromaqnit rezonans fenomeninə əsaslanır: antenadan gələn siqnal qapalı keçirici dövrədə induksiya edilmiş elektrik cərəyanına səbəb olur və bu, oxucuya cavab siqnalını modulyasiya edir.

Radiotezlik identifikasiya (RİS, ing. RFID- Radio Frequency IDentification) sistemi adətən çiplərdən (fişlərdən) və ya RFID etiketlərindən, onları tətbiq etmək və məlumatı qeyd etmək üçün cihazlardan, məlumatları oxuyan identifikatorlardan və əlaqəli proqram təminatından ibarətdir.

Passiv RFID çiplərinin enerji mənbəyi yoxdur, lakin onların iş prinsipi oxucudan gələn elektromaqnit siqnalı ilə antenada yaranan elektrik cərəyanının istifadəsinə əsaslanır. Çip siqnalı qəbul edir və oxucu tərəfindən qəbul edilən modullaşdırılmış dalğa yaradır. RFID etiketi bir çipdən (silikon və ya yarımkeçiricilərə əsaslanan) və çipdən iki dəfə böyük olan öz antenasından ibarətdir. Doğrudur, bu antenna çox az yer tuta bilər: adətən kiçik bir kart şəklində qatlanmış formada yerləşdirilir, bir millimetr qalınlığında bir fraksiyadan ibarətdir. Passiv RFID çiplərinin yaddaş tutumu adətən 1 kB-a qədərdir, onlar həm birdəfəlik qeyd etmək, həm də yenidən yazmaq və təkrar istifadə etmək üçün nəzərdə tutula bilər.

Oxucu qurğuların təyinatının xüsusiyyətləri ilə müəyyən edilən bir neçə növü var: portal, masaüstü və portativ. Stasionar qurğular adətən keçid məntəqələrində quraşdırılır və ya məhsulların keçdiyi yol boyunca əlavə olunur. Portal oxucuları daha çox gücə, daha geniş diapazona malikdirlər və eyni vaxtda bir çox çipdən məlumat qəbul edib emal edə bilirlər. Bu portallar öz iş yerində etiketlənmiş əşyaları müəyyən etmək üçün (məsələn, ticarət meydançasının çıxışında) və ya logistika terminallarında malların mərhələli hərəkətini izləmək üçün istifadə olunur. Masaüstü cihazları həcmi və əhatə dairəsi baxımından daha kiçikdir. Buna misal olaraq, operatorun satılan malları gətirdiyi satış məntəqəsinin kassa aparatındakı terminalı göstərmək olar. Stasionar terminallar tez-tez logistika nəzarətçiləri ilə əlaqələndirilir və xüsusi kompüter proqramları ilə xidmət göstərir. Portativ oxucular yığcamdır və uzun diapazona malik deyildir. Oxunan çiplərdən gələn məlumatlar daxili yaddaşa yazılır, lakin sonradan kompüterə qoşulduqda bu məlumat ona yüklənə bilər.

Radiotezlikli oğurluğa qarşı sistemlərin üstünlüyü ondan ibarətdir ki, onlar optik olaraq tanınan ştrix-kodların geniş yayılmış texnologiyasına alternativdir. RFID çiplərinin faydalarını aşağıdakı kimi ümumiləşdirmək olar:

1) Yüksək etibarlılıq. RFID etiketləri ətraf mühitə davamlıdır. Düzgün işləndikdə və qablaşdırıldıqda, onların qeyri-müəyyən xidmət müddəti var.

2) Pulsuz yer. Həmişə görünməli olan barkoddan fərqli olaraq, RFID etiketi hətta paketin içərisinə yerləşdirilə bilər, məkanda oriyentasiyanın əhəmiyyəti yoxdur. Bu halda, yerindən asılı olmayaraq, çipdən gələn məlumatlar tam oxunacaq.

3) İstifadə rahatlığı. Çipin məlumatlarını əldə etmək üçün onun oxucunun diapazonuna qısa müddətə daxil olması kifayətdir. Eyni zamanda, terminal çoxlu sayda RFID çiplərindən məlumatları oxumağa imkan verir ki, bu da malların emalını sürətləndirir. RFID oxuyucu cihazlarının əhatə dairəsi yalnız qısa məsafədə ştrix kodu tanıya bilən optik sistemlərdən xeyli böyükdür.

4) Böyük həcmli yaddaş. RFID çiplərinin yaddaşı, bir barkoddan istifadə edərək qeyd oluna biləndən daha çox məlumat toplamaq imkanı verir.

Burada qeyd olunan və istifadə olunan RFID sistemlərinin əksəriyyətinə aid olan üstünlüklərə əlavə olaraq, ixtisaslaşmış çiplər daha geniş imkanlara malikdir: məlumatların yenidən yazılması, əlavə məlumatların monitorinqi və ötürülməsi (temperatur və rütubət şəraiti, vibrasiya və s.), peyk rabitəsindən istifadə etməklə idarəetmə və s. [6].

**Akustomaqnit (AM) sistemləri.** Akustomaqnit texnologiyası universaldır və geniş çeşiddə məhsullara tətbiq olunur. Onun üstünlüklərindən biri müdaxilə və səs-küyə qarşı yüksək müqavimətdir ki, bu da yalançı siqnalların minimum ehtimalını təmin edir. Digər mühüm üstünlük-yüksək effektivlik əmsalının (95% - dən çox) olmasıdır. Sistemlərin işlədiyi diapazon elektromaqnit səs-küyünə və digər müdaxilələrə daha az meyllidir, ona görə də yalan siqnalların olma ehtimalı minimaldır. AM sistemləri astarların, yaxalıqların, ciblərin və s. altına yerləşdirilə bilən kiçik təhlükəsizlik etiketlərindən istifadə edir, buna görə də onlar müştərilər üçün faktiki olaraq görünməzdir. Qoruyucu sensorlar yalnız digər texnologiyalarda olduğu kimi maqnit olmayan xüsusi çəkicilərlə çıxarılır.

Oğurluğa qarşı sistemin işləmə prinsipi - mallar sərt və ya yapışqan etiketlərlə qeyd olunur. Malların pulunu ödədikdən sonra sərt izlər dartıcı ilə, yapışqan izlər isə deaktivatorla zərərsizləşdirilir. Ticarət meydançasının çıxışında antenalar quraşdırılıb ki, bu da ödənilməmiş malların çıxarılması zamanı siqnal verir. Bahalı parça mallar üçün təkrar istifadə edilə bilən sərt etiketlərdən, böyük miqdarda satılan mallar üçün isə ucuz yapışqan etiketlərdən istifadə etmək daha yaxşıdır.

İkili antennalı oğurluğa qarşı sistem bərk etketlər üçün 0,7 + 1,4 + 0,7 m və yapışan etiketlər üçün 0,65 + 1,3 + 0,65 m keçidi qorumağa imkan verir.

Akustomaqnit sistemlərinin çatışmazlıqları:

- etiketlərdən yalnız düz səthlərdə istifadə etmək imkanı (əyilmiş halda işləmir);
- məhsulun üzərindəki etiketin görünməsi;
- asanlıqla mexaniki məhvə məruz qalırlar (kəsdikdə, deformasiyaya uğradıqda və ya deşdikdə işləmirlər);
- sistemin və qoruyucu etiketlərin yüksək qiyməti.

Sensormatic akustomaqnit sistemlərinin istehsalçıları arasında tanınmış liderdir.

**Elektromaqnit sistemləri.** Elektromaqnit sisteminin əsas prinsipi radiotezlik texnologiyasına bənzəyir. Antenalar aşağı və yüksək tezlikli maqnit sahəsi yaradır ki, bu da müəyyən metal ərintisi ilə hazırlanmış etiketi aşkar etməyə imkan verir.

Elektromaqnit texnologiyası xüsusi olaraq böyük dövriyyəyə malik ticarət müəssisələri üçün hazırlanmışdır, yəni, supermarketlər və hipermarketlər üçün. Onlarda oğurluqdan qorunma sistemi üçün əsas tələb qoruyucu elementin dəyəri və görünüşüdür. Həqiqətən, böyük dövriyyənin olduğu bir supermarketdə, etiketlənmiş malların optimal faizini - təxminən 30% -ni nəzərə alsaq, etiketlər oğurluğa qarşı sistemlər üçün əsas xərc maddəsidir. Elektromaqnit sistemləri ilə istifadə edilən təmkinli, demək olar ki, görünməz bir etiket oğurluğa qarşı sistemin effektivliyini əhəmiyyətli dərəcədə artırır. Çox vaxt oğru etiketi belə tapa bilmir. Bundan əlavə, bu cür etiketlər oxumaq üçün məhsulun üzərində qiymət etiketləri və yazılar buraxır.

Elektromaqnit sistemləri qeyri-ferromaqnit metallardan hazırlanmış malları və folqa materialları ilə qablaşdırılmış malları mühafizə etməyə imkan verir.

Etiket xüsusiyyətləri: ən geniş çeşiddə malların mühafizəsi; aşağı qiymət; mallarda görünməzlik; kiçik ölçü; mexanik zədələrə qarşı müqavimətin artması.

Elektromaqnit sistemlərinin mənfi cəhətlərinə keçidin məhdud genişliyini (etiketin kiçik ölçüsünə görə), aşkarlanma səviyyəsinin digər texnologiyalara nisbətən aşağı olmasını, sistemin elektrik avadanlığının təsirinə məruz qaldığını və kredit kartlarına, maqnit qeydlərinə və s. təsir göstərə biləcəyini göstərmək olar.

**Radiomaqnit sistemləri.** Radiomaqnit texnologiyası sistemləri yüksək reaksiya dərəcəsi və geniş çeşiddə malların mühafizəsi imkanları ilə xarakterizə olunur. Radiotezlik və elektromaqnit texnologiyalarının müsbət və mənfi cəhətlərini özündə birləşdirir. Digər texnologiyalarla müqayisədə qoruyucu etiketlərin və sərt sensorların ən geniş çeşidinə malikdir. Sərt sensorları və iki texnologiyanın (elektromaqnit və radiotezlik) təhlükəsizlik etiketlərini birləşdirmək imkanı istehlak materiallarına 30%-ə qədər qənaət etməyə imkan verir.

Bu, radiotezlik texnologiyasındakı sərt sensorların elektromaqnitdən daha ucuz olması ilə əlaqədardır. Radiomaqnit texnologiya sistemləri hər iki texnologiyadan daha geniş məhsul çeşidini qoruyur. Bundan əlavə, metallaşdırılmış səthlərə qoruyucu etiketlərin yapışdırılması ehtimalı var.

Gateway (İsveç) radio-maqnit texnologiyası sistemlərinin yeganə istehsalçısıdır.

**Siqnalizasiya sistemləri.** Siqnalizasiya sistemi istifadəçinin polisə və ya müəssisənin mühafizə xidmətinə zəng etmək üçün gizli (cinayətkardan) istifadəsinin rahatlığını təmin etməlidir. Əl siqnallarından (düymələrdən) gizli istifadə etmək mümkün deyilsə, ayaq (pedallar), simsiz siqnalizasiya (radio düymələri, açar foblar) istifadə etmək lazımdır. Siqnaldan istifadə edərkən onun istifadə olunduğu otaqda səs siqnalının olmaması təmin edilməlidir [3 c.266].

**Avtomatik yanğınsöndürmə sistemləri.**Avtomatik yanğınsöndürmə sistemlərinin aşağıdakı növləri istifadə olunur: maye; karbon qazı; toz; köpük.

Ən çox yayılmış su sistemi sadəcə temperatura həssas klapanları olan çiləyici başlıqlarda bağlanmış su boruları sistemidir. İstiliyin təsiri altında çiləyici başlığın klapanı açılır və ondan mexaniki deflektorlar tərəfindən geniş şəkildə püskürən bir su axını çıxır. Hər bir başlıq, yerləşdiyi

yerdəki temperatura görə fərdi olaraq açılır. Sistemin düzgün işləməsi üçün çiləyici başlıqlar boya ilə örtülməməli, onlardan yad əşyalar asılmamalı, ətrafdakı boşluqlar dağınıq olmamalıdır [2].

**Sorğu güzgüləri.** Detex Line təhlükəsizlik güzgüləri ticarət meydançasında və kassa yerlərində oğurluğu azaltmaq üçün əla və ucuz vasitədir. Anket güzgüsü həm də video nəzarət sisteminə əla əlavə kimi xidmət edir və müşahidənin sərhədlərini əhəmiyyətli dərəcədə genişləndirməyə imkan verir.

Düzgün baxış güzgüsü:

- 75 mm-dən az olmayan yüksək qabarıq hündürlüyə malik olmaq;
- çevik qolla tamamlanmalı;
- yüngül olmaq.

Təhlükəsizlik güzgüləri kassa yerlərində və ticarət mərtəbələrində istifadə olunur.

## Ədəbiyyat


1. Барсуков В.С. Безопасность: технологии, средства, услуги. М., 2001, 496с.
2. Ярочкин В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. – М.: Академический проект: Трикста, 2005, 544 с.
3. Барсуков В.С. Современные технологии безопасности. М.: Нолидж, 2000, 496 с.
4. Зегжда Д.П. Основы безопасности информационных систем. М.: Горячая линия Телеком, 2000. 452 с.
5. Компьютерная преступность и информационная безопасность / А.П. Леонов [и др.]; под бщ. Ред.А.П. Леонова. Минск: АРИЛ, 2000. 552 с.
6. Власова Е.Н., Ковлякова В.Е. Оборудование предприятий (торговля): Учебн. пособие, ГОУВПО «МГУС». М., 2006. 371стр.
7. Арустамов Э.А. Оборудование предприятий торговли: Учебн. пособие, Издательско-торговая корпорация «Дашков и Ко». М., 2005, 452 стр.

# HƏRB VƏ MÜDAFİƏ SAHƏLƏRİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN TƏMİN OLUNMASININ AKTUAL PROBLEMLƏRİ

**Ənvər Həzərxanov[1], Amil Dadaşov[1], Vasif Neymətov[2]**
[1]Heydər Əliyev adına Hərbi İnstitut, Bakı, Azərbaycan
[2]Azərbaycan Dövlət Neft və Sənaye Universiteti, Bakı, Azərbaycan
e-mail: enver-xan@mail.ru, amilodas@gmail.com, neymvasif@mail.ru

Hərbi təhlükəsizlik strukturunda informasiya komponentinin çox yüksək əhəmiyyətinin olduğunu təsbit edən əsas amil odur ki, dövlətin aidiyyətli strukturları informasiya ehtiyatlarından və texnologiyalarından müdafiə maraqları naminə səmərəli istifadə etmək qabiliyyətinə malik olsun. Müdafiə kompleksinin informasiya təhlükəsizliyi onun informasiya sahəsindəki maraqlarının qorunmasının təminatıdır [4, 5]. Hərbi əməliyyatların ən yeni forma və üsulları informasiya üstünlüyünü təmin edəcək məqsədyönlü mexanizm və vasitələrin yaradılmasını təsbit edir.

Müasir hərbi əməliyyatlar zaman və məkan daxilində paralel yerinə yetiilən kəşfiyyat, əks-kəşfiyyat, müşahidə, hədəf seçmə, naviqasiya və s. kimi proseslərlə əlaqəli formada yerinə yetirilməlidir. Yeni informasiya texnologiyaları hərbi əməliyyatların mahiyyətini kökündən dəyişdirmiş, müasir hərbi strategiya və taktikanın əsas elementinə çevrilmiş və beləliklə də hərbi sahənin bütün obyektlərini və predmetlərini əhatə etmişdir. İnformasiya texnologiyaları, həmçinin, hərbi sənaye kompleksinə də dərindən nüfuz edərək, pilotsuz uçuş aparatlarının, "texniki görmə" cihazlarının, robototexniki avadanlıqların istehsalı və hava hücumundan müdafiə, radiomüşahidə-izləmə, hərbi təyinatlı naqilsiz, o cümlədən peyk rabitəsi sistemlərinin yaradılması və başqa bu kimi texnologiyaların inkişafında əsas komponentə çevrilmişdir [1].

[2] ədəbiyyatında müasir topoqrafik-geodeziya və naviqasiya təminatı sistemlərinin (TG NTS) dövlətin təhlükəsizliyi üçün özünəməxsus əhəmiyyətə malik olduğu xüsusən vurğulanır. Belə ki, həmin sistemlərin yüksək səviyyəli nümunələrinə malik olan dövlətlər məlumat toplanmasında və təhlilində, strateji və taktiki komanda qərarlarının qəbulunda, hərbi hissələrə operativ şəkildə çatdırılmasında qarşı tərəf üzərində üstünlük əldə edir. Bu mülahizə ilə razılaşaraq, onu da əlavə etmək lazımdır ki, hərbi münaqişədə olan dövlətlərdən birinin digəri qarşısında bu amillərlə təsbit olunan üstünlüyünü reallaşdıran şərtlər ödənməlidir. Yəni, TG NTS nisbi sakit döyüş bölgələrindən, nəzarət altında olan ərazilərdən cari vəziyyət haqqında operativ və dəqiq məlumatların əldə edilməsini, hərbi qüvvələrin yerdəyişmələrinin idarə olunması zamanı dərhal icrası tələb edilən, olduqca sərrast qərarların qəbul edilməsini və ümumiyyətlə, hərtərəfli nəzarətin bərqərar edilməsini təmin edən çox güclü, aparat-proqram xarakterli, avtomatik və operativ idarə olunan resurslara malik olan informasiya və kompüter texnologiyaları ilə təchiz edilməlidirlər.

Belə təchizat sayəsində xarici amillər (məkan, zaman və hava durumu aspektləri, gizlilik səviyyəsi, insan resurslarının kəmiyyət və keyfiyyət xüsusiyyətləri), döyüş şəraitindəki dinamika və dəyişikliklər nəzərə alınmaqla, insan və texniki ehtiyatların yerdəyişməsinin monitorinqi,

effektiv planlaşdırılması və idarə olunması həyata keçirilir. Hərbi əməliyyatda iştirak edən qüvvə və vasitələrin yerləşdirilməsi üçün strateji və taktiki planların işlənib hazırlanması əsasında kəşfiyyat işləri aparmaq, düşmənin proqnozlaşdırıla bilən hərəkət marşrutlarını, dislokasiyasını müəyyən etmək və bunların nəticəsində düşmən qüvvələrinə dəqiq zərbələr endirmək məqsədi ilə özünün ümumqoşun və aviasiya qüvvələrinin dislokasiyasını, marşrutlarını planlaşdırmaq, hərbi əməliyyatları məkan-zaman formatında optimallaşdırmaq mümkün olur.

İnformasiya-kompüter texnologiyaları və müxtəlif hərbi idarəetmə formalarının qarşılıqlı təsiri nəticəsində hərbi nəzarət, planlaşdırma və təsir formasının bir növü olan refleksiv (yansıtma) idarəetməni qeyd etmək olar. Refleksiv idarəetmə - idarəedici tərəfindən əvvəlcədən hazırlanmış qərarı qəbul etməyə sövq etmək üçün subyektlərə edilən təsirdir [2]. Bu konsepsiyanın yaradıcısı V.A.Lefevr qeyd edir ki, "refleksiv idarəetmə" ideyasının mənası, rəqibin mülahizəsini və ya mümkün davranışını təqlid etmək üçün müəyyən prosesləri təşviq etməklə, onu özü üçün əlverişsiz qərar qəbul etməyə məcbur etməkdir, çünki bu qərar mövcud vəziyyət barədə yalnız onun-düşmən tərəfin düşüncələri əsasında formalaşır. Düşmənə qarşı refleksiv nəzarət əməliyyatının aparılması zamanı mövcud vəziyyət haqqında yanlış təsəvvür yaratmaqla və ya onu təhrif etməklə düşmənin hərbi planlarına dolayı (və bəzi yerlərdə birbaşa) təsir etmək imkanı yaranır. Bu məsələlərin təhlili aparılmış, daha çox diqqət çəkən işlərdən biri olan [3] ədəbiyyatında göstərilir ki, refleksiv idarəetmənin effektiv vasitələrinə aşağıdakılar daxildir: dezinformasiya, məlumatın taktiki maraqlardan asılı olaraq, "kamuflyajı", aşkarlanması və təqdim edilməsi vasitələri, təxribatlar, düşmənin döyüş qabiliyyətini hər mənada zəiflədən psixoloji təsirli informasiya vasitələri.

Ən yeni tariximizdə, refleksiv xarakterli döyüş əməliyyatlarına nümunə olaraq, II Qarabağ müharibəsinin ilk 10 günündə yerinə yetirilmiş əməliyyatları göstərmək olar. Belə ki, Ermənistanın Hava Hücumundan Müdafiə sistemləri olan «S-300» markalı zenit-raket kompleksləri pilotsuz uçuş aparatlarına cevrilən «AN-2» təyyarələrini Azərbaycanın qırıcı təyyarələri zənn edərək onlara atəş açan zaman havada məhz bunun üçün keşik çəkən kəşfiyyatçı dronlarımız bu raketlərin yerini müəyyən edərək, koordinatları zərbə dronlarına ötürür. Zərbə dronları isə dərhal həmin «S-300» ZRK-ni darmadağın edir.

Hazırda informasiya təhlükəsizliyinin yüksəldilməsi istiqamətində fəal işlər görülür: lokal və kütləvi xarakterli təhdidlərlə dolu informasiya mənbələrinin və sistemlərinin qarşısının alınması və aşkarıanıb dəf edilməsi, onların nəticələrinin aradan qaldırılması məqsədi ilə təşkilati, hüquqi, texniki və texnoloji tədbirlər, əks-tədbirlər və s. İnformasiyanın mühafizəsi nəzəriyyəsi formalaşır, məlumatların qorunması üsulları və vasitələri yaradılaraq, praktikada reallaşdırılır, informasiyanın mühafizəsi texnologiyası, avtomatlaşdırılmış sistemlərin inteqrasiya olunmuş informasiya təhlükəsizliyi üzrə mütəxəssislər hazırlanır.

Hərbi sahədə informasiya texnologiyalarının geniş yayılması səbəbindən kiberhücumların ehtimalı artdığına görə kiberməkanın dayanıqlı və etibarlı kibertəhlükəsizlik texnologiyaları ilə təmin edilməsi istiqamətində zəruri tədbirlər görülür. Bu tədbirlərin əsas istiqaməti hərbi sistemlərə, şəbəkələrə və hərbi əməliyyatlara təsir göstərə biləcək kiberhücumları aşkarlamaq, cavablandırmaq, qarşısını almaq və onlardan qorunmaqdır. Kiberhücumların əksəriyyəti ilk öncə

sistemdəki ən az qorunan hissə müəyyənləşdirilməklə, sonra isə onun digər qorunan hissələrinə aparat və proqram təminatı hücumlarının kombinasiyası tətbiq edilməklə həyata keçirilir. Aparat hücumları daha mürəkkəb olduğundan, kiberhücumların əksəriyyəti getdikcə daha mürəkkəb üsullardan istifadə etməklə proqram təminatı ilə həyata keçirilir ki, bu səbəbdən də hər bir şəbəkə cihazı üçün müəyyən növ kibermühafizə tələb olunur.

Beləliklə, kibertəhlükəsizliyin əsas mahiyyəti rabitə və informasiya sistemlərinin mühafizəsini təmin etməkdir. Əslində, kibertəhlükəsizlik - sistemləri, şəbəkələri, məlumatları, kompüterləri və proqramları zədələrdən, xaker hücumlarından və icazəsiz müdaxilələrdən qorumaq üçün nəzərdə tutulmuş xüsusi metodlar, proseslər və texnologiyalar toplusudur. Bu istiqamətdə görülən işlərə 5G texnologiyaları, avtonom intellektual kibertəhlükəsizlik agentlərinin (Autonomous Intellectual Cybersecurity Agent) işlənilməsi, strateji kommunikasiyalar (Strategic Communications), peyk rabitəsi (Satellite Communications) və s. aiddir. Yalnız kibertəhlükəsizliyin təmin edilməsi ilə hərbi qüvvələr quruda, dənizdə və havada təhlükəsiz məlumat mübadiləsi həyata keçirməklə (təhlükəsiz mesajlar, zənglər) üzərinə qoyulan mühüm vəzifə və tapşırıqları yerinə yetirə bilər.

**Açar sözlər:** informasiya texnologiyaları, informasiya təhlükəsizliyi, kibermühafizə, kibertəhlükəsizlik.

### Ədəbiyyat

1. Ковалев А.А., Кудайкин Е.И. Информационные технологии в обеспечении военной безопасности государства. Управленческое консультирование №5. 2017.
2. Лефевр В.А. Лекции по теории рефлексивных игр. М. : Когито-Центр, 2009. 218 с.
3. Присяжнюк С.П., Филатов Н.В., Федоненков С.П. Геоинформационные системы
4. военного назначения: учебник. СПб. : БГТУ, 2009. 208 с.
5. Zhuravlov D., Anishchuk V., Chyzhov D., Pashynskyi V., Zaitsev M. The defense-industrial complex as the basis of the national security of the state. Journal of security and sustainability 9(3), 2020 https://doi.org/10.9770/jssi.2020.9.3(9)
6. https://www.eeas.europa.eu/eeas/stronger-eu-security-and-defence_en. A stronger EU on security and defence

## Current problems of ensuring information security in the military and defense areas

The purpose of the article is description of characteristics of use by armed forces of information technologies in spheres of management, logistics and material support when conducting fighting, and in peace time - for ensuring national and military security. As at the present stage of development of military data on the coming and happening armed conflict carry out the integrating role, in the article the attention is focused on a perspective of creation and increase in efficiency of developments in the field of information technologies, for the purpose of their application in the military sphere.

# SECURITY MEASURES FOR MICROCONTROLLERS IN EMBEDDED SYSTEMS

**Nuru Dashdamirli**
Azerbaijan Technical University, Baku, Azerbaijan
e-mail: nurudashdamirli@gmail.com

Since their introduction in the 1970s, microcontrollers have been very popular in embedded systems. They have a lot of real-world applications and are widely used in electronic devices nowadays. Especially in "Internet of Things" systems, microcontrollers are irreplaceable. That's why securing them for any potential threat is very important.

Security in microcontrollers is a very broad subject; it consists of different parts like network safety, firmware protection, integrity checks, failsafe mechanisms and more. Network safety means all communication must be over a secure channel, and this communication channel shouldn't be vulnerable to attacks like "Man In The Middle". Firmware protection means firmware must be protected from malicious attacks like hacked Over-The-Air firmware updates or reading firmware content to use it for malicious intentions. The most basic way to protect firmware is to shut the system down for a short period of time in case of an attack, but this isn't a robust enough approach. An integrity check is a verification process that runs before the microcontroller starts executing the main code. If some part of the main code is determined to be corrupted (or modified by a third party) by the integrity checking process, the microcontroller shouldn't execute any code. Failsafe mechanisms are for protecting the microcontroller or connected devices from possible hardware or software failures.

Network operations in microcontrollers can easily be secured with the use of secure communication protocols, which are used by almost all web technologies. One of the most commonly used secure communication protocols is TLS (Transport Layer Security). TLS can make use of different cryptosystems. To start a secure communication channel between client and server using TLS, the encryption key and cipher must be agreed on and exchanged. Afterwards, they can create a connection and exchange data securely. Exchanged information can't be altered during transmission because even the simplest alteration would invalidate it [1].

Firmware and data protection is more complicated compared to securing the network; firmware and data are stored in the microcontroller's storage units like flash, EEPROM, OTPROM, and others. Information stored on the microcontroller should be protected from both alteration and copying. As mentioned, microcontrollers not only store data in their flash chips; they also store the firmware, which contains program code for execution. If the firmware isn't protected enough, anyone with the correct equipment can easily read the contents of the firmware and use professional tools for disassembling and decompiling the code [2]. This brings an issue: if the flash content of the microcontroller isn't encrypted, an attacker can easily change a part of data or firmware to change the microcontroller's behavior however they want. In some cases, encryption is only used for the data

that's stored on the microcontroller, not for the whole firmware. But this isn't the correct approach because if the program code or firmware is understood by the attacker, they can easily figure out how to decrypt the data. The correct approach is to encrypt the whole flash storage so the decryption process happens when the microcontroller starts running the code. The encryption key must be stored in OTP memory (e.g. eFuse) and this section of memory can't be accessed or changed with the help of external devices [1]. This will allow us to have a secure boot mechanism combined with tamper protection.

Integrity checks are also essential for security and reliability. If the protection from ROM dumping (reading the flash storage of a microcontroller to a file) or flashing (writing to the flash storage of a microcontroller from a file) can't be prevented for a particular microcontroller [2], hashing could be used for integrity checking. Using a hash for securing a microcontroller from executing modified firmware is one of the most basic ways to protect firmware from third-party modifications. Before the microcontroller starts to run the code stored in the flash, it will first calculate the hash value of the whole firmware image. If the hash doesn't match the expected value, the system won't start. If hashing is used for integrity checking, there are a couple of nuances to be considered. Complicated hash algorithms can be computationally expensive for some low-power microcontrollers, but simple hash algorithms can easily be figured out, so algorithm complexity should be selected according to microcontroller specifications. Well-known unsalted hash algorithms are risky to use because an attacker can predict the algorithm and generate a new hash for modified hardware. The expected hash value should be stored outside of firmware; this could be a separate EEPROM or the last sector of flash. It should be noted that this approach won't encrypt the firmware, so an attacker can read and disassemble the firmware, then remove the hash check code. Hashing algorithms are widely used for verifying firmware images, combined with other security measures.

Failsafe mechanisms are mostly used for reliability rather than security. Life-critical equipment such as self-driving vehicles, airbags, airplane controllers, medical devices, and others needs to be prepared for failure scenarios. There are specific microcontroller architectures that are designed with fail-safe mechanisms built-in [3]. Microcontrollers with built-in hardware level failsafe mechanisms are better for life-critical equipment, but they are more costly compared to other microcontrollers. Software failsafe mechanisms could be used as a substitute for standard microcontrollers. A well-known failure point for computer equipment (even though it's not common) is bit-flips in RAM caused by cosmic rays [4]. Specialized microcontrollers have ECC (Error Correction Code) memory for fixing any bit-flips caused by cosmic radiation. Hardware connected to the microcontroller can also fail or malfunction, so software failsafe mechanisms should detect these and take immediate action for safety and security.

**Keywords**: microcontroller, security, encryption, firmware.

## References

1. Gedeon, A. S., Buttyán, L., & Papp, D. F. (2020). Secure boot and firmware update on a microcontroller-based embedded board. Faculty of Electrical Engineering and Informatics,

Department of Networked Systems And Services, Budapest University of Technology And Economics.
2. Obermaier, J., Tatschner, S. (2017). Shedding too much light on a microcontroller's firmware protection. In 11th USENIX Workshop on Offensive Technologies (WOOT 17).
3. Mariani, R., Kuschel, T., & Shigehara, H. (2010, January). A flexible microcontroller architecture for fail-safe and fail-operational systems. In Proc. of the HiPEAC Workshop on Design for Reliability.
4. O'Gorman, T. J. (1994). The effect of cosmic rays on the soft error rate of a DRAM at ground level. IEEE Transactions on Electron Devices, 41(4), 553-557.

## QUANTUM SECURE INSTANT MESSAGING: REVISITED

**Ahmet Faruk Dursun[1], Kübra Seyhan[1], Barış Kaan Aydın[2], Sedat Akleylek[1,3,4]**

[1]Ondokuz Mayıs University, Department of Computer Engineering, Samsun, Turkey

[2]Rönesans Holding, Ankara, Turkey

[3]Cyber Security and Information Technologies Research and Development Center, Ondokuz Mayıs University, 55139, Samsun, Turkey

[4]University of Tartu, Tartu, Estonia

e-mail: faruk.dursun@bil.omu.edu.tr, kubra.seyhan@bil.omu.edu.tr, bariskaan.aydin@ronesans.com, sedat.akleylek@bil.omu.edu.tr

**Abstract.** In this paper, a new post-quantum secure end-to-end encrypted instant messaging application is developed as an extended version of [1]. Advanced Encryption Standard (AES) is used for end-to-end encrypted instant messaging. To have quantum secure key exchange for AES, the PQC-Library [2] is used. In this application, with the help of PQC-Library, lattice-based CRYSTAL-KYBER, SABER and NTRU algorithms are used for post-quantum secure key agreement. The implementation details are discussed. According to the experimental results, while the NTRU algorithm has the lowest memory usage, it reaches maximum energy usage level. CRYSTAL-KYBER shows the best performance in terms of running times. Finally, SABER and CRYSTAL-KYBER present approximately the same CPU usage level and give better results than NTRU.

**Introduction.** The security of today's public-key cryptosystems (PKC) will be broken in the presence of large-scale quantum computers with Shor algorithm. In 2016, the National Institute of Standards and Technology (NIST) announced a call to standardize post-quantum secure public-key algorithms. In the first round, there were 82 algorithms in the encryption, KEM, and digital signature categories [3,4]. As a result of the evaluations, standard algorithms were announced on July 5, 2022. NIST announced CRYSTALS-KYBER as the standard KEM algorithm. CRYSTALS-Dilithium, Falcon and SPHINCS+ algorithms are declared as standard digital signature algorithms.

Today, one of the usage areas of public-key cryptosystems is messaging applications. Ensuring the post-quantum security of these applications is one of the open problems in the literature. Although

the most suitable algorithms are the NIST's algorithms, there are no versions of these algorithms compatible with mobile devices yet. In this paper:

- The main aim is to develop an end-to-end encrypted instant messaging application using the PQC-Library [2] for the post-quantum era.
- By extending the idea of [1], the post-quantum secure key sharing requirement of AES protocol is provided with PQC-Library.
- Finally, an post-quantum secure end-to-end encrypted instant messaging application compatible with Android devices is developed.

**Post-Quantum Secure End-to-End Encrypted Instant Messaging Application**

To develop a post-quantum secure end-to-end encrypted instant messaging application, the PQC-Library [2] is used**.** This application is developed in Java as it is the native language of Android. Android Studio Bumblebee (2021.1.1) environment and OpenJDK-13 Java development kit are used. Post-quantum **s**ecure key agreement is realized by selecting any algorithm from the PQC-Library, such as SABER, NTRU, and CRSYTAL-KYBER. The external libraries used in the development of the instant messaging application are given as follows:

- **Firebase Real-Time Database:** It is used to perform real-time messaging.
- **Firebase Authentication:** It is used for users to login and register to the application.
- **Firebase Storage:** It is used to store the media files sent by the users from within the application.
- **Android Picasso:** It allows the viewing of media files sent by users.

Using the PQC-Library, the developed application has three basic components presented in Figure 1.

- **Login & Register:** With the KEM algorithm selected from the PQC-Library, key sharing and storage operations are performed between the parties. The user's public key and personal information are sent to the database. The generated secret key is stored in the device's memory.
- **User List:** It is the interface where all users in the application are listed. The public key information of the users is kept in the user model.
- **Messaging:** It is the interface where end-to-end encrypted instant messaging takes place. In practice, the sender and receiver communicate encrypted using the shared key obtained with the KEM. The sender encrypts the message with the AES algorithm by using the shared key. It sends it to the other side. Then, by using the shared key in the AES decryption algorithm, the receiver obtains the plaintext from the ciphertext. In summary, end-to-end encrypted instant messaging is performed with post-quantum secure KEM algorithms.

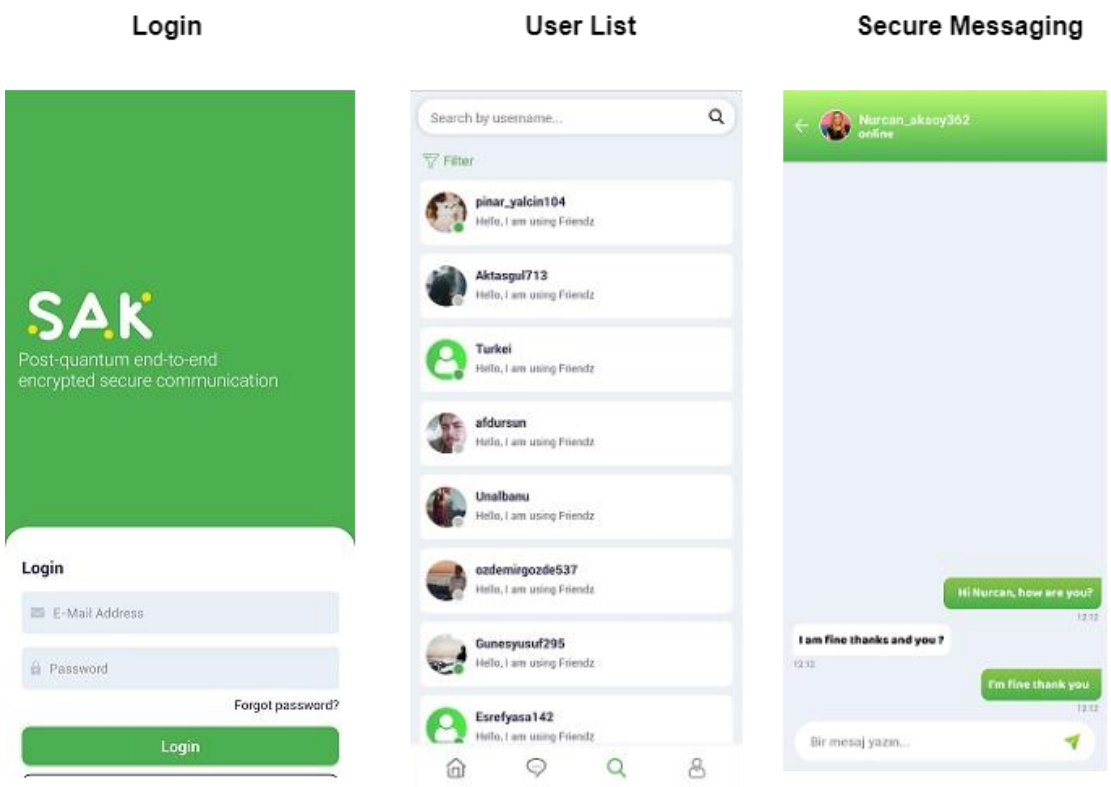



**Figure 1.** Application Interface Components

**Conclusion.** In this paper, a post-quantum secure end-to-end encrypted instant messaging application is developed. A solution is proposed for post-quantum secure communication of Android devices by adding the PQC-Library. The post-quantum secure key sharing is provided by choosing the KEM algorithm from the PQC-Library. An end-to-end encrypted instant messaging application is constructed using the AES protocol and post-quantum secure lattice-based KEM.

**Acknowledgements.** This research was partially supported by TUBITAK under Grant No. 121R006.

**Keywords:** post-quantum cryptography, post-quantum secure messaging, end-to-end encrypted messaging, android secure messaging application.

## References

1. Dursun A.F., Seyhan K., Akleylek S., End-To-End Encrypted Instant Message Application of Post-Quantum Secure Key Encapsulation Mechanisms For Mobile Applications, International Conference on Science, Engineering Management and Information Technology SEMIT 2022-Sep, pp. 48-49, Ankara, Turkey.
2. Dursun A.F., Seyhan K., Akleylek S., Mobil Cihazların Kuantum Sonrası Güvenliği İçin Uyarlanmış KEM Uygulamaları, IEEE International Conference on Information Security and Cryptology -ISC Turkey 2022, pp. 31-37, 20 September 2022, Ankara, Turkey.

3. Akleylek S., Seyhan K., Kuantum Bilgisayarlar Sonrası Güvenilir Kafes Tabanlı Kriptosistem Temellerine Giriş, Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık Cilt II, Eds: Sağıroğlu, Ş., Şenol, M., Ankara, Türkiye: Grafiker Yayınları, ch. 5, pp. 172-209, 2019.
4. Akleylek S., Seyhan K., Kuantum Bilgisayar Çağında Kriptosistemlere Bir Bakış. Siber Güvenlik ve Savunma-Blokzincir ve Kriptoloji. Eds: Sağıroğlu, Ş., Akleylek, S. Ankara, Türkiye: Nobel, ch. 6, pp. 239-276, 2021.

## INFORMATION SECURITY AND CYBER WARS: THE ROLE OF THE STATES AND THE RATIONAL BEHAVIOR OF SOCIETY

**Ramid S. Huseynov**
Military Institute after named Heydar Aliyev, Baku, Azerbaijan
e-mail: ramidhuseynov82@gmail.com

**Information security and Cyber wars: a conceptual approach.** When we consider that information is a very powerful weapon in our modern society, we realize how important it is to control and use it. Sometimes information warfare is no less effective than military warfare. In many cases, it can even surpass it. That is, enemy countries use the information resources they have, destroy the important information system of the other side, seriously affect the military-political-social environment, the thinking of the society [5].

Thus, the digital world, which is called the cyber world as a reflection of the struggle between individuals and institutions, is also becoming an environment where international struggle is actively experienced. This transformation in wars also changes the concept of a strong or weak state. Today, it is not enough for a state to be considered strong if it has an army with classic weapons and a large number of human resources. A state is considered strong to the extent that it can keep pace with technological development, isolate itself from threats around it and play a deterrent role. Because the damage that could be done in decades of attacks in the past can be done with a single computer at a hundred times lower cost.

This growing threat leads to a decrease in corporate reputation [2], which is a reflection of the image of enterprises and institutions in society, and a decrease in trust in organizations and companies engaged in online business. Today, cyber wars have reached a level ranging from simple information theft activities to the neutralization of a large nuclear reactor, from the landing of a drone to the collision of large passenger aircraft. It can even cause serious damage to the state's management structure.

In general, cyber warfare is defined as actions by one nation state to penetrate, damage, or disrupt the computers or networks of another nation state. The main actors of cyber warfare are nation states. But when we examine the events taking place in our modern world, it becomes clear that cyber wars are not only between states, but also non-state elements target various objects.

In an increasingly connected world, the establishment of effective cyber security mechanisms is of great importance. Excessive use of technology creates addiction and increases security risks [2]. This situation calls for global as well as individual and national cybersecurity precautions. Cyber threats, which have become one of the most important and effective threats today, are second only to nuclear threats due to their asymmetric structure [3]. This situation both increases the interest of countries in cyber defense and causes them to spend a significant amount of money. To counter the emerging risks, users traditionally use mechanisms that reduce threats, such as intrusion detection systems, as well as try to develop the worldview of society and increase rational behavior.

**The role of the state in information security and the rational behavior of society.** Let's try to explain the issue with a theoretical approach. Despite the fact that certain restrictions were imposed during the war period from the security point of view, the independence and freedom of the mass media in general is a characteristic feature of democratic societies. Also, meeting the information needs of each individual is an important condition for the information society. That is, correct, objective and timely information of citizens during wars is important in terms of preventing them from being influenced by the enemy's misinformation and preventing negative actions. Because the correct implementation of the state's information policy is very important from the point of view of the security of both the management system and society as a whole. In other words, in parallel with the protection of democratic principles and human rights, ensuring the information security of the state should be parallel. This can have a positive effect on ensuring efficiency.

The behavior of the Azerbaijani state and society during the Second Karabakh War can be shown as a practical explanation of the issue. The implementation of the war not only on the military front, but also on the political-diplomatic level, on the information platform, gave its results. In parallel with the struggle of the Azerbaijani army against the concrete enemy, the Armenian army and Armenian terrorists, the interview of the society and the country's leadership on the political level - to the representatives of the world's most influential news agencies, TV channels, and press bodies, and even answering provocative and biased questions is of quite serious importance for the war period. had [5]. Because the attacks, misinformation, and fake news of the Armenian media, both from Armenia and in different countries of the world, on the information space of Azerbaijan were aimed at influencing the socio-psychological condition of the army and society, and weakening the spirit of war. Also, he aimed to draw the attention of the world community to Armenia and help him. One of the important goals of disinformation was to blame Azerbaijan in this case, to gain the support of the international community, and to increase political pressure from the other side, even though they used terrorist and mercenary soldiers. With this, Armenia tried to compensate for its military defeat by gaining an advantage in the information war.

If we take into account that during the war, the majority of the Azerbaijani society demonstrated maturity in the direction of information security protection, correct transmission of information and propagation of truths. From the first day, every individual realized that this is important not only for the security of the state, but also for the society. Compared to the period during the military conflicts that occurred in 2016, the preventive steps taken by the state to ensure

information security during the Patriotic War in 2020 were accepted as normal by the society. Adequately, the part of the society with a sufficient political outlook was able to use the information correctly and rationally and behave sensitively with it.

Thus, as a result, it can be concluded that modern wars are becoming more of a technology race. Countries' technology and economic power also shape wars. Currently, many different actors besides armies are establishing themselves on the battlefield. Terrorist organizations and criminal groups have started to play a greater role. From this point of view, the nature of wars is formed according to the purpose of those groups. Now, countries are looking for ways to paralyze the enemy's entire technological infrastructure by using a cyber attack to inflict damage in a conventional war that will last for years. This leads to the conclusion that in the future, cyber wars and hybrid wars will be more dominant.

**Keywords:** cyber security, cyber war, information security, cyber crime, national security

**References**

1. Basaranel B.U., Turkshen U. (2019). Counter-terrorist financing law and policy: an analysis of Turkey, Routledge, UK, 310 p.
2. Güleryüz İ., Dalkılıç O.S. (2019). A research to determine the effect of corporate social responsibility projects on corporate reputation, International social sciences studies journal, 5 (33), pp. 2089-2098.
3. Hajoary P.K., Akhilesh K.B. (2019). Role of government in tackling cyber security threat, Smart technologies, Springer, Singapur.
4. (ITU), International Telecommunication Union, https://www.itu.int
5. Huseynov R. (2021), The Patriotic War revealed new approaches in information policy, https://ikisahil.az/post/221132-veten-muharibesi-informasiya-siyasetinde-yeni-yanashmalari-ortaya-qoydu-sherh

## ИССЛЕДОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СЕТЯХ ОБСЛУЖИВАНИЯ

**Балеми Исмайлов**
Национальная Академия Авиации, Баку, Азербайджан
e-mail: balemi@rambler.ru

Работа посвящена исследованию системы безопасности информации (СБИ) от несанкционированного доступа в сетях обслуживания. При этом рассматриваются проблемы, характерные для систем с потерями, с ограниченными и неограниченными объемами буферной памяти (БП) [1, 2, 3]. Предлагается сравнительный анализ результатов разработанных аналитических и имитационных моделей СБИ с потерями, с ограниченным и неограниченным объемом БП.

Анализ проблемы в области информационной безопасности и разработки СБИ указывает на наличие серьезных трудностей, которые во многом связаны с отсутствием единой системы оценки защищенности информации, позволяющей дать количественную оценку при проектировании и эксплуатации сети обслуживания. На ранних этапах проектирования подготавливаются результаты с целью построения СБИ, являющиеся оптимальными значениями структурных характеристик СБИ в пределах допустимых потерь запросов. Этими характеристиками являются: количество параллельно работающих приборов обслуживания (МЗ), число запросов НСД в системе, время ожидания запросов НСД в очереди, время пребывания запросов НСД в системе. Одной из наиболее очевидных причин нарушения СБИ является умышленный запрос НСД к конфиденциальной информации со стороны нелегальных пользователей и последующие нежелательные манипуляции с этой информацией. Эффективность защиты безопасности информации в сетях обслуживания определяется в основном классом защищенности сети обслуживания, который определяет набор механизмов защиты (МЗ), реализованных в сети. В работах предлагается структура СБИ с потерями (без буфера) [1], с ограниченным [2] и неограниченным [3] объемом буферной памяти, обеспечивающая максимальную информационную безопасность сетей обслуживания путем обеспечения контроля перехода всех запросов НСД через МЗ.

СБИ от НСД представляет собой аппаратно-программный комплекс, взаимодействующий с потоками случайных событий, которые обуславливаются действиями злоумышленников, неправильным распределением прав доступа, использованием несанкционированного программного обеспечения, ошибками в программно-технических комплексах идентификации, аутентификации.

В качестве математической модели СБИ рассматриваются системы массового обслуживания смешанного типа, которые включают предложенные структуры. Во всех этих случаях если один из МЗ свободен, то запрос НСД поступает в этот свободный МЗ, при котором исходный поток НСД разрежается с определенными вероятностями и образует выходной поток. В системе с потерями в случае занятости всех МЗ запрос НСД теряется. А в системах с ограниченными и неограниченными объемами буферной памяти в случае занятости всех МЗ запрос НСД ожидает в очереди в буферной памяти системы до освобождения одного из МЗ, если имеется свободное место в буферной памяти.

Целью работы является сравнительный анализ результатов разработанных аналитических и имитационных моделей СБИ с потерями, с ограниченным и неограниченным объемом БП [1 ,2, 3].

Предполагается, что входной поток информации, то есть запросы НСД, являются простейшими, а время обслуживания подчиняется экспоненциальному, постоянному и Эрланговому законам распределения. Проверки адекватности аналитических результатов, а также подробного анализа характеристик СБИ с потерями, с ограниченными и неограниченными объемами буферной памяти при экспоненциальных входных, экспоненциальных, постоянных и Эрланговых выходных потоков для их различных

значений, с учетом их трудоемкости, осуществлены на основе разработанных имитационных моделей на языке GPSS (General purpose simulation system). В модели рассматривается однофазная многоканальная СМО смешанного типа, в которую на обслуживание поступает пуассоновские входные потоки, а время обслуживания транзактов подчиняется экспоненциальному, постоянному и Эрланговому законам распределения.

В модели при поступлении транзакта в систему с потерями в случае занятости всех МЗ транзакт теряется. А в системах с ограниченными и неограниченными объемами буферной памяти в случае занятости всех МЗ транзакт ожидает в очереди в буферной памяти системы до освобождения одного из МЗ, если имеется свободное место и при наличии свободного прибора обслуживания (МЗ) транзакт получает обслуживание.

Проведены три прогона расчетов по имитационной модели. Полученные результаты показывают, что для трех случаев анализа с учетом всех транзактов и при наличии допустимого количества транзактов в очереди на входе СБИ коэффициент использования приборов (МЗ) составляет 0,952; 0,861; 0,772 соответственно.

Сравнительный анализ результатов аналитической модели с результатами имитационной модели показывает, что они хорошо согласованы и отклонение этих результатов находится в допустимых пределах 2…7%. Полученные результаты могут быть использованы при модификации существующих или построении новых СБИ в сетях обслуживания различного назначения.

**Ключевые слова:** системы безопасности информации, системы с потерями, с ограниченным и неограниченным объемом буферной памяти, механизм защиты, несанкционированный доступ, системы массового обслуживания, время обслуживания.

**Литература**

1. Исмайлов Б.Г. Анализ системы безопасности информации в сетях обслуживания объектов нефтегазодобычи. Автоматизация в промышленности. №3, 2020, с.16-19.
2. Исмайлов Б.Г. Моделирование системы безопасности информации в сетях обслуживания объектов нефтегазодобычи. Автоматизация в промышленности. №7, 2020, с.23-26.
3. Исмайлов Б.Г. Анализ системы безопасности информации с неограниченным объемам буферной памяти в сетях обслуживания. Проблеми інформатизації та управління, 65(1), 2021.

## Study of the information security system from unauthorized access in service networks

The work is devoted to the study of the information security system from unauthorized access in service networks. At the same time, problems are considered that are typical for systems with losses, with limited and unlimited buffer memory. A comparative analysis of the results of analytical and simulation models of a loss information security system with limited and unlimited buffer memory is proposed.

# İNFORMASİYA TƏHLÜKƏSİZLİYİ SİSTEMLƏRİNƏ ÜMUMİ BAXIŞ

**Anar İsmayılov, Bahar Nəzərova**
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
e-mail: anar.ismayilov@aztu.edu.az

İnformasiya təhlükəsizliyi sisteminin arxitekturası, informasiya aktivlərini qorumaq üçün mövcud informasiya təhlükəsizliyi təhdidlərinə qarşı durmağa və informasiya təhlükəsizliyi risklərini azaltmağa yönəlmiş texniki qorunma vasitələri və təşkilati tədbirlərin məcmusudur.

İTS-nin arxitekturası bir neçə əsas prinsipə uyğun olmalıdır:

1. Müdafiə anlayışını dərindən təcəssüm olunması. Bu bir firewall quraşdırmaqla bütün informasiya təhlükəsizliyi problemlərini həll etməyəcək.
2. Əməliyyat və diaqnoz etmənin asan olması. Səhv konfiqurasiya edilmiş qaydaya görə pozulmuş proqramların funksionallığını dərhal bərpa etmək üçün mərkəzləşdirilmiş idarəetmə sisteminə çıxışın itdiyi zaman məlumat mərkəzinə müraciətə tələsmək lazım deyil [1, 2].

İTS-nin əsas komponentləri bunlardır:

- perimetr mühafizə vasitələri (firewalllar, məlumat sızmasından qorunma sistemləri, poçt mühafizə sistemləri, müdaxilənin aşkarlanması və qarşısının alınması sistemləri, veb proqramlarını qorumaq üçün firewalllar, şəbəkə sandboxları, kompüter şəbəkəsinə təhlükəsiz uzaqdan girişin təşkili vasitələri, DDoS hücumdan müdafiə sistemləri );
- kriptoqrafik məlumatların mühafizəsi vasitələri (CIPF);
- server infrastrukturu və iş stansiyasının mühafizəsi vasitələri (antivirus həlləri, verilənlər bazası mühafizə vasitələri, host sandboxları, host,girişə nəzarət alətləri);

**Fortinet Təhlükəsizlik Parçası.**

Fortinet tərəfindən hazırlanmış Fortinet İTS-i etibarlılığı və dayanıqlılığı təmin etmək üçün səlahiyyət verən təhlükəsizlik yanaşmasını həyata keçirir. İstehsalçı hərtərəfli şəbəkə mühafizəsini təmin etmək üçün informasiya təhlükəsizliyi həllərini təklif edir: son nöqtələr, şəbəkə elementləri, giriş nöqtələri, məlumat mərkəzi və proqramlar [4].

Fortinet Security Fabric Fabric-Ready Partner Programına daxil edilmiş üçüncü tərəf məhsullarını əlavə edə bilər.


**Şəkil 1.** Fortinet Security Fabric konsepsiyası

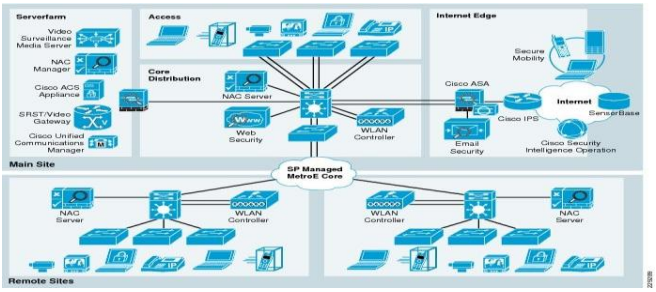
Fortinet Security Fabric yanaşması şəbəkə vəziyyətinin görmə qabiliyyətini artırır və real vaxt rejimində təhlükənin sürətli aşkar edilməsini təmin edir. Bundan əlavə, şəbəkənin hansı hissəsinin risk altında olmasından asılı olmayaraq mühafizə vasitələrinin əlaqələndirilmiş cavabını başlamaq və sinxronlaşdırmaq mümkün olur.

**Cisco SAFE arxitekturası.**

Cisco SAFE (Müəssisə üçün Təhlükəsizlik Arxitekturası) arxitekturası təhlükəsizlik məhsullarının düzgün yerləşdirilməsi və Cisco-nun platformalararası imkanlarının səriştəli istifadəsi sayəsində hər cür hücum vektorlarına qarşı dərin mühafizə və müqavimət təmin edir [5].

Cisco SAFE arxitekturasının əsas prinsipləri bunlardır:

- Dərin müdafiə (müdafiələr müxtəlif səviyyələrdə və arxitekturanın müxtəlif nöqtələrində yerləşdirilir);
- modul infrastruktur (bütün infrastruktur müxtəlif funksional təyinatlı modullara bölünə bilər);
- nasazlıqlara dözümlülük və fəlakətlərə dözümlülük (interfeys ehtiyatı, klasterləşmə, yol kənarları və s.);




**Şəkil 2.** Cisco SAFE arxitekturası.

**"Təhlükəsizlik kodu".**

Şirkətin məhsulları son stansiyaların və serverlərin, şəbəkə perimetrinin, müasir virtual infrastrukturların və işçilərin mobil cihazlarının qorunmasını təmin edir [3, 5].

Şirkətin əsas fəaliyyət istiqamətləri bunlardır:

- Şəbəkə təhlükəsizliyi — Continent APKSh, Continent TLS, Continent WAF, Continent AP, Continent IDS (IPS), həmçinin Continent Control Center İdarəetmə Mərkəzinə əsaslanan öz mərkəzləşdirilmiş idarəetmə sistemi.
- Son nöqtənin (cihazın) qorunması - SecretNet, Sobol.
- Virtual mühitlərin qorunması - vGate.
- Mobil platformaların qorunması - Continent AP, Continent TLS.

**Açar sözlər:** İnformasiya sistemləri, təhlükəsislik məsələləri, İTS-in arxitekturası, cisco safe arxitekturası, təhlükəsizlik kodları.

**Ədəbiyyat**

1. Qasımov V.Ə., İsmayılov A.Ə. Müasir bank sektorlarında kibertəhlükəsizlik strategiyalarının analizi, İnternational conference on Information security: problems and prospects, 29 October, 2021, Azerbaijan University.
2. Qasımov V.Ə. İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq. Monoqrafiya. Bakı. Elm, 2007, 192 səh.
3. Swanson M., Nadya B., Sabato J., Hash J., Graffo L. Security Metrics Guide for Information Technology Systems. National Institute of Standards and Technology Special Publication, No. 800–55, 2003.
4. Vaughn R., Henning R., Siraj A. Information Assurance Measures and Metrics: State of Practice and Proposed Taxonomy. Proceedings of 36th Hawaii International Conference on System Sciences (HICSS-03), 2003.
5. Alberts C., Dorofee A. Managing Information Security Risks: The OCTAVE Approach. Addison Wesley Professional, 2002.

**Review of the information security systems**

The article talks about the architecture of the information security system (ISS) from the point of view of technical means of protection, defines its components, classifies and compares the architecture of ISS.

## KRONECKER SUBSTITUTION FOR LATTICE-BASED CRYPTOGRAPHIC IMPLEMENTATIONS

**Melike Karatay[1], Erdem Alkım[2], Urfat Nuriyev[1]**

[1]Ege University, İzmir, Turkey

[2]Dokuz Eylül University, İzmir, Turkey

e-mail: karataymlk9@gmail.com, erdemalkim@gmail.com, urfat.nuriyev@ege.edu.tr

The National Institute of Standards and Technologies (NIST) in the USA recently announced that they have selected one key encapsulation protocol, Kyber [4], together with three electronic signature schemes, namely Dilithium [6], Falcon [8], and SPHINCS [3] as their new standard for internet security [1]. Three of the selected protocols are based on lattice problems, and they use arithmetic operations over some polynomial rings to provide smaller keys and efficient implementations. The only key encapsulation protocol, Kyber, is based on the module version of the Learning With Errors (MLWE) problem. The module uses matrices and vectors of polynomials in $\mathbb{Z}_q[x]/(x^n+1)$, where $q = 3329$, and $n = 256$ for the proposed parameter sets of Kyber. The polynomial multiplication is always performed as one of the inputs has coefficients that are uniformly random in $(0, q-1)$, and the other one has very small coefficients with respect to $q$.

Although NIST provides standards, new algorithms can only be used when they have software and hardware implementations on various platforms. Although deploying software implementations is easy, deploying new hardware implementations of dedicated hardware accelerators for new algorithms is not that easy. Thus, in this paper, we will focus on efficient implementations of lattice-based cryptosystems using hardware accelerators that are developed for accelerating multiplications of big integers. To be able to use big integer multipliers to perform polynomial multiplication one can use Kronecker Substitution (KS), which is a method to transform polynomial multiplication into big integer multiplication and vice versa [9].

There are four versions of the algorithm, KS1, KS2, KS3, and KS4 [7]. The main problem is to find the smallest representation that the result can be recovered and these algorithms mainly differ in the way they handle this problem. KS1 is the plain version of the algorithms and for multiplication of two $n-1$ degree polynomials $f$ and $g$ where $f_i$, $g_i$ in $(0,2^c)$, it requires that each coefficient should be encoded in $\lceil \log(f_i g_i) \rceil = 2c + \lceil \log(n) \rceil$ bits. Thus after multiplications of $n$ pairs of coefficients added together to calculate one coefficient of the output polynomial, there will be no carry bit passed to the next coefficient. The bit length in the conversion of a big integer with KS2 is $1/2.\lceil \log(f_i g_i) \rceil = c + 1/2.\lceil \log(n) \rceil$. As can be seen from here, KS2 performs its operations by halving the bit length. The difference between KS2 from KS1 is that it chooses a negative evaluation point as well as a positive evaluation point. The coefficients of the even-degree terms of the product polynomial are found using a positive evaluation point; coefficients of odd-degree terms are found using a negative evaluation point. Another version is the KS3 algorithm. The KS3 algorithm also halves the bit length like the KS2 algorithm. The other evaluation point is selected by taking the positive evaluation point and the inverse of this point. The coefficients are the elements of the shift addition operation that allow us to obtain the evaluated results. KS4 algorithm combines KS2 and KS3 to reduce the size further by requiring 4 multiplications instead 2 [7].

The use of the hardware accelerators for big integer multiplication in lattice-based cryptography was first introduced in [2], authors proposed efficient polynomial multiplication by using 2048-bit integer multiplication based on KS1 combined with Karatsuba Multiplication and based on KS2 combined with School book multiplication to calculate a complete result. The authors pointed out that the implementation of packing/unpacking operations in KS3 is complex because it requires a large number of bit shifts, and they do not use it because their platform is not conducive to efficient bit shifting. In [10], authors combined 2048-bit KS1 and toom-cook multiplication, in addition, the authors report comparisons of different choices for KS and outer multiplication algorithms. Lastly, in [5], authors proposed an NTT-based splitting algorithm for big integer multiplication instead of reducing the evaluation point of the polynomial.

In this paper, we will focus on KS2 and KS3 algorithms for performing polynomial multiplication $f.g$ where $f_i < 2^{13}$ and $g_i < 2^4$ show that 128 coefficients of the input polynomials can be fitted in 2048-bit integer which is convenient because our test platform, ESP-WROOM32, is capable to multiply two 2048-bit integers and return 4096-bit. In Table 1, we compared our results with results from [10] since we target the same platform.

**Table 1**. Comparison of performance KS1Mul, KS2Mul, KS3Mul

| Implementation | Degree | Size | Packing(bits) | Cycles |
|---|---|---|---|---|
| KS1Mul [10] | 64 | 2048 | 32 | 10.310 |
| KS2Mul [10] | 64 | 1536 | 24 | 30.555 |
| KS3Mul [our work] | 128 | 2048 | 16 | 25.746 |

As can be seen in Table 1 our implementation completes multiplication of 128 coefficients of target polynomials in time that is about the time required by 2.5 KS1 based implementation from [10]. Since the target polynomial ring has 256 coefficients, KS1 implementation requires 9 multiplication via two recursive calls to the karatsuba-based polynomial multiplication [10]. On the other hand, our KS3 implementations can calculate the full result with one level of karatsuba-based algorithm means that we only need 6 calls to the coprocessor. The number of big integer multiplications can further be reduced to 4 by utilizing KS4 algorithm, which we left this implementation as future work.

**Keywords:** Kronecker substitution, lattice-based crypto, ESP32, efficient implementation.

## References

1. Alagic G., Apon D., Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J., Miller C., Moody D., Peralta E., Perlner R., Robinson A., Smith-Tone D. & Liu Y. K. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process. National Institute of Standards and Technology, Gaithersburg.
2. Albrecht M.R., Hanser C., Hoeller A., Pöppelmann T., Virdia F., & Wallner A. (2018). Implementing RLWE-based schemes using an RSA co-processor. Cryptology ePrint Archive.
3. Bernstein D.J., Hopwood D., Hülsing A., Lange T., Niederhagen R., Papachristodoulou L., ... & Wilcox-O'Hearn Z. (2015, April). SPHINCS: practical stateless hash-based signatures. In Annual international conference on the theory and applications of cryptographic techniques (pp. 368-397). Springer, Berlin, Heidelberg.
4. Bos J., Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schanck J. M., ... & Stehlé D. (2018, April). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 353-367). IEEE.
5. Bos Joppe W., Joost Renes, and Christine van Vredendaal. "{Post-Quantum} Cryptography with Contemporary {Co-Processors}: Beyond Kronecker, {Schönhage-Strassen} & Nussbaumer." 31st USENIX Security Symposium (USENIX Security 22). 2022.
6. Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., & Stehlé D. (2018). Crystals-dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 238-268.
7. Harvey D. (2009). Faster polynomial multiplication via multipoint Kronecker substitution. Journal of Symbolic Computation, 44(10), 1502-1510.

8. Kiningham K., Levis P., Anderson M., Boneh D., Horowitz M., & Shih M. (2019, November). Falcon—A flexible architecture for accelerating cryptography. In 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) (pp. 136-144). IEEE.
9. Kronecker L. (1882). Grundzüge einer arithmetischen Theorie der algebraische Grössen.
10. Wang B., Gu X., & Yang Y. (2020, October). Saber on ESP32. In International Conference on Applied Cryptography and Network Security (pp. 421-440). Springer, Cham.

## TOWARDS PRACTICAL CRYPTOANALYSIS OF SYSTEMS BASED ON WORD PROBLEMS AND LOGARITHMIC SIGNATURES

**Yevgen Kotukh, Gennady Khalimov**
Kharkiv National University of Radio electronics, Kharkiv, Ukraine
e-mail: yevgenkotukh@gmail.com, hennadii.khalimov@nure.ua

Practical achievements in the creation of quantum computers led to consider feasibility to implement practical attacks on complex or difficult-to-solve math problems. The word problem [1] is one of such math problem. One of the first implementations of a cryptosystem based on the word problem was proposed by Magliveras [5] using logarithmic signatures for finite permutation groups and further proposed by Lempken et al. for asymmetric cryptography with random overlays [2]. The novelty of this idea lies in spreading a difficult word problem to many groups. The first implementation of such a cryptosystem was proposed for the Suzuki group under the name $MST_3$. Several improvements $MST_3$ with the Suzuki group were made so far. In 2010, more secure cryptosystem $eMST_3$ was proposed by adding a secret homomorphic cover. In 2018, a general method for constructing strong aperiodic logarithmic signatures for Abelian p-groups, which is a further contribution to the practical application of cryptosystems $MST_3$ was proposed. Attacks on a cryptosystem $MST_3$ in its basic design led to its compromise. The basic element of the cryptosystem $MST_3$ is logarithmic signatures - a special type of factorization [4].

Methods of generating logarithmic signatures significantly affect the security of the structure [5]. Our base group is the Suzuki 2-group over the field $\mathbb{F}_q$, where $q=2^m$. A general attack needs to find a size $q$ f or success: we fix $m=81$, such that this general attack becomes irreproducible. Note that the public key is already quite long when $m=81$: in the most efficient case we consider (see example 1 below), we need more than 19,000 bits to store the non-identifier elements in logarithmic signatures $\alpha$ and $\gamma$. Our methods are essentially independent of the automorphism $\theta$ in the definition of the Suzuki 2-group, so we fix $\theta$ it as equals to the quadratic automorphism in all our experiments. We construct our logarithmic signature $\beta$ and generate logarithmic signatures of the type

$(r_1, r_2, ..., r_s)$ where $\prod_{i=1}^{s} r_i = 2^m$ . Note that integers $r_i$ must be small enough to store logarithmic signatures efficiently. It suffices to consider logarithmic signatures that have an additional property: the elements $\beta_{i1}$ are equal to one, that is, we generate $\beta$ with this property from the beginning, and no generality is lost when generating logarithmic signatures in this way. We consider the success of the attack only if we obtain a valid private key after applying a small number of guessing attempts $t'$ under the initial conditions for $t$ as a consequence of what $\beta$ - bijectively. Then we choose $t'$ randomly under these conditions.

Recall the notation $S(a,b)$ for an element in the Suzuki 2-group defined in [2]. Based on the remarks in [8], we believe that $t = S(x,0)$ , where $x \in \mathbb{F}_q$ is unknown, and therefore we restrict our conjecture to $t'$ the form $S(y,0)$ for some $y \in \mathbb{F}_q$ . The conditions on $t$ , which we obtain, are $\mathbb{F}_2$ – linear conditions, so it is easy to choose $t'$ , which satisfies these conditions randomly. The exact conditions on $t$ , which we obtain, will depend on the number of components $r_i$ of type $\beta$ 2 equal to 2: when there are many such components, the condition we obtain is weaker. For this reason, we present three cases to illustrate our methods. In example 1 $r_i = 2$ for everyone $i$ In this case, we do not find conditions on $t$ , but simply randomly choosing a small number of values for $t'$ leads to a successful attack. In example 2 $r_i \neq 2$ for everyone $i$ In this case, we find that each condition we get restricts us $t'$ to such a small number of possibilities that a trivial exhaustive search can be performed. Example 3 , with approximately half of the components of type $\beta$ , equal to 2, illustrates an intermediate case. Here, each condition limits the number of possibilities to $t'$ significantly (about the $2^{40}$ possibilities). Very few guessing attempts $t'$ can simultaneously satisfy two of these conditions, so combining the two conditions allows an equivalent private key to be obtained by a trivial exhaustive search.

Let $t = S(x,0)$ , where $x \in \mathbb{F}_q$ is given randomly. We build $\gamma$ in $MST_3$ -way and define

$$\gamma_{i2} = \beta_{i2} t^{-1} \alpha_{i2} t = S(0, d_{i2}) S(x, x^{\theta} x) S(e_{i2}, f_{i2}) S(x,0) = \quad = S(e_{i2}, d_{i2} + f_{i2} + e_{i2} x^{\theta} + e_{i2}^{\theta} x) =: S(e_{i2}, g_{i2})$$

and choose $\gamma = [C_1, ..., C_{81}]$ where $C_i = \{1, \gamma_{i2}\}$ . The attack is implemented as follows. Let $t' = S(y,0)$ there be a random attempt to guess $t$ . We form $b = [B_1, ..., B_{81}]$ where $B_i = \{1, b_{i2}\}$ and $b_{i2}$ given as

$$b_{i2} = \gamma_{i2} t'^{-1} \alpha_{i2} t' = S(\mathrm{e}_{i2}, \mathrm{g}_{i2}) S(y, y^{\theta} y) S(e_{i2}, e_{i2}{}^{\theta} e_{i2} + f_{i2}) S(\mathrm{y}, 0) \quad = S(0, g_{i2} + f_{i2} + e_{i2} y^{\theta} + e_{i2}^{\theta} y)$$

If the set $\{b_{i2}\}_{i=1}^{81}$ is linearly independent, then $\overline{b}$ is a bijection , and it follows from [9] that we have an equivalent secret key. If the set is linearly dependent, we repeat this process with a second guess

attempt $t'$. In [ 12 ] , this attack was generated for 10,000 random instances $MST_3$ . The results are shown in Table 1.

**Table 1.** Experimental results

| Number of guesses $t'$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| Frequency | 2829 | 2111 | 1429 | 1048 | 799 | 490 | 374 | 279 | 181 |
| Number guesswork $t'$ | 10 | 11 | 12 | thirteen | 14 | 15 | 16 | 17 | 18 |
| Frequency | 133 | 98 | 66 | 47 | 31 | 26 | 19 | 11 | 5 |
| Number of guesses $t'$ | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| Frequency | 3 | 7 | 7 | 4 | 2 | 1 | 0 | 0 | 0 |

**Conclusions.** Note that until a method of creating secure weak logarithmic signatures is invented, it is $MST_3$ dangerous [6]. Many attacks exploit problems in the basic design using Suzuki-2 groups. Most attacks can be implemented using available computers. Researchers have been able to propose strengthened constructions of cryptosystems $MST_3$ due to the use of generalized groups [7] , automorphisms of groups and groups with enhanced security parameters [8]. In conclusion, we note that until a method of creating secure logarithmic signatures is invented, it is not $MST_3$ safe.

**Keywords:** logarithmic signature, MST3, word problem, public-key cryptography.

## References

1. Kotukh Y., Khalimov G., Hard problems for non-abelian cryptography, 2021: Fifth International Scientific and Technical Conference Computer And Information Systems And Technologies, 2021, pp. 39-40, https://doi.org/10.30837 /csitic52021232176
2. Lempken W.A., van Trung T., Magliveras S.S. Wei public key cryptosystem based he non-abelian finite groups. Journal of Cryptology, 2009, Vol.22(1), pp. 62 –74.
3. Magliveras S., D. Stinson, T. van Trung. New approaches that designing public key cryptosystems using one-way functions and trap-doors in fi nite groups. Journal of Cryptology, 2002, Vol.15, pp. 285 –297.
4. Nuss A. On group based public key cryptography [Electronic resource]: Phd thesis . Access mode http://nbn-resolving.de/urn:nbn:de:bsz:21-opus-63659.
5. Kotukh E., Severinov O., Vlasov A., Tenytska A., & Zarudna E. (2021). Some results of development of cryptographic transformations schemes using non-abelian groups. Radiotekhnika, 1(204), 66–72. https://doi.org/10.30837/rt.2021.1.204.07
6. Kotukh E., Severinov O., Vlasov A., Kozina L., Tenytska, A., & Zarudna, E. (2021). Methods of construction and properties of logarithmic signatures. Radiotekhnika, 2(205), 94–99. https://doi.org/10.30837/rt.2021.2.205.09
7. Khalimov G., Kotukh Y., Khalimova S. MST $_3$ Cryptosystem Based on a Generalized Suzuki 2-

Groups [Electronic resource] Access mode : http://ceur-ws.org/Vol-2711/paper1.pdf
8. Khalimov G., Kotukh Y., Khalimova S. MST3 cryptosystem based he the automorphism group of the hermitian function field. IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 – Proceedings , 2019, p . 865 - 868.

## DEVELOPMENT OF A LAYOUT FOR HACKING AN INDUSTRIAL COMPUTER USING THE HID ATTACK METHOD

**Igor Nevliudov, Vladyslav Yevsieiev, Svitlana Maksymova**
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine
e-mail: igor.nevliudov@nure.ua, vladyslav.yevsieiev@nure.ua, svitlana.milyutina@nure.ua

The introduction of advanced information technologies within Industry 4.0 (I4.0) has led to the rapid development of production, using digital approaches to managing technological processes, which are reflected in the Industrial Internet of Things (IIoT) [1-3]. But, unfortunately, the introduction of automated control systems using digital data transmission methods has entailed all the software and network vulnerabilities with which an attacker can gain access not only to confidential data, but also to gain access to the management of technological processes, which can cause shutdown of the production process and even a man-made disaster. A striking example is the attack by the Stuxnet virus through a vulnerability in the Simatic WinCC SCADA control system, as a result of which a large number of uranium enrichment centrifuges were disabled, which were controlled by Variable requency Drive (VFD) or in 2014 production files were stolen using software vulnerability at the Korean NPP [3]. As a result, the study of software and hardware tools with which attackers can gain access to production control systems or / and copy confidential data is a priority task to identify vulnerabilities in production systems.

In this paper, the authors conduct research on the vulnerability of industrial computers at different levels of PLC/SCADA/ERP/MES production control using HID attacks. A feature of this method is direct access to an industrial terminal (industrial computer) at any level, which is a rather difficult task, but at the same time this attack method is not determined by an antivirus or internal protection systems, and it takes a minimum amount of time to complete it (~ 1-2 sec). The block diagram of HID attacks to investigate the vulnerability of production computers running OS Windows 10/11 is shown in Figure 1. Denote by 1 the way a malicious algorithm is triggered by which an attacker can implement: copying and sending / deleting files via the Internet to a specified IP address, removal/adding of users and administrators of the attacked computer, as well as access to the local network of the enterprise.

For hardware implementation of the HID attack, the Arduino Pro Micro microcontroller module based on the ATmega32U4 microcontroller [4] will be used. On the basis of which the

following algorithm will be implemented, which will use the PowerShell vulnerability to transfer the specified files to an external server at a specific IP address. The generalized algorithm is shown in Figure 2.

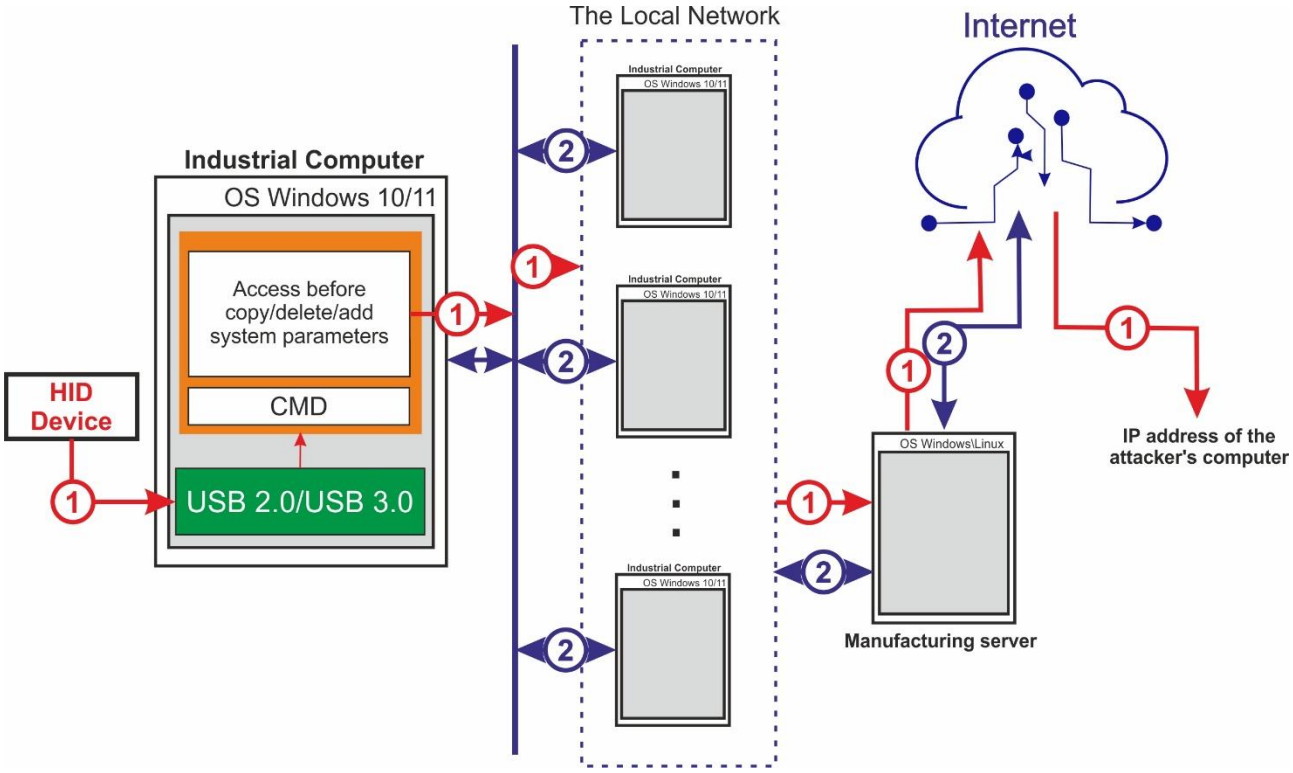



**Figure 1**. Structural Diagram of HID Attacks for Investigation the Vulnerability of Production Computers Running OS Windows 10/11

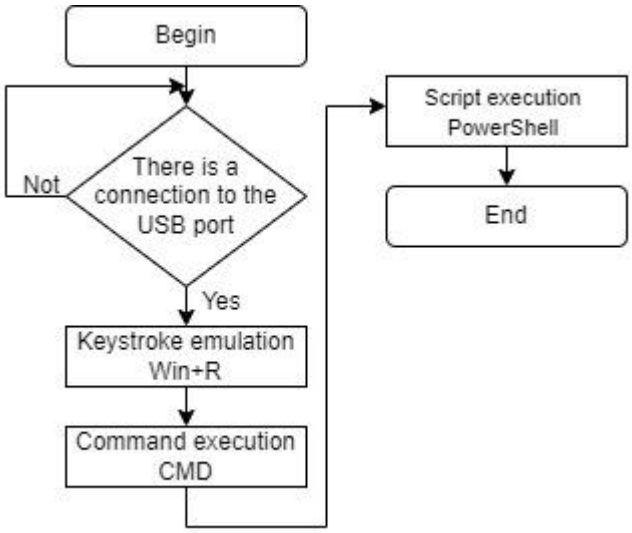



**Figure 2**. Generic HID Algorithm - Vulnerability Attacks in PowerShell

Let's describe some of the functions of HID-attacks implementation using the Arduino Pro Micro, in the Arduino IDE development environment. An example of implementation of the void winRun() functions for calling the command line (Win+R) is shown below:

```
Keyboard.press(KEY_LEFT_GUI);
Keyboard.press('r');
delay(30);
Keyboard.releaseAll();
delay(100);
```

A malicious script that will exploit a PowerShell vulnerability and make it possible to copy data to a remote server at the IP address http://1.2.3.4:8080/ using port 8080 is shown below:

```
powershell.exe -nop -w hidden -c $N=new-object net.webclient; $N.proxy=[Net.WebRequest]::GetSystemWebProxy();$N.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $N.downloadstring('http://1.2.3.4:8080/');
```

**Conclusions.** This example shows the possibility of a subtle vulnerability of industrial computers using the HID-attack method. With this type of malicious script, you can use more complex and malicious actions, making or opening access to configuration production files. It also makes it possible to create fake accounts with administrator rights (root), while modern antiviruses and protection systems do not perceive such types of attacks, believing that this is initialized by the user. A feature of this implementation is the ability to dynamically exploit different vulnerabilities and change the content of the script depending on the operating system of the victim. The execution time of the attack takes from 2-4 seconds, while it is almost impossible to quickly identify the source of the attack and the place of penetration.

**Keywords:** HID-attack, Industry 4.0, manufacturing systems, cyber security.

## References

1. Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry, 137, 103614. https://doi.org/10.1016/j.compind.2022.103614
2. Abu-Jassar A.T., Attar H., Yevsieiev V., Amer A., Demska N., Luhach A.K., & Lyashenko V. (2022). Electronic User Authentication Key for Access to HMI/SCADA via Unsecured Internet Networks. *Computational Intelligence and Neuroscience*, 2022, Article ID 5866922. https://doi.org/10.1155/2022/5866922
3. Nevliudov, I. et al. (2021). GUI Elements and Windows Form Formalization Parameters and Events Method to Automate the Process of Additive CyberDesign CPPS Development. Advances in Dynamical Systems and Applications, 16(2), 441-455.
4. Pro Micro Compatible ATmega 32U4 5V Micro USB Board Arduino 16MHz Leonardo. [Type of medium]. Available: https://www.ebay.com/itm/255283295146?hash=item3b7011f3aa:g:4XsAAOSwEVlb9wGE

# COMPARATIVE ANALYSIS OF MEANS FOR SUPPRESSING UNAUTHORIZED SPEECH RECORDING

**Anatoly Oleynikov, Volodymyr Pulavskyi, Oleksii Bilotserkivets**
Kharkov National University of Radio Electronics. Kharkov, Ukraine
e-mail: anatoly.oleynikov@nure.ua

Dictaphones, or in modern realities, any sound recording devices, are a dangerous threat in the acoustic channel of information leakage. It is enough for an attacker to enable recording on his smartphone in order to obtain information without authorization.

Currently, there are enough technical means to ensure the confidentiality of acoustic information at the facility. Usually, a technical tool is a relatively compact device that will help you keep your conversation private. Unfortunately, some manufacturers of such protection devices use marketing technologies that are impractical to use in the field of protection. These actions lead to the fact that the buyer, and then the user, will become a victim of unauthorized language recording. Therefore, in order to prevent this situation, the user must understand which method is used in his protection tool.

To date, we have three main methods of combating unauthorized speech recording, which are the acoustic suppression method, the electromagnetic suppression method, and the ultrasonic method.

Among these methods, the acoustic one is less difficult to implement. The essence of the method is based on the creation of an acoustic obstacle that will be directed in the direction of the likely location of the recording device. This method is considered ineffective due to the fact that interlocutors during the operation of this acoustic interference begin to speak louder, thereby increasing the amplitude of the signal that needs protection. Also, this method has a negative effect on the psychological state of the interlocutors.

The electromagnetic method is based on sending a high-frequency amplitude-modulated pulse signal to the sound recording device. This signal is received by conductors and elements of the recorder circuit, these elements create random antennas. These interference signals affect subsystems of sound recording devices that are responsible for converting acoustic signals. The electromagnetic method is effective against almost all household audio recording devices, but the development of the circuit-technical base of the elements and the use of shielding greatly reduces the effectiveness of this method. Today, most modern smartphones have a high level of shielding, which significantly reduces the impact of the electromagnetic method.

The ultrasonic method involves irradiating the sound recording device with powerful ultrasonic vibrations. Quite a large number of sound recording devices use electret microphones, their upper limit of bandwidth is 25-27 kHz [1]. Due to this, the bandwidth of the microphone falls into the ultrasonic range and the recording device is vulnerable to powerful ultrasonic vibrations, which will make it impossible to record a useful speech signal.

The ultrasonic method has two implementation options. Single-frequency suppression affects the automatic gain control system, which reduces the sensitivity of the recording device. With two-frequency suppression, two signals are created with different carrier frequencies that coincide with the speech range (0.3-3.4 kHz). These signals carry out energizing hiding of the useful signal in the sound recording path. The ultrasonic suppression method is not at all effective if the recording device works only in the speech range, has a filter that limits the input signal band, or the device is protected by a special material that does not pass ultrasonic vibrations.

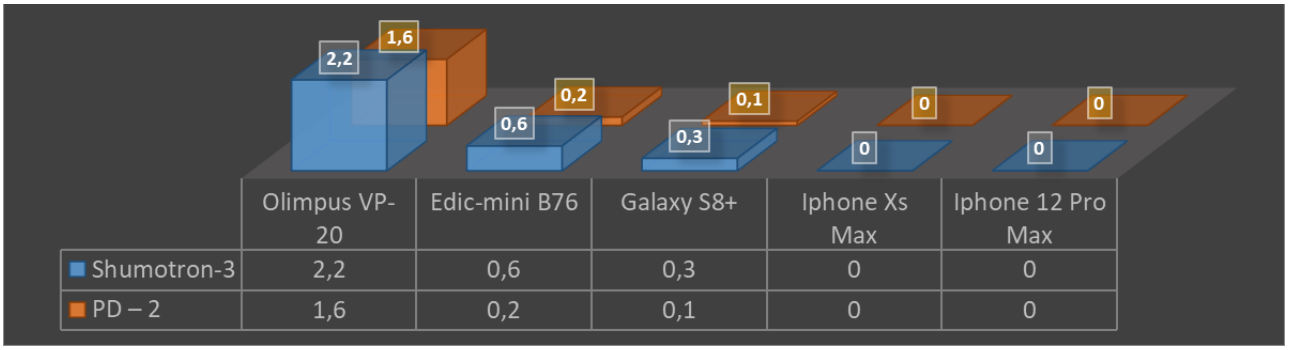
Analyzing the suppression methods presented in the article, we conclude that without knowing the type of sound recording device, it is impossible to ensure the confidentiality of the speech signal. To increase the protection against unauthorized recording of a speech signal, it is proposed to use an adaptive acoustic method [2].

The method differs from the usual acoustic one in that the interference is created on the basis of the speech of the interlocutor himself, and such interference is difficult to filter because it occupies the same frequency band as the speech signal. The distance between the source of interference and the recording device should be less than the distance between the source of the speech signal and the recording device. We can check the effectiveness of the adaptive method in an experimental study.

An experiment was conducted to evaluate the effectiveness of the adapted acoustic method of suppressing unauthorized speech recording using an obstacle formed by an electrostatic emitter. During the experiment, a comparison of technical parameters of means of protection against unauthorized speech recording was carried out. These means of protection are built on the basis of the methods analyzed in this article.

Adaptive acoustic (EST-ST, EST-P), electromagnetic (Shumotron-3, PD-2) and ultrasonic (USPD-C, UltraSonic-50) suppression methods were used. Suppression occurred for five modern types of sound recording devices, namely digital voice recorders and smartphones (Olimpus VP-20, Edic-mini B76, Galaxy S8+, Iphone Xs Max, Iphone 12 Pro Max.). The results of the experiment are presented in figures 1-3.

Figure 1 shows the distance in meters of complete suppression of voice recorders when using "Shumotron-3" and "PD-2" electromagnetic suppressors.




| | Olimpus VP-20 | Edic-mini B76 | Galaxy S8+ | Iphone Xs Max | Iphone 12 Pro Max |
|---|---|---|---|---|---|
| Shumotron-3 | 2,2 | 0,6 | 0,3 | 0 | 0 |
| PD – 2 | 1,6 | 0,2 | 0,1 | 0 | 0 |

**Figure 1.** Electromagnetic suppression.

Figure 2 shows the distance of complete suppression of voice recorders when using ultrasonic suppressors.

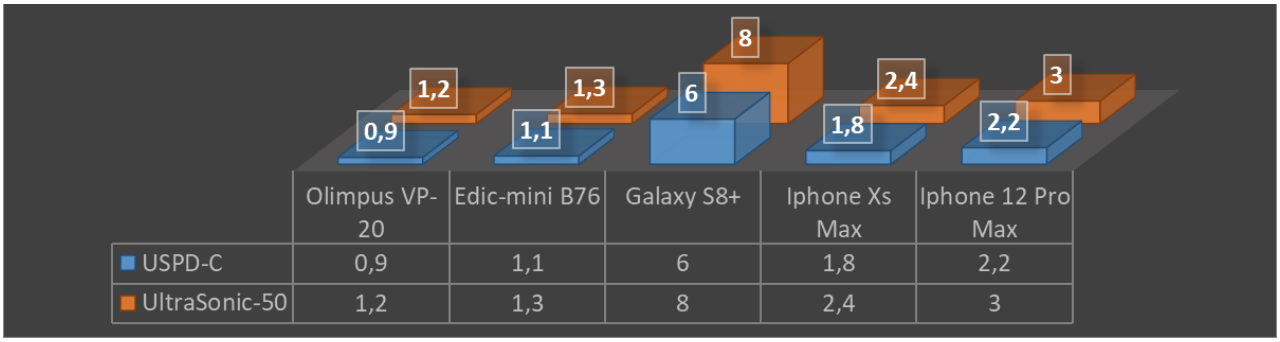



**Figure 2**. Ultrasonic suppression.

Figure 3 shows the full suppression distance of the recorders when using the "EST-ST" and "EST-P" suppressors.

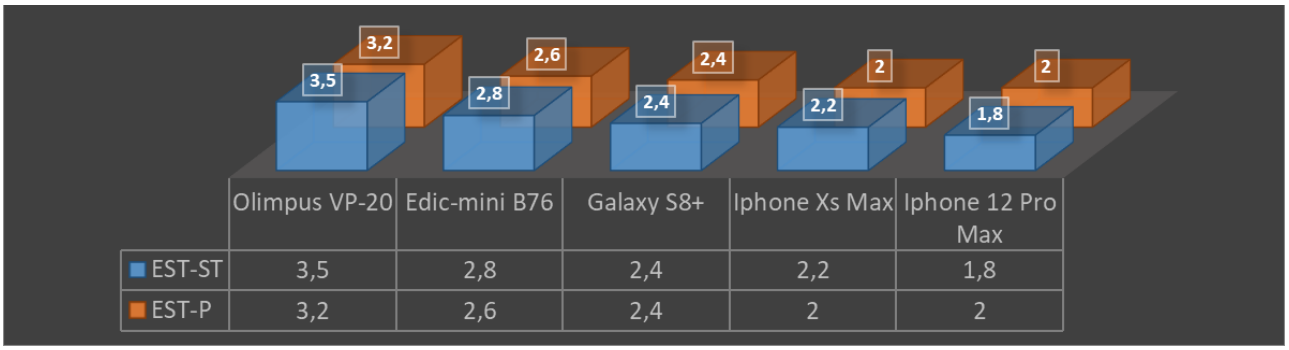



**Figure 3.** Suppression by adaptive method.

**Conclusions**. Analyzing the results of the experiment, we conclude that the adaptive acoustic method is the most effective. The effectiveness of the method is ensured not only by the range of suppression, but also by the fact that the method uses the same functional channel as the useful signal, which makes it possible to counteract all means of recording, regardless of their type.

## References

1. Олейников А.Н., Пулавский В.А., Кривенко М.А. Ультразвуковые методы защиты речевой информации. Радиотехника: Всеукр. межвед. науч.-техн. сб.-Харьков: 2012. Вып. 169. с.176-181.
2. Олейников А.Н., Пулавский В.А., Цыбулевский П.В. Оценка эффективности акустического противодействия несанкционированной записи на диктофон. Современная защита информации. Киев: 2010-№1, с. 8-16.

# ATTACKS AND COUNTERMEASURES IN AUTONOMOUS VEHICLES

**Selahattin Özdemir**
Ondokuz Mayıs Üniversitesi, Turkiye
e-mail: selahattin.ozdemir@gsb.gov.tr

**Abstract.** In this article, the levels of autonomous driving, one of the basic concepts of autonomous vehicles, are explained. Within the scope of autonomous vehicle elements, electronic control units, sensors and in-vehicle networks have been discussed in detail. Subsequently, information was given about VANETs within the scope of communication technologies. With the rapid development of digital technology in the world, there have also been developments in autonomous vehicles. Accordingly, With The Spread Of Autonomous Vehicles, The İmportance Of Safety Has İncreased, Which indicates that there are higher safety requirements. That is why many security researchers have worked on attacks and defenses for autonomous vehicles. However, there has been no systematic research on attacks and defenses against autonomous vehicles. In this review, we analyzed previously conducted academic studies on attack and defense, described in the article, from 2015 to 2022, for a systematic and comprehensive review of autonomous vehicles. We have classified autonomous attacks as autonomous control and driving system components and communication technologies. Defense against such attacks was classified as security and intrusion detection. Due to the development of big data and communication technologies, techniques for detecting an attack are gradually being improved. We offer inferences based on our systemic research, in which future research on autonomous attacks and defenses is strongly combined with the main component of technology. Finally, in this study, deficiencies in the studies examined are identified. Thus, a perspective is provided for future studies on autonomous vehicle safety.

**Introduction.**

With the advent of autonomous vehicles, safety concerns have occurred. For this reason, research has been conducted on attacks and defenses against autonomous vehicles. However, although there are many articles about attacks and defenses related to autonomous vehicles, no comprehensive compilation has been made [1].

In this study, we reviewed the literature from 2015 to 2022 and examined the attack and defense technologies related to autonomous vehicles. We focused on research results that meet certain criteria. We searched Google Academic for specific keywords such as "autonomous vehicles", "cyber", "autonomous", "attack", "defense", "vehicle" and "security". We have selected recently published articles for the attack and defense categories.

**Table 1.** Query Sentences And Search Fields

| Database | Query | Query Field |
|---|---|---|
| Google Scholar | autonomous vehicles, cyber, autonomous, attack, defense, vehicle, security | all fields |

The contributions of this work are as follows:

• The research for attacks and defenses against autonomous vehicles is organized in a chronological order, which briefly and succinctly shows the technologies used over time.

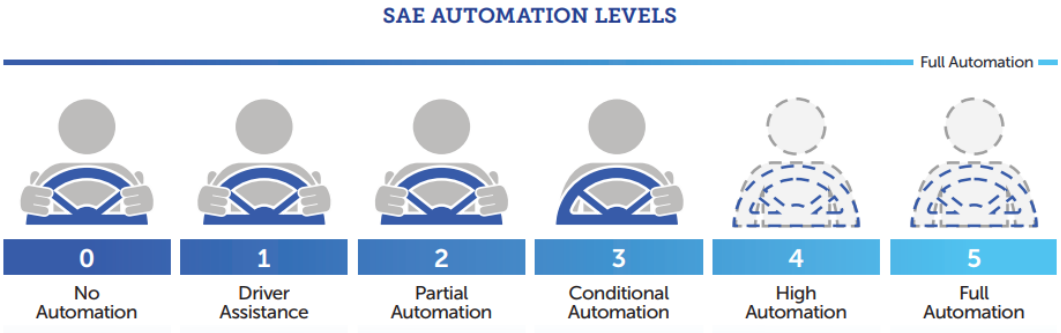
• articles on attacks and defenses against autonomous vehicles from 2015 to 2022 have been summarized.

• Thanks to a comprehensive study of attacks on autonomous vehicles, it can be observed that attacks on autonomous vehicles in the future will increasingly target communication technology, rather than other simple elements of vehicles.

• The research trend in autonomous vehicle security has shown that artificial intelligence with big data is being used to defend against autonomous vehicle attacks.

**Autonomous vehicle levels**

Autonomous driving levels were stated by the Society of Automotive Engineers in 2014 [2]




*Layer 0:* This is the level at which the entire responsibility lies with the driver.

*Layer 1:* It is the level at which control is partially relinquished.

*Layer 2:* It is the level at which we can completely stop driving our vehicle for a short period of time.

*Layer 3:* It is the level at which elements such as the face and steering wheel are made without receiving commands from the vehicle thanks to the censors found in the vehicles.

*Layer 4:* This is the level at which the driver is completely free.

*Layer 5:* It represents the fully autonomous vehicle that no longer needs human interaction.

**Autonomous vehicle architecture**

In order to investigate the safety aspects of autonomous vehicles, we have identified two basic elements such as control and driving systems and communication Technologies [3].

| CONTROL AND DRIVING SYSTEMS | | | COMMUNICATIONS TECHNOLOGIES |
|---|---|---|---|
| ELECTRONIC CONTROL UNITS | SENSORS | IN-VEHICLE NETWORKS | VANETs |
| Body Control Unit | Global Positioning System | Local Interconnect Network | V2V |
| Engine Control Unit | Inertial Measurement Unit | Controller Area Network | V2I |
| Anti-Lock Braking System (ABS) Control Unit | Radar | FlexRay | V2X |
| Transmission Control Unit | Lidar | MOST | V2N |
| | Ultrasonic Sensors | Ethernet | V2G |
| | Digital Cameras | | Platooning |
| | | | V2R |

***Control and driving systems*.** The vehicle consists of three different categories: electronic control units, sensors and in-vehicle communication.

***Electronic Control Units***

It consists of an embedded system that controls one or more electrical systems. It gives information about different parts of the vehicle [4].

*Body Control Unit (BCU):* Electronic control is used to control the communication of units.

*Engine Control Unit (ECU):* Controls all functions of the engine.

*Anti-Lock Braking System (ABS) Control Unit (ABS):* The braking system prevents locking by slipping when braking.

*Transmission Control Unit (TCU):* It is used for power transmission to actuators.

***Sensors***

Autonomous vehicles are used to collect information about their surroundings and determine their position on Earth [5].

*Global Positioning System (GPS)*: GPS is a sensor system used to detect the position of the vehicle on the earth at any time of the day and in any weather conditions by means of radio signals broadcast from satellites.

*Inertial Measurement Unit (İMU):* It is used to obtain location information of autonomous vehicles in environments where satellite signals do not reach.

*Radar:* It is a system that allows us to understand, detect or measure the speed of moving or immobile objects that are further away from our visual distance with the help of electromagnetic waves.

*Digital Cameras:* It is used to transfer images of objects around and inside the vehicle to the host computer inside the vehicle.

*Lidar:* Lidar systems determine the distance to obstacles with a laser distance sensor. It is also used to calculate the distance to an object or surface.

*Ultrasonic Sensors:* It is used in the detection of objects and distance measurement with the help of sound waves. Ultrasonic sensors work on the principle of calculating the time elapsed when the sent sound waves hit and return to the surrounding objects.

***In-Vehicle Networks***

They are the protocols used to ensure efficient communication between different components such as electronic control units. Dec [6].

*Local Interconnect Network (LİN):* The LIN protocol is a serial bus system used for low-cost vehicle applications with low bitrate and asynchronous data requirements.

*Controller Area Network* (CAN): It is a message-based protocol that is widely used inside vehicles to send and receive data between electronic control units and sensors Dec.

*FlexRay:* It is a deterministic, and high-speed automotive network communication system protocol for controlling automotive electronic control units.

*MOST (Media-Oriented System Transportation):* MOST is a ring topology developed for infotainment systems that need high bandwidth [7].

*Ethernet:* It is used for infotainment, camera system and diagnosis of electronic control units such as engine, body, chassis.

***Communications technologies.***

They are connections Decked out with communication capabilities to establish communication between vehicles or parts of the transport system.

***VANETs***

They are networks that allow vehicles to communicate with each other and with their surroundings. Private car networks also have different types of communication allowed [8].

*V2V:* It is a smart technology that enables the exchange of vehicle data from one vehicle to another.

*V2I*: It captures data about the situation occurring in traffic and the environment, and then wirelessly transmits information about the conditions so that drivers can drive safely and quickly.

*V2X*: V2X technology makes every car on the road smarter and safer by giving it the power to "communicate" with the traffic system, including other cars and infrastructure.

*V2N:* It provides vehicle-to-vehicle communication over wireless networks.

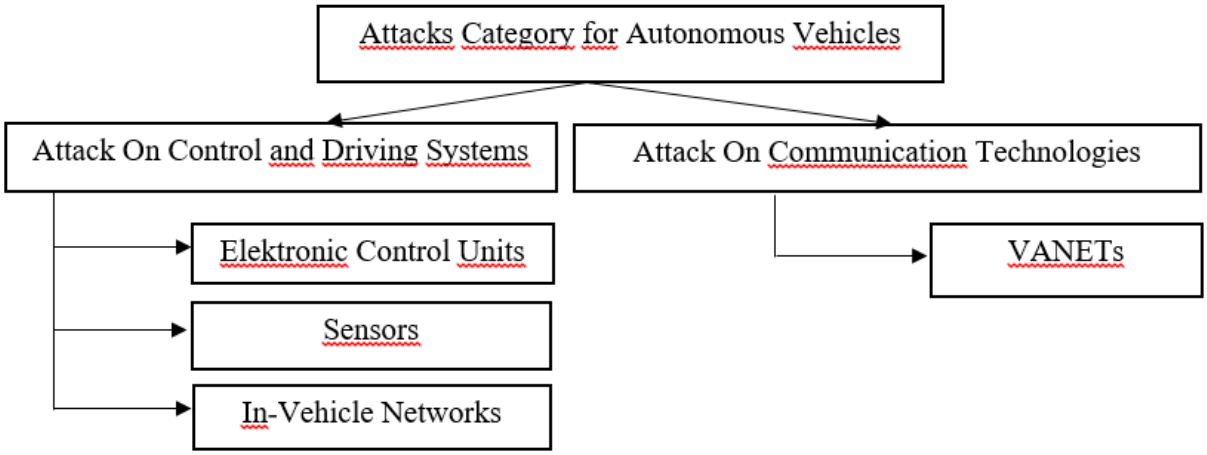
*V2G:* V2G technology focuses on the idea of using batteries (batteries) in electric cars and trucks as a power source in electrical networks based on real-time demands for power.

*Platooning:* A convoy is a group of vehicles that travel safely together. The idea of the convoy is to create a cooperative system through subsystems with which the participating vehicles are compatible.

*V2R:* It collects traffic data from a static detection area along a road and transmits the data to traffic control devices and a central traffic management center.

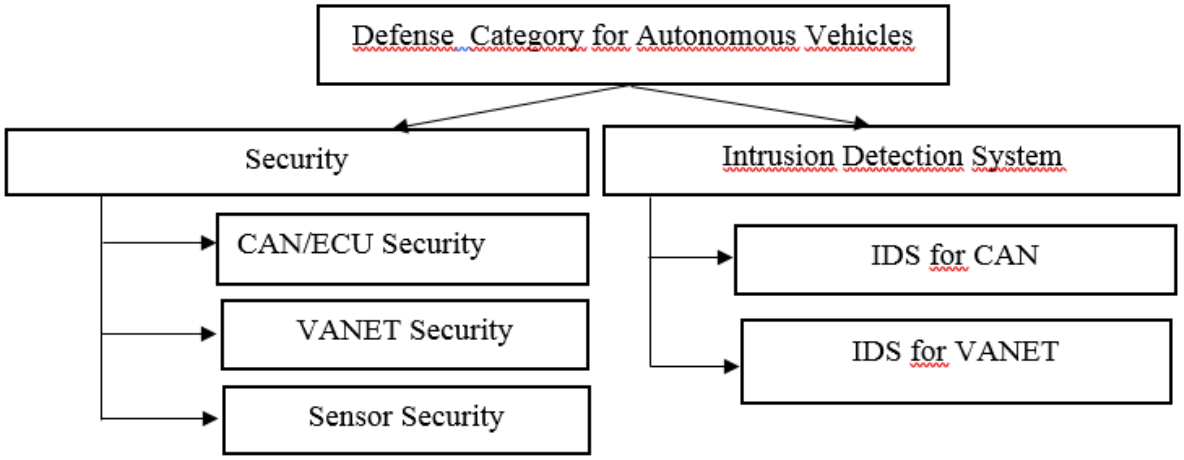
**Cyber attacks on autonomous vehicles**

In this section, we have investigated attacks on autonomous vehicles, classified as attacks on control and driving systems and attacks on communication Technologies [9].




**Defense of autonomous vehicles**

Regarding the security of autonomous vehicles, we have divided the defense literature into the following categories and classified them as security and intrusion detection systems [9].




**Conclusion**

Vehicles and their defense. Recently, the design of risk and possible attack scenarios for vehicles has been studied. The first car attack was an attack on the interior of the car, which primarily involved the ECU and CAN. In recent years, autonomous driving technology has improved, and attacks on communication technologies have been extensively investigated. As defense methods for autonomous vehicles, CAN/ECU security is constantly being researched in areas such as private vehicle network security and sensor security. We know that the networks and protocols currently used in vehicles are insecure, but we restrict ourselves due to the fact that it is difficult to respond quickly to attacks. Therefore, methods for detecting attacks are constantly being studied. Autonomous vehicle security models have been studied from IDS, a traditional security model, to security models that combine technologies. With the current technology, the future of cars will be combined with fully autonomous vehicle functions. Major car brands Volkswagen, BMW, Mercedes-Benz, Nissan,

Hyundai and Toyota are developing autonomous driving technologies, as are IT companies such as Google, Apple and Samsung. In this case, cyber attacks on autonomous vehicles will intensify even more, after which they will have a serious impact on human life and the safety of the city. Security requirements in critical infrastructure help in the creation of security elements of autonomous vehicles of the future. In order to make the world we live in safer; We hope that this paper document will help all researchers working on attacks and defenses related to autonomous vehicles.

**Keywords**: Autonomous vehicle, technology, attack, security research, intrusion detection system.

## References

1. Chowdhury A., Karmakar G., Kamruzzaman J., Jolfaei A., & Das R. (2020). Attacks on self-driving cars and their countermeasures: A survey. IEEE Access, 8, 207308-207342.
2. Yiğit E., Öner A.E., & Yöntem O. (2020). Otonom Araçların Otomotiv Sektörüne Etkileri ve Beraberinde Getirdiği Yenilikler. Avrupa Bilim ve Teknoloji Dergisi, 181-186.
3. Gökozan H., Taştan M. (2018). Akıllı taşıtlar ve kontrol sistemleri. Mesleki Bilimler Dergisi (MBD), 7(2), 58-62.
4. Kurt, H., & Kaymaz, H. In-Vehicle Network for Conventional and Next-Generation Vehicles. Full text book, 31.
5. Yeong D.J., Velasco-Hernandez G., Barry J., & Walsh J. (2021). Sensor and sensor fusion technology in autonomous vehicles: A review. Sensors, 21(6), 2140.
6. Sun J., Iqbal S., Arabi N. S., & Zulkernine M. (2020). A classification of attacks to in-vehicle components (IVCs). Vehicular Communications, 25, 100253.
7. Sumorek A., Buczaj M. (2014). The Evolution of "Media Oriented Systems Transport" Protocol. Teka Komisji Motoryzacji i Energetyki Rolnictwa, 14(3).
8. Avcı İ., Özarpa C., Özdemir M., Kınacı B.F., & Kara S.A. Akıllı Ulaşım Araçlarında Siber Saldırılar Açısından Çok Katmanlı Güvenlik Sisteminin Analizi. Full Text Book, 53.
9. Kim K., Kim J. S., Jeong S., Park J.H., & Kim H.K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. Computers & Security, 103, 102150.

# SÜNİ İNTELLEKT KİBERFİZİKİ SİSTEMLƏRİ NECƏ TƏKMİLLƏŞDİRƏ BİLƏR?

**Asif Paşayev[1], Elçin Həsənov[1,2]**
[1]Azərbaycan Universiteti, Bakı, Azərbaycan
[2]Azərbaycan Respublikasının Prezidenti yanında Dövlət İdarəçilik Akademiyası, Bakı, Azərbaycan
e-mail: asif.pashayev@au.edu.az

Kiberfiziki sistemlər informasiya əsrinin mühüm hissəsidir. Bu cür sistemləri necə dizayn etməyi, təhlil etməyi, qorumağı və təkmilləşdirməyi nə qədər yaxşı başa düşsək, ətrafımızdakı dünyanı bir o qədər yaxşı, təhlükəsiz işlədib, aydın anlaya bilirik. Yuxarıda müzakirə edilən nümunələrdən göründüyü kimi, süni intellekt bütün səviyyələrdə CPS-nin işini təkmilləşdirə bilər və bu iki müvafiq sahənin (AI + CPS) sinerjisi həyatımıza bir çox maraqlı və gözlənilməz təkmilləşdirmələr gətirəcək. Bu yanaşmanın tətbiqi kibertəhlükəsizlik risklərinin təfərrüatların qiymətləndirilməsini təmin edəcək və nəticədə Müdafiənin dərinlikdə strategiyasının həyata keçirilməsi üçün vasitələrin daha ağlabatan seçimini təmin edəcək.

Kiberhücumların vektorunun təhlili nəticəsində ekspert istifadə olunan zəifliklər nəzərə alaraq, bütün mümkün icra ssenarilərini müəyyən edib, hər bir ssenarinin ayrı-ayrılıqda və bütövlükdə kiberhücumların həyata keçirilməsinin təhlükə səviyyəsini qiymətləndirə bilər.

**Giriş**

Kiberfiziki sistemlər nədir, onlar niyə bu gün bu qədər aktualdır və süni intellekt onların inkişafında hansı rol oynayır?

İnformasiya texnologiyaları sistemlərinin müxtəlif xassələrinin, onların fiziki və rəqəmsal komponentlərinin qarşılıqlı əlaqəsinin öyrənilməsi müasir kiberfiziki sistemlər elmində yeni və aktual istiqamətdir.

İstənilən kiber-fiziki sistemin əsas komponentləri bunlardır:

- sistemin fiziki qatı (ən müxtəlif təbiətli real fiziki dünyanın müxtəlif obyektləri);
- sistemin rəqəmsal qatı (kompüterlərin yaddaşında saxlanılan sistem haqqında verilənlər toplusu, fiziki obyektlərin idarə olunması alqoritmləri, informasiyanın emalı alqoritmləri və s.);
- rəqəmsal və fiziki qatlar arasında qarşılıqlı əlaqə üçün interfeys (müxtəlif sensorlar, idarəetmə mexanizmləri və s.);
- insanla rəqəmsal və fiziki təbəqənin qarşılıqlı əlaqəsi (müxtəlif XR texnologiyaları) [1]

Bu komponentlər zaman və məkanda bir-biri ilə qarşılıqlı əlaqədə olur, konkret problemin həllinə yönəlmiş vahid ekosistemi təşkil edir.

Sistemlərin təkamülü nöqteyi-nəzərindən, kiberfiziki sistemlər böyük miqyaslı qranularlığa (artıma, böyüməyə) malik növbəti addımdır, yəni, belə bir sistemin özü bir çox başqa mürəkkəb sistemlərdən ibarətdir.

**Şəkil 1.** Analoq dünyası, e-ticarət və bulud xidmətləri

Kiberfiziki sistem kimi həm nisbətən kiçik obyektlər, məsələn, pilotsuz uçuş aparatı, ağıllı qapalı qurğular sistemi, həm də çox iri miqyaslı obyektlər: təyyarə istehsalı üçün fabriklər və ya hətta bütün şəhərlər hesab edilə bilər.

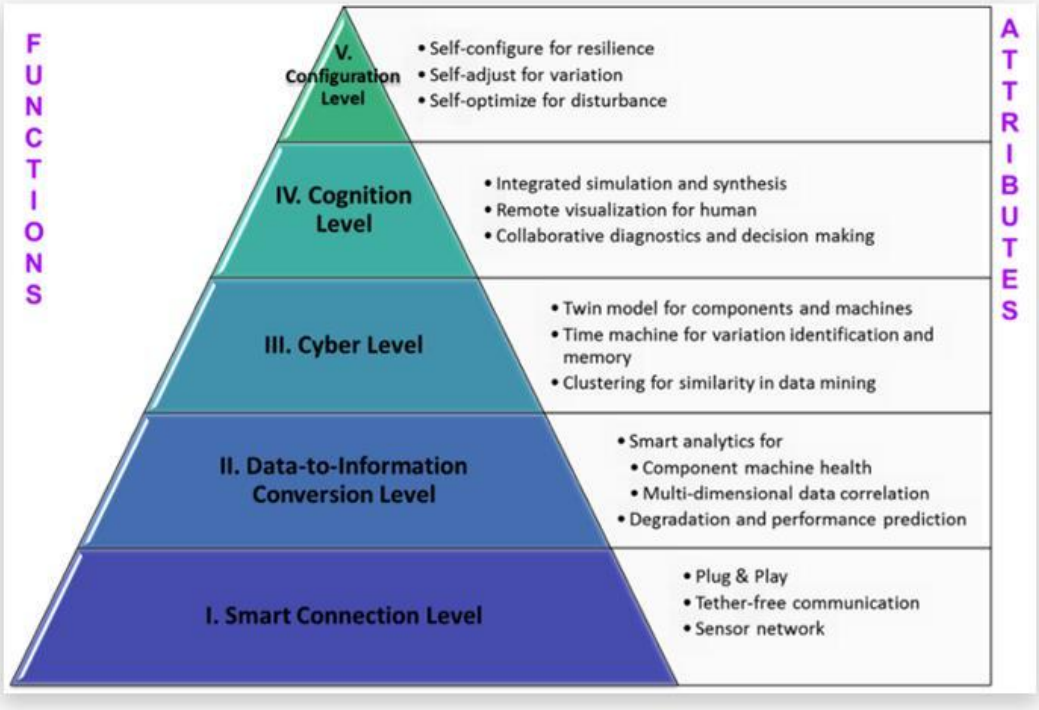
Kiberfiziki sistemlər CPS- (Cyber-physical systems, CPS) dünyanın bir çox laboratoriyaları tərəfindən intensiv tədqiqat obyektidir [2].

Bunlar dünyanın aparıcı universitetlərinin laboratoriyalarıdır: Los-Ancelesdəki Kaliforniya Universitetinin CyPhyLab, MİT media laboratoriyasının bir sıra bölmələri, Bosch, Toshiba və ya PTC kimi texnologiya sənayəsi liderlərinin laboratoriyaları.

**Rəqəmsal təbəqə daxilində real dünya obyektləri arasında qarşılıqlı əlaqə səviyyələri.**

CPS-in əşyaların interneti, ağıllı toz və duman hesablamaları kimi digər informasiya texnologiyaları anlayışları ilə çoxlu ortaq cəhətləri var, misal üçün şəbəkə strukturlarını qeyd etmək olar. Ancaq anlamalıyıq ki, CPS yuxarıda sadalananlardan daha geniş anlayışdır və onlar bütün kiber-fiziki sistemin komponentlərini təşkil edə bilər.

Üstəlik, kiberfiziki sistemin kompozit cihazlarını nəzərə alsaq, digər anlayışlara münasibətdə CPS-də onlar daha yüksək qarşılıqlı təsir səviyyəsindədirlər.




**Şəkil 2.** Rəqəmsal təbəqə daxilində real dünya obyektləri arasında qarşılıqlı əlaqə səviyyələri.

Kiberfiziki sistemlərin həyatımıza təsir dərəcəsini nəzərə alsaq, o zaman sənayə 4.0-a keçidin bu konsepsiyanın reallaşması və mövcud oxşar sistemlərin meydana çıxması ilə bağlı olduğunu söyləmək kifayətdir.

Sənayə 4.0-ın inkişafında liderlərdən biri olan Alman Akademiyası Acatex artıq üç növ şəbəkədən ibarət olan milli kiberfiziki platformaların perspektivlərindən danışır: insanların interneti, əşyaların interneti və insanlara xidmətlər interneti [3].

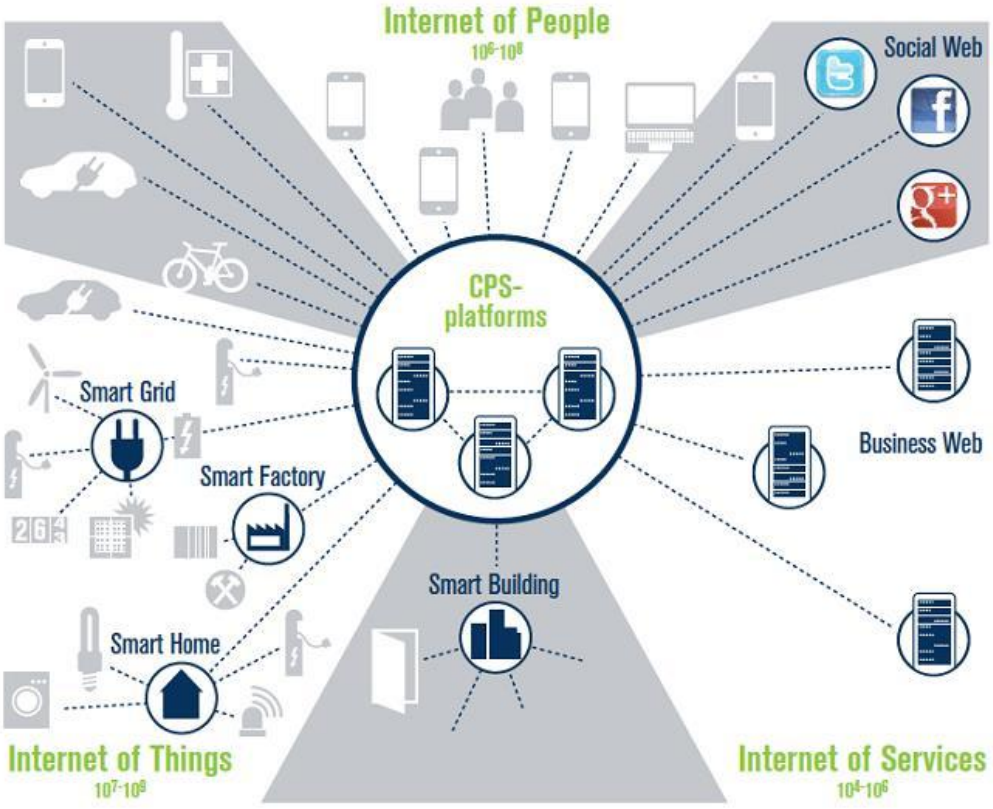
Əgər kiberfiziki platformaların prototiplərindən danışırıqsa, onda bu gün ən uğurlu nümunə Sinqapur dövlətidir ki, burada qanunvericilik səviyyəsində Smart Nation təşəbbüsü qəbul edilib ki, bu da kiberfiziki platforma əsasında sosial və iqtisadi inkişafı nəzərdə tutur.

Amma nəinki Sinqapur kiberfiziki platformalar və sistemlər üzərində fəal işləyir – məsələn, ABŞ-da bu texnologiya 2011-ci ildən ən mühüm strateji texnologiyalardan biri kimi qəbul edilib.

Son zamanlar bütün CPS komponentlərinin işini yaxşılaşdırmaq üçün süni intellekt metodlarından, xüsusən də dərin öyrənmə alqoritmlərindən getdikcə daha çox istifadə olunur. Texnologiyaların bu yaxınlaşması süni intellektin inkişafı üçün zəruri olan böyük miqdarda əlaqə və məlumat yaradır.

Bu yaxınlarda istifadəyə verilmiş 3-cü süni intellekt inqilabına görə, bu gün çox fərqli xarakterli məlumatların işlənməsi üçün kifayət qədər üsullar mövcuddur, istər şəkillər, mətn, elektrik və ya digər xarakterli siqnallar, üçölçülü məlumatlar və s.

Hər gün həm fundamental riyazi səviyyədə, həm də daha təkmil hesablama aparat vahidləri şəklində mövcud dərin öyrənmə alqoritmlərini təkmilləşdirmək üçün yeni alətlər mövcuddur.




**Şəkil 3**. Əşyaların, insanların və xidmətlərin İnternetinin qarışması nəticəsində kiber-fiziki platformalar.

Süni intellekt sahəsinin inkişafı ilə yanaşı, kiberfiziki sistemlər də inkişaf edir, çünki belə sistemlərin işinin keyfiyyəti əsasən sistemdə mövcud olan məlumatların işlənməsinin keyfiyyəti ilə müəyyən edilir.


**Şəkil 4.** Klassik kompüter qrafikası alqoritmləri və neyron şəbəkələrin istifadəsi ilə göstərmə keyfiyyətinin müqayisəsi.

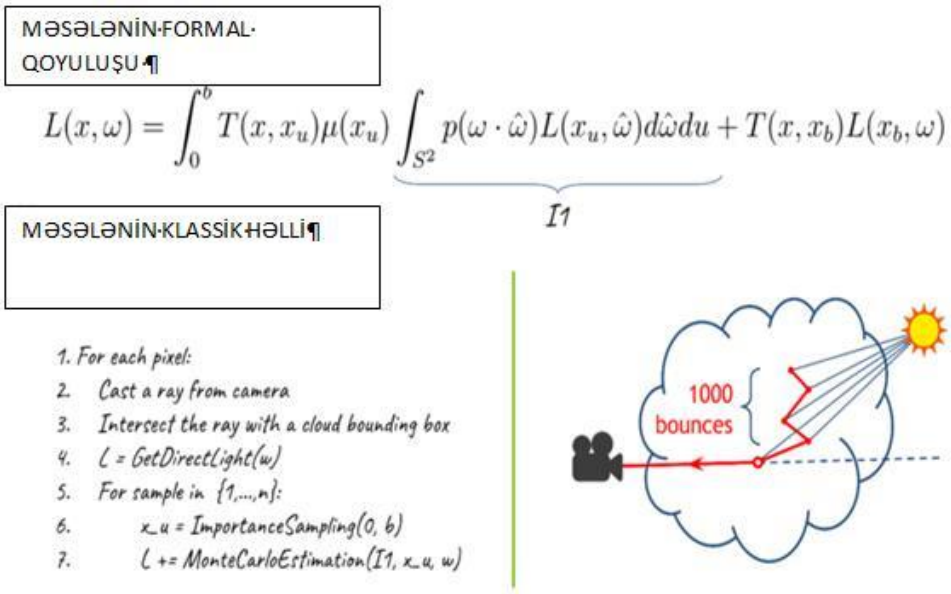
**Süni intellektin rəqəmsal model simulyasiyalarına təsiri.**

Kiberfiziki sistemlərin layihələndirilməsi və istismarı prosesində bir sıra problemlər yaranır. Onlardan biri fiziki obyektlər və onların rəqəmsal modelləri arasında zaman ardıcıllığı problemidir.

Real dünyada obyektləri idarə etmək və onların davranışını proqnozlaşdırmaq üçün, virtual məkanda riyazi modellər əsasında rəqəmsal obrazlar yaradılır.

Belə bir modeli simulyasiya etmək üçün tələb olunan vaxt, simulyasiya edilmiş obyektdə real fiziki proseslərin apardığı vaxtdan fərqli ola bilər. Tez-tez olur ki, riyazi model o qədər mürəkkəbdir ki, kompüter simulyasiya müddəti real olanı üstələyir.

Hesablamaları sürətləndirmək üçün simulyasiyanın keyfiyyətini qorumaqla, dərin öyrənmə üsullarından istifadə etmək təklif olunur.




**Şəkil 5.** Bulud göstərmə probleminin məsələsinin qoyuluşu

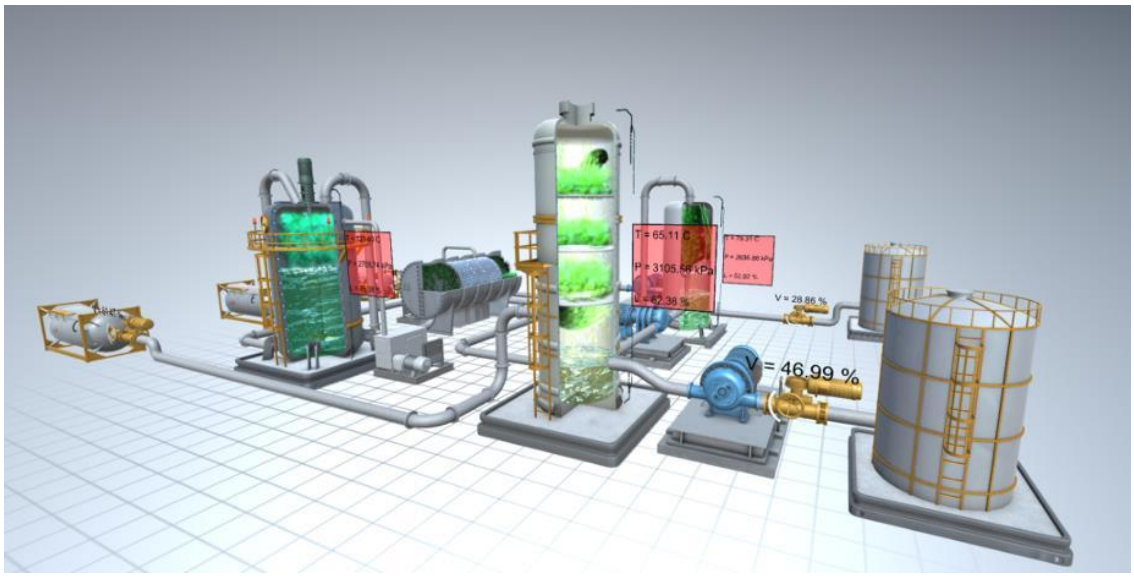
Bu problemi həll etmək üçün ənənəvi yanaşma, 2-ci növ Fredholm inteqral tənliyi olan hesablanmış təsvirin hər pikseli üçün əsas göstərmə tənliyini həll etməkdir.

Bu tip tənliklərin həlli mürəkkəb alqoritmik işdir və çox vaxt tələb edir. Bu halda hesablamaları sürətləndirmək üçün əsas ideya - klassik ədədi metodun ən çox vaxt aparan hissəsinin həllini əvəz edən universal yaxınlaşdırıcı kimi, neyron şəbəkəsindən istifadə etməkdir.[4]

Digər mühüm məsələ CPS-nin təhlükəsizliyinin təmin edilməsidir - kiberfiziki hücumlardan müdafiə sistemlərinin yaradılması, informasiya təhlükəsizliyi sahəsində yeni aktual sahəyə çevrilmişdir.

Gəlin FİGİTALİZM komandası tərəfindən həyata keçirilən PlantSim adlı praktiki işə baxaq. Layihənin əsas məqsədi neft emalı zavodunda texnoloji proseslərə nəzarət edən PLC (proqramlaşdırıla bilən məntiq nəzarətçisi) ilə mühəndislik monitorinqi sistemi (SCADA) arasında rabitə kanallarında anomaliyaların aşkarlanması sisteminin yaradılması olub.

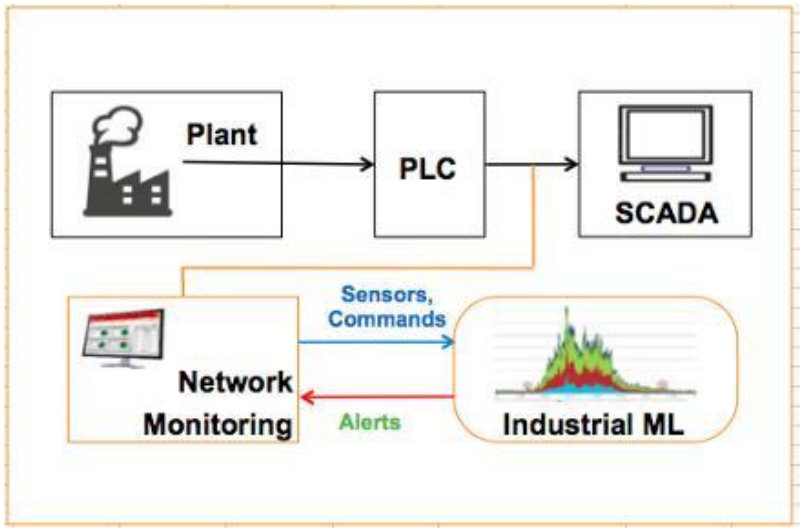
CPS təhlükəsizliyi üçün keşiyində olan AI




**Şəkil 6.** Zavodun rəqəmsal modelində texnoloji proseslərin simulyasiyasının vizuallaşdırılması.

İdarəetmə kanallarında anomaliyaları axtarmaq üçün təkrarlanan neyron şəbəkəsindən istifadə etmək təklif edilmişdir.

Belə bir şəbəkənin hazırlanması üçün məlumat kimi zavodun rəqəmsal modelindən alınan sintetik məlumatlar istifadə olunur. Rabitə kanallarını idarə etmək üçün məntiqi qaydalara əsaslanan ənənəvi həll yolu ilə müqayisədə bu yanaşmanın üstünlüyü süni intellekt sisteminin aşkar edə biləcəyi vəziyyətlərin müxtəlifliyindədir.




**Şəkil 7.** Nəzərdən keçirilən kiberfiziki sistemin blok diaqramı.

Zavodun rəqəmsal modelinin köməyi ilə hətta reaktor partlayışı kimi nadir, lakin potensial təhlükəli vəziyyətləri də nəzərdən keçirmək olar. Əlbəttə ki, mühüm amil sistemin təlimi üçün yeni məlumatların əldə oluna bilmə sürətidir.

**Açar sözlər**: Süni intelekt, əşyaların interneti, xidmətlərin interneti, kiber fiziki sistemlər-CPS.

**Ədəbiyyat**

1. https://habr.com/ru/company/toshibarus/blog/438262/
2. Модель активного мониторинга как основа управления безопасностью промышленных киберфизических систем. Москва, 2016 г, стр. 51-60.
3. Васильев В.И., Кириллова А.Д., Вульфин А.М., Когнитивное моделирование вектора кибератак на основе меташаблонов capec. 2010, стр. 34-41.
4. Нашивочников Н.В., Пустарнаков В.Ф., Топологические методы анализа в системах поведенческой аналитики. 2013 г, стр. 26-36.

## KİBERTƏHLÜKƏSİZLİK SAHƏSİNDƏ PHISING, HACKING, PENTEST, DOS VƏ DDOS PROBLEMLƏRİN PRAKTİK ANALİZİ

**Asif Paşayev, Etibar Məmmədov**
Azərbaycan Universiteti, Bakı, Azərbaycan
e-mail: asif.pashayev@au.edu.az, etibar.mammadov@student.au.edu.az

Hər birimiz gündəlik peşə fəaliyyətimizdə və məişət problemlərimizin həllində informasiya texnologiyalarından müxtəlif səviyyələrdə istifadə etməklə informasiya cəmiyyətinin quruculuğunda bilavasitə iştirak edirik. İnternet əşyaları (İoT) və internet istifadəçiləri, müxtəlif sosial media platformaları artdıqca informasiya təhlükəsizliyi problemləri də getdikcə daha qabarıq formada üzə çıxır. Xüsusilə infrastruktur, şəbəkə, bulud, İoT texnologiyaları və proqram təminatı sahəsində :

1. Critical infrastructure cyber security
2. Network security
3. Cloud security
4. IoT (Internet of Things) security
5. Application security

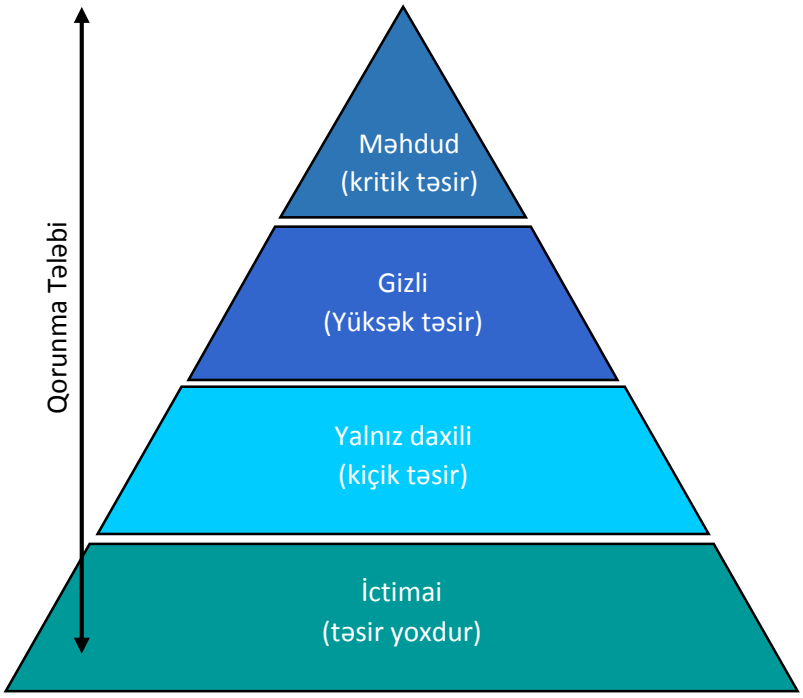
Tez-tez **Phising, Hacking, Pentest, Dos və Ddos** kimi müxtəlif təhdid vasitələri ilə qarşılıaşırıq. Bu məruzədə də məhz sadalanan problemlər praktik analiz olunmuş, ayrı-ayrı üsullarla realizasiyası araşdırılmışdır. Sosial mediya təhlükəsizliyi və qırılma yolları: Fişinq (Phishing), Brute Force, Cihaz təhlükəsizliyi, izlənməsi və qırılması,Trojan (Troyan) anti-virus və firewall tətbiq etmək imkanları analiz edilmişdir. Məruzədə sadalanan problemlərdən qorunma yolları da praktik olaraq şərh ediləcəkdir.

**Açar sözlər**: Phising, Hacking, Pentest, Dos və Ddos. Cloud security, IoT (Internet of Things) security.

# İNFORMASİYA TƏHLÜKƏSİZLİYİNDƏ MƏLUMATIN SİNİFLƏNDİRİLMƏSİNİN ANALİZİ

**Həsən Paşayev**
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

İnformasiya təhlükəsizliyi sahəsindəki bütün məlumatların bərabər tutulmadığı yaxşı başa düşülür. Ən vacib məlumatların qorunmasını təmin etmək üçün nəzarət səviyyələrini artırmaqdır və bu təhlükəsizliyin bu üsul ilə təmini xərc tələb edir. Burada məlumatların təsnifatı məsələsi meydana çıxır. Hər bir təşkilatın struktur olaraq özünə xas 'Çox Gizli' məlumatlarla işləmə metodu məlumdur. Məlumat Təsnifatı, sənədlərin müxtəlif səviyyələrdə məxfilik etiketlənməsi (labeling) ilə başlayır. Bu səviyyələr adlara uyğunlaşdırılır, nəticədə daxili və xarici iş prosessində necə istifadə ediləcəyi, ötürüləcəyi və nəticədə qorunacağı ilə birbaşa bağlıdır. Bu təsnifat Şəkil 1-də göstərildiyi kimidir.




**Şəkil 1.** Məxfilik dərəcəsinin təsviri

Ümumlikdə baxsaq hökumət təşkilatlarında məlumatların təsnifatına, ümumiyyətlə, beş səviyyə daxildir [1]:

- Tam Gizli,

- Gizli,
- Həssas
- Təsnif edilməmiş.

Bunlar kommersiya təşkilatları tərəfindən qəbul edilə bilər, lakin əksər hallarda məhdud, gizli, daxili, ictimai kimi dörd səviyyə qəbul edilir. Bu dörd təsnifat daha açıq qaynaqlıdır və adları necə işlənməli olduqlarına uyğunlaşır.

İctimai (Public): Bu məlumatlar ümumi məlumatdır və veb saytınızda açıq şəkildə paylaşıla bilər, İctimaiyyətlə və hər kəslə müzakirə edilə bilər. Adından da göründüyü kimi ümumi məlumat hər kəsə açıqdır və bu məlumatda istifadə edildikdə əlavə nəzarət tələb olunmur.

Daxili (**Internal):** Daxili məlumatlar şirkət(təşkilat) səviyyəsindədir və məhdud nəzarətlə qorunmalıdır. Daxili məlumatlar işçilər üçün kitabçanı, müxtəlif qaydaları və şirkət miqyaslı qeydləri ehtiva edə bilər. Əgər məlumat açıqlanarsa, daxili məlumatlar iş üçün minimal təsir göstərir.

Gizli (Confidential): Məxfi məlumatlar komanda səviyyəsindədir və istifadəsi iş daxilində olmalıdır. Bu məlumatlar qiymətlər, marketinq materialları və ya əlaqə məlumatlarını əhatə edə bilər. Əgər bu məlumat açıqlanarsa, Gizli məlumatlar işinizi və nəticədə markanızı mənfi təsir edə bilər.

Məhdud (Restircted): Məhdud məlumatlar olduqca həssasdır və istifadəsi bilmə ehtiyacı əsasında məhdudlaşdırılmalıdır. Məhdud məlumatlar, qanuni riski minimuma endirmək üçün, ümumiyyətlə, məlumat yaymamaq haqqında müqavilə ilə qorunur. Məhdudlaşdırılan məlumatlar ticarət sirlərini, potensial olaraq müəyyən edilə bilən məlumatları , kart sahibi məlumatlarını (kredit kartları) və ya sağlamlıq məlumatlarını əhatə edir. Əgər bu məlumat açıqlanarsa, iş üçün əhəmiyyətli bir maliyyə və ya qanuni təsir olacaqdır.

Qeyd etmək lazımdır ki, Məlumat sinifləndirmə standartına sahib olmaq ilk addımdır. Əgər bu məlumat təsinf edilməmişdirsə və ya sıfırlanıbsa, məlumatı təsnif etmək üçün bir çox yol var. Həmçinin bununla yanaşı iki əsas metod var:

Birincisi, bütün Şəxsi Olaraq Müəyyənləşdirilən Məlumat PII (Personally İdentifiable İnformation), Ödəmə Kartları Sənayesi PCI (Payment Card Industry), Şəxsi Sağlamlıq Haqqında Məlumat Qoruma Qanunu PHIPA (Personal Health Information Protection Act) və s. kimi kommersiya sirlərinə, məhdud (Restircted) olaraq baxılmasını və sistemlərinizdə bir texnologiyadan istifadə edərək avtomatik etiketləmək üçün qaydalar yaratmağa cəhd etməyi əhatə edir. Kredit kartları 16 rəqəmdir və etibarlı kartlar mod 10 yoxlamasından keçir. Texnologiya, kredit kartlarını tapmaq və məlumatları müvafiq olaraq idarə etmək qabiliyyətinə malikdir.

İkincisi, işçilərinizə təsnifat səviyyələrini başa düşmək və sənədləri məqsədlərinə uyğun istifadə edərək etiketləmək üçün təlim verilməsi daxildir. Bu, texnologiyanın məlumatları və konteksti anlamaqda çətinlik çəkdiyi sadə ən səbəbdən çətinə qədər tətbiq olunduqda ən təsirli həll vatiantıdır.

Verilərin etiketlənməsi vəzifəsi məlumat sahibinə düşür. Məlumat sahibi, məlumatdan məsul olan iş lideri və ya şəxsdir. Müvafiq təsnifatı təyin etmək və məsuliyyəti qəyyumun ixtiyarına vermək məlumat sahibinə aiddir. Mühafizəçi, həssas məlumatların təhlükəsiz saxlanılması, daşınması və

saxlanmasından məsul olan qrup üzvüdür. Həssaslıq səviyyəsinə əsasən təhlükəsizlik nəzarətinin tətbiq edilməsindən cavabdehdirlər.

Veriləri təsnif etmək üçün bir neçə səbəb var. Başlamaq üçün həssas məlumatları aşkarlamağı asanlaşdırır. İçərisində bir məzmun siyasəti olan bir məktub (Office 365) və "Tam məxfi" ilə başlayan mövzu sətri, alıcının məlumatla diqqətli olmağının çox açıq bir göstəricisidir. Numünə Şəkil-2-də göstərilmişdir.


**Şəkil 2.** E-maildə etiket vurulmuş sənədin vizual görünüşü

Artıq burada "Məxfi İnformasiya" etiketini görən işçi bu sənədlə daha intizamlı davaranacaq və bu sənədin hansı məqsədlər üçün istifadə ediləcəyini biləcəkdir. Eyni zamanda informasiyanı mühafizə edən şəxs bu məlumatı daha dəqiq izləmə halı yaranır.

Məlumatlarınızı etiketləmək işçilərin yerini tapmaqla yanaşı məlumat itkisinin qarşısının alınması (DLP) kimi texnologiyaların da bunu etməsini asanlaşdırır. Məsələn, siz həmin məlumatın hansı istifadəçidə hansı vaxtda və hansı məqsəd üçün istifadə edilməsini asanlıqla nəzarətdə saxlaya bilərsiniz. Məhdud məlumatların, işdən kənarlaşdırılmaması (e-mail ilə başqa şəxsə göndərmə), çap edilməməsi və ya etibarsız bir yerdə saxlanılması və s. kimi hallar hər zaman önəmli məsələ olmaqdadır və nəzarət tələb edir.

**Nəticə.** Məlumatların təsnifatı hər hansı bir təhlükəsizlik proqramının əsas təməl hissəsidir. Bu yanaşma işininiz ən həssas məlumatlarının qorunmasını təmin edən bir çərçivədir. İctimai məlumatların açıq şəkildə istifadəsi nəzərdə tutulur və açıqlanması gözlənilir. Məhdud məlumatlara keçərkən təhlükəsizlik nəzarətinin təbəqələrini tətbiq etmək, xərc effektivliyini təmin etməyin ən yaxşı yoludur. Bu üsulla işçilərinizdə etiketlənmiş həssas məlumat olduqda onların bu məlumatları necə idarə edəcəyini başa düşməsi daha asandır.

## Ədəbiyyat

1. Harold C. Relyea, Security Classified & Controlled Information. Nova Biomedical Books, 2008, 58 p.
2. Don Murdoch, Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter. 2019, 258 p.

# A REVIEW ON ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

**Rufat Gadirov**
Baku Engineering University, Baku, Azerbaijan
e-mail: rqedirov@std.beu.edu.az

**Abstract**

Cybersecurity and artificial intelligence have a wide range of transdisciplinary techniques. Aside from experiments, AI technologies like deep learning may be used in cybersecurity to develop intelligent models for deploying malware. AI models require special cybersecurity protection, including rating and detection of invasive and dangerous intelligence sensing to combat anti-machine learning, maintaining confidentiality in machine learning, secure federated learning, etc. Security technologies, AI and cybersecurity are used to research one another. Regarding the two aforementioned elements, details about the methods and advantages are provided in this article. As well as artificial intelligence's drawbacks in cybersecurity [1].

**Introduction**

Cybersecurity is expanding and getting better every day. Artificial intelligence integration in cyber security systems. The integration of machine learning and artificial intelligence is progressing. Spanning a wide range of industries and applications any other period in recent memory as computing power and storage have increased data gathering and capability. This enormous volume of data can not be the individuals labored slowly. Additionally, this apex of machine learning AI data can be fractionalized of time, which aids in identifying the business and recovery from security risks.

**Function of artificial intelligence in cyber security:**

**Artificial intelligence:** Artificial intelligence is a method of producing computers, computer-controlled robots, or software think tanks that think as intelligently as a man can. The way the human mind works, along with how people learn, make decisions, and seek to find solutions to problems, are researched in order to develop intelligent software and systems. Generally, artificial intelligence is seen as a must acquiring information and making decisions based on that information to solve complicated issues. Intelligent machines will soon take the place of humans in many people's skills.

**The emergence of AI in cyber security**: Machine learning and artificial intelligence, more full cross-wise linkages. More than ever, enterprises and applications rely on information as a registering power to expand capacity and boost accumulation. It's essential to have access to this abundance of information. The capacity of AI to analyze and assess every area of cyber security suggests that new efforts and holes may be quickly found. Other attacks were investigated to help minimize. It can be take a portion of the weight from human safety. They are alerted when something happens. If they choose to, they may direct their energy into actions that are more imaginative and beneficial. If you decide to employ this star depiction when making your plans. Machine learning and artificial intelligence software will make AI as intelligent as your best staff [2].

**Where can artificial intelligence be used in cyber security:** Artificial intelligence is currently looking for some of them or has already begun using some of them. These cybersecurity options are available, gmail uses artificial intelligence to identify and filter spam and fraudulent emails. Regardless of whether an email is spam or not, every time you click on it, you help millions of other points where even the most subtle spam can be found. Emails that attempt to pass as "repeated" emails.

**Benefits of AI in cyber security:** For illustration, the company Siemens AG, a global leader in automation, electrification, and digitalization, is utilized. For its Siemens Cyber Defense Center, Amazon Web Services (AWS) will improve AI-based speed, self-control, and a very adaptable platform (CDC). The deployment's AI was able to determine that it could hold 60,000 people. Per unit attack time. Due to the use of AI, this capacity was managed by a team of less than 12 people without any adverse effects on system performance. Cybersecurity organizations can comprehend and re-apply danger patterns in innovative identification by utilizing AI. About 64% of administrators report redress threats while recognizing and looking into problems. As a result, detecting and reacting to AI is less expensive. To prevent cyberattacks, violations need to be addressed right away. Cyber possibilities are made possible by AI. Identity is evolving more quickly than manually thanks in large part to the cyber security scenario. AI can recognize unique and difficult situations and automatically respond and mitigate them. attack extension editing [3].

**The disadvantages of Artificial Intelligence in cyber security:**

**a**. **Cybercriminals are aware of AI:** Cybercriminals will quickly catch up since AI knowledge is widely available. Artificial intelligence is utilized to develop cybersecurity solutions and to take advantage of malware. They can develop malevolent, AI-proof technologies that can more effectively penetrate websites and businesses.

**b. AI is still expensive**: Artificial intelligence is expanding as a result of data science and big data. Because of this, it's almost unreachable to marketers or challenging to locate in this region. Numerous firms run the danger of spending more money because there aren't enough AI solutions for cybersecurity.

**c. Cyberthreats evolve:** This does not imply that you should come resistive to everything without thinking. If you include them, you'll be in trouble. Even AI is continually improving, as are infections and viruses. Continuous system improvement and discussion are required [4].

**Conclusion**

So in this article, we looked at the importance of artificial cyber security and various intelligence problems that come with it and how they can do it. Although there are some drawbacks, artificial intelligence still plays an important role in cyber security. To overcome errors, artificial intelligence will help advance cyber security.

**Keywords:** Threats, Security, Cyber Security, Artificial Intelligence.

## References

1. G.P.S.K. Arockia Panimalar. S, Intelligence Techniques For Cyber Security, International Research Journal of Engineering and Technology (IRJET), vol.05, no.03, pp.2395-3056, 2018.
2. Kumar R., Artificial Intelligence : A Path to Innovation," *International Journal of Scientific Research in Science and Technology (IJSRST)*, vol.3, no.1, pp.2395-4011, 2017.
3. Mohammed I.A., Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature, International Journal Of Innovations In Engineering Research And Technology [IJIERT], vol.7, no.9, 2020, pp. 2394- 3696.
4. Shamiulla, A.M. (2019). Role of artificial intelligence in cyber security. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4628-4630.


# BIG DATA TEXNOLOGİYASINA ƏSASƏN IoT ŞƏBƏKƏSİNƏ EDİLƏN KİBER-HÜCUMLARIN TƏHLİLİ


**Vagif A. Qasımov, Cabir I. Məmmədov, Cavid Y. Abbaslı**

Azərbaycan Texniki Universiteti, Bakı, Azərbaycan



**Xülasə**

BIG DATA anlayışı və onun analitikasına baxış zamanı aydın olur ki, bu verilənlərə edilən və ya ehtimal olunabilən kiber-hücumların qarşısını ənənəvi üsullarla almaq bəzən heç də əlverişli sayılmır. IoT şəbəkəsinə edilən hücumlar böyük həcmli və dəyərli verilənlərə gedən yolda hücum edənlər üçün bir açar sayılır. Bu cür hücumların təhlilindən aydın olur ki, verilənlər göllərində təhlükəsizliyin "Supervised Machine Learning" ilə qorunması ən önəmli faktordur. Təhlükəsizliyin bu yöndən təmin olunması Weka proqram mühitində formalaşdırılır.


**Giriş**

Müasir dünyada hər saatda onlarla ekzabayt həcmində verilənlər BIG DATA-ya mübadilə olunur. BIG DATA analitikasına əsasən bu verilənlərin böyük bir həcmini konfidensial məlumatlar təşkil edir. Özündə həcmliliyi, dəyərliliyi, müxtəlifliyi, sürətli mübadilə və məlumatın doğruluğunu ehtiva edən bu texnologiya verilənləri, xüsusilə müxtəliflilik prinsipinə görə Verilənlər göllərində (*eng: Data Lakes*) saxlayır [4]. Həmçinin, qeyd edilməlidir ki, böyük həcmli verilənlərin saxlanıldığı Verilənlər anbarları (*eng: Data Warehousing*) BIG DATA-da toplanan verilənlər üçün əlverişli sayılmır. Belə ki, verilənlərin çox böyük həcmli olması, sürətli axını, onların öncədən işlənilməməsi (*eng: Data pre-processing*), strukturlaşdırılmaması, xam verilən (*eng: Raw data*) olması verilənlər anbarının strukturuna ziddir və bu kimi verilənlər üçün heç də münbit saxlama mühiti deyildir.

**Verilənlər göllərinə bilavasitə IoT texnologiyası ilə edilən kiber-hücumlar**

Verilənlər göllərinin iş prinsipi bulud texnologiyalarına əsaslanır və bazarda lider olan AWS (*eng: Amazon Web Services*), Cloudera, Google Cloud kimi vendorlar öz verilənlər göllərində saxlanılan verilənlərin təhlükəsizliyini üst səviyyədə təmin edirlər. Lakin, bilavasitə verilənlər göllərini hədəf alan kiber-hücumçular, bu bazaya bağlı olan serverlər ilə əlaqəli olan şəbəkə kanallarına sızırlar.Verilənlər gölünə bağlı serverlərin şəbəkə kanallarına edilmiş hücumlar içində yayılmış ən geniş hücumlardan biri də bilavasitə IoT texnologiyası ilə edilən kiber-hücumlardır. Məlumdur ki, insan əməyinə qənaət edən bu texnologiya özündə müxtəlif ağıllı elektronik cihazların bir-birinə bağlanması və verilənlərin mübadiləsi üçün nəzərdə tutulur.

**IoT texnologiyalarına edilən kiber-hücumların ümumi təşkili**

IoT texnologiyaları əksər hallarda TCP/IP və UDP/IP şəbəkə protokolları üzərində qurulur. Bu şəbəkəyə olan kiber-hücumun əsas məntiqi yeni casus qurğunun əlavə edilməsidir [2]. Belə ki, əslində, belə bir qurğu reallıqda olmur. Aydındır ki, IoT texnologiyasına bağlı olan hər hansı bir ağıllı qurğunun server ilə verilənlər mübadiləsi zamanı verilənlər dəstləri müəyyən şəbəkə paketləri vasitəsi ilə göndərilir. Bu mübadilə zamanı hər şəbəkə paketinin özünəməxsus xüsusiyyətləri mövcuddur. IPLength, IPHeaderLength, IPID, IPCheckSum, SourcePort, DestPort və s. kimi başlıqlar hər şəbəkə paketi üçün təyin olunmuş fərqli xüsusiyyətlər olmaqla yanaşı, hər bir cihaz üçün məxsusi xarakter daşıyır. Əksər hallarda DestPort, yəni ünvanlanmış port nömrəsi eyni şəbəkəyə qoşulmuş cihazlar üçün eyni olur. Lakin, cihazlar üçün fərqli DestPort-ların istifadəsi kiber səviyyədə daha uyğun sayılır. Bu hücumların ilkin mərhələlərində şəbəkə kanalından, nümunə olaraq, bir şəbəkə paketi götürülür. Daha sonra, hücum edən öz qurğusunun Terminalında kiber-hücumu gerçəkləşdirərkən, qoşma proqram təminatını dəstəklədiyi üçün Python proqramlaşdırma dilindən istifadə edir. Sinifləndirmə üçün istifadə etdiyi əlavə "tool" isə T-Shark qoşma proqram təminatı olur.

**Məlum kiber-hücumun ilkin proqram təminatı və vendorların həlli yolları**

Terminalda yaradılmış .pcap (*eng: Packet CAPture*) uzantılı, mətn formatlı faylın əsas məqsədi cihazları sinifləndirmək, başqa sözlə, neçə cihazın eyni IoT şəbəkəsinə qoşulduğunu bilmək, hər bir cihazdan şəbəkəyə ötürülən paketlərin, onların IP xüsusiyyətlərini təhlil etməkdir. Məlumdur ki, bu halda şəbəkəyə qoşulmuş hər bir cihazın IP ünvanında məxsusi HostID-lər olur. Fərz edək ki, təhlükəsizlik kameraları IoT texnologiyası əsasında eyni şəbəkəyə qoşulmuşdur [3]. Belə ki,

NetworkID: 180.157.23

Kameraların HostID-ləri: 41, 85, 99, 74

məlumdur. İlkin .pcap uzantılı faylın yaradılması zamanı cihazlar sinifləndirilməmiş halda bir .pcap uzantılı faylda saxlanılır və filtrləmə üçün açıq hala gətirilir. Terminalda T-Shark qoşmalı Python proqramlaşdırma dilində yazılmış aşağıdakı kod fraqmentinə baxaq:

```
import os
import glab
ip_filter [ ` TCP_Kamera `] = ``` tcp & ( ip.src == 180.157.23.41 ) || ( ip.src == 180.157.23.85 ) || ( ip.src == 180.157.23.99 ) || ( ip.src == 180.157.23.74 ) ` ```
```

Hücum edən ilkin .pcap faylını qurduqdan sonra artıq istifadə olunmuş cihazları sinifləndirir, IP ünvanların strukturundan xəbərdar olur. Bu isə, yeni casus şəbəkə paketinin yaradılmasına imkan verir. Lakin hücum edənin əsas məqsədi bəzən heç də IoT şəbəkəsinə qoşulu olan cihazları ələ keçirmək deyil. Serverə bağlı olan verilənlər göllərinə qanunsuz əlçatanlığını təmin etmək və yeni, müxtəlif verilənləri ələ keçirməkdir.

Verilənlər gölləri vendorları bu təhlükəsizlik problemlərini aradan qaldırmaq üçün verilənləri klasterləşdirməyə üstünlük verir və bunun üçün nəzarət olunan maşın öyrənmə üsulundan (*eng: Supervised Machine Learning*) istifadə edir. Belə ki, hər yeni daxil olan böyük həcmli verilənlər üçün yeni .pcap fayllar yaradılır və bu verilənlərin təmizlənməsi, işlənilməsi sonrası həmin verilənlər Weka proqram təminatında Naive – Bayes alqoritminə əsasən klasterləşdirilir [1]. Beləliklə, şəbəkə paketlərinin təhlilinə əsasən klasterləşdirilmə nəticəsində verilənlər gölü cari verilənlərin IP ünvanlarını yadda saxlayır. Bu da yeni verilənin işlənilmədən öncə saxlama mühitində depolanmasına mane olur.

**Nəticə**

BIG DATA-ya toplanan verilənlərə olan bəzi kiber-hücumların qarşısını almaq üçün nəzarət olunan maşın öyrənmə üsulundan istifadə etmək, yeni şəbəkə paketində göndərilmiş verilənin, əvvəlki verilənlərin şəbəkə paket analizinə əsaslanır. IoT texnologiya istifadəçisi yeni qoşulmuş cihazlara statik IP ünvan daxil edə bildiyi halda belə hücumlar qaçılmazdır. Verilənlər gölündə nəzarət olunan maşın öyrənmə üsulundan istifadə edərək klasterləşdirmə və şəbəkə paketinin "Payload" başlığının kriptoqrafik şifrlənməsi kiber-hücumların baş vermə ehtimalını aşağı salır.

**Açar sözlər:** BIG DATA, IoT texnologiyası, machine learning, kiber-hücum.

**Ədəbiyyat**

1. Alex Smola, S.V.N. Vishwanathan. An Introduction to Machine Learning. 2010, pp.20-22.
2. Keyurbhai Arvindbhai Jani, Nirbhay Kumar Chaubey. Quantum Cryptography and the Future of Cyber Security. IoT and Cyber Security: Introduction, Attacks, and Preventive Steps, 2020, pp.203 – 235.
3. Ricardo Calix. Getting Started with Deep Learning: Programming and Methodologies using Python, 2017, pp.88 – 96.
4. Youssra Riahi. International Journal of Research and Engineering. Big Data and Big Data Analytics: Concepts, Types and Technologies, 2018, pp.524 – 526.

**BIG DATA technology mainly applied to IoT network analysis of cyber-attacks**

When looking at the concept of BIG DATA and its analytics, it becomes clear that it is sometimes not convenient to prevent cyber-attacks on this data by traditional methods. Attacks on the IoT network are considered a key for attackers on the way to large and valuable data. Looking at the analysis of these attacks, it is clear that the protection of security in the data lakes with "Supervised Machine Learning" is the most important factor. Ensuring security in this direction is formed in the Weka software environment.

# MATRİS - ƏSASLI YENİ AÇAR MÜBADİLƏSİ PROTOKOLU

**Vagif A. Qasımov, Cabir I. Məmmədov, Nərgiz F. Məmmədzadə**
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

İnformasiyanın asimmetrik şifrləmə alqoritmlərinə nisbətən simmetrik alqoritmlər daha sürətlə yerinə yetirilir və bu, həmin alqoritmlərin böyük üstünlüyü olmaqla onların daha çox istifadə olunmasına imkan verir. Lakin simmetrik alqoritmlərdən istifadə zamanı məxfi açarların informasiya mübadiləsini həyata keçirən tərəflərə maneəsiz çatdırılması prosesi müəyyən problemlərlə bağlıdır [1]. Belə ki, istifadə olunan məxfi açarların kənar şəxslərin əlinə keçməməsi üçün qorunan məxfi kanalların yaradılmasına ehtiyac yaranır bu da əksər hallarda çox böyük vəsait hesabına başa gəlir. Açıq açarlı şifrləmə sistemlərinin yaradılması sahəsində görülən işlər məhz belə problemin aradan qaldırılması üçün çox böyük addım olmuşdur. Bu cür sistemlərdə informasiya mübadiləsini həyata keçirən tərəfin hər biri iki açardan istifadə edir: açarlardan biri açıq açardır və o, tərəflərin hər birinə məlum olmaqla informasiyanın ötürülməsi üçün istifadə edilir, digəri isə, məxfi açar olub qəbul edilmiş şifrmətni deşifrə etmək üçün istifadə olunur. Tərəflərdə generasiya edilmiş məxfi açarlar yalnız onların özlərinə məlum olur. Açıq açarlı şifrləmə sistemlərinin yaradılması üzrə ilk böyük iş Diffi və Hellman tərəfindən yerinə yetirilmişdir [2].

Diffie-Hellman prinsipli istənilən açar mübadiləsi protokollarının əsasını biristiqamətli funksiyalar təşkil edir. Bu funksiyaların bir istiqamətdə hesablanması sadə, tərsinə hesablanması isə olduqca mürəkkəbdir.

Qeyd etmək lazımdır ki, tərsinin riyazi olaraq hesablanması ümumiyyətlə mümkün olmayan funksiyalar da vardır. Təqdim edilən bu tədqiqat işi tərsinin hesablanması mümkün olmayan matrislər əsasında açıq açarlı mübadilə protokolunun işlənməsinə həsr olunmuşdur.

Məlumdur ki, iki matrisin hasilinin hesablanması yalnız birinci matrisdəki sütunların sayının ikinci matrisdəki sətirlərin sayına bərabər olması halında mümkündür. Xüsusi halda, hər iki matris eyni ölçülü kvadrat matrislər olduqda, onların hasilinin tapılması həmişə mümkün olur.

Bu şərtləri ödəyən A və X matrislərini bir-birinə vurduqda müvafiq ölçülü C matrisi alınır:

$$A \cdot X = C \tag{1}$$

Əgər (1) ifadəsində C və A verilərsə, onda X matrisini aşağıdakı ifadə əsasında hesablamaq olar:

$$X = C \cdot A^{-1} \tag{2}$$

Burada $A^{-1}$ matrisi A matrisinin tərs matrisidir. Tərs matrisin tapılması üçün aşağıdakı ifadədən istifadə edilir:

$$A^{-1} = \frac{1}{\det A}\begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix} \tag{3}$$

Burada, A matrisinin determinantı *det A* ilə işarələnmişdir, $A_{nm}$ (i,j=1,2,...,n) isə matrisinin minorudur. Qeyd etmək lazımdır ki, hər matrisin tərsi mövcud deyil. Matrisin tərsinin mövcud olması üçün iki şərtin ödənməsi zəruridir: birincisi – verilmiş matris kvadrat matris olmalıdır, yəni onun sütun və sətirlərinin sayı bərabər olmalıdır, ikincisi - matrisin determinantı sıfırdan fərqli olmalıdır. Düsturdan aydın görünür ki, det A=0 olarsa, sıfıra bölmə hadisəsi baş verir, bu da qeyri- müəyyənliklə nəticələnir, yəni matrisin tərsi tapıla bilmir. Beləliklə, iki matrisin hasilinin tapılması həmişə mümkün olsa da, hasil və vuruqlardan biri verildikdə, digər vuruğun tapılması müəyyən hallarda mümkün olmur. Bu onunla əlaqədardır ki, məlum vuruq tərsi olmayan matris olarsa, digər vuruq üçün (1)-tənliyini ödəyən sonsuz sayda həll mövcud olar. Məhz bu xüsusiyyət matrislər vasitəsilə birtərəfli funksiya yaratmağa imkan verir [3].

Yuxarıda göstərilənlər nəzərə alınaraq, tərsi olmayan matrislərə əsaslanan açar mübadiləsi protokolu tərtib edilmişdir.

Tərtib edilmiş protokola görə ümumi gizli açarın generasiyası əməliyyatları aşağıdakı ardıcıllıqla yerinə yetirilir:

1. İnformasiya mübadiləsini həyata keçirən A və B tərəfləri elə nxn ölçülü qeyri-məxfi kvadrat C matrisi seçirlər ki, onun determinantı sıfra bərabər olsun;

2. A tərəfi nxn ölçülü gizli $M_1$ və $K_1$ matrislərini və B tərəfi isə eyni ölçülü gizli $M_2$ və $K_2$ matrislərini seçir.

3. A tərəfi $S_{A1}$ =M1xC hasilini hesablayıb B tərəfinə göndərir, B tərəfi də $S_{B1} = M_2xC$ hasilini hesablayıb A tərəfinə göndərir.

4. A tərəfi B tərəfindən əldə etdiyi $M_2xC$ matrisini sağdan $M_1$ matrisinə, soldan isə C matrisinə vurub $S_{A2}= CxM_2xCxM_1$ matrisini əldə edir.

5. A tərəfi $S_{A2}$ matrisini soldan $K_1xCxM_1$matrisinə vurub $S_{A3}=K_1xCxM_1xCxM_2xCxM_1$ matrisini əldə edib B tərəfinə göndərir.

6. B tərəfi də A tərəfindən aldığı M1xC matrisini soldan C-yə sağdan isə $M_2$-yə vuraraq $S_{B2}=CxM_1xCxM_2$ matrisini əldə edir.

7. B tərəfi $S_{B2}$ matrisini soldan $CxM_2$, sağdan isə $K_2$ matrisinə vuraraq $S_{B3}=CxM_2xCxM_1xCxM_2xK_2$ matrisini əldə edib A tərəfinə göndərir.

8. A tərəfi əldə etdiyi $S_{B3}$ matrisini soldan $K_1xCxM_1$-ə vurub S= $K_1xCxM_1xCxM_2xCxM_1xCxM_2xK_2$ yekun acarı əldə edir.

9. B tərəfi isə oz növbəsində əldə etdiyi $S_{A3}$ matrisini sağdan $CxM2xK_2$ matrisinə vuraraq yekun acar olan S= $K_1xCxM_1xCxM_2xCxM_1xCxM_2xK_2$ matrisini hesablayır.

Qeyd edək ki, baxılan alqoritmdə $K_1$ və $K_2$ matrislərinin əlavə olunması dəyişənlərin sayının tənliklər sistemində olan tənliklərin sayından daha çox olmasını təmin etmək üçündür. Bu, protokolun xətti cəbr hücumlarına davamlı olmasını təmin edir.

Nümunə. Real ədədlər üzərindən protokolu tətbiq edək:

Determinantı 0 olan matris seçək. Matrislərin vurulması nəticəsində onların elementlərinin müəyyən çərçivədə saxlanılması üçün p sadə ədədi seçilir və bütün hesabatlarda *mod p* əməliyyatından istifadə olunur.

p=97 $C = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 6 & 8 & 4 \end{pmatrix}$ $\det C = 0$ $A = \begin{pmatrix} 0 & 2 & 7 \\ 2 & 3 & 2 \\ 4 & 0 & 0 \end{pmatrix}$ $B = \begin{pmatrix} 1 & 3 & 1 \\ 1 & 3 & 6 \\ 3 & 7 & 1 \end{pmatrix}$

$K1 = \begin{pmatrix} 8 & 4 & 3 \\ 6 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}$ $K2 = \begin{pmatrix} 6 & 3 & 1 \\ 1 & 1 & 6 \\ 9 & 0 & 5 \end{pmatrix}$

$S_{A1}$ =(A·C)= $\begin{pmatrix} 44 & 60 & 34 \\ 17 & 26 & 23 \\ 4 & 8 & 12 \end{pmatrix}$ $S_{B1}$ =(B·C)= $\begin{pmatrix} 10 & 16 & 16 \\ 40 & 56 & 36 \\ 16 & 28 & 34 \end{pmatrix}$

$S_{A2}$=$CS_{B1}A$ ==$\begin{pmatrix} 20 & 39 & 32 \\ 20 & 39 & 32 \\ 94 & 43 & 55 \end{pmatrix}$ $S_{B2}$=$CS_{A1}B$ = $\begin{pmatrix} 89 & 35 & 52 \\ 89 & 35 & 52 \\ 93 & 86 & 97 \end{pmatrix}$

$S_{A3}$=$K_1CA$ $S_{A2}$=$\begin{pmatrix} 95 & 45 & 79 \\ 25 & 66 & 8 \\ 43 & 10 & 61 \end{pmatrix}$ $S_{B3}$= CB $S_{B2}K_2$=$\begin{pmatrix} 38 & 94 & 24 \\ 38 & 94 & 24 \\ 55 & 13 & 47 \end{pmatrix}$

S= $K_1CA$ $S_{B3}$ = $\begin{pmatrix} 24 & 77 & 0 \\ 46 & 12 & 85 \\ 78 & 13 & 45 \end{pmatrix}$ S= $S_{A3}CBK_2$=$\begin{pmatrix} 24 & 77 & 0 \\ 46 & 12 & 85 \\ 78 & 13 & 45 \end{pmatrix}$

Göründüyü kimi, informasiya mübadiləsini həyata keçirən hər iki tərəfdə eyni qiymətli açar S= $\begin{pmatrix} 24 & 77 & 0 \\ 46 & 12 & 85 \\ 78 & 13 & 45 \end{pmatrix}$ müəyyən edilir. Bu açar mübadilə kanalları vasitəsilə ötürülmür və tərəflərdə gizli saxlanılır.

Beləliklə, protokolun əsas üstün cəhəti ondan ibarətdir ki, o, xətti cəbri hücumlarla qarşı daha davamlıdır. Belə ki, kriptoanaliz prosesində tapılmasına ehtiyac olan matrisin hesablanması riyazi olaraq həlli olmayan məsələ üzərində qurulmuşdur.

## Ədəbiyyat


1. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Dərslik, Bakı, 2009, 340 səh.
2. Diffie W., Hellman M. New direction in cryptography. IEEE transactions on information theory, Vol. IT-22, No. 6, November 1976.
3. Brown D., Koblitz N., LeGrow J., Cryptanalysis of `MAKE', Cryptology ePrint Archive, Paper 2021/465, 2021, https://eprint.iacr.org/2021/465

# AĞILLI ŞƏHƏRLƏRDƏ ENERJİ TƏMİNATI SİSTEMİNİN TƏHLÜKƏSİZLİYİNDƏ BLOKÇEYN TEXNOLOGİYASI

**Vaqif Qasımov[1], Məryəm Əsədova[2]**
Azərbaycan Texniki Universteti, Bakı, Azərbaycan
Mingəçevir Dövlət Universiteti, Mingəçevir, Azərbaycan
e-mail: vaqif.qasimov@aztu.edu.az, esedova.m92@gmail.com

Ağıllı şəhər sistemləri vətəndaşların yaşayış şəraitini yaxşılaşdırmaq və səmərəliliyi artırmaq üçün yaradılmış rəqəmsal texnologiya sistemləridir [5]. Ağıllı sistemlər nəqliyyat vasitələri, evlər, parklar, ticarət mərkəzləri kimi bir çox sahədə istifadə olunur. Ağıllı sistemlər insanların ehtiyaclarına uyğun yaradılmış texnologiyalardır. İnsanların ehtiyaclarını bilmək və onlara uyğun texnologiyalar istehsal etmək də məlumatların toplanması və təhlili yolu ilə mümkündür [2]. Vətəndaşlara səmərəli dövlət xidmətləri göstərmək və şəhər idarəçiliyini təkmilləşdirməyə kömək etmək üçün toplanmış məlumatların toplandığı qədər təhlükəsiz saxlanılması çox vacibdir. Çünki rəqəmsal məlumatlar daim kiberhücumlara məruz qala bilər[3]. Bu səbəbdən ağıllı şəhər sistemləri blokçeyn texnologiyası ilə inteqrasiya edilməsi tövsiyə olunur. Məlumatların icazəsiz modifikasiyasına imkan verməyən blokçeyn texnologiyası təhlükəsizlik həddini daha yüksək dəyərlərə qaldırır.

Blokçeyn texnologiyası ilk dəfə 2008-ci ildə Satoshi Nakamoto [1] tərəfindən Bitcoin-də kriptovalyuta və maliyyə əməliyyatları üçün rəqəmsal platforma kimi yaradılsa da, son vaxtlar bir çox sahələrdə istifadə olunur. Blockçeyn əsaslı bərpa olunan enerjilər insan həyatında günü-gündən daha çox yer alır. Bu tətbiqlərdən biri də panellərlə damda günəş enerjisi istehsalıdır [4]. İstehsal olunan enerjinin artıqlığı bəzi hallarda şəbəkəyə satıla bilər. Ancaq üçüncü şəxslər olmadan şəbəkədə qonşu istifadəçilərlə alış-veriş etmək mümkün deyil [8]. Blockchain vasitəsilə mərkəz elektrik enerjisi satışını insandan insana edə biləcək. Bu satış əməliyyatlarından əvvəl ağıllı müqavilələrdə mübadilə şərtləri təyin olunacaq. Bloklara smart müqavilələr saxlanılacaq. Bu sayədə istifadəçilərə elektrik enerjisini daha ucuz istifadə etmə fürsəti yaranacaq. Bundan əlavə, edilən əməliyyatlar əbədi olaraq qeyd olunacaq. Vergidən yayınma kimi halların qarşısını almaq üçün ödənilməli olan vergi məbləği nəzarət altına alına bilər [6].

Aşağıda blockchain istifadə edərək elektrik enerjisi ticarətinin mərhələləri verilmişdir:

1. İstehsalçı ağıllı müqavilə istifadə edərək ediləcək ticarət qaydalarını təyin edir.
2. Qaydalara görə satış qiymətini satıcı müəyyən edir.
3. İstehlakçı almaq niyyətini bildirir və uyğunlaşma prosesini satıcıya ötürür.
4. Ödəniş edilir və ticarət tamamlanır.

Qeyd edilməlidir ki, ödəniş kWh kriptovalyuta ilə həyata keçirilir. Satıcı və ya alıcı kWh kriptovalyutadan istifadə etmirsə, bu ticarət yerli və ya beynəlxalq valyutalar vasitəsilə də həyata keçirilə bilər [9]. Əməliyyat tarixçəsi silinə bilmədiyi üçün şəbəkədə istehsal və satış arasındakı itkilərin müəyyən edilməsi, insandan insana enerji satışında mərkəzi bir quruluşa ehtiyac

duyulmaması kimi faydalar təmin edir [7]. Bundan əlavə, smart sayğaclara tətbiq edilərsə, IOT (internet of things) cihazlarının şəbəkəyə təsiri və onların şəbəkədən çəkdiyi elektrik enerjisini ölçmək və daha səmərəli etmək kimi üstünlüklərə malikdir.

**Nəticə.** Ağıllı şəhərlərə tətbiq edilən blokçeyn texnologiyaları günü-gündən artır. Blockchain texnologiyası ağıllı şəhərlər sahəsində ağıllı şəhər, ağıllı sağlamlıq, ağıllı nəqliyyat və sair baxımından geniş istifadə olunur. Blockchain əsaslı ağıllı şəhərlərdə təhlükəsizlik və məxfilik hər şeydən üstündür. Bu xüsusiyyəti ilə seçilən blokçeyn texnologiyası inkişaf etməkdə davam edir. Eyni zamanda, ağıllı şəhər sistemlərində blokçeyn texnologiyasının tətbiqi ilə bağlı araşdırmalar kifayət qədər genişdir. Qabaqcıl blokçeyn texnologiyası ilə ağıllı şəhər sistemlərinin səmərəliliyi artır və artmağa davam edəcək.

**Açar sözlər**: blokçeyn texnologiyası, ağıllı şəhərlər, ağıllı enerji, təhlükəsizlik.

## Ədəbiyyat

1. Biswas K., Muthukkumarasamy V. (2016, December). Securing smart cities using blockchain technology. In 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS) (pp. 1392-1393). IEEE.
2. Duman B., Özsoy K. (2019). Smart Agriculture in Industry 4.0 Perspective. 4th International Congress on 3D Printing (Additive Manufacturing) Technologies and Digital Industry, 11-14 April 2019, 540-555, Antalya.
2. Gabison G. (2016). Policy considerations for the blockchain technology public and private applications. SMU Sci. & Tech. L. Rev., 19, 327.
3. Liao D. Y., Wang X. (2017, October). Design of a blockchain-based lottery system for smart cities applications. In 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC) (pp. 275-282). IEEE.
4. Mingxiao D., Xiaofeng M., Zhe Z., Xiangwei W., & Qijun C. (2017, October). A review on consensus algorithm of blockchain. In 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 2567-2572). IEEE.
5. Nakamoto S., Bitcoin A. (2008). A peer-to-peer electronic cash system. Bitcoin. URL: https://bitcoin. org/bitcoin.pdf.
6. Pilkington M. (2016). Blockchain technology: principles and applications. In Research handbook on digital transformations. Edward Elgar Publishing.
7. Ruta M., Scioscia F., Ieva S., Capurso G., Loseto G., Gramegna F., ... & Di Sciascio E. (2017). Semantic-enhanced blockchain technology for smart cities and communities. In 3rd Italian conference on ICT.
8. Sharma P.K., Park J.H. (2018). Blockchain based hybrid network architecture for the smart city. Future Generation Computer Systems, 86, 650-655.

**Blockchain technology in the security of energy supply system in smart cities**

Smart city systems are digital technology systems created to improve the living conditions of citizens and increase efficiency. It is also possible to know people's needs and produce technologies that suit them through data collection and analysis. To provide efficient public services to citizens and help improve city governance, collected data must be kept as secure as it is collected. Because digital data can be constantly exposed to cyber-attacks. For this reason, smart city systems are integrated with blockchain technology. Blockchain technology, which does not allow unauthorized modification of data, raises the security threshold to higher values. in this article, a blockchain-based system is recommended for the secure provision of energy exchange in smart cities.

# MOLEKULLARIN XAOTİK HƏRƏKƏTİNƏ ƏSASLANAN YENİ SİMMETRİK ŞİFRLƏMƏ ALQORİTMİ

**Vagif A. Qasımov , Cabir I. Məmmədov, Nərgiz F. Məmmədzadə**
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

**Xülasə**

Kriptoanalizə davamlılıq baxımından son vaxtlar digər bir çox üsullarla yanaşı xaos əsaslı şifrləmə üsullarının tədqiqinə geniş yer verilir. Belə üsullarda şifrləmə üçün istifadə olunan psevdo-təsadüfi ədədlərin generasiyası müxtəlif xaotik proseslərə əsaslanır. Aparılan bu tədqiqat işində xaotik proses qismində molekulların toqquşmaları ilə mürəkkəbləşən xaotik hərəkəti əsas götürülmüşdür. Molekulların hərəkət trayektoriyası və toqquşma nöqtələrindən istifadə etməklə generasiya edilən psevdotəsaddüfi ədədlərin tərkib hissələri təklif olunan yeni şifrləmə üsulunda birdəfəlik açar kimi istifadə olunur.

**Giriş**

K.Şennon özünün klassik əsərində [1] "xaos" sözünü işlətməsə də kriptoqrafik mühafizə məsələlərinin xaotik proseslərlə əlaqəsini təsvir etmişdir. O, təklif etmişdir ki, arqumentdən asılı olaraq, çevirmə əməliyyatı aparmaqla informasiyanın tərkib hissələrinin qarışdırılması həyata keçirilməlidir. Bu bir faktdır ki, kriptoqrafik mühafizə alqoritmlərinin əksəriyyətində xaotik çevirmə prosesləri bu və ya digər formada mütləq istifadə olunur.

Deterministik xaosun kriptoqrafik sistemlərdə istifadəsinin səmərəli nəticələr verməsi çoxsaylı tədqiqatçıların marağını cəlb etmiş, informasiyanın kriptoqrafik qorunması üçün bu istiqamətdə bir çox elmi-tədqiqat işlərinin meydana gəlməsinə təkan vermişdir. Əvvəlki tədqiqatlarımızın nəticəsi olaraq, real DNT simvollarından əldə edilmiş DNT psevdosimvolları ardıcıllığı və xaotik çevirmə funksiyası əsasında təsvirlərin şifrlənməsi alqoritmi işlənmişdir [2-3]. Təklif olunan alqoritmdə DNT simvolları ardıcıllığının Gen Bankından seçilməsi üçün ünvan, DNT simvollarının kodlaşdırlması qaydası, həmçinin xaotik çevirmə funksiyasının başlanğıc parametrləri əsasında məxfi açar müəyyən edilir. Burada təsvir piksellərinin modifikasiyası DNT psevdosimvollarının xaos oyununun təsviri ilə

alınmış xaotik nöqtələr çoxluğu koordinatlarının ədədi qiymətlərinə, piksellərin yerlərinin dəyişdirilməsi isə xaotik çevirmə funksiyası ilə qurulan yerdəyişmə cədvəlinə əsaslanır.

Aparılan bu tədqiqat işində isə xaotik proses qismində molekulların xaotik broun hərəkəti əsas götürülmüşdür.

**Molekulların xaotik hərəkət modeli əsasında psevdotəsadüfi ədədlərin generasiya edilməsi**

Brown hərəkəti tamamilə nizamsız, təsadüfi bir hərəkətdir. Rəqs hərəkətləri sabit bir nöqtə ətrafında müəyyən dövrə malik olduğu halda, Brown hərəkətində heç bir period yoxdur və zərrəciklər hərəkət nəticəsində yerlərini dəyişdirə bilir. Təqdim edilən tədqiqat işində məhz bu amil nəzərə alınmış və yaranan təsadüfilik əsasında generasiya olunan psevdotəsaddüfi ədədlər şifrələmə prosesində istifadə olunmuşdur.

Yeni alqoritmin mahiyyəti informasiya mübadiləsini həyata keçirən tərəflərdə aparılan bir sıra riyazi çevirmələrə əsaslanır. Belə ki, tərəflər, əvvəlcə, gizli saxlanılan başlanğıc koordinatları ($x_0$,$y_0$), başlanğıc sürəti ($V_0x$,$V_0y$), toqquşma anına qədər keçən zamanı imitasiya edən T parametrini və dəyişdirici k əmsalını seçirlər. Burada nəzərə alınır ki, molekulun hər bir toqquşmadan sonrakı sürəti onun toqquşmaya qədərki sürətindən və toqquşma nöqtəsinin koordinatından, növbəti $\Delta T_i$ hərəkət müddəti isə əvvəlki $\Delta T_{i-1}$ müddətindən asılı olaraq dəyişir. Növbəti mərhələdə aşağıdakı düsturla sürətin və $\Delta T_i$ zamanının hər bir toqquşma üzrə dəyişməsi hesablanır:

$$V_{xi} = Round\left(\left(\left(\left(V_{xi-1} * (X_i + k)\right) mod\ (V_{xi-1} + X_i + k)\right) mod\ X_{max}\right), r\right) + k \quad (1)$$

$$V_{yi} = Round\left(\left(\left(\left(V_{yi-1} * (Y_i + k)\right) mod\ (V_{yi-1} + Y_i + k)\right) mod\ Y_{max}\right), r\right) + k \quad (2)$$

$$T_i = Round\left(\left(\left(\left(T_{i-1} * (k)\right) mod\ (T + k)\right) mod\ X_{max}\right), r\right) + k \quad (3)$$

Burada, $r$ kəmiyyəti hesabatların yuvarqlaşdırma dəqiqliyini göstərən əmsaldır. Bu əmsalın qiyməti ümumi toqquşmalar sayını göstərən ədədlərdəki rəqəm sayından nə qədər böyük olarsa, təsadüfilik daha yüksək olar və qiymətlərin təkrarlanma ehtimalları azalmış olar.

**Şifrləmə prosesi**

Təklif edilən üsulla generasiya edilən psevdotəsadüfi ədədlərdən istifadə etməklə N simvoldan ibarət mətn faylının ($f_{ilk}$) şifrlənməsi prosesi aşağıdakı ardıcıllıqla həyata keçirilir:

1. Molekulların hərəkətinin təqdim etdiyimiz modelinə görə sərhədləri müəyyən olunmuş sahədə (1)-(3) ifadələri əsasında başlanğıc koordinat, sürət, zaman və dəyışdirici əmsaldan asılı olaraq, birinci nöqtənin koordinatları hesablanır;

2. Şifrlənməsi tələb olunan ilkin $f_{ilk}$ faylının ilk 8 simvolunun ASCII-kodlarının ikilik təsviri alınır;

3. Hesablanmış Xi və Yi koordinatlarının hər birindən 64 bit (16 bit tam hissədən, 48 bit isə kəsr hissədən) olmaqla, cəmi 128 biti götürülür;

4. Şifrlənən məlumatın seçilmiş simvollarının 128 bitdən ibarət ikilik kodu nöqtənin hesablanmış koordinatlarının 128 bitli kodu ilə 2 moduluna görə cəmlənir (XOR əməliyyatı);

5. Alınmış ikilik kodlara uyğun ASCII-kodlaşdırma cədvəlindən müvafiq simvollar müəyyən edilir və şifr-fayla ($f_{şifr}$) yazılır;

6. $f_{ilk}$ faylının növbəti 8 simvolu seçilir;

7. molekulların hərəkət modelinə uyğun olaraq, növbəti nöqtənin koordinatları hesablanır;

8. Alqoritmin 3-5 bəndləri üzrə çevirmə əməliyyatları yerinə yetirilir;

9. Alqoritmin 3-8 bəndləri ilkin faylın bütün simvollarının şifrlənməsi başa çatanadək təkrarlanır və sonda $f_{şifr}$ faylında olan informasiya ilkin faylın şifri kimi qəbul edilir.

İnformasiyanın deşifrlənməsi alqoritmi də şifrlənmə alqoritminə analoji olaraq əks istiqamətdə həyata keçirilir.

**Nəticə**

Təklif edilən alqoritm C# proqramlaşdırma mühitində reallaşdırılmış və çoxsaylı mətn nümunələri üzərində onun səmərəliliyi təcrübi olaraq təsdiq olunmuşdur. Alqoritmin kriptodavamlılıq səviyyəsi açar sahəsinin analizi, statistik analiz, NIST testləri kimi standart təhlükəsizlik analizləri vasitəsilə də yoxlanılmışdır.

**Açar sözlər**: Brown hərəkəti, xaotik, psevdo-təsadüfi, şifrələmə, kriptografiya.

**Ədəbiyyat**

1. Клод Шеннон. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369.
2. Gasimov V., Mammadov J. Image encryption algorithm using DNA pseudo-symbols and chaotic map. 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, IEEE Turkey Section, June 11-13, 2021, Turkey. IEEE Xplore. 25.06.2021. https://ieeexplore.ieee.org/document/9461339.
3. Gasimov V.A., Mammadov J.I., Hasanova A.A. Symmetric DNA encryption algorithm based on relative index. Modern Movement of Science: abstracts of the 12th International Scientific and Practical Internet Conference, April 1-2, 2021, Dnipro, Ukraine, 2021, Part.1, pp.53-55.

**A new symmetrical encryption algorithm based on the chaotic movement of molecules**

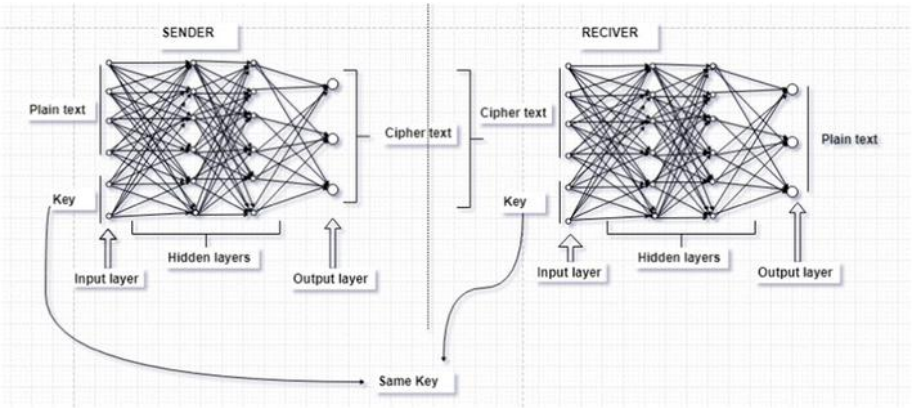
In terms of durability, cryptanalysis has recently been given a lot of space to explore chaos-based encryption methods, along with many other methods. In such methods, the generation of pseudo-random numbers used for encryption is based on various chaotic processes. In this research work, the chaotic movement considered by the collisions of molecules is taken as a chaotic process. The pseudorandom numbers generated using the trajectories of molecules and collision points are used as one-time keys in the proposed new encryption method.

# ELEKTRON TƏHLÜKƏSIZLIK TEXNOLOGIYALARI, DNT KRIPTOQRAFIYASI VƏ DƏRIN ÖYRƏNMƏ

**Selcan Qasımzadə**
Azərbaycan Dövlət İqtisad Universiteti, Bakı, Azərbaycan
e-mail: selcan.gasimzada@gmail.com

Maşın Öyrənməsi, açıq şəkildə proqramlaşdırılmadan müəyyən bir vəziyyətdə problemi anlamaq, öyrənmək və həll etmək eləcə də böyük miqdarda verilənləri idarə etmək və onları səmərəli və effektiv hesablamaq üçündür [1]. Hazırda Süni İntellekt dövründə biz maşına keçmiş təcrübələr vasitəsilə öz-özünə öyrənməyi və ya insanın real həyatda etdiyi kimi mövcud vəziyyətə uyğun işləməyi öyrətmək üçün çalışırıq. Dərin Öyrənmə Maşın Öyrənməsinin və insan beyni neyron şəbəkəsi tərəfindən təkan verilən süni neyron şəbəkəsinin tətbiqinin alt sahəsidir. Dərin Öyrənmədə giriş qatı və çıxış təbəqəsi aralıq olaraq bir sıra gizli təbəqələrlə əlaqələndirilir [3].

Şəkildə verilənləri şifrələmək və deşifrə etmək üçün Dərin Öyrənmə üsulundan istifadə edilmişdir.




Dərin Öyrənmə şəbəkə rabitəsi arasında itmiş məlumatları geri qaytarmağa kömək edə bilər [2]. Dərin Öyrənməyə nəzarət edilən (supervised), nəzarətsiz (unsupervised) və dərindən möhkəmləndirilmiş (deepreinforcement) öyrənmə kimi müxtəlif yanaşmalar mövcuddur [5]. Biz DNT Kriptoqrafiyası və Dərin Öyrənməni birləşdirdikdə, hər ikisi konkret yanaşmalar olduğundan təhlükəsizliyin gücü və səmərəliliyi də artır.

Kriptoqrafiya, bu gün elektron təhlükəsizlik texnologiyalarının müasir dünyasında qiymətli informasiya və dataların qorunmasının təməlinə çevrilmişdir. Kriptoqrafiyanın kökləri XVIII əsrə dayanır. Ən erkən şifrələmə üsullarından bəziləri, açıq mətnin əlifbalarının bəzi başqa əlifbalarla əvəz edildiyi Sezar Şifrəsi kimi Əvəzetmə Şifrələridir Bu şifrələrin açıq mətn dilinin xüsusiyyətlərini ehtiva etməsi onların zəif və asanlıqla qırıla bilən olmasına səbəb olur.

Müasir kriptoqrafiya qeyd edilən anlayışlardan ibarətdir: Düz mətn - ötürülməli olan orijinal mesaj düz mətn kimi müəyyən edilir; Şifrə mətni - yalnız nəzərdə tutulan şəxs və ya sistem tərəfindən başa düşülə bilən mesaj şifrəli mətn kimi müəyyən edilir; Şifrələmə - düz mətnin açar istifadə edilərək

şifrəli mətnə çevrilməsi prosesi şifrələmə adlanır; Şifrənin açılması - eyni və ya fərqli açardan istifadə etməklə (şifrələmə zamanı istifadə edilən) şifrə mətninin açıq mətnə çevrilməsi prosesi şifrənin açılması kimi müəyyən edilir; Açar - rəqəm və ya alfa-rəqəm mətninin və ya xüsusi simvol mətninin kombinasiyası açar adlanır. Alqoritm açardan asılı olduğundan açar kriptoqrafiyanın ən vacib hissəsidir.

**Kriptoqrafiyanın növləri**

Gizli Açar Kriptoqrafiyası: həm şifrələmə, həm də şifrənin açılması üçün unikal tək açardan istifadə edir, simmetrik şifrələmə də adlanır. Açıq Açar Kriptoqrafiyası: şifrələmə üçün bir açıq açar və şifrənin açılması üçün şəxsi açardan istifadə edir, asimmetrik şifrələmə də adlanır.

1994-cü ildə yarandığı gündən, Leonard Maks Adleman Hamilton Path Probleminin həllini tapmaq üçün ondan istifadə etdikdə, bir çox tədqiqatçının diqqətini cəlb etdi. Kriptoqrafiya sahələrində DNT hesablamaları qırılmaz alqoritmlər üçün yeni ümidlər gətirə biləcək mümkün texnologiya kimi təsvir edilmişdir . Bu, məlumatların DNT zəncirlərində kodlaşdırıla bilməsi və bioloji əməliyyatların məlumatların daha da şifrələnməsi üçün şifrələnmiş məlumatlarda kriptoqrafik alqoritmlər əvəzinə istifadə edilə bilməsi ilə əlaqədar idi [4].

DNT, mahiyyət etibarilə, canlı orqanizmlərdə məlumat saxlayan hissəcikdir, bir nəsildən digərinə ötürülən genlərdir. Tək zəncirli DNT dörd müxtəlif əsas nüvə gelgitindən: adenin (A), timin (T), sitozin (C) və quanin (G) -dən ibarətdir. Məlumat bu dörd hərfli DNT kodunun sətirlərində saxlanılır və bu kodlar dezoksiriboza ($C_5H_{10}O_4$) birləşdirildikdə uzun informasiya ardıcıllığı yaradır.

DNT hesablamasında məlumat ənənəvi kompüterlər tərəfindən istifadə edilən ikili əlifbadan çox $\sum = (A, C, T, G)$ olaraq dörd simvollu genetik əlifba ilə təmsil olunduğundan $\sum = (0,1)$ DNT zəncirləri ənənəvi kompüterlərdə istifadə olunan yaddaş sistemlərindən daha çox məlumat saxlaya bilir.

Dərin Öyrənmə DNT Kriptoqrafiyası - DNT hesablamalarından istifadə edərək uzun DNT Ardıcıllığı kimi məlumatların gizlədilməsi prosesidir. Bu yazıda DNT-dəki nukleotidlərin ardıcıllığı kimi: A – 00 C – 01 G – 10 T - 11 istifadə edilir.

DNT-nin ən böyük üstünlüyü onun saxlama qabiliyyətidir. Bir qram DNT-də 1021 DNT bazası 108 Terabayt məlumat var ki, bu da çox yığcam formada saxlanıla bilər. Həmçinin, hesablama aparılarkən DNT hesablaması üçün heç bir güc tələb olunmur. DNT-nin qurucu blokları olan kimyəvi bağlar heç bir kənar enerji mənbəyi olmadan baş verir.

Məlumatların əvvəlcədən emalı DNT hesablamalarına əsaslanan DNT Dərin Öyrənmə kriptoqrafiyası üçün əvəzolunmazdır. Bu təbii olaraq məlumatların ikiqat təhlükəsizliyini təmin edir. DNT böyük saxlama mühiti təmin edir, beləliklə həm hesablama, həm də saxlama problemlərini həll edir. Bu, kriptosistemin bioloji proseslərdə necə tam şəkildə layihələndirilə və həyata keçirilə biləcəyini əks etdirir.

**Açar sözlər**: Kriptoqrafiya; DNT kriptoqrafiyası; İnformasiya Təhlükəsizliyi; Təhlükəsizlik texnologiyaları; Kriptoqrafiyanın növləri; Dərin Öyrənmə; DNT hesablaması.

**Ədəbiyyat**

1. Kaur H., Chauhan R., Wasan S.K. Ehtimalın qiymətləndirilməsi üçün Bayes şəbəkə modeli, İnformasiya Elmləri və Texnologiyaları Ensiklopediyası, IGI Global, Üçüncü Nəşr, 2015.
2. Liao X., Yin J., Guo S., Li X., & Sangaiah A.K. (2017). Bloklararası asılılıqların qorunmasına əsaslanan tibbi JPEG təsvir steqanoqrafiyası. Kompüterlər və Elektrik Mühəndisliyi.
3. Mislovaty, R., Klein, E., Kanter, I. and Kinzel, W. Neyrokriptoqrafiyanın təhlükəsizliyi, Elektronika, sxemlər və sistemlər üzrə 2004-cü il 11-ci IEEE Beynəlxalq Konfransının materialları, 2004.
4. Tornea O., Borda M.E., DNT kriptoqrafik alqoritmləri, MEDITECH 2009. IFMBE Proseslər, 2009.
5. Zhang R., Shen J., Wei F., Li X., & Sangaiah A.K. (2017). Çox miqyaslı qeyri-mənfi ayrı-ayrı kodlaşdırmaya əsaslanan tibbi təsvirin təsnifatı. Tibbdə süni intellekt.

**Electronic security technologies, DNA cryptography and Deep Learning**

Information has grown to be a crucial strategic resource, especially for huge organizations. Because of this, information and data security become crucial. The risks of eavesdropping encountered by the sender and the receiver have increased with the advent of new techniques and advances in information technology. To break DES, AES and other contemporary security methods, software has been created. The location of where the ciphers are kept is one of several potential weak points in a security system. Such issues are resolved by DNA cryptography, which raises the possibility of creating algorithms that cannot be cracked. The information is protected either inside the DNA or by encoding the text with DNA sequences, which can only be unlocked with the right key or DNA base sequence. We have introduced the idea of DNA Deep Learning Cryptography, which is characterized as a method of data concealment using deep learning and the DNA sequence.

## İNFORMASİYAYA QARŞI YARANAN TƏHLÜKƏLƏR VƏ ONLARIN QARŞISININ ALINMASI ÜSULLARI

**Turan Qədirova**
Heydər Əliyev adına Hərbi İnstitut, Bakı, Azərbaycan
E-mail: turan_huseynova@mail.ru

**Giriş.** Hesablama texnikası vasitəsilə informasiyanın geniş emalı cəmiyyətin informasiyalaşmasına və yeni informasiya texnologiyalarının yaranmasına səbəb oldu. Yeni texnologiyaların yaranmasının müsbət cəhəti olduğu kimi çatışmamazlıqlarıda vardır. Bu günkü gün informasiya təhlükəsizliyindən bir çox müəsisələrin işi və hətta insan həyatıda asılı ola bilər. Bunlara informasiyanın avtomatlaşdırılmış yayılma sistemini və emal sistemini misal göstərmək olar.

**1. İnformasiya təhlükəsizliyi anlayışı.** İnformasiya təhlükəsizliyi dedikdə ilk başa düşülən informasiya sistemlərinə məqsədli və ya təsadüfi ziyan verərək istifadəçi və ya istifadəçilərə ziyan vurmaqdır. İnformasiya təhlükəsizliyinin praktiki tətbiqinin 3 əsas aspekti mövcuddur: tez əldə edilə bilmə imkanı, tamlıq, gizlilik.

**2. İnformasiya təhlükəsizliyinin əsas təhlükələri.** Müasir informasiya sistemi bir-biri ilə qarşılıqlı əlaqəli və fərqli asılılıq dərəcəsi olan mürəkkəb sistemi təşkil edir. Demək olar ki, hər bir element ayrılıqda xarici təsirə məruz qala bilər və sıradan çıxa bilər.

Avtomatlaşdırılmış informasiya sisteminin komponentlərini növbəti qruplara bölmək olar:

- aparat vasitəsiləri kompyuter və onları təşkil edən hissələr (prosessor, monitor, terminal, periferiya qurğuları, disk oxuyucu, printer, kabel və s.);

- proqram təminatı əldə edilmiş yeni proqramlar, başlanğıc, obyekt, yükləmə modulu, əməliyyat sistemi və sistem proqramı, utilit, diaqnostika proqramları və s.

- maqnit oxuyucularda, çap arxivlərində, jurnal sistemlərində müvəqqəti və daimi olaraq yadda saxlanıla bilər, xidmət göstərən personal və istifadəçi, kompyuterdə yerləşən informasiya sisteminə məqsədli və ya təsadüfi təhlükəli təsir göstərmək olar.

İnformasiya sisteminin layihələndirilməsi təcrübəsi, hazırlanması və informasiya sisteminin istifadəsi göstərir ki, informasiya sistemin varlığının hər bir mərhələsində təhlükəli təsirə məruz qalır.

İstifadə zamanı informasiyanın məruz qaldığı təsadüfi təsirlərə aşağıdakıları misal göstərmək olar:

- elektrik enerjisinin kəsilməsi, qurğularda yaranan nasazlıqlar və nasazlıqlar nəticəsində qurğunun sönməsi, proqram təminatındakı səhvlər, şəxsi heyətin işindəki səhv,əlaqə kanallarında kənar təsirlər nəticəsində yaranan əngəllər.

Planlaşdırılan təsirlər pozucular tərəfindən informasiya təcavüzkarının məqsədyönlü təsirləridir. Təcavüz kimi qulluq edici, qonaq, müttəfiq və pullu tutulan şəxs ola bilər.Qanun pozucusunun əməlləri müxtəlif motivlərlə xarakterizə etmək olar. Bu motivlərə öz işindən narazı olan əməkdaş, rüşvət, marağa görə, quruculuq mübarizəsi, istənilən yolla özünü təsdiq etmə k istəyən şəxs.

Potensial pozucunun hipotetik modelini də qurmaq olar:

- verilmiş sistemin hazırlanmasında iştirak edən əməkdaş, pozucu kənar şəxs və ya sistemin öz istifadəçisi ola bilər, pozucuya sistemin iş prinsipi məlum ola bilər.

Pozucular adətən sistemin qorunması zəif olan bölməsinə təsir edə bilirlər. Daha çox yayılmış və çoxsahəli kompyuter pozuntuları qanunsuz müdaxilə nəticəsində baş verir.Qanunsuz müdaxilə sistemin istənilən zəif nöqtəsindən təsir edə bilər. Qanunsuz müdaxilə nəticəsində informasiyanın oğurlanması, dəyişdirilməsi və məhv edilməsini növbəti şəkildə siniflərə bölmək olar.

İnsan vasitəsilə: informasiya daşıyıcısının oğurlanması, informasiyanın ekran və ya klaviaturadan oxunması, çap şəklində olan informasiyanın oxunması.

Proqram vasitəsilə: kodun əldə edilməsi, şifrlənmiş informasiyanın deşifrlənməsi, informasiya daşıyıcısından qurğu vasitəsilə informasiyanın sürətinin çıxarılması.

Qurğu vasitələri: 1. İnformasiyaya müdaxilə etmək üçün xüsusi hazırlanmış aparat vasitələrinin qoşulması; 2. Əlaqə vasitələri, elektrik gərginlik şəbkələrində yayılan mənfi təsirli elektromaqnit şualanmaların əldə edilməsi.

Ən çox kompyuter şəbəkələrində olan təhlükələrə diqqət yetirmək lazımdır. Kompyuter şəbəkəsinin xüsusiliyi onun tərkib hissələrinin boşluqda paylaşdırılmış olmasıdır. Şəbəkə düyünləri arasındakı əlaqə fiziki olaraq şəbəkə xətləri və mesajlar mexanizmi ilə yaradılır. Bununla belə şəbəkə düyünləri arasında idarəedici mesaj və verilənlər paketlər şəklində düzülürlər. Şəbəkələrə hücum əsas serverdə 1000 km-lər qədər uzaq məsafələrdə həyata keçirilə bilər və bu zaman təkcə komyuter deyil orada saxlanılan məlumatda hücuma məruz qalır.

**3. İnformasiya təhlükəsizlyinin təminatı.** İnformasiya təhlükəsizliyinin formalaşdırılması kompleks problemdir və onu 5 mərhələyə bölmək olar: Qanunvericilik (qanun, normativ akt, standart), mənəvi-etik (özünü aparma qaydaları və s), adminstrativ (ümumi xarakter əməliyyatları), fiziki (mexaniki, elektro və elektromexaniki məhdudiyyətlər), aparat-proqram (elektrik qurğular və informasiya qorunmasının xüsusi proqramları).

Bütün qeyd edilən 5 bölmə birləşərək müdafiə sistemini yaradır. Ən etibarlı müdafiə sistemi növbəti prinsiplərə malik olmalıdır: qorunmaya xərclənən vəasit dəyəcək ziyandan az olmalıdır və hər bir istifadəçi minimal üstünlük dərəcəsinə malik olmalıdır.

**4. İnformasiya təhlükəsizliyinin qorunmasının aparat proqram təminatı.** Baxmayaraq ki, müasir əməliyyat sistemləri Windows 2000, Windows XP, Windows NT informasiyanın qorunması üçün öz altsistemləri vardır yenədə əlavə proqramların yaradılmasına ehtiyac duyulur. Bir çox sistemlər onlardan kənarda məsələn şəbəkədə yerləşən informasiyanı qoruya bilmirlər. İnformasiyanın qorunmasının aparat-proqram təminatını aşağıdakı bölmələrə ayırmaq olar: 1.İstifadəçilərin identifikasiya sistemləri (tanıma) və audentifikasiya (həqiqiliyin tanınması). Bu tip verilənlərin əsas məqsədi sistemə daxil olaraq orada yerləşən məlumatdan istifadə etmək istəyən istifadəçinin kimliyini təsdiq etmək və onun təhlükəsiz olduğunu müəyyən etdikdən sonra sistemə daxil olmaq icazəsini verməkdir. 2.Disk verilənlərin şifrlənmə sistemi. Kriptoqrafiya adlanan vasitələrlə verilmiş informasiyanı müttəfiqlər üçün lazımsız səviyyəyə çatdırır. Sistem verilənləri fayl və disk səviyyəsində kriptoqrafik olaraq dəyişdirir. Bunlara ARY və RAR arxivləşdirmə proqramlarını misal göstərmək olar. 3.Şəbəkədə ötürülən disk verilənlərinin şifrlənmə sistemi. Bu vasitələrdə əsas 2 şifrlənmə vasitəsi vardır: kanal şifrlənmə və abonent şifrlənməsi. Kanal şifrlənməsi zamanı bütün informasiya şifrlənir. Abonent şifrlənməsi isə iki istifadəçi arasında ötürülən informasiyanı qoruyur. 4.Elektrik verilənlərinin audentifikasiya sistemi. Məlumatların şəbəkədə ötürülməsi zamanı həm məlumatın, həm də müəllifin qorunması problemi meydana çıxır.Verilənlərin audentifikasiyası üçün mesajların identifikasiya kodu və ya elektron imzadan istifadə edir. 5. Kriptoqrafik açarların idarə edilməsinin idarə sistemi. İstənilən kriptosistemlərin təhlükəsizliyi nəticəsində təcavüzkar tam və ya bütün informasiyanı ələ keçirə bilər.

**Nəticə.** İnformasiya resursdur. İnformasiyanın itirilməsi maddi və mənəvi zərərə gətirir. Müasir qurğularda informasiya təhlükəsizliyi xüsusi kompleks sistemlərlə təchiz edilir. İnformasiyanın kompleks müdafiə sistemi: kəsilməz, planlı, məqsədyönlü, aktiv, konkret, etibarlı

olmalıdır. Müasir cəmiyyətimizin əsasında informasiya resursu durur və bu resursun ziyan görməsinin qarşısı mümkün dərəcədə alınmalıdır.

**Açar söz:** informasiya, təhlükəsizlik, proqram, istifadəçi.

**Ədəbiyyat**

1.İnformasiya təhlükəsziliyi - http://protect.htmlweb.ru
2.İnformasiya təhlükəsziliyi – https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html

**Threats to information and methods of their prevention**

Information is a resource. Loss of information causes material and moral damage. Information security in modern devices is equipped with special complex systems. Complex protection system of information: should be continuous, planned, purposeful, active, specific, reliable. The basis of our modern society is the information resource, and damage to this resource should be prevented as much as possible.

## "ZERO TRUST" MODELİ İLƏ TƏHLÜKƏSİZLİK ARXİTEKTURASININ QURULMASI

**İradə Quliyeva**
Azərbaycan Dövlət İqtisad Universiteti, Bakı, Azərbaycan
e-mail: iquliyeva21@gmail.com

**Xülasə**

"Zero Trust" arxitekturası kibertəhlükəsizliyə müasir yanaşmadır - bulud xidmətləri ilə getdikcə daha çox müəyyən edilən İT ekosisteminin ən son tendensiyalarına və ehtiyaclarına cavabdır. Ölkəmizdə ZTA-nın tətbiqi bir gündə baş verməsə də, keçidə kömək etmək üçün alətlər və həllər artıq mövcuddur. Ümumi təhlükəsizlik vəziyyətini yaxşılaşdırmaq istəyən təşkilatlar təhlükəsizlik modellərini yenidən qiymətləndirmək və ZTA kimi ən son sənaye təcrübələrinə doğru hərəkət etmək üçün mövcud texnologiyalardan və dizayn nümunələrindən istifadə edə bilərlər.

"Zero Trust" (sıfır etibar) 2010-cu ildə keçmiş Forrester analitiki Con Kindervag tərəfindən hazırlanmış təhlükəsizlik modelidir [1]. O vaxtdan bəri "Zero Trust" modeli kibertəhlükəsizlik sahəsində ən məşhur konsepsiyaya çevrildi. Bu yaxınlarda baş verən kütləvi məlumat sızıntıları şirkətlərin kibertəhlükəsizliyə daha çox diqqət yetirməsi zərurətini təsdiqləyir və Zero Trust modeli bunun üçün düzgün yanaşma ola bilər.

Son bir neçə ildə bütün beynəlxalq informasiya təhlükəsizliyi ictimaiyyətinin diqqəti "Zero Trust" Arxitekturasına (ZTA) yönəlir: müxtəlif beynəlxalq platformalarda aktiv müzakirələr gedir, kommersiya və dövlət təşkilatlarının müvafiq metodik sənədləri peydə olur. Belə ki, xüsusilə, bu ilin (2022) yanvar ayının sonunda ABŞ agentlikləri və departamentləri üçün ZTA-ya keçidlə bağlı tövsiyələri əks etdirən memorandum çap olundu.

Bu arxitekturanın əsas prinsipi təhlükəsizlik perimetri xaricində və ya daxilində fəaliyyət göstərən heç bir şəxsə, sistemə, şəbəkəyə və ya xidmətə etibar edilməməsidir. Bu model hər bir istifadəçinin və ya cihazın şəbəkə daxilində və ya kənarda hansısa resursa giriş tələb etdikdə hər dəfə öz məlumatlarını təsdiq etməli olduğunu nəzərdə tutur [3].

Bundan əlavə, proqramlar icazəsiz girişdən qorunmaq üçün şəbəkə perimetri təhlükəsizliyinə etibar edə bilməz. İstifadəçilər şəbəkəyə deyil, proqram və tətbiqlərə daxil olmalıdırlar və korporativ proqramlar İnternet üzərindən istifadə oluna bilməlidir.

Ənənəvi təhlükəsizlik arxitekturaları müəyyən fərziyyələrə əsaslanaraq bütün məlumatların və əməliyyatların standart olaraq təhlükəsiz olduğunu güman edir. Bununla belə, verilənlərin sızıntısı, serverə icazəsiz giriş və digər insidentlər bu etibarı sarsıda bilər. “Zero Trust” arxitekturası etibar modelini elə dəyişdirir ki, bütün məlumatlar və əməliyyatlar əvvəldən etibarsız hesab edilir.

ZTA qurmaq üçün bir neçə yanaşma var: identifikasiya idarəetməsi, məntiqi mikro seqmentasiya və şəbəkə əsaslı seqmentasiya. Bu yanaşmaların hər biri eyni məqsədə malikdir: bir tətbiqi və ya komponenti pozan bədniyyətli təşkilat daxilində asanlıqla hərəkət edə bilməməsi üçün mühitləri mümkün qədər təcrid etmək [2].

Təşkilatdakı hər bir məsul şəxs “Zero Trust” arxitekturasının necə işlədiyini tam başa düşməlidir. “Zero Trust” arxitekturasını həyata keçirmək üçün təşkilatın İT sistemlərinin tam transformasiyası mürəkkəb bir prosesdir. Bunun əvəzinə təşkilatlar kiçik addımlarla öz təhlükəsizliklərini daim təkmilləşdirməyə çalışmalıdırlar. Azərbaycanda müəssisələrin “Zero Trust” arxitekturasına keçidi belə görünə bilər:

1. Təşkilatın işçilərinin müəssisə tərəfindən idarə olunan hesabları var ki, bu da onlara işlərini təhlükəsizliyi qoruyaraq yerinə yetirmək üçün lazım olan hər şeyə daxil olmaq imkanı verir.
2. İşçilərin öz işlərini yerinə yetirmək üçün istifadə etdikləri cihazlara daim nəzarət edilir və daxili resurslara giriş verilərkən onların təhlükəsizlik səviyyəsi nəzərə alınır.
3. Təşkilatın sistemləri bir-birindən təcrid olunur və onların arasından və daxilindən keçən şəbəkə trafiki şifrələnir və autentifikasiya olunur.
4. Müəssisə proqramları daxili və xarici sınaqdan keçirilir və işçilər tərəfindən İnternet üzərindən təhlükəsiz şəkildə istifadə edilə bilər.
5. Təhlükəsizlik şöbələri məxfi məlumatlara icazəsiz girişi avtomatik aşkar etmək və bloklamaq üçün verilənlər kateqoriyalarını və təhlükəsizlik qaydalarını müəyyən edir.

**Açar sözlər:** informasiya təhlükəsizliyi, “Zero Trust” Arxitekturası (ZTA), kibertəhlükəsizlik.

**Ədəbiyyat**

1. Kindervag John (2010-11-05). Build Security Into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research. Retrieved 2022-07-22.
2. Rose S., Borchert O., Mitchell S., Connelly, S. Zero Trust Architecture. *nvlpubs.nist.gov*. NIST. Retrieved 17 October 2020.
3. Zero Trust Security: An Enterprise Guide [Garbis Jason, Jerry W. Chapman] 2021.

**Establıshıng a securıty archıtecture wıth “Zero Trust” model**

Zero Trust Architecture is a modern approach to cybersecurity - a response to the latest trends and needs of an IT ecosystem that is increasingly defined by cloud services. While ZTA in our country doesn't happen overnight, tools and solutions are already available to help with the transition. Organizations that want to improve their overall security posture can use existing technologies and design patterns to re-evaluate security models and move towards the latest industry practices such as ZTA.

## ONLAYN SOSİAL ŞƏBƏKƏLƏRDƏ ANOMALİYALARIN AŞKARLANMASI VƏ MAŞIN ÖYRƏNMƏ METODLARININ TƏTBİQİ

**Dilarə Quluzadə, Validə Məmmədova**
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
e-mail: dilare.quluzade@aztu.edu.az, memmedova.valide@aztu.edu.az

Son onillikdə onlayn sosial şəbəkələrdə istifadəçilərin sayında, texnologiya imkanlarında böyük irəliləyiş aydın şəkildə nəzərə çarpır. Onlayn Sosial şəbəkə (OSŞ) virtual cəmiyyətdəki insanlar arasında faylların mübadiləsini və interaktiv əlaqəni təmin edən veb xidmətləri kimi müəyyən edilə bilər.

OSŞ-dəki zərərli fəaliyyətlər, anormal davranışlar sadə spam göndərməklə məhdudlaşmır, istifadəçilərin məxfiliyini pozmağa meylli olan nisbətən daha ağıllı hücumlara çevrilir. Zərərli fəaliyyətlərin aşkarlanması OSŞ-də istifadəçilərin məxfiliyinin pozulmasının qarşısını almaq üçün çox vacibdir. Sosial medianın və onlayn sosial sistemin eksponent böyüməsi səbəbindən bir çox sosial şəbəkələr zərərli şəxslər üçün əsas hədəf obyektinə çevrilib. Bununla əlaqədar olaraq son dövrlərdə saxta profillər yaratmaq, spam göndərmə, sybil hücumları və s. kimi halların yüksək sürətlə artması müşühidə olunur [1].

OSŞ-də anomaliya, istifadəçilərin əksəriyyətindən kənara çıxan anormal və ya gözlənilməz davranış kimi adlandırıla bilər. Facebook, Twitter və s. kimi sosial şəbəkələrin populyarlığı ilə əlaqədar olaraq son dövrlərdə zərərli fəaliyyətlər artıb. Anomaliyaların aşkarlanması tədqiqatçılar üçün vacib bir sahəyə çevrilmişdir [2]. Bəzi mənbələrə görə anomaliyalara kənar göstəricilər, yeniliklər, səs-küy, sapmalar və istisnalar aid edilə bilər. Anomaliyaların aşkarlanması gözlənilən nümunəyə uyğun gəlməyən hadisələrin və ya müşahidələrin müəyyən edilməsidir. Anomaliya aşkarlanması müdaxilənin aşkarlanması, saxtakarlığın aşkarlanması, nasazlığın aşkarlanması, sistemin sağlamlığının monitorinqi, sensor şəbəkələrində hadisələrin aşkarlanması və s. kimi müxtəlif sahələrdə tətbiq olunur [5]. OSŞ-lərdə anomaliyaların aşkarlanması taksonomiyasını aşağıda göstərildiyi kimi hissələrə bölmək olar:

*Qrafik əsaslı aşkarlama* - İstifadəçilər arasındakı sosial əlaqələr asılılıq qrafiki yaratmaq üçün istifadə edilir. Bu qrafiklər gözlənilməz davranışı və ya anormal fəaliyyət göstərən hər hansı istifadəçi

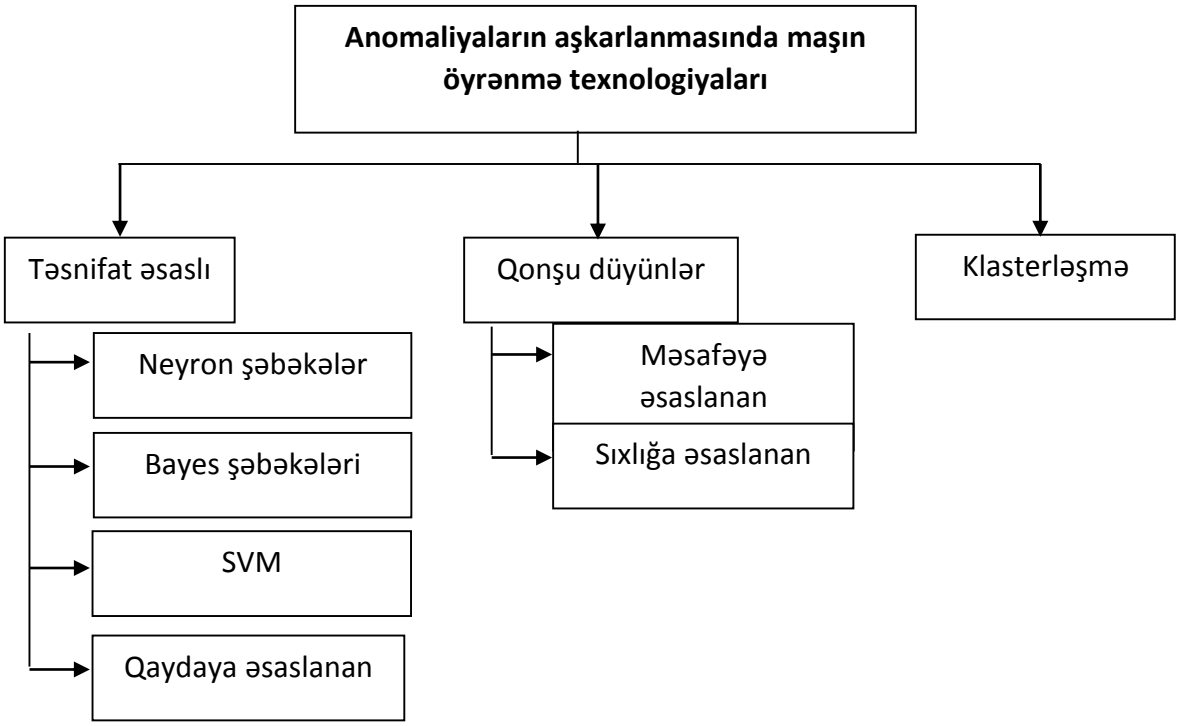
və ya qrupu tapmağa kömək edir. Belə qrafiklər üzrə anomaliyaların aşkarlanması qrup əsaslı; istifadəçi əsaslı kimi iki əsas istiqamətdə aparılır:

*Təhdid modelləşdirmə əsaslı aşkarlanma* - Təhlükənin modelləşdirilməsi OSŞ-lərdə hər hansı növ anomaliyaları tapmağa kömək edir. Təhdidlərin modelləşdirilməsi davranışlar, istifadəçilər arasında məlumat axını, istifadəçilərin və icmaların xüsusiyyətləri kimi müxtəlif parametrlərin köməyi ilə həyata keçirilir. Təhdid modelləşdirməyə əsaslanan anomaliya aşkarlanması siyasət/qayda əsaslı; davranışa əsaslı kimi iki əsas istiqamətdə aparılır:

*Analiz əsaslı aşkarlama* - OSŞ-lərdə məlumat verilənlər toplusu şəklində saxlanılır. Bu verilənlər bazasında anomaliyalar fərdi və ya üçüncü tərəf operatorları tərəfindən təhlil və məlumatların çıxarılmasının köməyi ilə aşkar edilir. Bundan əlavə, analiz OSŞ verilənlər bazası üzərində dinamik və ya statik olaraq həyata keçirilə bilər. Analizə əsaslanan anomaliya aşkarlanması statistika əsaslı; maşın öyrənmə əsaslı; klaster əsaslı; fərdi izləmə əsaslı kimi istiqamətlərdə həyata keçirilir [3,8].

Dərin öyrənmə, maşın öyrənmə metodlarının ən geniş tətbiq sahələrindən biri kimi sosial media analizinə (sosial şəbəkələrdə istifadəçi davranışlarının izlənilməsi, saxta profillərin müəyyənləşdirilməsi və s.) aid edilir. Anomaliyaların aşkarlanması kontekstində maşın öyrənməsi alqoritmi adətən görünməyən şəbəkə anomaliyalarına uyğunlaşan xəritələşdirməni təmin edir [4].

OSŞ-də anomaliyaların aşkarlanması texnologiyalarının təsnifatını aşağıdakı blok sxem vasitəsilə nəzərən keçirək:




**Şəkil 1.**OSŞ-də anomaliyaların aşkarlanmasında maşın öyrənmə texnologiyaları

*Təsnifat əsaslı:* Bu alqoritmlərin xüsusiyyətləri hər bir məlumat nümunəsini əvvəlcədən müəyyənləşdirilmiş siniflər üzrə təyin etməkdir. Tipik nümunələrə aşağıdakılar daxildir:

- *Neyron şəbəkələri*;
- *Bayes şəbəkələri;*
- *SVM;*
- *Qaydaya əsaslanan.*

*Qonşu düyünlər (KNN):* Bu alqoritmlər verilmiş məlumata uyğun ən yaxın nümunələr arasındakı məsafəni metrik olaraq ölçməklə məsafəyə əsaslanan, ya da sıxlığa əsaslanan funksiyalardan istifadə edir [5].

*Klasterləşmə.* Bu nəzarətsiz öyrənmə alqoritmləri oxşar təlim verilənləri nümunələrinin qruplarını (yəni klasterləri) müəyyən etməyə çalışaraq fəaliyyət göstərir.

**Açar sözlər:** onlayn sosial şəbəkələrdə arzuolunmaz davranışlar, anomaliyalar, maşın öyrənmə metodları ilə anomaliyaların aşkarlanması.

## Ədəbiyyat

1. https://fardapaper.ir/mohavaha/uploads/2019/03/Fardapaper-Anomaly-detection-in-online-social-network-A-survey.pdf
2. https://www.kdd.org/exploration_files/Vol18-Issue1.pdf.
3. https://arxiv.org/pdf/1901.03407.pdf.
4. https://link.springer.com/article/10.1007/s00530-020-00731-z.
5. https://www.researchgate.net/publication/348905144_Deep_learning_methods_for_anomalis_detection_in_social_networks_using_multidimensional_networks_and_multimodal_data_a_survey.
6. An efficient hybrid system for anomaly detection in social networks.
7. S42400-021-00074-w.pdf.
8. https://www.researchgate.net/publication/364359768_Sosial_sbklrd_thluksizlik_prinsiplri_v_anomaliyalarin_askarlanmasi.

## Establıshıng a securıty archıtecture wıth “zero trust” model

Zero Trust Architecture is a modern approach to cybersecurity - a response to the latest trends and needs of an IT ecosystem that is increasingly defined by cloud services. While ZTA in our country doesn't happen overnight, tools and solutions are already available to help with the transition. Organizations that want to improve their overall security posture can use existing technologies and design patterns to re-evaluate security models and move towards the latest industry practices such as ZTA.

# BİG DATA TEXNOLOGİYALARINDA TƏHLÜKƏSİZLİK PROBLEMLƏRİ

**Aynur Səmədova**
Azərbaycan Dövlət İqtisad Universiteti, Bakı, Azərbaycan
e-mail: aynur_samedova99@mail.ru

Bəzi layihələr informasiya təhlükəsizliyi nəzərə alınmadan tərtib edilir və həyata keçirilir ki, bu da mühafizə əhəmiyyətinin artmasına səbəb olur. İnformasiya təhlükəsizliyi nəzərə alınmadıqda sistemlər və bəzən biznes üçün kədərli nəticələrə səbəb olur. Böyük verilənlər layihələrini həyata keçirərkən təhlükəsizlik məsələləri əvvəldən nəzərə alınmalıdır, əks halda layihələr biznes imkanlarından yeni biznes risklərinə çevrilə bilər.

Bu gün Big Data texnologiyaları biznes üçün əhəmiyyətli bir mövqedə dayanır. Satışların artırılması, xərclərin azaldılması, riskin azaldılması, əməliyyat səmərəliliyinin yüksəldilməsi-Big Datanın biznes problemlərinin həllində əldə etdiyi qazanclardan yalnız bir neçəsidir. Big Data texnologiyaları müxtəlif sənaye sahələrində istifadə olunur: telekommunikasiya, maliyyə, pərakəndə satış, səhiyyə, informasiya texnologiyaları və bir çox başqa sahələr.

Big data layihələri üçün təhlükəsizlik - təkcə verilənləri əlçatan etmək məsələsi deyil. Təhlil üçün mənbə kimi xidmət edən verilənlər, bir qayda olaraq, biznes üçün həssas məlumatları ehtiva edir: ticarət sirləri, şəxsi məlumatlar. Bu cür məlumatlarla işləməyin məxfiliyinin pozulması ciddi problemlərlə, o cümlədən tənzimləyicilərdən cərimələr, müştərilərin xaricə axını, bazar kapitallaşmasının itirilməsi ilə nəticələnə bilər.

Big Data layihələrinin digər mühüm problemi həm təhlil edilən məlumatların, həm də onların işlənməsi zamanı əldə edilən kommersiya dəyəri olan nəticələrin bütövlüyünü təmin etməkdir.

Narahatlıq üçün bir çox səbəb var. Sızmalarla bağlı hesabatlar heyrətamizdir: 2017-ci ilin birinci yarısında Gemalto-ya görə, dünyada 1,9 milyarddan çox, InfoWatch-a görə - 7,78 milyarda qədər qeyd sızdırılıb ki, bu da ötən illə müqayisədə bir neçə dəfə çoxdur. Əgər təhlükəsizlik məsələlərinə lazımi diqqət yetirilməsə, o zaman sızmaların həcmi qat-qat arta bilər.

Big Data texnologiyalarını qorumaq üçün mövcud yanaşmalar vahid qorunma konsepsiyası tədbirlərinə əsaslanır. Bu gün strukturlaşdırılmış və strukturlaşdırılmamış Big Dataların qorunması üçün sistematik addımları və hərəkətləri təsvir edən dəqiq müəyyən edilmiş metodlar yoxdur. Kritik məlumatların emalının bütün mərhələlərində - toplanması və ötürülməsindən təhlil və saxlanmasına qədər onların qorunmasına yönəlmiş yanaşmalar tələb olunur. Big Data standartlaşdırılmasında bir sıra aparıcı standartlar institutları iştirak edir: Beynəlxalq Standartlaşdırma Təşkilatı və Beynəlxalq Elektrotexniki Komissiya (ISO/IEC), Beynəlxalq Telekommunikasiya İttifaqı (ITU), Britaniya Standartlar İnstitutu (BSI), ABŞ Milli Standartlar və Texnologiya İnstitutu (NIST). "Rusiya Federasiyasının Rəqəmsal İqtisadiyyatı" dövlət proqramının "İnformasiya Təhlükəsizliyi" bölməsində böyük məlumatların qorunması məsələlərinə də xüsusi diqqət yetirilir.

Ən uzaq irəliləyən NIST , böyük verilənlərlə işin bütün aspektlərini təsvir edən sənədləri özündə birləşdirən Interoperability Framework V1.0 spesifikasiyası [1]: “Təriflər”; Taksonomiyalar;

"İstifadə halları və tələblər"; "Təhlükəsizlik və Məxfilik"; "Memarlıq Ağ Kağız Sorğusu"; "İstinad Memarlığı"; Standartların Yol Xəritəsi. Bu dəstdə təchizatçılara, texnologiyalara və layihələrin infrastruktur xüsusiyyətlərinə münasibətdə neytral olan böyük verilənlər arxitekturasının konseptual modelini təqdim edən informasiya təhlükəsizliyi məsələlərini də əhatə edən metodologiya var. NBDRA (NIST Big Data Reference Architecture) konseptual modeli qarşılıqlı fəaliyyət interfeysləri ilə birləşdirilmiş beş məntiqi funksional komponentdən ibarət böyük verilənlər sistemidir: Məlumat təminatçıları və proqram təminatçıları arasında qarşılıqlı əlaqə; proqram təminatçısı və məlumat istehlakçıları arasında interfeys; tətbiq təminatçısı və böyük məlumat platforması arasındakı interfeys; müxtəlif texnologiyaların və böyük məlumat platformalarının daxili qarşılıqlı əlaqəsində məlumatların qorunması; böyük verilənlər sistemi nəzarətinin təmin edilməsi.

Interoperability Framework tələblərinin praktiki həyata keçirilməsinə misal olaraq, NIST ekspertləri Bulud Təhlükəsizlik Alyansının (CSA) [2] inkişaflarına işarə edir və dörd qorunma sahəsinə diqqət yetirməyi tövsiyə edirlər: infrastrukturun təhlükəsizliyi; məlumat məxfiliyi; məlumatların idarə olunması; dürüstlük və cavab prosedurları.

Böyük verilənlər sistemlərinin mühafizəsi üzrə layihələrin həyata keçirilməsi üçün əsas müvafiq məsələlərin kompleks həllini nəzərdə tutan Data-Centric Security yanaşması olmalıdır.

Mühafizə sistemlərini tərtib edərkən, layihə komandasına keyfiyyətli nəticə əldə etməyə kömək edə biləcək bir sıra sənədlərə diqqət yetirilməlidir. CSA bu cür sistemlər üçün təhlükəsizliyin layihələndirilməsi və tətbiq edilməsində bilik və təcrübə toplayan böyük verilənlər sistemlərinin təhlükəsizliyini təmin etmək üçün ən yaxşı təcrübələr sənədini nəşr etdi [3]. Avropa İttifaqının Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi (ENISA) təhdidlərin siyahısını və onların qarşısının alınması üçün tövsiyələri özündə əks etdirən sənəd hazırlayıb - Böyük Məlumat Təhlükəsizliyi Landşaftı və Yaxşı Təcrübə Bələdçisi [4]. Bundan əlavə, unutmamalıyıq ki, dizayn edilmiş sistem əlavə texniki xidmət, qorunma vasitələri və tədbirlərinin monitorinqi və buna görə də müvafiq əməliyyat xərcləri tələb edəcəkdir.

**Açar Sözlər:** Big Data, təhlükəsizlik, informasiya təhlükəsizliyi.

## Ədəbiyyat

1. Big Data Threat Landscape and Good Practice Guide.
   URL: file:///C:/Users/user/Downloads/Big%20Data%20Threat%20Landscape.pdf (5.12.2017)
2. Big Data Taxonomy, Cloud Security Alliance.
   URL: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Taxonomy.pdf (5.12.2017).
3. Big Data Security and Privacy Handbook: 100 Best Practices in Big Data Security and Privacy. Cloud Security Alliance URL: https://downloads.cloudsecurityalliance.org/assets/research/big-data/BigData_Security_and_Privacy_Handbook.pdf
4. NIST Special Publication 1500-1. NIST Big Data Interoperability Framework. URL: https://bigdatawg.nist.gov/uploadfiles/NIST.SP.1500-1.pdf (5.12.2017).

**Securıty problems ın bıg data technologıes**

Some projects are designed and implemented without taking into account information security, which increases the importance of protection. Ignoring information security can have dire consequences for systems and sometimes businesses. When implementing big data projects, security issues must be considered from the beginning, otherwise projects can turn from business opportunities into new business risks.

## SİLAHLI QÜVVƏLƏRDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ VƏ ONUN İDARƏ EDİLMƏSİ

**Naibə Şəmşiyeva**
Heydər Əliyev adına Hərbi İnstitut, Bakı, Azərbaycan
e-mail: naibashamshiyeva04@mail.ru

Giriş. Cəmiyyətin inkişafının müasir mərhələsi informasiya mühitinin artan rolu ilə xarakterizə olunur. Vətəndaşların, cəmiyyətin və dövlətin həyatında informasiyanın, informasiya resurslarının və texnologiyalarının rolunun genişlənməsi informasiya təhlükəsizliyi məsələlərini ön plana çıxarır [1, s.12].

Müasir dövrdə müharibə aparılması taktikasında tətbiq olunan son yeniliklər informasiya təhlükəsizliyi məsələsinin əhəmiyyətliliyini artırır, bizləri ona yeni rakursdan baxmağa vadar edir. Xüsusən də hazırda dünyada baş verən silahlı münaqişələr zamanı geniş şəkildə tətbiq edilən müasir hibrid döyüş üsulları, Silahlı Qüvvələrin informasiya təhlükəsizliyini təmin etməyi labüd bir zərurət kimi ortaya qoyur, onu prioritet bir məsələ kimi önə çəkir.

Hibrid müharibə (*hybrid warfare*) – təcavüzkarın klassik hərbi müdaxiləyə (odlu döyüş texnikası) müraciət etmədiyi, ancaq gizli əməliyyatlar, təxribatlar, kiberhücumlar kombinasiyasından istifadə edərək, düşmən bölgəsində fəaliyyət göstərən üsyançılara dəstək verən müharibə növüdür. [3, s.110].

**Əsas hissə.** Strateji bir sahə kimi digər dövlət qurumları içərisində böyük əhəmiyyət kəsb edən Silahlı Qüvvələrin informasiya təhlükəsizliyi, həm də dövlətin özünün təhlükəsizliyinin qarantı kimi çıxış edir. Ordunun informasiya resurslarının mühafizəsi, təhlükəsizlik mütəxəssisləri üçün prioritet məsələ kimi daim diqqətdə saxlanılmalıdır. Orduda informasiya təhlükəsizliyinin təmin olunması üçün zəruri olan tədbirlər kimi beynəlxalq hüquqi mexanizmlərin ciddi araşdırılması, milli normativ-hüquqi bazanın formalaşdırılması, təhlükəsizlik siyasətinin təkmilləşdirilməsi, xüsusi texnologiyaların tətbiqi, ölkə və korporativ səviyyədə informasiya təhlükəsizliyinin monitorinqi və menecmentinin aparılması, kadr hazırlığı kimi məsələlərə önəm verilməlidir.

Beynəlxalq təcrübəyə əsaslansaq, bu sahədə mümkün təhdidləri üstün keyfiyyətə malik, təsirli üsullarla zərərsizləşdirmək üçün onları mənşəyinə və təsir dairəsinə, təhlükəlilik dərəcəsinə görə

müəyyən etmək və təsnifata ayırmaq lazımdır. Mütəxəssislər təhlükənin mənbələrini iki qrupa ayırırlar: 1. Daxili mənbələr; 2. Xarici mənbələr [4, s.18].

***Daxili təhlükə mənbələri*** qismində təhdidlər, ölkə sərhədləri daxilində informasiya xarakterli texniki təhdidləri ( yerli əhalinin milli-etnik xüsusiyyətlərinə əsaslanan təxribat əməlləri fonunda təhdidlər), hərbi texnikanın təhlükəsizliyinə yönəlik təhdidləri (sistemə yanlış kodun daxil edilməsi fonunda təhdidlər) və s. özündə ehtiva edir [4, s.18].

***Xarici təhdid mənbələri*** ölkə sərhədlərindən kənarda yerləşən dislokasiya yelərini əhatə edir. Bu təhlükə növü çoxşaxəlidir, onun vasitəsilə yeni informasiya və şəxsi heyətə psixoloji təsir tədbirləri hazırlanır və o, düşmən tərəfindən müntəzəm istifadə olunur [4, s.19].

Son dövrlər Silahlı Qüvvələrin təhlükəsizliyi üçün ciddi problemə çevrilən mənbələrdən biri də cəmiyyət üzərində hakim gücə malik olan sosial şəbəkələrdir. Hərbi qulluqçular onlardan istifadə etdikləri zaman təsadüfən də olsa vacib məlumatları (dislokasiya yerləri, özləri haqqında informasiyaları) yayaraq həm özlərini, həm də tərkibində olduqları hərbi birləşmələri ciddi risklərlə üz-üzə qoyurlar. Çox təəssüf ki, biz bunun bəzi acı nəticələrini Vətən Müharibəsi zamanı yaşamalı olduq. Dövlətin təhlükəsizliyinin qorunmasında əsas vəzifələrdən biri belə təhlükələrin vaxtında aşkar edilməsi və dərhal aradan qaldırılması olmalıdır. İnformasiyanın qorunması və təhlükəsizliyin təmin edilməsi üçün tətbiq edilməsi nəzərdə tutulan tədbirlər də öz növbəsində iki qrupa bölünür:

- informasiya sistemlərinin zədələnmədən və informasiyanın sızma və ələ keçirilməsindən qorunması; - kadrların psixikasının qəsdən məlumat və psixoloji təsirdən qorunması.

*Birinci qrup tədbirlər:* - qoşunların dislokasiya obyektlərinin və onlarda yerləşən avtomatlaşdırılmış idarəetmə sistemlərinin və kompüter texnikasının yanğın və ya məqsədli şəkildə qəsdlər nəticəsində yararsız hala düşməkdən mühafizəsi; - dövlət və ya hərbi sirr xarakteri daşıyan məlumatların sızmalardan və ya məqsədyönlü oğurluqdan qorunması;

*İkinci qrup tədbirlərə aşağıdakılar daxildir:* - qoşunların psixikasının məqsədyönlü psixoloji təsirdən qorunması; - potensial rəqib tərəfindən yayımlanan məlumatın korreksiyası [5, s.480].

***Hərbi qulluqçuların məqsədyönlü psixoloji təsirdən qorunması.*** Qoşunların mənəvi və psixoloji təminatı hibrid müharibə zamanı tətbiq olunan tədbirlərin qarşısını almağa yönəlmiş bir sıra tədbirlərdən istifadəni ehtiva edir. Orduda belə tədbirlər aşağıdakılardan ibarətdir:

- psixikaya təsir yollarına dair tədqiqatların aparılması; - hərbi qulluqçularla bütün mövcud sosial-psixoloji vasitələrdən istifadə etmək, - məqsədyönlü mühafizə tədbirlərinin həyata keçirilməsi. [2, s.4].

***Profilaktik tədbirlər.*** Potensial rəqibin hansı tədbirlər kompleksindən istifadə edəcəyini əvvəlcədən müəyyənləşdirməyi bacarsaq, onun imkanlarını zəiflətmək, hadisələri qabaqlamaq üçün alternativ hücum vasitələrindən istifadə etməklə məqsədimizə nail ola bilərik. Bunun üçün aşağıdakı tədbirlər realllaşdırılmalıdır: [6, s.522].

- informasiya təhlükəsizliyinə təhdidlərlə mübarizənin təklif olunan tədbirləri və üsulları ilə bağlı düşməni qəsdən çaşdırmaq;
- düşmənin informasiya sistemlərinin işinə qəsdən təhrifedici məlumatların daxil edilməsi;

***İnformasiya silahı.*** İnformasiya silahlarının hazırlanması da müdafiə strategiyasının ayrıca istiqaməti kimi nəzərdən keçirilir. O, təkcə təhdidləri dəf etmək üçün deyil, həm də onları qabaqlamaq üçün hazırlanmalıdır. Düşmən informasiya silahlarından kifayət qədər səmərəli istifadə edir, bunu hərbi münaqişələrə qərq olmuş ölkələrin nümunəsində də görmək olar [6, s.523].

**Nəticə.** Hərbi sahədə uğurlu informasiya təhlükəsizliyi strategiyası siyasi, hüquqi, idarəetmə və texnoloji səviyyələrdə həllər təklif edən multi-disiplinar yanaşmaya əsaslanaraq təşkil edilərsə, uğurlu nəticələr əldə etmək olar. Hibrid müharibələr fonunda informasiya sahəsində kəskinləşən beynəlxalq rəqabət şəraitində informasiya təhlükəsizliyinin etibarlı təmin edilməsi dövlətin texnoloji müstəqilliyi ilə müəyyən edilir və mükəmməl nəticələrin əldə olunması üçün bu amil mühüm şərt kimi çıxış edir.

**Açar sözlər:** informasiya təhlükəsizliyi, hibrid müharibə, daxili təhlükə mənbəyi, xarici təhdidlərin mənbəyi, profilaktik tədbirlər, informasiya silahı.

## Ədəbiyyat

1. Əliquliyev R.M., İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyi: aktual tədqiqat istiqamətləri. İnformasiya cəmiyyəti problemləri, 2010, №1, s.3-13.
2. İnformasiya təhlükəsizliyi. Azərbaycan Ordusu qəzeti, 14 may 2022, səh 4.
3. Клименко С. Теория и практика ведения Гибридных войн» (по взглядам НАТО) 2015. «Зарубежное военное обозрение» № 5, 2015 год, с.109-112.
4. Поздняков А. Информационная безопасность страны и вооруженные силы: сущность, структура, актуальные проблемы обеспечения. Вестник МГУ, Серия 12, 2004, №2.
5. Security *in* Dictionary of Military and Associated Terms, 2001 (As amended through 31 July 2010) op.cited. Pg 477. Accessed 26 September 2010. Paleri, Prabhakaran (2008).
6. National Security: Imperatives and Challenges. Tata McGraw-Hill. p. 521. September 2010.

## Information security and its management in the armed forces

The article is focused on researching the problem of information security in the Armed Forces, which is particularly relevant due to the abundance of information in the modern era. In the article, referring to international experience, the author drew attention to the sources of information threats in the army, the protection of military personnel from targeted psychological influence, the issues of information security management, and investigated ways to eliminate existing threats.

# КИБЕР БЕЗОПАСНОСТЬ – УГРОЗА НОВОГО ТИПА

**Кенуль Ширинова**
Азербайджанский Университет Языков, Баку, Азербайджан
e-mail: Konulmusab@gmail.com

Процесс глобализации, а следовательно глобальная информатизация активно управляет жизнедеятельностью государств мирового сообщества. Новейшие информационные технологии используются при решении задач обеспечения национальной, экономической, дипломатической и военной безопасности. Таким образом фундаментальным последствием глобальной информатизации политических и военных структур стало возникновение новой среды противоборства враждующих государств – это пространство называется киберпространство.

Киберпространство не является географическим детерминантом в общем своем смысле, но охватывает международное пространство. Размывание физических границ, отсутствие географических границ между государствами является последствием появления киберпространства. В исторической перспективе международных отношений, между государствами сложился определенный паритет в области применения классических видов оружия массового поражения, а также принципы на основе которых происходили взаимодействия как на суше, космосе, в море, в воздухе то вопрос о паритете взаимоотношений в киберпространстве остается открытым до настоящего времени.

В процессе установления и полного формирования киберпространства происходит активная конвергенция компьютерных технологий в гражданских и военных сферах, создаются специализированные кибернетические центры, которые имеют цель по защите государственных и военных инфраструктур, а также контратаки в виде подготовки и проведения активных деструктивных действий в киберпространстве противоборствующих сторон.

В поддержку вышесказанных мыслей можно сказать, что США, Израиль, Германия, Англия и Франция уже обладают официальными кибервойсками.

Столкновение в киберпространстве это обсалютно новый уровень противоборства между странами. Так все новые и новые термины, с приставкой кибер, стали появляться во внутригосударственных и международных документах ,а также находят свое отражение в стратегически важных и новейших доктринах мировых держав и международных организаций, в частности НАТО.

США, как лидер в военно-технологической сфере сохраняет за собой преимущество и в киберпространство, принимая доктрины и разрабатывая стратегии регламентирующие политическую и военную деятельность в новой сфере. Так Пентагон признает киберпространство потенциально новым полем возможных боевых столкновений, а НАТО рассматривает кибератаку как вооруженное нападение .Здесь уместно вспомнить слова

заместителем министра обороны США Уильяма Линая «В 21 веке биты и байты могут быть такими же опасными ,как пули и бомбы» А специалисты в облости информационных технологий единогласно утверждают что, государство которое держит в руках контроль над киберпространством ,контролирует мир и войну.

Важным термином в международной безопасности в контексте киберпостранства выступает кибербезопасность – что является стратегической проблемой государства, которая затрагивает все слои общества и все сферы жизни. Кибербезопасность информационных систем государства (в ряде государств производятсы учения сайбер дефенс эксисайсерс).

Термин кибербезопасность стал использоваться с момента создания компьютера и компьютерных систем и мощными корнями укрепился в системе международных отношений, потому что общество перешло в руки бурной и масштабной информатизации. В современном мире уже вопросы кибербезопасности не рассматриваются на уровне защиты информации на отдельном объекте, а переходит на уровень создания единой системы кибербезопасности государства, как составной части национальной безопасности, которая нацелена защиту не только информации, как отдельно взятой единицы ,но всего киберпространства.

Однако, на сегодняшний день не существует однозначного определения киберпостранства признанного мировым сообществом.

Наиболее часто используемые определения термина киберпостранство зависит либо от точки зрения обеспечение обеспечения защиты информационной инфраструктуры государства, либо с точки зрения проведения усиленных боевых действий в киберпространсве. В2001г. прозвучало определение киберпространства как всеохватывающее множество связей между людьми и государствами , созданное на основе компьютеров и телекоммуникации полностью независимой от физической географии. Также важным является термин «кибервооружение» что вбирает в себя киберсредства, инфраструктуры, кадровые ресурсы, которые используются с целью осуществления военных операций в киберпространстве и тем самым заключает в себе особенности оказывать влияния на мировые процессы. Таким образом кибербезопасность, которая стала одним из ключевых задач в достижении национальной безопасности, является безопасностью в киберпротранстве, которая в силу отсутствия ранее существующих классических границ государств, которая сводилась к географическим детерминантам, становится новым полем для противоборств между мировыми державами

Мир который состоял из отдельных государств в результате такого процесса как глобализация стало единым пространством, с размытыми географическими то-есть классическими границами ,противоборства вышли за рамки столкновений между отдельными государствами или альянсами и стали полем сражений между цивилизациями, культурами и средствами введение войны, которыми являлись бомбы и снаряды заменились киберпространсвом и киберугрозами нацеленными на взаимное уничтожение.

Где возникновение киберугрозы является непосредственно результатом наличие высокотехнологических информационных средств передачи хранения и использования информации ,которыми обладают мощнейшими государствами, а основной проблемой этих

же государств является обеспечение кибербезопасности, которая и является логическим результатом наличия этих кибертехнологий –то-есть кибервооружений. Таким разом и угроза и обеспечение все также сосредотачивается в руках мощнейших сил, которые определяют судьбу международных отношений на ближайшие десятилетия, как когда то атомное оружие в ходе холодной войне.

**Ключевые слова**: информатизация, киберпространство, кибератаки, кибербезопасность, международные отношения, географические границы , угрозы.

**Литературы**

1. Cyber Space Policy Assuring Trusted and Resilient Information and Communications-Washington D/C The White House, 2009.
2. Достижения в сфере информатизации и телекоммуникации в контексте меж.безоп. Генеральная Ассамблея ООН 58 сессия 2003 г.
3. Правила проведения в области обеспечения международной информационной безопасности. Генеральная Ассамблея ООН 2011г. 66 сессия.

**Cyber security - a new threat**

The actual problem international and national cyber security are considered .The approaches to the development of an adequate of the present treats of cyber security of the military and government automated systems are given.

## MOBIL TƏTBİQLƏR ÜZƏRİNDƏ APARILAN NÜFUZETMƏ SINAQLARI ZAMANI QARŞILAŞILAN TƏHLÜKƏSİZLİK PROBLEMLƏRİ

**Cəbrayıl Tağıyev, Rəşad Məstəliyev**
Cyberpoint Company, Bakı, Azərbaycan
Azərbaycan Universiteti, Bakı, Azərbaycan
İdarəetmə Sistemləri İnstitutu, Bakı, Azərbaycan
y-mail: cebrayiltagiyev@gmail.com; rashad.mastaliyev@au.edu.az

Günümüzdə rəqəmsallaşmanın artması ilə birlikdə proseslərə və əməliyyatlara qarşı baş verə biləcək kiberhücumların da sayı kəskin artmaqdadır. Rəqəmsallaşmanın daha böyük kütlələrə xitab etməsi kiberhücumların artmasının əsas səbəblərindən biridir. Artıq bir çox əməliyyatı mobil tətbiqlər vasitəsilə həyata keçirtmək mümkündür. Belə olan halda mobil tətbiqlərin təhlükəsizlik məsələləri daha vacib formaya gəlir. Mobil tətbiqi tərtib edən proqramçıların tətbiq üzərində həyata keçirtdiyi hər bir yeniliyin hər hansı bir təhlükəsizlik problemi yaratmayacağına əmin olmaq lazımdır. Bu təhlükəsizlik yoxlamaları nüfuzetmə sınaqçısı (Penetration Tester) tərəfindən test edilməlidir. Bu nüfuzetmə testlərinin keçirilməsinin əsas məqsədi mobil tətbiqlərdə yarana biləcək zəifliklərin qeyri-

qanuni xakerlərdən öncə müəyyən edilərək aradan qaldırılmasıdır. Əgər mobil tətbiqlər nüfuzetmə sınağı aparılmadan istifadəyə buraxılarsa və qeyri-qanuni xakerlər zəifliklərı əvvəlcədən müəyyən edərsə,bu çox böyük problemləri ortaya çıxara bilər. Mobil tətbiqlər üzərində nüfuzetmə sınaqları aparılarkən "Penetration Tester"-in diqqət etməli olduğu bəzi vacib məsələlər vardır. Bunlar:

**1. SSL pinningin tətbiq olunması** [1] – Mobil tətbiqlərin ən vacib ehtiyaclarından biri məlumatların serverə təhlükəsiz bir kanal vasitəsilə göndərilməsi və qəbul edilməsidir. SSL pinning vasitəsilə məlumatlar daha çox qoruna bilir. Bu metodda serverdəki ssl sertifikatının bəzi byte kodları tətbiqin kodlarının içərinə qeyd olunur. Mobil tətbiq serverlə əlaqəyə keçdikdən sonra sertifikatın yoxlanılması mərhələsi başlayır. Burada əsas məsələ eyni byte kodun olub olmamasıdır. Əgər eyni olmaz isə SSL sertifikat xətası alınacaq. Düzgün tətbiq olunmuş SSL pinning vasitəsilə 3-cü bir şəxsin istifadəçinin mobil tətbiqi və server arasında olan trafiki izləməsinin və dəyişdirməsinin qarşısını almaq mümkündür.

**2. Məlumatların təhlükəsiz formada saxlanmaması (Insecure data storage)** [2] – Bu zəifliyin yaranmasının əsas səbəbi mobil tətbiqi hazırlayan proqramist düşünür ki, istifadəçilər və ya zərərli proqramlar mobil cihazın fayl sisteminə və cihazdakı məlumat bazasında olan həssas məlumatlara daxil ola bilməyək. Mobil cihazların fayl sistemlərinə daxil olmaq qeyri-qanuni xakerlər üçün çox çətin deyil. Şirkətlər zərərli istifadəçinin və ya zərərli proqramın həssas məlumat bazalarını ələ keçirmə riskini həmişə nəzərə almalıdır. Bunun üçün saxlanılan məlumatlar şifrələnməlidir və zəif şifrələmə kitabxanalarından istifadənin qarşısı alınmalıdır.

**3. Tərsinə mühəndislik (Reverse engineering) -** Mobil tətbiqlərin tərs mühəndisliyi onun mənbə kodlarını oxuya bilmək üçün edilən prosesdir. Tətbiq normal axınında çalışdığı zaman arxada fonda baş verən prosesləri dərk etmək çətindir. Qeyri-qanuni xakerlər mobil tətbiqlərin mənbə kodlarını ələ keçirərək proqramın işləmə prinsiplərini tam olaraq başa düşür. Mobil tətbiqlərin mənbə kodlarının pis niyyətli insanlar tərəfindən analiz edilməsinin qarşısını almaq üçün "Code Obfuscation" adlanan proses icra edilir. Bu metod kodları oxuna bilməyəcək formaya gətirir. Pis niyyətli insanlar tərs mühəndislik texniklarını icra etsə belə kodlar oxuna bilməyəcək halda olduğu üçün arxa fonda gedən prosesləri öyrənmək çox çətin olacaq.

**4. API Təhlükəsizliyi –** Bildiyimiz kimi mobil tətbiqlər sadəcə istifadəçi tərəfdən ibarət deyil. Proqramın daxilindəki funksionallıqlar əsasən APİ-lər vasitəsilə həyata keçirilir. Müasir texnologiyalarda APİ təhlükəsizliyi ən vacib məqamlardan biridir. API-lərdə zəif autentifikasiya və avtorizasiya, müəyyən məhdudiyyətinin olmaması kimi zəifliklər ola bilər. Şirkətlər zəifliklərı müəyyən etmək üçün mütəmadi olaraq API-ləri sınaqdan keçirməli və ən yaxşı təhlükəsizlik təcrübələrindən istifadə edərək bu zəifliklərı aradan qaldırmalıdır.

**5. Root və Jailbreak olunmuş mobil cihazların müəyyən olunması (Root and Jailbreak detection)-** Bu proses mobil əməliyyat sisteminin istifadəçilərinə müxtəlif alt sistemləri üzərində imtiyazlı nəzarət əldə etməyə imkan verən prosesdir. Root və ya Jailbreak olunmuş mobil cihazlarda qeyri-qanuni xakerlər mobil tətbiqlər üzərində manipulyasiyalar aparmaq üçün istifadə olunan alətləri istifadə edə bilir. Bu tip cihazdan istifadə edərək, həssas məlumatların tətbiq tərəfindən saxlanıla biləcəyi lokal fayl sisteminin hissələrinə daxil olmaq mümkündür. Belə olan halda cihaz üzərində tam

nəzarət əldə edən pis niyyətli istifadəçi ortaya çox böyük risklər çıxara bilir. Bütün bu riskləri nəzərə aldıqda, mobil tətbiqinin root və ya jailbreak olunmuş cihazlarda işləməsinin qarşısını almaq vacibdir. Bu problemin qarşısını almaq üçün **DexGuard** və **iXGuard** adlanan əlavələr istifadə oluna bilir. Bu tip metodlar tətbiqimizin təhlükə altında olan mühitdə icrasının qarşısını alacaq. Bundan əlavə, bu proqramlar saxtalaşdırma, tərs mühəndislik üsullarına qarşı da effektiv metod sayılır.

**Açar sözlər:** mobil tətbiqlər, kibertəhlükəsizlik, nüfuzetmə sınaqları.

**Ədəbiyyat**

1. https://cwe.mitre.org/data/slices/919.html
2. https://owasp.org/www-project-mobile-top-10/

**Securıty ıssues encountered durıng penetratıon testıng on mobıle applıcatıons**

Today, along with the increase in digitalization, the number of cyber-attacks that can occur against processes and operations is also increasing dramatically. One of the main reasons for the increase in cyber-attacks is the fact that digitalization appeals to larger masses. It is now possible to perform many operations through mobile applications. In this case, the security issues of mobile applications become more important. In the presented work, some important issues that the Penetration Tester should pay attention to when conducting penetration tests on mobile applications are indicated.

## TƏHSİL MÜƏSSİSƏLƏRİNİN FƏALİYYƏTİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ

**Ədilə Xəlfəquliyeva**
Azərbaycan Universiteti, Bakı, Azərbaycan

İnformasiya texnologiyalarınını cəmiyyətin bütün sferalarına daxil olması artıq normal hala çevrilib. İnformasiya texnologiyalarının inkişafı tempi çox yüksəkdir və bu yüksək göstəricilər bir tərəfdən cəmiyyətin özünü təkmilləşdirməyə doğru davamlı hərəkətindən xəbər verir, digər tərəfdən isə texnologiyaların inkişafı və informasiya resurslarının təhlükəsizliyi ilə bağlı problemlər yaradır.

Təhsil prosesində informasiya texnologiyalarının tətbiqi, internet məkanından fəal istifadə ilə əlaqədar təhsil müəssisələrində təhlükəsizliyin təmin edilməsi zəruridir. Təlim prosesinin effektivliyi bilavasitə informasiya istehlakının səmərəliliyindən və informasiyanın yaradılmasından asılıdır ki, bu da təhsil alanları müəyyən dərəcədə onlara zərər verə biləcək informasiyadan qorumaq zərurəti məsələsini ortaya çıxarır.

Müasir təhsil müəssisələrində informasiya təhsil prosesinin ən mühüm komponentidir. Təhsil təşkilatlarının ən mühüm resurslarına maliyyə resursları ilə yanaşı informasiya resursları da daxildir [1]. Tədris prosesinə informasiya texnologiyalarının tətbiqi və sinif otaqlarının kompüter avadanlığı ilə aktiv şəkildə təchiz edilməsi ilə bütün təşkilatın informasiya təhlükəsizliyinin tam təmin edilməsi

zərurəti yaranır ki, bu da kompüter texnikasının fasiləsiz işləməsinə və informasiya dövriyyəsinə kömək edir.

Tədris prosesinin informasiya təhlükəsizliyinin əsas komponentləri kompüter təhlükəsizliyi və istifadəçilərin mühafizəsidir. Ali təhsil müəssisələrində istifadəçilərin mühafizəsi ən vacib komponentdir. Bu, ilk növbədə, təhsil prosesinin bütün iştirakçılarının şəxsi məlumatlarının, o cümlədən onların şəxsi, maliyyə, tədris məlumatlarının qorunması ilə bağlıdır. İnformasiya təhlükəsizliyinin təmin edilməsi qəbul komissiyasından başlayaraq kadrlar şöbəsinə qədər qurumların bütün struktur bölmələrinə şamil edilməlidir. Bu gün informasiya təhlükəsizliyini təmin etmək üçün vahid siyasətin işlənib hazırlanması zəruridir [2].

Aydındır ki, açıq kommunikasiya kanalları vasitəsilə şəbəkə istifadəsi zamanı qarşılıqlı əlaqənin bütün iştirakçıları təhsil müəssisəsinin və şəxsin informasiya təhlükəsizliyinə həm obyekt, həm də təhdid mənbəyi ola bilər. Bəzi müəlliflərin məqalələrində göstərildiyi kimi, "İnternet azad kiberməkandır" ifadəsi heç vaxt doğru olmayıb. İnternetin həqiqətən tək sahibi yoxdur, lakin əsas resursların və əsas funksiyaların idarə edilməsi fəaliyyətlərinə nəzarət təşkilatlar dairəsi tərəfindən həyata keçirilir.

İnformasiya tədris sisteminin bir sıra üstünlüklərinə baxmayaraq (istifadəçinin istənilən vaxt istənilən yerdən təhsil materiallarına çıxışı, təlimin və nəzarətin fərdiləşdirilməsi, qabaqcıl təhsil təcrübələrinin sürətlə yayılması və s.), qeyd etmək lazımdır ki, informasiya təhlükəsizliyinin təmin edilməsi problemi təkcə tədris prosesinin subyektləri üçün deyil, həm də təhsil təşkilatı üçün aktualdır.

Planlaşdırılmış keyfiyyət göstəricilərinə nail olmağa yönəlmiş bir təhsil müəssisəsinin idarə edilməsi prosesi, digər məsələlərlə yanaşı, bütün təhsil prosesi subyektlərinin informasiya təhlükəsizliyinin təmin edilməsi, eləcə də, təhsil müəssisəsinin informasiya təhlükəsizliyi mühitinin lazımi səviyyədə yaradılmasına və saxlanmasına yönəldilməlidir.

Təhsil müəssisəsinin informasiya təhlükəsizliyi mühiti aşağıdakıları təmin etməlidir:

− təhsilalanların sağlamlığına və inkişafına zərər verə biləcək məlumatlardan qorunması;

− təhsil təşkilatının informasiya resurs və sistemlərinin qorunması;

− təhsil prosesinin bütün iştirakçılarının şəxsi məlumatlarının qorunması.

Effektiv kompleks mühafizəni təmin etmək üçün ilk növbədə informasiya təhsil sisteminə təhlükə yaradan amilləri nəzərə almaq və təhlil etmək lazımdır. Uşaq və gənclər üçün potensial təhlükə yaradan informasiya mühitinin risk faktorlarına aiddir:

1) gənc nəslin mənəvi inkişafına təsir göstərən qeyri-qanuni məzmun, zərərli məlumatlar;
2) təhsilalanların psixofizioloji vəziyyətini məqsədyönlü şəkildə dəyişdirən spesifik elementlər;
3) təhsilalanların diqqətini yayındıran, manipulyasiya xarakterli materiallar;
4) gizli məlumatların mühafizəsi mexanizmlərinin həyata keçirilməsində çətinliklər.

İnformasiya məkanının qorunması və informasiya təhlükəsizliyinin təmin edilməsi probleminin aktuallığı bilavasitə informasiya təhlükəsizliyinin real və potensial təhlükə və riskləri ilə bağlıdır. Bu təhdid və risklərin səviyyəsi və miqyası son on ildə dəfələrlə artmış, onların təsirinin nəticələri son dərəcə təhlükəli olmuşdur.

İnformasiya təhlükəsizliyi sahəsində əsas anlayışlardan biri təhdid anlayışıdır. Ümumi halda təhdid kiminsə maraqlarına potensial olaraq zərər vura bilən mümkün hadisə, hərəkət və ya proses kimi başa düşülür. İnformasiya təhlükəsizliyi obyektinə təhdid müxtəlif obyektlər və ya onların elementləri arasında qarşılıqlı əlaqə prosesində yaranan və konkret informasiya təhlükəsizliyi obyektinə mənfi təsir göstərə bilən amillər və şərtlər toplusudur.

Elmi ədəbiyyatda informasiya təhlükəsizliyi təhdidlərinin müxtəlif təsnifatları mövcuddur. Mənfi təsirlər vurulmuş zərərin xarakterinə görə fərqlənir, yəni: təhlükəsizlik obyektinin xassələrinin dəyişmə dərəcəsinə və təhlükənin təzahürünün nəticələrinin aradan qaldırılması imkanlarına görə.

İnformasiya təhlükəsizliyinə təhdidlərlə bağlı təhsil prosesinin subyektləri üçün dörd təhlükə səviyyəsi mövcuddur (Cədvəl 1).

Təhsilalanların şəbəkə vasitəsilə əldə etdikləri informasiya təcrübəsi növü onların məruz qaldıqları risk növlərini və buna görə də ən təsirli ola biləcək təhlükəsizlik növlərini müəyyən etmək üçün vacib amildir. İnformasiya təhlükələrinə bu sistemin elementləri kimi təkcə İnformasiya tədris sisteminin subyektləri deyil, həm də onlar arasındakı əlaqələr də məruz qalır. Nəzərə alsaq ki, İnformasiya tədris sistemi çərçivəsində onun subyektlərinin qarşılıqlı əlaqəsi mövcuddur, informasiya qarşılıqlı əlaqələrini təhsil prosesinə təhlükə hesab etmək olar.

**Cədvəl 1.** İnformasiya təhlükəsizliyi təhdidlərin səviyyələri və təzahürləri

| Təhdid səviyyəsi | Tədris prosesinin subyektləri üçün təhlükənin həyata keçirilməsinin mümkün təzahürləri |
|---|---|
| Aşağı | kiçik neqativ təsirlər |
| orta | Neqativ təsirlər |
| Yüksək | Neqativ nəticələr |
| Kritik | əhəmiyyətli mənfi nəticələr |

Risklərin idarə edilməsi metodologiyası dörd əsas risk qiymətləndirmə addımını əhatə etməlidir:

1. Qiymətləndirmənin əhatə dairəsinə daxil olan şəbəkə resurslarının inventarlaşdırılması;
2. Bu aktivlərlə bağlı təhlükələrin müəyyən edilməsi;
3. İnformasiya tədris sistemi və əlaqələrin subyektləri üçün təhlükələrin həyata keçirilməsi ehtimalının və potensial nəticələrinin təsnifatı;
4. Müəyyən edilmiş riskləri məqbul səviyyəyə endirmək üçün zəruri olan nəzarət vasitələrinin müəyyən edilməsi.

Təhsil müəssisələrində informasiya təhlükəsizliyi sisteminin yaradılmasının məqsədi aşağıdakılardan ibarət olmalıdır:

1) tələbələrin, müəllimlərin, onların hüquq və mənafelərinin, habelə əmlakının informasiya mühitinin yaratdığı təhlükəli təsirlərdən qorunması;
2) təhsil müəssisəsinin səmərəli fəaliyyətinin və inkişafının təmin edilməsi;

3) informasiya təhlükəsizliyi təhdidlərinin mənfi təsirlərindən zərərin azaldılması, təhlükələrin baş vermə ehtimalının və riskin reallaşdırılması nəticələrinin azaldılması;

Təhsil müəssisəsində informasiya təhlükəsizliyi sistemi yaradılarkən şəbəkə qarşılıqlı əlaqəsinin həyata keçirildiyi informasiya mühitinin əsas xüsusiyyətlərini nəzərə almaq lazımdır. Belə bir mühit aşağıdakı xüsusiyyətlərə malikdir:

• konkret məqsədlər üçün yaradılır və saxlanılır;
• dinamikdir;
• sürətlidir;
• nisbətən qeyri-məhduddur;
• zəif giriş baryerlərinə malikdir;
• sürətlə inkişaf edir;

**Açar sözlər:** İnformasiya tədris sistemi, informasiya təhlükəsizliyi, təhlükə.

**Ədəbiyyat**

1. Филяк П.Ю. Информационная безопасность и комплексная система безопасности анализ, подходы. Информация и безопасность. 2016, Т. 19, № 1, с. 72–79.
2. Роберт И.В. Перспективные научные исследования, определяющие развитие информа тизации образования. Педагогическое образование в России. 2014, №4, с. 199-204.

## KİBERTƏHLÜKƏ VƏ ONDAN QORUNMAĞIN BƏZİ ASPEKTLƏRİ

**Ayşən Baxışova**
Heydər Əliyev adına Hərbi İnstitut, Bakı, Azərbaycan
e-mail: aysenbaxisova1975@gmail.com

Münaqişələrin döyüş meydanından virtual məkana daşındığı bir dövrdə regionda əsas enerji layihələrinin baş aktoru olan Azərbaycan Respublikasının öz informasiya arealını kənar hücumlardan qoruması dövlətin qarşısında duran ən vacib məsələlərdəndir. İstər dövlət strukturları, istər resursların hasilatı və daşınması ilə bağlı infrastrukturların, istərsə də sadə vətəndaşların öz şəxsi məlumatlarının, dövlət, kommersiya və peşə sirri ilə bağlı məxfi informasiyanın mühafizə edilməsi dövlətin, millətin gələcəyi naminə kibertəhlükəsizlik probleminin həllini daim gündəmdə saxlayır.

**Kibertəhlükəsizlik** (kompüter təhlükəsizliyi) – kompüter, server, mobil qurğu, elektron sistem, şəbəkə və elektron məlumatları təhlükəli hücumlardan mühafizə etmək məqsədilə həyata keçirilən metodların məcmusunu əhatə edir. **Kibertəhlükənin növləri: 1. Kibercinayətkarlıq** – sistemin işini pozmaq və yaxud maliyyə vəsaiti əldə etmək məqsədilə təkbaşına və ya mütəşəkkil formada həyata keçirilən fəaliyyətdir. **2. Kiberhücum** - əsasən siyasi xarakterli informasiyanın toplanmasına yönəlmiş fəaliyyətdir. Dövlət orqanlarının, daha çox güc strukturlarının işini iflic etmək, sistem məlumatlarına zərər yetirmək, məxfi məlumatların deşifrə edilməsi kimi pozuculuq

hallarını əhatə edir. **3. Kiberterrorizm** – qorxu və vahimə yaratmaq məqsədilə elektron sistemlərin stabilliyinin pozulmasına yönəlmiş fəaliyyətdir. [4]

Kompüter sistemləri üzərində nəzarəti ələ keçirmək üçün ən müxtəlif üsullardan istifadə olunur:

**Zərərverici proqram təminatı (PT)** Bu proqram xakerlər tərəfindən istifadəçinin kompüterini və ya ordakı informasiyanı qəsdən korlamaq üçün yaradılır. Adətən, zərərsiz fayl, poçt ismarıcı kimi yayılır, siyasi motivlərə hücum və ya pul qazanmaq məqsədilə istifadə edilir. **Zərərverici PT**-ləri ümumi adla hər birimiz "virus" adlandırsaq da, onların çeşidi çox, təyinatı isə müxtəlifdir. **Viruslar, Troyalılar**, **Casus PT, Fırıldaqçı-proqramlar**, **Botnetlər, SQL – inyeksiya**, **Fişinq (balıq ovu), Man-in-the-Middle ("Mərkəzdəki insan") hücumu, DoS-hücumlar ("xidmətdə imtina" tipli)** obyektinin şəbəkə və serverində sistemin normal fəaliyyətini pozur və istifadəyə yarasız hala gətirərək müəssisənin infrastrukturunun vacib komponentlərini sıradan çıxararaq fəaliyyətini sabotaj etmiş olur [1].

Müdafiə vasitələrində elektron poçtu, faylları və digər vacib məlumatları şifrələməyə imkan verən kriptoqrafik protokollardan istifadə olunur. Bu mexanizm kibercinayətkarın məlumatlara girişini və onları əldə etməsini əngəlləyir. Həmin vasitələr son istifadəçinin qurğusunda zərərli kodun olub-olmamasını yoxlayır, varsa: onları "karantinə" alır, sonra isə sistemdən tamamilə silir. Belə proqramlar əsasən endirilmiş (Dounload) hər hansı material və ya sənədin içində gizlədilmiş zərərvericini deşifrə edir və sərt diskdə olan informasiyanı tamamilə silə bilir. Müdafiə vasitələri real vaxt rejimində zərərli proqramları aşkar edir, onlardan bir çoxu evristik analiz və davranış analizi tətbiq edərək zərərverici və onun kodunun hərəkətlərini izləyir. Onlar xüsusi virtual mühitdə potensial zərərverici proqram təminatını təcrid etməyi bacarır, onun davranışını təhlil edərək yeni təhlükə mənbələrini daha yaxşı öyrənməyə imkan yaradır. Bu sahədə yeni təhlükələrin aşkar edilməsi, təhlili və onlarla mübarizə üsulları təkmilləşdirilir. Müdafiə vasitələrinin öz funksiyalarını effektiv yerinə yetirməsi üçün onlar daim qoşulu olmalı və müntəzəm olaraq yenilənməlidir.

İnformasiya sızması şirkətlərə həm birbaşa maliyyə itkiləri, həm də sonradan müəssisənin imicinə xələl gətirə biləcək vəziyyətlərə səbəbiyyət verir. Qorunan informasiyaya 2 cür hücum edilə bilər: **xarici və daxili: Xarici müdaxilə** zamanı hücum edən kənardan mühafizə olunan informasiya məkanına daxil ola bilir**. Daxildən hücum** zamanı sızma şirkətin öz əməkdaşları ucbatından baş verir.

Statistikaya əsasən, banklara edilmiş kiberhücumların 91%-i satın alınmış bank işçiləri, 8%-i bank əlaqələndiriciləri və yalnız 1%-i xakerlərin payına düşür. Parol kinofilmlərdə göstərilən kimi bir neçə saniyə deyil, ən azı bir neçə saata "sındırıla" bilir. Parolu "sındırmaq" üçün xaker müxtəlif simvollardan istifadə edərkən istifadəçinin adı, soyadı, onun üçün vacib olan tarixləri və digər şəxsi məlumatlardan ibarət kombinasiyalara üstünlük verir. İstifadəçinin kompüterdə olan məlumatlarını tədqiq edərək qanunauyğunluğun aşkar edilməsi ilə parolun tapılması mümkün olur.

Azərbaycan Respublikasının Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyi yanında Elektron Təhlükəsizlik Xidməti fəaliyyət göstərir [3]. **II Qarabağ müharibəsində kibertəhlükəsizlik məsələləri.** 19.09.2020-ci il Azərbaycan Respublikası Prezidentinin çıxışında

ermənilərin yeni müharibəyə hazırlaşması ilə bağlı məlumatın olduğu qeyd olunurdu. Xüsusi təhlükəsizlik xidmət orqanları tərəfindən hansı istiqamət və hansı qüvvələrlə hücumun planlaşdırıldığı aşkar edilmiş, bu məlumatlara müvafiq əks tədbirlər görülmüşdü. Vətən müharibəsi dövründə ermənilər tərəfindən dəfələrlə dövlət kiberməkanına müdaxilə cəhdləri edilmiş, lakin preventiv tədbirlərin görülməsi nəticəsində kibertəhdidlərin ünvanı dəqiqləşdirilərək hətta üzvlərinin sayı və kimlikləri təyin olunaraq qarşısı alınmışdır.

Müharibə dövründə kibermüdafiəni effektiv təmin etmək, dövlətin milli təhlükəsizliyinə ziyan vurulmasının qarşısını almaq üçün məqsədyönlü şəkildə sosial şəbəkələrin işinin məhdudlaşdırılması həyata keçirilmişdir. Bunun sayəsində əhali arasında dezinformasiya yaymaq cəhdlərinin qarşısı alındı. Cəhdlərin hamısı qeydə alınmış və erməni kiberhücumların əksəriyyətinin Azərbaycanın dövlət informasiya resurslarına və kritik informasiya infrastrukturlarına uğursuz cəhdlərdən sonra Wi-Fi şəbəkələrinə müdaxilə edərək adlarını dəyişdirməyə çalışdılar. İşğal altında olan ərazilərimizdə xarici ölkələrdən gətirilmiş erməni və digər əsilli muzdluların (900-950 ev) elektrik enerjisi ilə təmin olunduğu günəş panelləri sisteminə hücum təşkil edərək müharibə dövründə 3 gün enerjisiz qalmasından duyuq düşərək internet provayderlər və digər sahələrdə də kommunikasiyalara tərəfimizdən müdaxilənin effektiv olduğunu anladılar. Həmçinin, başqa ölkələrdən erməni və digər mənşəli muzdluların siyahısı əldə edilərək ordumuza verilmiş, onların əsir götürülməsi təqdirində Azərbaycanın antiterror əməliyyatında ermənilər tərəfindən kənar ölkə vətəndaşlarının iştirakının sübutu idi. AN-2 təyyarələrindən istifadə edərək S-300 ZRQ-nin sıradan çıxarılması DTX və Sərhəd xidmətinin birgə həyata keçirdiyi unikal əməliyyat idi. Sərhəd xidmətinin pilotları zərər görmədən uğurla sınaqdan keçirilir. 6 gün ərzində 20 ədəd AN-2 (xalq arasında "kukuruznik") təyyarəsi məişətdə istifadə olunan maddələrdən istifadə edilərək müxtəlif elektron qurğular, partlayıcılarla (hər birində 260 kq-a qədər) təchiz olunaraq düşmən üzərinə göndərilir. Həmin təyyarələr ermənilərin kabusuna çevrilərək rəqibdə ruh düşkünlüyü yaradır [5].

Hücumlardan necə qorunmalı: kibertəhlükəsizlik üzrə faydalı tövsiyələr.

Proqram təminatı və əməliyyat sistemini müntəzəm olaraq yeniləyin. Antivirus proqramlarından istifadə edin. Etibarlı parollardan istifadə edin. Naməlum ünvanlardan gələn poçt əlavələrini açmayın. Elektron poçtunuza daxil olmuş naməlum göndəricidən və ya veb-saytlardan gələn səhifələrə keçid etməyin. Müdafiə olunmayan Wi-Fi şəbəkəsindən istifadə etməkdən çəkinin.

**Açar sözlər:** kibertəhlükəsizlik, kiberhücum, zərərverici proqram təminatı.

## Ədəbiyyat

1. https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security
2. Y.İmamverdiyev "Milli kibertəhlükəsizlik strategiyalarının analizi" Konfrans materialı, 2013
3. N.Mehdiyev "Qərbin Azərbaycana qarşı informasiya müharibəsi" "Virtual Qarabağ" informasiya-kommunikasiya texnologiyaları mərkəzi,oktyabr, 2022
4. Э.Камышев «Информационная безопасность и защита информации » Томск, 2009
5. https://hit.az/az/read/240060/

## Cyber threat and some aspects of protectıon against IT

At a time when conflicts are moving from the battlefield to the virtual space, one of the most important issues facing the state is protecting its informational area from external attacks for The Republic of Azerbaijan, the main actor in the main energy projects in its region.The protection of state structures, infrastructures related to the extraction and transportation of resources, as well as the protection of the private information of ordinary citizens and confidential information related to state, commercial, and professional secrets are always on the agenda for the future of the state and the nation.