



**Azerbaijan University**



**Kharkiv National University  
of Radioelectronics**

# **PROCEEDINGS**

**International Conference on**

**INFORMATION SECURITY: PROBLEMS AND  
PROSPECTS**

**October 22, 2021**

**BAKU | AZERBAIJAN**

## ORGANIZING COMMITTEE

### Conference Chairs

**Saadat Aliyeva**, Rector, Azerbaijan University, Azerbaijan

**Valeri Semenets**, Rector, Kharkiv National University of Radio Electronics, Ukraine

### Members

**Yusif Gasimov** (co-chair), Azerbaijan University

**Murad Omorov** (co-chair), Kharkiv National University of Radioelectronics

**Ali Abbasov** Institute of Control, Systems, ANAS

**Ramiz Alguliyev** ANAS Institute of Information Technology

**Ivan Antipov** Kharkiv National University of Radio Electronics

**Carlo Cattani** University of Tuscia, Italy

**Latifa Agamalieva** Azerbaijan University

**Yuriy Lykov** Kharkiv National University of Radio Electronics

**Urfat Nuriyev** Ege University, Turkey

**Sharif Guseynov** Liepaja University, Latvia

**Denis Gorelov** Kharkiv National University of Radio Electronics

**Alakber Aliyev** Baku Sate University

**Gennadi Khalimov** Kharkiv National University of Radio Electronics

**Elvin Azizbayov** Academy of Public Administration under the President of the Republic of Azerbaijan

**Victor Ruzhenkov** Kharkiv National University of Radio Electronics

**Abzeddin Adamov** ADA University, Azerbaijan

**Alexander Severinov** Kharkiv National University of Radio Electronics

**Kamaleddin Ramazanov** Azerbaijan National Aviation University

**Yevgeniy Kotukh** Kharkiv National University of Radio Electronics

**Marina Yevdekimenko** Kharkiv National University of Radio Electronics

**Asif Pashayev** Azerbaijan University

**Tamara Raduvilova** Kharkiv National University of Radio Electronics

**Yadigar Imamverdiyev** ANAS Institute of Information Technology

**Alexsander Fedushin** Kharkiv National University of Radio Electronics

**Etibar Seidzade** Bakı Engineering University, Azerbaijan

**Alexsander Lemeshko** Kharkiv National University of Radio Electronics

**Vagif Gasimov** Azerbaijan Technical University

**Anatoli Aleynikov** Kharkiv National University of Radio Electronics

**Bahram Azizov** Azerbaijan University

**Oleksadra Yeremenko** Kharkiv National University of Radio Electronics

## CONTENTS

### PLENARY TALKS

|  |   |
|--|---|
| <b>А.В. Лемешко, М.А. Евдокименко, А.С. Еременко</b> .....           | 6 |
| СЕТЕВАЯ БЕЗОПАСНОСТЬ СРЕДСТВАМИ МАРШРУТИЗАЦИИ:<br>ПРОБЛЕМЫ И РЕШЕНИЯ |   |

|  |   |
|--|---|
| <b>S. Akleylek</b> .....   | 9 |
| CHALLENGES AND OPPORTUNITIES IN CRYPTOGRAPHY: LATTICE-BASED AND<br>CODE-BASED CRYPTOGRAPHY IN THE QUANTUM ERA WITH FORMAL ANALYSIS |   |

### SECTION TALKS

|  |    |
|--|----|
| <b>G. Abdiyeva-Aliyeva Alishan, M. Hematyar Mahmud</b> .....   | 12 |
| AI APPROACHED DYNAMICALLY DETECTING SECURITY THREATS AND<br>UPDATING A SIGNATURE-BASED IDS'S DATABASE IN NGN |    |

|   |    |
|---|----|
| <b>И.Е. Антипов, Т.А. Василенко, Л.Ф. Сайковская</b> .....    | 16 |
| МЕТОД СРАВНЕНИЯ СПЕКТРОВ WI-FI УСТРОЙСТВ ДЛЯ ИХ ИДЕНТИФИКАЦИИ |    |

|   |    |
|---|----|
| <b>В. Əzizov, Е. Нəсənov, А. Раşayev</b> .....    | 18 |
| TƏHSİLDƏ KİBERTƏHLÜKƏSİZLİK PROBLEMLƏRİNİN İCMALI |    |

|  |    |
|--|----|
| <b>В. Əzizov, Е. Нəсənov, А. Раşayev</b> ..... | 21 |
| CYBERCRIME AND CYBER RISKS                     |    |

|   |    |
|---|----|
| <b>С. Багирова, О. Мухтарова</b> .....  | 24 |
| ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПО ВОПРОСАМ РЕГУЛИРОВАНИЯ<br>ТРАНСПОРТНЫХ ПОТОКОВ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ |    |

|  |    |
|--|----|
| <b>N.D. Səfərov, Z.Y. Qasimova</b> .....   | 26 |
| MÜASİR ƏLAQƏLİ VERİLƏNLƏR BAZASI İDARƏETMƏ SİSTEMLƏRİNDƏ<br>İNFÖRMASİYA TƏHLÜKƏSİZLİYİ |    |

|  |    |
|--|----|
| <b>A.S. Dadaşov</b> .....  | 30 |
| DÖVLƏTİN GÜC STRUKTURLARINDA İNFÖRMASİYA TƏHLÜKƏSİZLİYİNİN<br>İDARƏ EDİLMƏSİ |    |

|   |    |
|---|----|
| <b>В.В. Должиков, В.П. Давыдова</b> .....                                       | 33 |
| ПРОДОЛЬНОЕ РАСПРЕДЕЛЕНИЕ ИНТЕНСИВНОСТИ ПОЛЯ КРУГЛОЙ<br>СФОКУСИРОВАННОЙ АПЕРТУРЫ |    |

|  |    |
|--|----|
| <b>В.В. Дубина</b> .....   | 36 |
| АВТОМАТИЗАЦИЯ ОБРАБОТКИ ИНФОРМАЦИИ<br>МЕТОДЫ ОТСЛЕЖИВАНИЯ ТРАНЗАКЦИЙ В БЛОКЧЕЙН-СИСТЕМАХ |    |

|  |    |
|--|----|
| <b>А. Fəxrəddinqızı</b> .....  | 38 |
| DBSCAN ALQORİTMİNİN TƏTBİQİ İLƏ BIG DATA - DA KÜY VERİLƏNLƏRİN<br>AŞKARLANMASI |    |

|   |    |
|---|----|
| <b>Ү.Ə. Qasimov, А.Ə. İsmayilov</b> .....                                 | 42 |
| MÜASİR BANK SEKTORLARINDA KİBERTƏHLÜKƏSİZLİK<br>STRATEGİYALARININ ANALİZİ |    |

|   |    |
|---|----|
| <b>V.Ə. Qasimov, D.A. Quluzadə, M.İ. Cavadova</b> .....   | 46 |
| BIG DATA TƏHLÜKƏSİZLİYİ TEXNOLOGİYALARI: İSTİFADƏ DAİRƏSİ VƏ PROBLEMLƏRİ                                  |    |
| <b>V. Qasimov, M. Cavadova</b> .....  | 49 |
| İoT-DA KİBERTƏHLÜKƏSİZLİYİN TƏŞKİLİ VƏ KİBERRİSKLƏRİN İDARƏ OLUNMASI                                      |    |
| <b>A. Hasanov, E. Azizbeyov, G. Mirzayeva</b> .....   | 52 |
| ANALYSIS THE MOST SIGNIFICANT RISKS IN TECHNOLOGY AND FINANCIAL SERVICES                                  |    |
| <b>Ə.T. Həzərhanov, V.A. Neymətov</b> .....   | 54 |
| BEYNƏLXALQ İNFORMASIYA TƏHLÜKƏSİZLİYİ SİSTEMİNDƏ PANDEMİYA ÖZƏLLİKLƏRİ: ZOOM VASİTƏSİ İLƏ DAĞIDICILIQ     |    |
| <b>İ.M. İsmayılov, Ə.T. Həzərhanov</b> .....  | 57 |
| AVIASIYA SİSTEMLƏRİNDƏ İNFORMASIYA TƏHLÜKƏSİZLİYİ   |    |
| <b>E.N. İsrailova, A.M. Mustafayeva, A.M. Abdurrahmanova</b> .....  | 60 |
| İNFORMASIYA TƏHLÜKƏSİZLİYİNİN TƏMİNATINDA SÜNİ İNTELLEKTİN ROLU   |    |
| <b>M. Karatay, E. Alkim, U. Nuriyev</b> .....   | 63 |
| IMPROVEMENTS ON POLYNOMIAL MULTIPLICATION IN NTRU PRIME   |    |
| <b>M. Karatay, E. Emirtekin</b> .....   | 66 |
| MACHINE LEARNING APPLICATIONS FOR ANOMALY DETECTION   |    |
| <b>N.A. Khankishiyeva</b> .....   | 69 |
| NEW NUMBER SYSTEM, ITS CRYPTOGRAPHY AND DATA COMPRESSION APPLICATIONS                                     |    |
| <b>В.Г. Лихограй, Д.В. Грецких, А. Шербина</b> .....  | 71 |
| АНТЕННАЯ СИСТЕМА КОМПЛЕКСА ПАССИВНОЙ РАДИОПЕЛЕНГАЦИИ БПЛА   |    |
| <b>Ю.В. Лыков, А.А. Паниотова, А.А. Лыкова, Э.А. Костенко</b> .....                                       | 74 |
| АНАЛИЗ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ LPWAN СЕТЕЙ ДЛЯ ПОСТРОЕНИЯ РАДИОЗАКЛАДНЫХ УСТРОЙСТВ                      |    |
| <b>Ю.В. Лыков, И.В. Хрипко, А.А. Лыкова</b> .....   | 77 |
| АНАЛИЗ ВОЗМОЖНОСТИ ПЕРЕХВАТА ВИБРОАКУСТИЧЕСКОЙ ИНФОРМАЦИИ ПУТЕМ ЕЕ ПЕРЕХВАТА С ПОМОЩЬЮ ДАТЧИКОВ СМАРТФОНА |    |
| <b>A. Murzaeva, S. Akleylek</b> .....   | 81 |
| IMPLEMENTATION OF LATTICE-BASED IDENTIFICATION SCHEMES IN C   |    |
| <b>Ş.İ. Mustafayeva</b> .....   | 84 |
| İDARƏETMƏ PROSESİNDƏ VERİLƏNLƏR BAZASININ TƏHLÜKƏSİZLİYİ  |    |
| <b>N. Müzəffərli, L. Ağamalhyeva</b> .....  | 87 |
| MÜASİR PROQRAM-TEXNİKİ, TƏŞKİLATİ METODLAR VƏ İNFORMASIYANIN QORUNMASI VASİTƏLƏRİ                         |    |

|   |     |
|---|-----|
| <b>I. Nevludov, M.A. Omarov, S. Novoselov</b> .....   | 90  |
| MODELING AND SELECTION OF OPTIMAL PARAMETERS OF SECURITY GATEWAYS TO PROTECT INDUSTRIAL EQUIPMENT FROM CYBERATTACKS |     |
| <b>V.A. Nuriyeva</b> .....  | 93  |
| APACHE HADOOP PLATFORMASI: BÖYÜK HƏCMLİ VERİLƏNLƏRİN EMALI ÜÇÜN MÜASİR YANAŞMA                                      |     |
| <b>В.И. Огарь</b> .....   | 96  |
| МЕТОДИКА КАЛИБРОВКИ ПРИБОРОВ ДЛЯ ПОИСКА СКРЫТЫХ КАБЕЛЕЙ   |     |
| <b>А.Н. Олейников, И.Н. Чигирев</b> .....   | 99  |
| ВЫБОР ТЕХНИЧЕСКИХ ПАРАМЕТРОВ СРЕДСТВ ДИСТАНЦИОННОЙ АКУСТИЧЕСКОЙ РАЗВЕДКИ  |     |
| <b>А. Олейников, В. Пулавский, И. Чигирев</b> .....   | 102 |
| ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ МЕТОДОВ И СРЕДСТВ ПОДАВЛЕНИЯ НЕСАНКЦИОНИРОВАННОЙ ЗАПИСИ РЕЧИ                                |     |
| <b>В.В. Просолов</b> .....  | 105 |
| АНАЛИЗ БЕЗОПАСНОСТИ АТОМАРНЫХ ОБМЕНОВ МЕЖДУ BITCOIN И LITECOIN  |     |
| <b>V. Qasimov, C. İsmayilov</b> .....   | 107 |
| İOT TEXNOLOGİYASINA YÖNƏLMİŞ “MIRAF” KİBERHÜCUMU VƏ ONDAN MÜHAFİZƏNİN TƏŞKİLİ                                       |     |
| <b>М.Ə. Salmanova</b> .....   | 110 |
| İNFORMASYA SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİN PROQRAM VASİTƏLƏRİ   |     |
| <b>K. Seyhan, S. Akleylek, E. Kılıç, Y. Oruç</b> .....  | 112 |
| HARD PROBLEMS IN LATTICE-BASED CRYPTOGRAPHY: X-LWE  |     |
| <b>Л.В. Сухостат</b> .....  | 115 |
| ОБ ОДНОМ ПОДХОДЕ ПО ОБНАРУЖЕНИЯ АНОМАЛИЙ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ НА ОСНОВЕ АКУСТИЧЕСКИХ СИГНАЛОВ                 |     |
| <b>V. Strukov, V. Gudilin</b> .....   | 118 |
| ABOUT SOME APPROACHES FOR DETECTING VULNERABILITIES IN WEB APPLICATIONS   |     |
| <b>O. Yeremenko, A. Mersni, A. Akulynichev</b> .....  | 120 |
| THE OVERVIEW OF CYBER RESILIENCE APPROACH USING TRAFFIC ENGINEERING FAST REROUTE FEATURES                           |     |

## PLENARY TALKS

### СЕТЕВАЯ БЕЗОПАСНОСТЬ СРЕДСТВАМИ МАРШРУТИЗАЦИИ: ПРОБЛЕМЫ И РЕШЕНИЯ

**А.В. Лемешко, М.А. Евдокименко, А.С. Еременко**

Харьковский национальный университет радиоэлектроники, Харьков, Украина

e-mail: [oleksandr.lemeshko@nure.ua](mailto:oleksandr.lemeshko@nure.ua), [marina.ievdokymenko@nure.ua](mailto:marina.ievdokymenko@nure.ua),

[oleksandra.yeremenko@nure.ua](mailto:oleksandra.yeremenko@nure.ua)

Обеспечение информационной безопасности страны является важной государственной проблемой, решение которой требует максимальной концентрации сил и средств на всех этапах, связанных с формированием, передачей/приемом, хранением, обработкой, отображением и даже уничтожением информации. В последнее время все больше внимания уделяется именно проблематике обеспечения сетевой безопасности, когда объектом атак и компрометации передаваемых сообщений становится коммуникационное оборудование [3], [5]. Именно разнотипные и взаимодополняющие организационные, социальные, технические (аппаратные и программные) меры и средства должны обеспечить надлежащий уровень безопасности информации, передаваемой в современных телекоммуникационных сетях (ТКС).

Достаточно действенным средством обеспечения сетевой безопасности в ТКС являются протоколы маршрутизации. Именно они должны обеспечить проактивную и реактивную защиту сети на основе сбора и анализа информации о ее состоянии. В то же время протоколы безопасной маршрутизации, кроме привычных данных о состоянии сети, должны прогнозировать и оценивать значение ключевых показателей безопасности коммутационного и серверного оборудования ТКС, уровни их уязвимости и компрометации. С этой целью математическое и алгоритмическое обеспечение протоколов маршрутизации в ТКС должно быть усовершенствовано и расширено под новые условия и задачи, связанные с обеспечением заданного уровня сетевой безопасности.

В зависимости от перечня и содержания требований, которые предъявляются к уровням сетевой безопасности и QoS, маршрутизирующие решения могут достаточно сильно различаться [1]-[7]. Первая большая группа решений посвящена маршрутизации конфиденциальных сообщений (КС) с использованием, например, механизма SPREAD (Secure Protocol for Reliable dAta Delivery) [2]. В его основу положен принцип порогового разделения КС в соответствии с выбранной схемой Шамира на отдельные фрагменты (части), которые в дальнейшем передаются в ТКС к получателю по множеству непересекающихся путей. В работе [6] предложены решения по усовершенствованию механизма SPREAD, в рамках которых допускается определенный характер пересечения путей в ТКС, что сопровождается улучшением показателей сетевой безопасности при передаче КС. Закон (схема) разделения

сообщения на фрагменты в общем случае может быть известна злоумышленнику, но скомпрометировать конфиденциальное сообщение он сможет только тогда, когда скомпрометирует все используемые пути. Поэтому уровень сетевой безопасности в этом случае полностью зависит от количества и безопасности путей, используемых для доставки фрагментов КС.

Вторая группа решений по безопасной маршрутизации [4], [7] основана на использовании соответствующих маршрутных метрик, которые, в общем случае, должны учитывать множество показателей сетевой безопасности (Network Security, NS) каналов связи и маршрутизаторов ТКС. Так, в работе [7] для расчета маршрутных метрик используются выражения, характеризующие риск информационной безопасности элементов ТКС в соответствии с рекомендациями NIST, учитывая убытки от нарушения конфиденциальности и целостности информации, доступности сетевого ресурса в случае использования имеющихся уязвимостей, а также показатели сложности использования уязвимостей на узлах сети и доступа к сетевым элементам и сети в целом вследствие использования указанных уязвимостей. Метрический подход используется и при организации безопасной маршрутизации мультимедийных потоков пакетов, т.е. когда, например, необходимо обеспечить для передаваемой в ТКС аудиовизуальной информации высокий уровень и качества обслуживания (Quality of Service, QoS), и сетевой безопасности. Основной научной и прикладной задачей тогда становится поиск моделей композитного учета показателей NS/QoS [4].

Третья группа решений, касающаяся маршрутизации потоков пакетов с целью повышения показателей NS/QoS, основана на реализации принципов Traffic Engineering (TE) [1]. При этом балансировка нагрузки в ТКС происходит с учетом не только сетевых параметров, которые характеризуют уровень ее качества обслуживания, например, пропускную способность, но и уровень сетевой безопасности – вероятность компрометации узлов и каналов сети. В рамках решений Secure TE заложена возможность регулировать чувствительность потоков пакетов к показателям NS/QoS, так как нередко повышение уровня сетевой безопасности отрицательно сказывается на показателях QoS.

Таким образом, в зависимости от особенностей структурно-функционально построения ТКС, ее состояния и загруженности, требований относительно уровней NS и QoS на практике могут использоваться различные подходы к организации процессов безопасной маршрутизации. Разнотипные математические модели и методы безопасной маршрутизации могут быть положены в основу алгоритмическо-программного обеспечения маршрутизаторов традиционных IP/MPLS-сетей, серверов или контроллеров маршрутов в программно-конфигурируемых сетях, реализуясь в форме перспективных протоколов маршрутизации.

**Ключевые слова:** сетевая безопасность, маршрутизация, балансировка нагрузки, телекоммуникационная сеть, уязвимость, метрика.

### Литература

1. Lemeshko O., Shapovalova A., Al- Dulaimi A.M.K., Yeremenko O., Yevdokymenko M. (2020), Flow-Based Routing Model With Load Balancing Under Network Security Parameters, Information and Telecommunication Sciences, No. 2, pp. 44-50.
2. Lou W., Liu W., Fang Y. (2004), SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks”, INFOCOM 2004: Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, Hong Kong, China, 7–11 March, P. 2404-2413.
3. Santos O., Kampanakis P., Woland A. (2016), Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP, 1st edition, Cisco Press, 368 p.
4. Snihurov A., Chakrian V. (2015), Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters, Scholars Journal of Engineering and Technology, No. 3(8), P. 707-714.
5. Stallings W. (2016), Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 768 p.
6. Yeremenko O., Lemeshko O., Persikov A. (2018), Secure Routing in Reliable Networks: Proactive and Reactive Approach, Advances in Intelligent Systems and Computing II, CSIT 2017, Advances in Intelligent Systems and Computing, No. 689, Springer, Cham, P. 631–655.
7. Yevdokymenko M., Yeremenko O., Shapovalova A., Shapoval M., Porokhniak V., Rogovaya N. Investigation of the Secure Paths Set Calculation Approach Based on Vulnerability Assessment. Workshop Proceedings of the MoMLeT+DS 2021: 3rd International Workshop on Modern Machine Learning Technologies and Data Science, June 5, 2021, Lviv-Shatsk, Ukraine. pp. 207-217.

### **Network security by routing means: problems and solutions**

An overview of the main solutions related to secure routing in telecommunication networks is carried out. The review covers theoretical approaches based on optimizing secure routing processes associated with implementing the SPREAD mechanism, the metric approach, and the principles of Secure Traffic Engineering. The analyzed solutions can form the basis of promising routing protocols in traditional and software-defined networks.

## **CHALLENGES AND OPPORTUNITIES IN CRYPTOGRAPHY: LATTICE-BASED AND CODE-BASED CRYPTOGRAPHY IN THE QUANTUM ERA WITH FORMAL ANALYSIS**

**Sedat Akleylek**

Department of Computer Engineering, Ondokuz Mayıs University, Samsun, Turkey

e-mail: [sedat.akleylek@bil.omu.edu.tr](mailto:sedat.akleylek@bil.omu.edu.tr)

Cryptographic techniques are necessary to provide information security concepts such as confidentiality, integrity, authentication, non-repudiation. In other words, cryptographic techniques are the most important components for the realization of secure communication. There has been a rapid development in public-key cryptography in recent years. In parallel with this development, cryptanalysis has been developed for the protocols (algorithms) and algorithms with polynomial time (or close to) runtime have been developed to show that these systems are not secure. The most outstanding of these developments is the work that solves the factorization and discrete logarithm problem proposed by Shor in 1997 on a quantum computer in polynomial time. Therefore, when quantum computers emerge, public key cryptosystems such as RSA, DSA, ECDSA, Diffie-Hellman, which are now known to be secure and rely on hardness of factorization and discrete logarithm problems, will be insecure in quantum era. Then, there is a huge demand for new cryptographic protocols based on hard problems that cannot be solved with quantum computers for the operations performed with them (encryption, especially key exchange and signing). These systems are called post-quantum cryptographic protocols. Post-quantum cryptography can be grouped into five main groups: code-based, hash-based, multivariate cryptography, isogeny< and lattice-based.

Quantum computers are an active field that has been studied for a long time. A company called D-Wave has announced that it produces quantum computers and sells them to various institutions. In this context, it is thought that research on post-quantum cryptography is very important. All systems whose hardness are based on the factorization and discrete logarithm problems are threatened by quantum computers. According to the algorithm proposed by Grover in 1996, the security level of symmetric ciphers is approximately half with quantum computers. When quantum computers are evaluated in terms of conflict finding, no effect on the security of hash functions has yet been found. However, it has been shown that the level of security is reduced to approximately half that of symmetric ciphers.

Quantum cryptography is based on applying quantum mechanics and cryptographic techniques suitable for this structure. A solution has been presented to the key sharing/exchange problem with quantum cryptography, which requires a special infrastructure. Post-quantum cryptography, on the other hand, includes cryptosystems that can be used in today's information and communication technologies, based on mathematically hard problems, and do not require any special application/implementation platform. With post-quantum cryptosystems, secure solutions have been

found for public key encryption, electronic signing, hashing and key sharing problems in quantum era.

The roadmap to be followed for the design of cryptographic algorithm/protocol and architecture resistant to quantum computers can be summarized as follows: The points to be considered here can be summarized as general algorithm design, parameter selection for different security levels, and updating algorithms that will allow these platform-specific algorithms to work efficiently.

- a) **Finding hard problems that are resistant to quantum computers:** Mathematically hard problems that are resistant to quantum computers are in the class of NP-Complete or NP-Hard. These problems can be exemplified as finding the solution of the set of quadratic equations on a finite field, finding the shortest vector on the lattice, finding the closest point to a given point in the lattice, learning problems with errors, finding the code with the desired properties, finding overlap for hash functions. These problems have been identified in the literature and studies on their difficulties continue.
- b) **Cryptosystem/Cryptographic protocol design based on the selected hard problem:** There are many protocol proposals for post-quantum cryptography in the literature. Standardization studies have started for some of these: Criteria for selection of public-key cryptographic algorithms for quantum-safe hybrid cryptography, Quantum-Safe Hybrid (QSH) Ciphersuite for Transport Layer Security (TLS) version 1.3, XMSS: Extended Hash-Based Signatures, P1363.1: Standard Specifications for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices, Hash-Based Signatures. Various algorithms have been proposed for signing and encryption in these standard proposals, which are in the draft stage. There are many open problems on this subject and research and development studies need to be done on it.
- c) **Theoretical and practical implementation of the security analysis of the designed cryptographic algorithm/protocol**
- d) **Performing security analysis operations in the architecture to be used:** During the operation of the selected algorithms and protocols on different architectures or devices, various insecurities may arise about the exposure of extra information and the vulnerabilities of the system by using them. Examination of these in detail is an open problem in the literature.
- e) **Determining algorithm/protocol parameters for different levels of security (Confidential, Top Secret, etc.) and verifying their security analysis:** One of the open problems in the literature is how to generate parameters for different security levels. The issue of parameter generation for the selected algorithm/protocol needs to be studied in detail.
- f) **Making necessary updates on the operation of the algorithm in accordance with the target platform:** Since cryptographic algorithms are designed for general structure (excess system resources), it may not be possible to run these algorithms on some platforms. Therefore, there is a need for algorithm design that will allow efficient working on the selected

platform. Since these will be different for each system, they are considered important in terms of efficiency.

Lattice-based and code-based cryptosystems have received much more attention during NIST Post-Quantum Cryptography Project. Moreover, the cryptosystems based on these have selected for the third of NIST Post-Quantum Project. Security analysis of this protocols needs much more attention. Then, formal analysis has an important role for the security analysis. There are automated tools for the security analysis of cryptographic protocols. However, due to the special structures of lattice-based and code-based cryptosystems, modifications and updates of these tools should be studied. Then, to give a chance to the researchers is needed for post-quantum cryptographic issues.

## SECTION TALKS

### AI APPROACHED DYNAMICALLY DETECTING SECURITY THREATS AND UPDATING A SIGNATURE-BASED IDS'S DATABASE IN NGN

**G. Abdiyeva-Aliyeva Alishan<sup>1</sup>, M. Hematyar Mahmud<sup>2</sup>**

<sup>1</sup>Baku Engineering University, Khirdalan, Azerbaijan

<sup>2</sup>Azerbaijan Technical University, Baku, Azerbaijan

e-mail: [geliyeva@beu.edu.az](mailto:geliyeva@beu.edu.az), [mehran@aztu.edu.az](mailto:mehran@aztu.edu.az)

**Abstract.** Cyber-attacks threatening the network and information security have increased, especially during the current rapid IT revolution. Therefore, a monitoring and protection system should be used to secure the computer networks. Intrusion detection system (IDS) is one of the most important security systems on the market. IDS is a system that can then be used to monitor network traffic and display alerts for illegal activities or illegal access to the network. IDS is divided into three main types: signature-based IDS, anomaly-based IDS and a mixture of both. Automatically updating the attack list to overcome new attack types is one of the main challenges of signature-based IDS. Most IDS (by network administrators) or websites that use newly detected attack signatures to manually or remotely update their databases. This article proposes a new AI model that uses a filter engine that functions as a second IDS engine to update the attack list by AI and automatically. The results show that using the proposed model can improve the overall accuracy of IDS. The proposed model uses an IP-Factor(IPF) and Non-IP-Factor(NIPF) blacklist that can automatically detect the threats and update the IDS database with new attack features without manual intervention, as well as define new attack features based on similarity.

#### 1 Introduction

Due to the popularity of technology, Internet (WAN) and Local Area Networks (LAN) in the past decades, the number of security attacks has been growing and developing rapidly, more than detection and defense. This can violate the privacy, integrity, and availability of computers and networks when changing critical data and disabling critical services. Even with the most advanced protection systems, computer systems are not highly (more than 96%) secure. Many companies have purchased security systems to protect from possible computer and network attacks, including firewalls, antivirus software, intrusion detection systems, access control and encryption mechanisms [1]. Each of these mechanisms has disadvantages and deficiencies. For example, firewalls serve only against unauthorized data transmission. They do not provide anti-virus, anti-malware, or anti-spyware functions. Intrusion detection software cannot process encrypted software packages. Installing and running antivirus software can take up too much computer memory and hard disk space, resulting in slower computer speed. The disadvantage of these security mechanisms is that intruders can be used,

so they must be confused. Although IDS can be used with the Help of a firewall in a network, these two tools should not be considered as the same tool [2].

In fact, new types of attacks can be carried out through many security systems, including IDS and firewalls. Therefore, a strong, fast and reliable IDS is urgently needed to manage and protect computers and networks from such events. In 2016 setting the appropriate frequency threshold levels for updating the database of known attack signatures and detecting intrusion detection is the biggest problem facing SIDS. On this basis, a unified algorithm (CA-NIDS) that uses three databases to enable SBS to use a unified algorithm, attack signature database, new attack database, and normal traffic database.

They chose a combination algorithm for the analysis engine, used 12 thresholds to sort the matching score values below the intrusion threshold and entered classification values greater than or equal to the intrusion threshold value. general. In this article, we propose a new model that uses multiple smaller databases to install a filtering engine to detect new attacks after the IDS engine function [3].

## **2 Challenges and contributions**

One of the main challenges discussed in this article includes a large number of signatures in the IDS database. Therefore, these small signature databases can improve and improve the performance of the signature-based IDS, as software packages need to match fewer signatures but a huge database can decrease the performance and efficiency. When IDS is exposed to a large amount of network traffic that exceeds its monitoring potential, all it can do is drop the packets. Therefore, it may miss dangerous attacks. Another challenge is to increase the performance of the proposed model. Model solves this problem by distributing complementary databases and small databases by protocol type to improve performance and reduce the time spent in the matching process. Another challenge is to detect new attacks, since the signature-based IDS cannot detect unknown attacks. Therefore, the database is not updated, making it easy to attack the network and override the IDS. Therefore, the proposed model solves this challenge by proposing a filtering engine as a double check after the IDS engine, updating the complementary database and small database, and automatically updating without manual intervention without new intervention signatures.

Another challenge is how to measure the similarity between the new packaged signature and the signature stored in the IDS database. The proposed model addresses this problem based on IP blacklist factors and source IP, target IP, packet load, and many features of the protocol used to detect new attacks. Another challenge is how to determine an appropriate similarity threshold without affecting IDS performance. The proposed model solves this problem by using many similarity thresholds and evaluating its output. The last challenge is how to determine the right priority between the similarity between IP elements and blacklists [4].

## **3 Suggested solutions**

The proposed model has been inspected, analyzed and developed to process large signature databases, detect new attacks that are not stored in the IDS database, and then dynamically update the IDS database with new attack signatures, thereby improving the performance and accuracy of

IDS. The proposed model will solve many issues not covered in previous studies, such as detecting new attacks with signatures not stored in the IDS database and automatically updating the CDB and small database with new attack signatures without new attack signatures. It identified and developed previous work on large IDS database problems.

The component of the proposed model is the IDS engine, which is a CDB that stores all rare signatures and is distributed to three small databases based on protocol type (TCP, UDP and ICMP). This protocol type is the most commonly used signatures (TCP, UDP and ICMP). It is distributed to three small databases according to the filter engine and update engine. The purpose of the IDS engine is to capture incoming data packets, process them beforehand and sign them, and then match the extracted signatures with signatures stored in the signature database by AI.

If there is a match or AI detect an unknown activity, the engine sends a warning, logs the warning, and blocks this package. Otherwise, the packet will be rechecked by the filtering engine based on two factors (similarity and IP blacklist)[5].

The different stages shown in the flow chart above will be described in detail below.

- **IDS Engine Stage.**
- **Training Stage:** 1- Collect the ready-to-use attack feature dataset with 12,000 different attack features.

Using the previous dataset, create two additional databases as follows:

- First database containing the most frequent signatures occurring during the dataset, called the frequent signatures database (FSDB).
- Second database containing the rest of the signatures occurring during the training stage, called the complementary database (CDB).

The first database that contains the most common signatures that appear in the dataset is called the Favorite Signature Database (FSDB). The second database, called the complementary database (CDB), contains other signatures that appear during the training phase. 3- Signatures in the CDB and FSDB are distributed to smaller databases according to the type of protocol signed, that is, the CDB is distributed to these three small databases:

- The TCP database contains all signatures that use the TCP protocol.
- The UDP database includes those that use the UDP protocol All signatures. FSDB is distributed in the following three small databases:
- The TCP database contains all signatures that use the TCP protocol. UDP database contains all signatures that used the UDP protocol.
- ICMP database contains all signatures that the used ICMP protocol.

#### **4 Similarity factor with AI**

The filter engine uses this factor to measure the similarity between the signature of the new package and the stored signature, based on four factors: the source of the new package, the destination IP, the package load, and the package using the new protocol. Each property is assigned a default value (score = 0). If the newly packaged signature matches one of these functions, the value (score) changes from 0 to 20 and the match rate is more than 25%. The remaining attributes will be checked

in the same way to determine the final value of the score and will then be compared to the determined similarity threshold. If there is no match, the filtering engine will measure the similarity between the newly wrapped signature and the stored signature based on the determined similarity threshold (only the performance of the model using the same protocol with the new packaging to match the stored signature). To reduce and improve pairing time). If there is a similarity (score > = set threshold), the new package will be blocked and automatically updated with the CDB signature, IP blacklist and the IP of the new package. If no similarity is detected, the new packet is clean and can safely pass through the target network. When the signature of the new data packet passes through the IDS engine, the filtering engine first starts working to carefully check the IP of the new data packet using the IP blacklist. If there is a match, this package will be blocked and automatically updated with the CDB signature [6],[7].

### Conclusion

This paper first emphasized the motivation to write this article. Then he introduced his challenges and contributions. Then, the proposed model is designed and output. This article describes how IDS performs when deploying large databases to smaller databases. As for the contribution of this article, the proposed solution provides detection of new attacks with unknown IDS signatures. This solution usually connects to a filtering engine that uses two factors to detect new attacks. <br><br> Four similarity factors based on the measure of similarity between the characteristics of the signature and the stored signature of a new package: the source of a new package, the IP target, and the data packet load of a new package.

**Keywords:** Intrusion detection, signature-based, anomaly-based, traffic, artificial intelligence.

### References

1. Almutairi A.H., Abdelmajeed N.T. (2017). Innovative signature based intrusion detection system. In Information Technology, published in 2017 International Conference on the Frontiers and Advances in Data Science on (pp. 1-7). IEEE.
2. Sheenam S.D. (2016). Comprehensive review: intrusion detection system and techniques. IOSR Journal of Computer Engineering, 18(4), pp.1507-1516.
3. Debar H. (2000). An introduction to intrusion-detection systems. Proceedings of Connect, 2002, pp.1-18.
4. Folorunso O., Ayo F.E., Babalola Y.E. (2016). Ca-NIDS: A network intrusion detection system using a combinatorial algorithm approach. Journal of Information Privacy and Security, 12(4), pp.181-196.
5. Innella P., McMillan O. (2001). An introduction to intrusion detection systems.
6. <https://securelist.com/kaspersky-security-bulletin-2019>
7. Mutep Y., Yousefa A., Dr. Abdelmajeed N.T. Dynamically Detecting Security Threats and Updating a Signature-Based Intrusion Detection System's Database. Procedia Computer Science.

## МЕТОД СРАВНЕНИЯ СПЕКТРОВ WI-FI УСТРОЙСТВ ДЛЯ ИХ ИДЕНТИФИКАЦИИ

И.Е. Антипов, Т.А. Василенко, Л.Ф. Сайковская

Харьковский национальный университет радиоэлектроники, Харьков

e-mail: [ivan.antipov@nure.ua](mailto:ivan.antipov@nure.ua)

Методы идентификации пользователей в Wi-Fi сетях хорошо известны. К сожалению, методы «взлома», похищения, имитации данных, на основании которых происходит идентификация, также хорошо известны и доступны злоумышленникам. По этой причине Wi-Fi сети остаются небезопасными с точки зрения уязвимости к различным атакам.

В работе [1] авторами предлагается метод идентификации Wi-Fi устройств, основанный на сравнении спектров их излучения. Как показали проведённые исследования, спектры различных Wi-Fi устройств в целом соответствует типовому шаблону, но при этом имеют свои особенности, которые могут быть использованы для идентификации. Примеры спектров 4 разных устройств приведены на рис. 1.

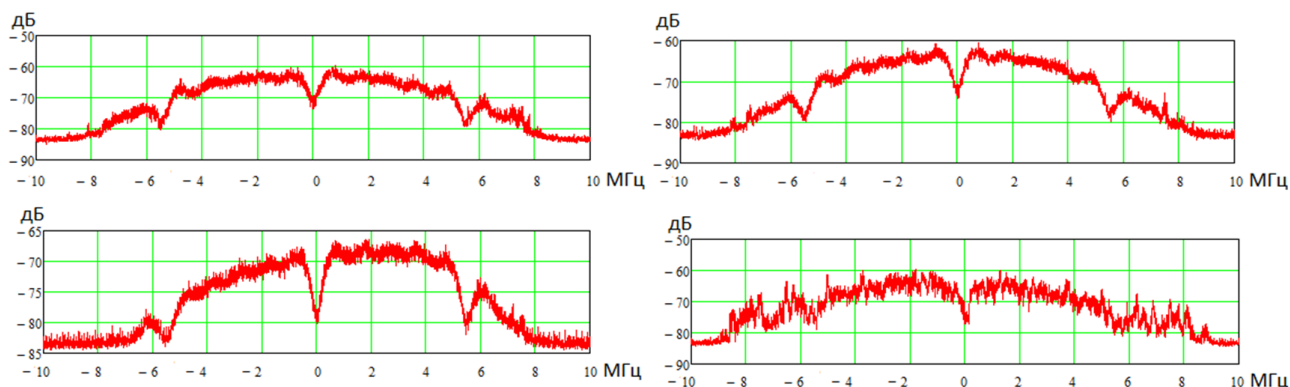


Рисунок 1. Спектры четырёх различных W-Fi устройств

Как видно из рисунков, спектры различаются даже визуально. В предлагаемом докладе рассматривается метод, который позволяет оценить различия в цифровой форме и сформулировать критерий определения его принадлежности тому или иному устройству. Для анализа спектра предлагается использовать спектральный анализатор, способный работать в соответствующей полосе частот (2,4 или 5,1 ГГц) с шагом по частоте не более 2 кГц, который должен быть размещён на точке доступа (ТД). Сложность задачи сравнения спектров состоит в том, что на их форму могут влиять взаимное расположение антенн устройства, мощность, которая может адаптивно меняться в зависимости от дальности до ТД, а также воздействие шума и помех. Эти факторы могут мешать выявлению индивидуальных особенностей спектров, поэтому их влияние необходимо учитывать.

В ходе исследований удалось установить, что изменение уровня сигнала приводит только к изменению среднего значения спектральных отсчётов, что может быть учтено добавлением (или вычитанием) постоянной составляющей. Что же касается возможного поворота устройства, то изменение формы спектра при этом оказывается несущественным и находится в пределах определённого допуска, который может быть найден для каждой пары сравниваемых спектров.

Для решения задачи идентификации Wi-Fi устройства по его спектру нами предлагается:

1) в идеальных условиях (в отсутствии помех и при фиксированном расстоянии от ТД) снять спектральные характеристики каждого из устройств, которые могут подключаться к данной ТД в разных положениях;

2) сохранить указанные характеристики в виде шаблонов, «связав» их с MAC-адресами соответствующих устройств;

3) в процессе идентификации необходимо вычислять средний квадрат разности спектральных отсчётов сигнала, принимаемого от идентифицируемого устройства и его шаблона;

4) в случае, если значение среднего квадрата разности принятого и шаблонного спектров не превышает порогового значения, можно разрешать работу данного устройства в сети. В случае превышения порога устройство следует блокировать, поскольку это может быть признаком атаки на сеть с подменой MAC-адреса.

Полученные в ходе экспериментальных исследований значения порогов находятся в пределах 1...2 дБ, что видно из рис. 2.

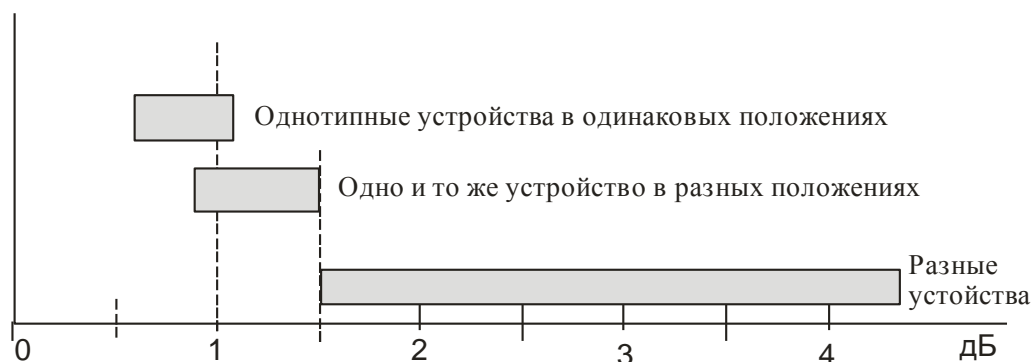


Рисунок 2. Значения средних квадратов разности спектральных отсчётов

**Ключевые слова:** безопасность Wi-Fi сетей, спектр сигнала, идентификация.

### Литература

1. Антипов И.Е., Василенко Т.А. Идентификация мобильных устройств по особенностям спектров их сигналов. Межведомственный научно-технический сборник «Радиотехника», 2020, Вып. 179, с. 91 – 97.

## The comparison method of the Wi-Fi devices spectra for their identification

This is about the method of comparing the spectrum of the signal received from the wi-fi device with its template, which allows to identify the device and to detect the hacker attacks attempts on the Wi-Fi network.

### TƏHSİLDƏ KİBERTƏHLÜKƏSİZLİK PROBLEMLƏRİNİN İCMALI

**B. Əzizov<sup>1</sup>, E. Həsənov<sup>2</sup>, A. Paşayev<sup>1</sup>**

<sup>1</sup>Azərbaycan Universiteti, Bakı, Azərbaycan

<sup>2</sup>Azərbaycan Respublikası Prezidenti yanında Dövlət İdarəçilik Akademiyası

e-mail: [bahram.azizov@au.edu.az](mailto:bahram.azizov@au.edu.az), [elgafgas@yahoo.com](mailto:elgafgas@yahoo.com), [asif.pashayev@au.edu.az](mailto:asif.pashayev@au.edu.az)

Klassik informasiya texnologiyaları ixtisasları ilə yanaşı müasir əmək bazarında «Kiber təhlükəsizlik» ixtisasına tələbat getdikcə artır. Demək olar ki, hər hansı bir dövlət qurumu və ya özəl şirkətin strateji informasiya resursları bazasının qorunması üçün informasiya təhlükəsizliyi ən vacib problem və əsas vəzifədir. Bu istiqamətdə təhsil alanlar verilənlər bazalarını saxlama metodlarını, şəbəkə fəaliyyətini izləmə üsullarını, məlumatları qorumaq prinsiplərini, haker hücumlarını dəf etmək üçün texnologiyaları öyrənirlər. Ümumiyyətlə, ABŞ və Avropadakı müasir universitetlərdə əsas fənlər bunlardır: kompüter təhlükəsizliyi, şəbəkə təhlükəsizliyi, rəqəmsal məhkəmə ekspertizası, təhlükəsizlik sistemlərindəki risklərin idarəedilməsi və kiber cinayətlərin araşdırılması.

#### **Tələbələr hansı proqramlardan və terminologiyalardan istifadə edirlər?**

Kiber Təhlükəsizliyi öyrənərkən tələbələr aşağıdakılardan istifadə edir və öyrənirlər: ENCASE; Nessus paketləri, MetaSploit, Kali Linux, OpenSSH, SSL və s. Tələbələr davamlı olaraq görünən və yenilənən ən yeni və inkişaf etmiş proqramı öyrənir və istifadə edirlər.

**Cyber Security**, əmək bazarında aktuallığı və tələbi zamanla artan müasir bir peşədir. Bu peşə üzrə ABŞ kimi bir ölkədə belə son dərəcə yetkin mütəxəssis çatışmazlığı var. ABŞ-da və dünyanın bütün ən böyük İT şirkətləri (Facebook, Google, Pixar, Twitter, IBM, eBay, Amazon), davamlı olaraq müvafiq peşələrini genişləndirərək bu peşə üzrə işçilər götürürlər.

Rəsmi statistikaya görə ABŞ Əmək Statistika Bürosu, CIS (Beynəlxalq Məktəblər Şurası) və Comodo İnternet Təhlükəsizliyi işçilərinin orta əmək haqqı 2017-ci ildə ildə 160.000 ABŞ dollarını keçdi! Yalnız bir nisbi dar çərçivədə olan "kiber təhlükəsizlik" ixtisası üçün 2021-ci ilədək iş sayı eyni ABŞ Statistika Bürosunun proqnozuna görə 210.000 olacaqdır!

Çox spesifik olmaq üçün İKT tələbələri aşağıdakı səriştələrə sahib olmalıdırlar:

- peşə fəaliyyətində yaranan problemlərin mahiyyətini müəyyənləşdirmək, elmin ümumi qanunlarından istifadə etmək və riyazi aparatı informasiya peşə tapşırıqları sahəsində tətbiq etmək;

- informasiya resursları və infrastrukturaların kənar müdaxilələrdən qorunması üçün hüquqi, təşkilati, aparat və proqram təminatı sahəsində nəzəri bilik və praktik bacarıqlara yiyələnmək;
- müasir cəmiyyətdə, informasiya texnologiyalarının tətbiqində, müxtəlif mənbələrdə və qlobal kompüter sistemlərində hədəfli məlumat axtarışında məlumatın mahiyyətini və əhəmiyyətini başa düşmək;
- peşə sahəsində hüquqi məsləhətlərdən istifadə;
- qanuni əsaslar, inzibati və texnoloji tətbiqetmə və iqtisadi səmərəliliyi nəzərə alaraq, mümkün təhdidləri müəyyənləşdirərək məlumat təhlükəsizliyini təmin etmək üçün köməkçi tədbirlər kompleksinin idarə olunması;

### **Kiber təhlükə**

**Kiber təhlükə** - siyasi, sosial və ya digər məqsədlərə çatmaq üçün virtual məkana qanunsuz giriş və ya zərərli müdaxilə təhlükəsidir.

Kiber təhlükə, məlumatları ehtiva edən, fiziki və ya virtual bir cihazın materiallarını saxlayan bir kompüterin məlumat sahəsini təsir edə bilər. Hücum ümumiyyətlə istifadəçinin şəxsi məlumatlarının saxlanması, işlənməsi və ötürülməsi üçün xüsusi hazırlanmış bir saxlama mühitinə təsir edir.

### **İnsanlar niyə kiberhücumlar edirlər?**

Təcavüzkarlar korporativ sistemlərdəki zəifliklərdən istifadə etməyə çalışırlar ki, bu da kibercinayətlərin illik artımına səbəb olur. Tez-tez hakerlər fidyə (girov) tələb edirlər: kiber hücumların 53% -i 500.000 dollar və ya daha çox zərərlə nəticələndi.

Kiberhücumlarda gizli məqsədlər də ola bilər. Hakerlərin sistemləri və məlumatları məhv etmək üçün bəzi cəhdləri "hacktivism" in özünəməxsus təzahürləridir.

### **Botnet nədir?**

Botnet - viruslar kimi zərərli proqram təminatlarına yoluxmuş cihazlar şəbəkəsidir. Hackerlər, hücumların miqyasını artırmaq üçün sahiblərini bilmədən bir botnet'i tək bir qrup olaraq idarə edə bilərlər. Botnetlər tez-tez DDoS (Distributed Denial of Service ) hücumları nəticəsində sistemlərə dözülməz bir yük yaratmaq üçün istifadə olunur.

### **Fişinq**

Fişinq - etibarlı bir alıcıya göndərilmiş kimi görünən saxta mesajların ümumiyyətlə e-poçt yolu ilə paylanmasıdır. Bu fəaliyyətin məqsədi kredit kartları və ya hesablar kimi məxfi məlumatları oğurlamaq və ya zərər çəkmiş şəxsin kompüterinə zərərli proqram yükləməkdir. Fişinq getdikcə daha çox yayılmış bir kiber təhiddir.

### **Kriptografiya**

Kriptografiya (qədim yunan dilindən hiddenροπτός "gizli" + γραφω "yazıram") məxfiliyi (məlumatı yad insanlar tərəfindən oxumağın mümkünsüzlüyü), məlumatların bütövlüyünü (məlumatdakı hiss olunmayan dəyişikliklərin mümkünsüzlüyünü), identifikasiyanı (doğrulamağı) təmin edən metodlar haqqında elmdir. bir obyektin müəllifliyinin və ya digər xüsusiyyətlərinin həqiqiliyi), şifrələmə (məlumatların kodlaşdırılması).

Başlangıçda kriptografiya məlumat şifrələmə metodlarını - gizli alqoritmlər və ya açar əsasında açıq (orijinal) mətnin şifrə mətninə çevrilməsini öyrənirdi. Ənənəvi kriptografiya simmetrik kriptosistemlərin bir hissəsini təşkil edir ki, burada şifrə və şifrənin açılması eyni gizli açardan istifadə olunur.

Kriptografiya ən qədim elmlərdən biridir, tarixi bir neçə min il əvvələ gedib çıxır.

**Şifrə mətni**, şifrə (qapalı) mətn - kriptosistemdən istifadə edildikdən sonra əldə edilən məlumatlar (ümumiyyətlə müəyyən bir açarla). Başqa bir ad: kriptogram.

**Şifrə, kriptosistem** - düz mətnin şifrəli mətnə çevrilə bilən çevrilmələr ailəsi.

**Şifrələmə** - düz mətnin bir alqoritmlər və açara əsaslanan şifrəli mətn çevrilməsinin normal tətbiqi.

**Şifrənin açılması** şifrəli mətni düz mətnə kriptografik olaraq çevirmək üçün tətbiq olunan normal prosesdir.

**Simmetrik şifrələmə** - paylaşılan mesajın həm şifrələnməsini, həm də şifrəsini açmağı həyata keçirmək üçün yalnız bir açarın istifadəsinə imkan verən bir texnikadır.

**Asimmetrik şifrə** - iki açar şifrə, açıq açar şifrə - şifrələmə və şifrəni açmaq üçün xüsusi açardan istifadə edən şifrədir. Eyni zamanda, yalnız şifrələmə düyməsini bilməklə mesajın şifrəsini açmaq mümkün deyil və əksinə.

**Kriptanaliz** məlumatların məxfiliyi və bütövlüyünün pozulmasının riyazi metodlarını araşdıran bir elmdir.

**Kriptanalizator** kriptanaliz metodlarını yaradan və tətbiq edən bir elm adamıdır.

**Kriptografik hücum** - kriptanalizatorun hücum edilən təhlükəsiz məlumat mübadiləsi sistemində səpmələrə səbəb olma cəhdidir. Uğurlu bir kriptografik hücumla hack və ya hücum deyilir.

### **Tədqiqatın əsas nəticələri**

Araşdırmalar kibernetik cinayətkarların hər zaman imkanları maksimum dərəcədə artırmağa çalışdıqlarını göstərdi. Həftə içi və həftə sonları kibernetik öldürmə zənciri fəzalarının veb süzgəcinin miqdarını iki mərhələ ilə müqayisə etdikdə, güzəştədən əvvəl aktivliyin iş həftəsi ərzində üç dəfə yüksək olduğu, bu baxımdan güzəştədən sonra trafik az olduğu fərqləndirildi.

Bu, əsasən zəifliklərin axtarılması üçün kiminsə fişinq e-poçtundakı bir keçidi izləmək kimi bir hərəkətin tələb etməsi ilə bağlıdır. Bunun əksinə olaraq, aktiv addımlar üçün belə bir tələb yoxdur (command-and-control, C2), buna görə də bu cür fəaliyyət hər an müşahidə oluna bilər. Kibernetik cinayətkarlar bunu başa düşür və istifadəçilər ən çox İnternetdə olduqları iş həftəsi ərzində imkanlardan maksimum istifadə etməyə çalışırlar.

Müxtəlif təhdidlərin müəyyən bir infrastrukturdan istifadə dərəcəsi bir sıra vacib tendensiyalar barədə məlumat verir. Bəzi təhdidlər digərlərinə nisbətən vahid və ya ixtisaslaşmış infrastrukturlardan daha çox bir ümumi infrastrukturdan istifadə etmək ehtimalı daha yüksəkdir. Təhlükələrin demək olar ki, 60% -i ən azı bir ümumi domen daxilində həyata keçirilmişdir ki, bu da əksər botnetlərin artıq qurulmuş bir infrastrukturdan istifadə etdiyini göstərir.

**Açar sözlər:** İKT, kibernetik hücum, internet şəbəkə, xakerlərin məqsədi, saytların yarılməsi.

## Ədəbiyyat

1. [https://reports.beazley.com/2021/rr/index.html?utm\\_source=bing&utm\\_medium=cpc&utm\\_campaign=Beazley%20R%26R%20%7C%20Types%20Of%20Risk&utm\\_term=%2Bcyber%20%2Brisks&utm\\_content=Non-Branded%20-%20Cyber](https://reports.beazley.com/2021/rr/index.html?utm_source=bing&utm_medium=cpc&utm_campaign=Beazley%20R%26R%20%7C%20Types%20Of%20Risk&utm_term=%2Bcyber%20%2Brisks&utm_content=Non-Branded%20-%20Cyber)
2. <https://www.channelfutures.com/strategy/what-do-hackers-want-anyway-a-look-at-different-cyberattack-goals>
3. <https://www.channelfutures.com/security/kaseya-ransomware-attack-sparks-scrutiny-of-msp-rsecurity-practices>
4. <https://www.pravda.ru/science/1054060-kragalichnosty/>
5. <https://www.rebellionresearch.com/cyber-attacks-examples>
6. <https://cpab.ru/trevozhnyj-rost-kolichestva-nanimaemyh-hakerov-cloudsavvy-it/>
7. <https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions>
8. <https://www.mcafee.com/blogs/consumer/family-safety/7-types-of-hacker-motivations/>

### Overview of cyber security problems in education

The cybercriminal community in its activities takes into account national strategies and methodologies, as well as the technical features of the devices and network technologies to which their attacks are directed. Organizations should rethink their strategies to better protect against cyber risks and learn how to better manage them.

One of the first important steps is to treat cyber security as a science and be as scrupulous about the core of your infrastructure, which, in turn, requires high speed and network connectivity of cyber space for effective protection.

The use of a platform-based approach to security, micro- and macro-segmentation, machine learning and automation technologies as building blocks of artificial intelligence opens up tremendous opportunities for effectively countering cybercriminals.

## CYBERCRIME AND CYBER RISKS

**B. Əzizov<sup>1</sup>, E. Həsənov<sup>2</sup>, A. Paşayev<sup>1</sup>**

<sup>1</sup>Azərbaycan Universiteti, Bakı, Azərbaycan

<sup>2</sup>Azərbaycan Respublikası Prezidenti yanında Dövlət İdarəçilik Akademiyası  
e-mail: [bahram.azizov@au.edu.az](mailto:bahram.azizov@au.edu.az), [elgafgas@yahoo.com](mailto:elgafgas@yahoo.com), [asif.pashayev@au.edu.az](mailto:asif.pashayev@au.edu.az)

First, let's present the statistics of cybercrime for this year only.

May 2021 A British man was detained in Spain in the case of hacking politicians on Twitter.

June 2021. Fraudsters intensify in connection with new payments for schoolchildren

July 2021. Hackers stole \$ 1 billion in cryptocurrency in a year

July 2021. By "code" of the case: the number of cyberattacks on critical infrastructure of the Russian Federation increased by 150%

July 2021. Biden announced a meeting of representatives of the United States and the Russian Federation on cybersecurity

What are the risks of a delay in the transition to domestic software and hardware.

### **Network maturation**

In order to adequately compete in foreign sales markets, for example, in the production of household appliances, automotive, mechanical engineering, we need to learn how to create a product that outstrips imported counterparts in its characteristics, - says Vladislav Ozorin.

However, in most cases, attacks are not aimed at disabling equipment or implementing accidents: for the most part, they are reconnaissance, the deepest possible consolidation and long-term presence in the infrastructure of attacked objects, said Dmitry Darensky, head of industrial cybersecurity practice at Positive Technologies.

### **World experts gave tips on communicating with the scammers "of technical support"**

You need to initiate communication with technical support services yourself, and it is better to ignore calls from unknown numbers. Information security experts spoke about the rules of how not to become a victim of scammers who pretend to be IT specialists.

“In order not to fall for the bait of intruders, always remember one important rule: communication with technical support must be initiated by you. There are exceptions, but they relate to the internal IT departments of the company, "said Olga Zinenko, senior analyst at Positive Technologies, in an interview with RIA Novosti.

The expert clarified: in order to check that the call is desirable, it is necessary to call the number from the company's phone book.

### **World Bank warns banks of a new scheme to steal company money through API applications**

What is an API? The Application Programming Interface (API), or application programming interface, is a set of tools that allows one program to work with another. The API provides that programs can run on different computers as well. In this case, you need to organize the API so that the software can request each other's functions over the network.

### **Development and protection of RB systems**

Banks began to focus on the development of their RBS systems, despite the fact that many of their offices and branches during the pandemic continued their work in a limited manner. This trend can be seen from the frequency of updates of the respective applications.

### **Varonis: Bank employee has access to an average of 11 million confidential files**

Varonis, one of the innovators in the global security and data analytics market, has released the fourth annual 2021 Financial Data Risk Report, which outlined the most pressing issues related to the security of corporate data.

### **Information security priorities of banks in 2021**

By the end of 2020, Tadviseer interviewed domestic experts in the field of information security and learned from them how the needs of their clients from the banking sector have changed. Building a secure "remote control", developing and protecting RBS systems, meeting the requirements of

legislation in the field of information security are the key priorities of banks in the field of information security, which experts are talking about in 2020.

«**Remote control**» - a function that gives the user the ability to connect to a computer using another device via the Internet from almost anywhere. The user works with files and programs in the same way as if he was near this computer.

### **Between Scylla and Charybdis"**

That is, the phraseological unit to be between Scylla and Charybdis means to be between two dangers. The essence of such a situation is better reflected by the expressions “between two fires” or “between a rock and a hard place”, “out of the fire into the fire”.

**Keywords:** cyber attacks, hacking of banking and financial systems, cyber risks associated with critical infrastructure, network ransomwares, penetration of RBS systems, remote control, vendor, back office

### **References**

1. <https://www.itweek.ru/security/article/detail.php?ID=179029>
2. <https://iz.ru/tag/kiberprestupnost>
3. <https://www.websitehostingrating.com/ru/cybersecurity-statistics-facts/>
4. <https://www.investopedia.com/articles/personal-finance/012117/cyber-attacks-and-bank-failures-risks-you-should-know.asp>
5. <https://www.globalbankingandfinance.com/financial-sector-cyber-attacks-the-ever-evolving-threat/>
6. <https://www.bai.org/banking-strategies/article-detail/the-top-five-cyber-threats-for-banks-and-how-to-meet-them/>
7. <https://www.stoodnt.com/blog/cybersecurity-in-banking-financial-services/>
8. <https://www.afr.com/companies/financial-services/cyber-is-the-biggest-risk-in-banking-today-20210330-p57f5n>

### **Kiber cinayət və kiber risklər**

Elektron hökumətin həyatında müasir dünyanın aktual problemlərindən biri də kiber cinayətlərdir, yəni müxtəlif kiber cinayətkar qrupları tərəfindən qlobal maliyyə sistemində edilən kiber hücumlardır. Bu çərçivədə kiber risklər mühüm rol oynayır. Avropa və Asiyadakı bir çox vacib infrastruktur, hakerlərin kiberhücumlarından əziyyət çəkir və bu baxımdan uzaqdan idarəetmə işi çox vacibdir.

Bu diuistant idarəetmədir, yəni obyekt hərəkət edərsə, xeyli məsafədə və ya aqressiv vəziyyətdə yerləşsə belə, birbaşa siqnal ötürülməsinin mümkünsüzlüyü səbəbindən bir idarəetmə hərəkətinin (siqnalının) operatorndan məsafədə yerləşən idarəetmə obyektinə ötürülməsi deməkdir.

Maliyyə qurumları həmişə hakerlər üçün cazibədar hədəflər olub. Buna görə, hücumlara qarşı qorunmanın gücləndirilməsi və bütün şəbəkələrdə kompüterlər üzərində nəzarətin yaradılması İnternet bankçılıq sistemində ilkin və ən vacib vəzifədir.

## **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПО ВОПРОСАМ РЕГУЛИРОВАНИЯ ТРАНСПОРТНЫХ ПОТОКОВ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ**

**С. Багирова, О. Мухтарова**

Академия Управления при Президенте Азербайджанской Республики,

Кафедра Управление интеллектуальными системами

e-mail: [sofnene@bk.ru](mailto:sofnene@bk.ru), [ovmukhtarova@mail.ru](mailto:ovmukhtarova@mail.ru)

Управление жизнью современного города является достаточно сложной задачей для городских властей. Совершенно очевидно, что определяющим направлением в этом смысле стала работа по информатизации всех сфер практической деятельности, позволяющая принимать эффективные решения по оптимизации среды обитания человека. Поэтому учёные активно разрабатывают и внедряют высокотехнологичные решения, которые можно объединить названием «Умный город». С этой точки зрения интеллектуальный транспорт - основа современного умного города. По сути интеллектуальная транспортная система (ИТС) - это механизм, который включает в себя движение, чтобы город работал в режиме нон-стоп. Естественно, транспортная система умного города модифицируется: изменяются средства передвижения, появляется возможность автоматически регулировать транспортные потоки с целью предотвращения образования пробок, а водителям - выбирать маршруты, избегая загруженных дорог. Вместе с этим в составе ИТС выделяется автоматизированная система транспортной информации (АСТИ) для сбора любого рода информации о дорожном движении, которая может использоваться не только в рамках ИТС, но и вообще в любых системах любого сегмента умного города [2]. Наиболее важным для этих целей является матрица корреспонденций (модель для описания оценки динамики изменения транспортных потоков). Поэтому вопрос информационной безопасности стоит здесь крайне остро; зависимость такова, что любой сбой в системе может привести к прекращению нормальной деятельности любого звена ИТС. Рост целевых атак с использованием различных элементов становятся вызовами для информационной безопасности объектов ИТС и игнорировать серьезность данного тренда нельзя. Нужна система управления безопасностью.

Система должна включить интегрированную консолидацию и корреляцию происходящего с технологий.

В Азербайджане внедряется Интеллектуальная система управления транспортом последующей обработкой, которая является залогом успеха в создании Транспорт Смарт Сити и самым перспективным инструментом проектов «Smart Siti» [1,3].

За последние годы Республика Азербайджан прилагает большие усилия для внедрения интеллектуальной и эффективной городской системы за счет современных технологий, которая регулирует многие транспортные проблемы. Распоряжением Президента Азербайджанской Республики от 27 февраля 2020 г утверждён «Национальный план действий

по поощрению открытого правительства на 2020-2022 годы». В Баку запущен пилотный проект «Умный город». Последние годы между Южной Кореей и Азербайджаном было подписано несколько проектов в транспортной сфере. В рамках проекта в первую очередь создана система управления пассажирскими автобусами. В результате внедрения этой системы отрегулировано маршрутное движение, стал возможен контроль над графиком их движения. В рамках системы стал возможен в ходе чрезвычайных ситуаций сбор информации об авариях (ДТП, терактах и др.) на дорогах, путепроводах, стоянках и остановках, а также информирование об этом соответствующих органов.

Другая устанавливаемая система называется «Система сбора информации о транспорте», которая будет осуществлять сбор информации на серверы Интеллектуальной транспортной системы посредством видеокамер, микроволновых определителей и др.

Третья система называется «Система передачи данных и поручений по регуляции транспорта». Система призвана информировать пользователей об общем положении посредством кабельного телевидения, интернета, мобильной связи, электронных табло, информационных табло на остановках, управлять парковкой и др. В рамках этой системы на остановках, при въезде в город и радиальных дорогах устанавливаются информационные табло. На последующих этапах предусмотрено внедрение системы оплаты посредством электронной карты. В рамках проекта на всех дорогах установлены приборы по электронно-оптическому наблюдению.

Функционирование модели «умной» транспортной системы нацелено на повышение безопасности дорожного движения и имеет возможность не только организовывать, направлять трафик, контролировать потоки движения, но и анализировать транспортные ситуации. Функционирование модели «умной» транспортной системы нацелено на многие транспортные ситуации.

В апреле 2021 года Президент Ильхам Алиев подписал распоряжение о подготовке концепции «Умный город».

**Ключевые слова:** транспортная система, безопасность интеллектуальной транспортной системы.

### Литература

1. Душкин Р. Интеллектуальные транспортные системы. ДМК. 2020, 283 с.
2. Иванов Ф. Интеллектуальные транспортные системы. Белорусская наука. 2014 г, 216 с.
1. Шатунов Е. Цифровизация в сфере транспортной безопасности: проблемы и перспективы. Журнал: Транспортная безопасность и технологии, 2020, N 4.

## Information security on the regulation of traffic flows: problems and prospects

The paper deals with the problems of the functioning of the city's transport system. The importance of information security of an intelligent transport system is shown. The problems and prospects of the "Smart City" project in Azerbaijan are described.

## MÜASİR ƏLAQƏLİ VERİLƏNLƏR BAZASI İDARƏETMƏ SİSTEMLƏRİNDƏ İNFORMASIYA TƏHLÜKƏSİZLİYİ

**N.D. Cəfərov<sup>1</sup>, Z.Y. Qasımova<sup>2</sup>**

<sup>1</sup>Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

<sup>2</sup>Azərbaycan Memarlıq və İnşaat Universiteti, Bakı, Azərbaycan

e-mail: [nizami\\_cd@mail.ru](mailto:nizami_cd@mail.ru), [zemfiraqasimova@mail.com](mailto:zemfiraqasimova@mail.com)

Müasir şəraitdə istənilən fəaliyyət sahəsi geniş insan cəmiyyəti tərəfindən həyata keçirilən böyük miqdarda informasiyanın emalı ilə əlaqədardır. Məlumatların icazəsiz müraciətdən qorunması hər hansı bir informasiya sisteminin layihələndirilməsində prioritet vəzifələrdən biridir. İnformasiyanın əhəmiyyətinin son vaxtlar artması, məlumatların məxfiliyinə yüksək tələblər qoymuşdur [1,2,5]. Verilənlər bazası idarəetmə sistemləri, xüsusən də relyasiyalı (əlaqəli) VBİS - lər bu sahədə dominant vasitəyə çevrilmişdir. İnformasiya təhlükəsizliyinin üç əsas aspekti - məxfilik, tamlıq və əlçatanlıq VBİS-lər üçün vacibdir. Bu məqalənin mövzusu bunlardan birincisinin-informasiyaya icazəsiz girişdən mühafizə vasitələrinə həsr olunub.

Təhlükəsizlik siyasəti verilənlər administratoru tərəfindən müəyyən edilir. Lakin, məlumatların qorunması həlləri yalnız VBİS çərçivəsində məhdudlaşdırılmamalıdır. Məlumatların mütləq qorunması praktiki olaraq həyata keçirilmir, buna görə də adətən informasiyanın nisbi mühafizəsi ilə kifayətlənirlər - ona icazəsiz daxil olmağın hər hansı nəticələrə səbəb olduğu müddət ərzində onu zəmanətli şəkildə qoruyurlar.

*İnformasiya təhlükəsizliyinə aid bəzi şərhlər:*

Məxfi məlumatlar (həssas məlumatlar- sensitive information) - qorunması tələb olunan məlumatlar.

Məlumat əldə etmək və ya informasiyaya çıxış (access to information) - məlumatla tanışlıq, onun işlənməsi (xüsusən də kopyalanması), dəyişdirilməsi, məhv edilməsi.

Giriş subyekti (access subject) - girişin məhdudlaşdırılması qaydaları ilə tənzimlənən bir şəxs və ya prosesdir

Giriş obyektı (access object), girişi idarəetmə qaydaları ilə tənzimlənən avtomatlaşdırılmış sistemin məlumat vahididir. VBİS -də giriş (nəzarət) obyektləri praktiki olaraq son məlumatları ehtiva edən hər şeydir: cədvəllər, təsvirlər, həmçinin daha kiçik məlumat elementləri: sütunlar və cədvəl sətirlər və hətta sətir sahələri (qiymətlər).

Girişin (müraciətin) məhdudlaşdırılması qaydaları (security policy) təhlükəsizlik siyasəti) - giriş obyektlərinə çıxış subyektlərinin hüquqlarını tənzimləyən qaydalar toplusu.

Məlumata icazəli (səlahiyyətli) giriş (authorized access to information) - girişə nəzarət qaydalarını pozmayan məlumatlara giriş.

İcazəsiz giriş (unauthorized access to information) - hesablama texnikası vasitələri və ya avtomatlaşdırılmış sistemlər tərəfindən verilən ştat vəsaitlərindən istifadə etməklə girişin məhdudlaşdırılma qaydalarını pozan informasiyaya çıxış.

Giriş identifikatoru (access identifier) bir obyektin və ya giriş mövzusunun unikal əlamətidir.

Eyniləşdirmə (identification) - obyektlərə və subyektlərə identifikatora giriş imkanı verilməsi və (və ya) təqdim olunan identifikatorun təyin edilmiş identifikatorların siyahısı ilə müqayisəsi.

Şəxsiyyət, giriş obyektlərinə və subyektlərinə bir identifikatorun verilməsi və (və ya) təqdim edilən identifikatorun təyin edilmiş identifikatorların siyahısı ilə müqayisəsidir.

Şifrə (password-parol) – subyektin identifikatoru, hansı ki, onun sirri sayılır.

Doğrulama (authentication) - subyektin təqdim etdiyi identifikatorun daxil olmasının yoxlanması, həqiqiliyin təsdiq edilməsi.

*Diskresion ( istəyə baağlı) mühafizə.* Müasir VBİS-lərdə diskresion mühafizə vasitələri kifayət qədər inkişaf etmişdir.

Diskresion girişin idarə edilməsi (discretionary access control) — adı çəkilən subyektlər və adı çəkilən obyektlər arasında girişin məhdudlaşdırılmasıdır. Müəyyən giriş hüququ olan subyekt bu hüququ istənilən başqa subyektə verə bilər.

Diskresion mühafizə çoxsəviyyəli məntiqi mühafizə hesab olunur. VBİS-də məntiqi mühafizə qorunan bir obyektə münasibətdə bir sıra imtiyazlar və ya rollardır. Məntiqi qoruma, cədvəlin (təsvirin) sahibliyini də əhatə edə bilər. Cədvəl sahibi bir sıra imtiyazları dəyişə bilər (genişləndirmək, çıxarmaq, girişini məhdudlaşdırmaq). Məntiqi qorunma məlumatları verilənlər bazası sistem cədvəllərində yerləşir və qorunan obyektlərdən (cədvəllərdən və ya təsvirlərdən) ayrılır.

Verilənlər bazası qeydiyyatdan keçmiş istifadəçilər haqqında məlumat sistem kataloqunda saxlanılır. Müasir VBİS-lər verilənlər bazası əlaqəli SQL-in ümumi sintaksisinə malik deyildir, çünki onların öz sintaksisi ISO standartından daha əvvəl inkişaf etmişdir. Lakin tez-tez belə bir əlaqələndirici ifadə CONNECT vasitəsilə yaradılır. Aşağıda müvafiq olaraq Oracle və IBM DB2 üçün bu ifadələrin yazılışlarının sintaksisi verilmişdir:

```
CONNECT [[<logon>] [as {SYSOPER / SYSDBA}]<istifadəçi / parol> [@verilənlər bazası]  
CONNECT TO <verilənlər_bazası> USER< istifadəçi> USING <parol>
```

Bu ifadədə atributların lazımi dəsti əks olunur. Verilənlər bazasının atributu formatı, bir qayda olaraq, VBİS istehsalçısı tərəfindən, eləcə də qeyri müəyyən sistem imtiyazları olan istifadəçi adı (Oracle vəziyyətində SYSDBA/SYSOPER) ilə müəyyən edilir.

Hər bir bazanın administratoru yaratdığı VB-nin mümkün istifadəçiləri dairəsinin yaradılması və bu istifadəçilərin səlahiyyətlərinin məhdudlaşdırılması ilə məşğul olur. Verilənlərin məhdudlaşdırıcı sərhədlər haqqında məlumatlar VB-nin sistem kataloqunda yerləşir. Aydındır ki, bu

məlumat icazəsiz giriş üçün istifadə edilə bilər və buna görə də qorunmalıdır. Bu məlumatların qorunması VBİS özü tərəfindən həyata keçirilir.

VBİS istifadəçini qeydiyyatdan keçirməyə və onun unikal identifikatoru haqqında məlumatları saxlamağa imkan verir. Məsələn, Oracle təhlükəsizlik alt sistemində bu aşağıdakı kimi ifadə olunur:

```
CREATE USER IDENTIFIED <istifadəçi> BY <parol>
```

IBM DB2 təhlükəsizlik alt sistemi əməliyyat sistemi istifadəçi identifikatorundan istifadə edə bilər, onun SQL sintaksisində CREATE USER təlimatına bənzər təlimatı yoxdur. Microsoft SQL Server həm verilənlər bazası, həm də əməliyyat sistemi identifikasiyasından istifadə edə bilər. Ancaq burada istehsalçıların seçdiyi identifikasiya üsullarının üstünlüklərini və çatışmazlıqlarını müzakirə etməyəcəyik - hamısı istifadəçilərin dəqiqliyini təyin etmək üçün düzgün sxemlər qurmağa imkan verir. İnformasiya sistemi daxilində əlavə identifikasiya vasitələrinin istifadəsi qadağan edilmir.

Xüsusilə, qeyd edilməlidir ki, saxlanılan prosedurları və interaktiv sorğuları yerinə yetirərkən bir sıra istifadəçi imtiyazları necə əldə edildiyindən (açıq şəkildə və ya rol vasitəsilə) asılı ola bilər. İstifadəçinin əldə etdiyi imtiyazların açıq şəkildə saxlanılan prosedurlarda istifadə olunduğu Oracle - da da həyata keçirilir. Əgər sizin istifadə etdiyiniz reallaşdırma bu cür xüsusiyyətə malikdirsə, istifadəçi qrupundakı imtiyazların dəyişməsinə əmr dəsti kimi və ya inzibati prosedur kimi (administratorun üstünlüklərindən asılı olaraq) həyata keçirmək lazımdır.

*İmtiyazların idarə edilməsi təlimatları* [1,3]:

- imtiyaz təyinatı:

```
GRANT <imtiyaz> [ON <obyekt> ] TO <subyekt> [WITH GRANT OPTION]
```

- imtiyazların ləğvi:

```
REVOKE <imtiyaz> [ON <obyekt>] FROM <subyekt>
```

- Əgər subyekt= istifadəçi olarsa, bu imtiyaz ona açıq şəkildə verilir. Əgər subyekt = rol olarsa, imtiyazları idarə etmək üçün aşağıdakılardan istifadə olunur:

```
GRANT ROLE <rolların_adı> [ON <obyekt>] TO <subyekt> [WITH GRANT OPTION]
```

```
REVOKE ROLE <rolların_adı> [ON <obyekt>] FROM <subyekt>
```

- Sistemin bütün istifadəçilərinə imtiyaz təyin edilməsi aşağıdakı kimi verilir:

```
GRANT <imtiyaz> [ON <obyekt>] TO PUBLIC
```

Bu halda, yaradılan hər yeni istifadəçi avtomatik olaraq bu imtiyazı alacaq. İmtiyazın ləğvi isə aşağıdakı kimi aparılır:

```
REVOKE <imtiyaz> [ON <obyekt>] FROM PUBLIC
```

- Nəzərə alın ki, IBM DB2 kimi bəzi reallaşmalar əməliyyat sistemində müəyyən edilmiş istifadəçi qruplarından istifadə edir. Buna görə də, bu VBİS-də rolların analoqlarını tətbiq etməyin xüsusiyyətlərinə diqqət yetirilməlidir. SQL-ifadəsində aşağıdakı reallaşmaların olmasını dəqiqləşdirmək lazımdır:

```
CREATE ROLE <rolların_adı>
```

```
DROP ROLE <rolların_adı>.
```

Cədvəllərə və təsvirlərə giriş idarə edərkən, VBİS-in həyata keçirilməsində bir sıra imtiyazlar istehsalçı tərəfindən müəyyən edilir.

Mandat (məcburi) mühafizəsi [3,5]. Mandat mühafizəsi vasitələri VBİS-in xüsusi (trusted) versiyaları ilə təmin edilir. Mandat girişin idarə edilməsi (mandatory access control)- subyektlərin məlumat obyektlərinə çıxışının obyektlərdə olan informasiyanın məxfiliyinin qeydinə əsaslanan və subyektlərin həmin məxfilik səviyyəsinə dair informasiyaya müraciət etmək üçün rəsmi razılıqda (icazədə) məhdudiyətdir.

Məcburi qorunma nədir? İxtiyari giriş nəzarətləri C təhlükəsizlik səviyyəsi üçün xarakterikdir. Bir qayda olaraq, kommersiya reallaşmalarının böyük əksəriyyəti üçün bu kifayətdir. Buna baxmayaraq, çox vacib bir vəzifə - məlumat ötürülməsini izləmə vəzifəsi həll edilmir. İxtiyar giriş nəzarəti səlahiyyətli bir istifadəçinin qanuni olaraq həssas məlumat əldə etməsinə və sonra digər icazəsiz istifadəçilərə təqdim etməsinə mane ola bilməz. Bunun niyə belə olduğunu anlamaq çətin deyil.

**Açar sözlər:** əlaqəli VBİS, məxfilik, mandat mühafizəsi, imtiyaz.

### Ədəbiyyat

1. Kərimov S.Q. İnformasiya sistemləri. Bakı: Elm, 2008, 676 s.
2. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı. 2009, 340 s.
3. Зрюмов, Е. А. Базы данных для инженеров: учебное пособие Изд-во АлтГТУ, 2010.
4. Базы данных. Проектирование, реализация и сопровождение. Теория и практика, Томас Коннолли, Вильямс, 2017, с. 700-760.
5. <http://www.iso27000.ru/chitalnyi-zai/bezopasnost-baz-dannyh/informacionnaya-bezopasnost-v-sovremennyh-sistemah-upravleniya-bazami-dannyh>

### Information security in modern related database management systems

The article provides a number of key factors of information security in modern related database management systems, some comments on information security, and is mainly devoted to the means of protection against unauthorized access to information. Also, the types of security and the syntax of the instructions that they implement in some DBMS are given.

## DÖVLƏTİN GÜC STRUKTURLARINDA İNFORMASIYA TƏHLÜKƏSİZLİYİNİN İDARƏ EDİLMƏSİ

(post müharibə dövründə informasiya təhlükəsizliyi planlanması, metodları və simulyasiyası)

**A.S. Dadaşov**

Azərbaycan Universiteti, Bakı, Azərbaycan

e-mail: [amilodas@gmail.com](mailto:amilodas@gmail.com)

Yeni reallıqların yaranmasını və bu reallıqlarla regionun ayaqlaşmasını təmin etməyə yönəlmiş tədbirlərin vacibliyini nəzərə alsaq ciddi nəaliyyətlər əldə etmiş, dövlətimizin güc strukturu olan müasir ordu quruculuğu modelində hərtərəfli yeni layihələrin sürətlə həyata keçirilməsinin şahidi olarıq. Belə ki, istər müharibə dövründə, istərsə də hazırkı müharibədən sonrakı dövrdə informasiya müharibəsinin (İM) qloballaşdığı zamanda hər birimizi narahat edən əsas sual budur: informasiya təhlükəsizliyi riskini minimuma endirmək üçün İM- mühitində güc strukturunda (bir hərbi təşkilat daxilində) məlumatların məxfiliyini, bütövlüyünü və mövcudluğunu necə təmin etmək olar?

Müharibənin bəzi prinsiplərini rəhbər tutaraq və düşmənin məlum hərəkət üsullarını nəzərə alaraq aşağıdakı planlama aparılmaqla bir üsulu nəzərdən keçirək.

İM-də planlaşdırma metodu aşağıdakıları müəyyən etməyə imkan verir:

- 1) baş verə biləcək İT yönəlmiş hücumun əsas üsulları;
- 2) hərbi təşkilatlarda tətbiq olunan nəzarətin əsas xətti;
- 3) hücumla görə tətbiq olunan təhlükəsizlik nəzarəti və effektiv qorunma təbirləri.

İT -nin hücum silahı kimi istifadə edilməsi, hazırkı dövrdə və post müharibə zamanı döyüş sahəsinin yeni bir ölçüsü olaraq kiberməkənin ortaya çıxması və İnformasiya müharibəsi mühitində məlumat üstünlüyünə nail olmaq üçün məlumatların vacibliyi səbəbiylə yüksək əhəmiyyət kəsb edir. Buna görə də informasiya təhlükəsizliyinə yeni yanaşmalar və hərbi təşkilatlarda təxirəsalınmaz planların hazırlanması vacib sayılmalıdır.

Şərhini verməyə çalışdığımız bu fəaliyyətə informasiya müharibəsində qurulmuş "İnformasiya müharibəsinin müdafiəsi planı" kimi baxmaq olar. Bu təsvir modeli forma baxımından, rəqibin mümkün hərəkət üsullarına (yəni onların hücum üsullarına) əsas diqqət yetirildiyini nəzərə alaraq, hərbi təşkilatlar üçün yeni informasiya təhlükəsizliyi planlaşdırma metodunun hazırlanmasının *aktuallığını* əsaslandırır.

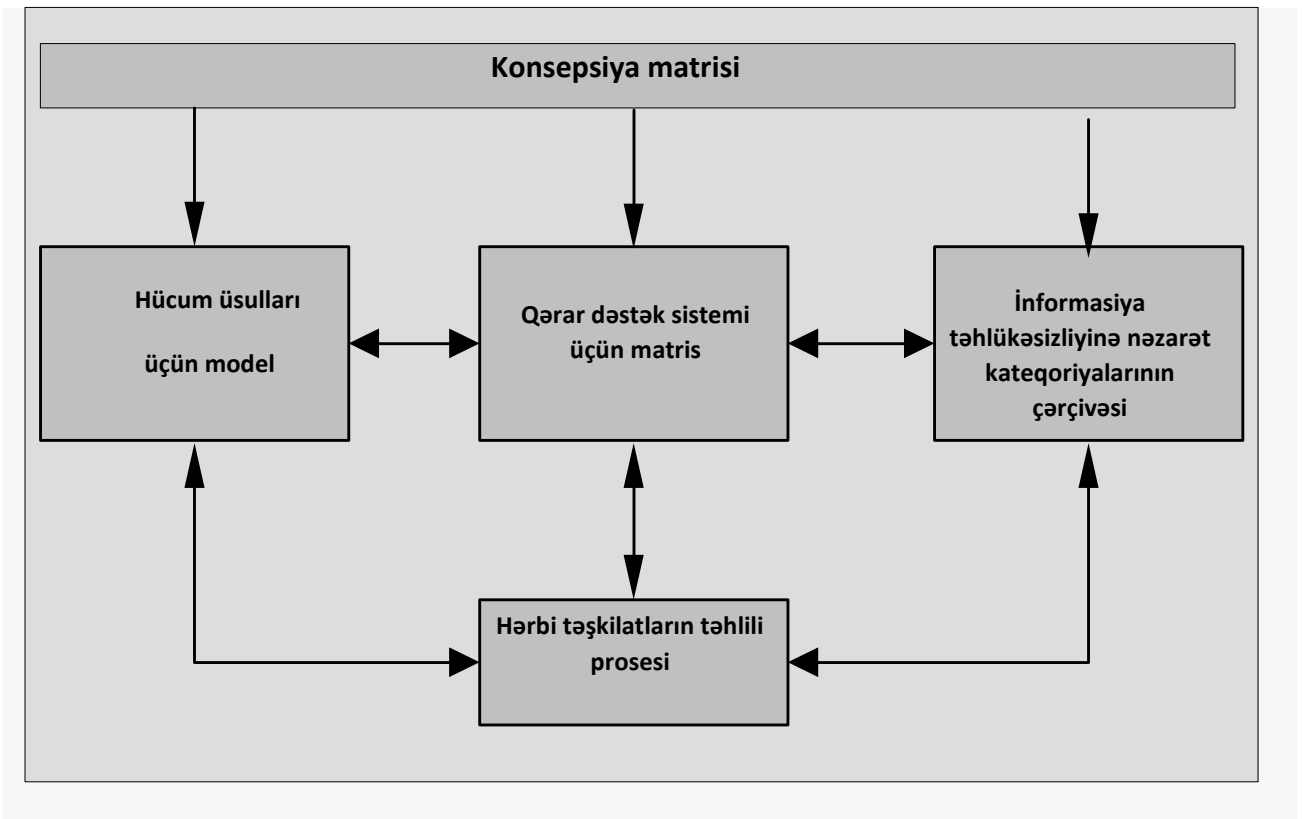
İnformasiyanın əsas obyektini olan məlumatların təhlükəsizliyinin təmini baxımından planlaşdırılan və tətbiqini təklif edəcəyimiz planlaşdırma metodunu cari və gələcək zamanda icra ediləcəyini nəzərə almaqla tətbiq etmək üçün, İM-in cari məzmununun təhlili və Xüsusi işçi qrup üçün əsas tədqiqat metodu kimi istifadə olunan şərhlər və analizatorlar tərəfindən keyfiyyətli, yüksək bilik və bacarıqla araşdırılmasına təlimatlar tərtib etdik.

Təklif olunan planlaşdırma metodu aşağıdakılara əsaslanır:

1. Fiziki, İnsan və Texnoloji infrastruktur hücumlarının vektorları;

2. informasiya təhlükəsizliyinə nəzarət kateqoriyalarının çərçivəsi (təhlükəsizlik ölçüləri: Təşkilati, Fiziki və Ətraf Mühit, İnsan və Texnoloji);
3. Rəqibin hücum vektorları tərəfindən dəstəklənən qərar dəstəyi matrisi və informasiya təhlükəsizliyi nəzarətinin mümkün təsirləri (Qarşısının Alınması, Çəkilməməsi, Çıxması, Qurtarılması və Reaksiya verilməsi);
4. Təşkilatların təhlili prosesi.

Düşmənin ehtimal olunan kiber təhlükəsi ilə qarşılaşan zaman, dost qüvvələrin missiyasını nəzərə alaraq, təklif olunan planlaşdırma üsulu, hücum üsulları modelinin və informasiya təhlükəsizliyi kateqoriyalarına istinad edərək qərarın dəstəklənməsinə imkan verir. Burada mütəxəssislərin təcrübəsini unutmadan tətbiq ediləcək qərar ən yaxşı təhlükəsizliyə nəzarət dəstini seçməkdir.



Şəkil 1: Informasiya təhlükəsizliyinin planlaşdırma metodunun əsas komponentləri modeli

Nəticələr.

1. Təklif olunan üsul, müəyyən bir hücum üsuluna qarşı tətbiq ediləcək təhlükəsizlik nəzarətlərinin ən yaxşı birləşməsini müəyyənləşdirməyə kömək edir, informasiya səhnəsində əldə edilən dərslər də (xarici informasiya hücumlarından əldə edilən təcrübələr) nəzərə alınmaqla istifadə olunur. Keçmiş hallara uğurla tətbiq olunan seçim və bərpa həllərinə əsaslanır. Bu, hərbi qərar verənlərə informasiya təhlükəsizliyinə uyğunlaşdırılmış müharibə prinsiplərini (Güc İqtisadiyyatı, Manevr, Komandanlıq Birliyi, Təhlükəsizlik və Hücum) nəzərdən keçirərkən rəqibin hərəkət üsullarına diqqət yetirərək plan qurmağa imkan verir.

2. Gələcəkdə bu planlama işinin əsas nəticələrini aşağıdakı kimi ümumiləşdirmək olar:
  1. məlumatlara hücum üsulları modeli;
  2. informasiya təhlükəsizliyinə nəzarət kateqoriyaları;
  3. hərbi təşkilat daxilində tətbiq ediləcək informasiya təhlükəsizliyi nəzarətlərinin seçilməsini planlaşdırmaq üçün qərar dəstək sistemi üçün bir şablon və ya cədvəl;
  4. hərbi təşkilatların təcrübələrindən əldə edilən dərslərin həyata keçirməsi və davamlı təkmilləşdirilməsinə imkan verən məlumat təhlükəsizliyi bazsında planlaşdırılması.

Planlaşdırma metodunun gələcəkdə tətbiqi üçün kritik əhəmiyyət kəsb edən bu işdə əhatə olunmayan bir məsələ var ki, bu da cari vəziyyətə (baş verə biləcək İT-təhlükəyə) əsaslanan avtomatlaşdırılmış qərar dəstək sisteminin inkişafıdır .

İnformasiya müharibəsi mühitində hərbi təşkilatlarda informasiya təhlükəsizliyi, informasiya üstünlüyünə töhfə vermək üçün informasiya təhlükəsizliyinin əsas xüsusiyyətlərini təmin etmək məqsədi daşıyır.

### **Ədəbiyyat**

1. Abbasov Ə.M., Qasımov V.Ə., Quliyev R.Ə. İntellektual informasiya sistemlərinə qərar qəbul etmə üsulları. Dərslük. Bakı, “İqtisad universiteti” nəşriyyatı, 2003, 256 s.
2. Rüstəmov Q.Ə., Riyazi modelləşdirmə və Simulyasiya. Dərs vəsaiti. Bakı, AzTU, 2015, 120 s.
3. AAP-6. (2009). NATO Glossary of Terms and Definitions.
4. Alberts D., Garstka J., Hayes R., Signori D. (2001). Understanding Information Age Warfare, CCRP Publication Series, Washington, United States of America.
5. Chesla A. (2004). Information Security: A Defensive Battle. Information Security Journal: A Global Perspective, 12(6), 24-32.
6. ISO/IEC13335-1. (2004). Information technology- Security techniques-Management of information and communications technology security. Part 1: Concepts and models for information and communication technology security management.
7. ISO/IEC27001. (2005). Information technology – Security techniques – Information Security Management Systems - Requirements.

## ПРОДОЛЬНОЕ РАСПРЕДЕЛЕНИЕ ИНТЕНСИВНОСТИ ПОЛЯ КРУГЛОЙ СФОКУСИРОВАННОЙ АПЕРТУРЫ

**В.В. Должиков, В.П. Давыдова**

Харьковский национальный университет радиоэлектроники, Харьков, Украина

e-mail: [vladimir.dolzhikov@nure.ua](mailto:vladimir.dolzhikov@nure.ua)

Одной из характерных особенностей современной теории антенн является резко возросший интерес к изучению структуры поля излучения антенн в их зоне Френеля. Это обусловлено широким внедрением в практику систем, в основе которых лежит взаимодействие поля излучения антенны с объектом, находящимся в ее зоне Френеля. К ним относятся системы ближней радиосвязи и радиолокации; беспроводной передачи энергии; антенны с синтезированной апертурой; системы медицинской диагностики и гипертермии, использующие сфокусированные антенны для получения высокого пространственного разрешения; системы беспроводной зарядки мобильных устройств; системы RFID; беспроводная персональная связь, передача данных и питания на имплантаты в биологическую среду и т.д. Второй причиной повышенного интереса к зоне Френеля является резкое обострение проблемы ЭМС из-за быстрого роста числа радиоэлектронных средств (РЭС), повышения мощности излучения и чувствительности их приемных устройств, существенно возросших требований к обеспечению нормального функционирования близкорасположенных друг к другу РЭС, что характерно, например, для современных морских судов и летательных аппаратов. К проблеме ЭМС примыкает и важнейшая задача защиты биологических объектов от облучения электромагнитным полем, актуальность которой также заметно усилилась в связи с увеличением числа и мощностей излучения РЭС. Третья причина – это рост электрических размеров современных антенн, в частности из-за интенсивного освоения все более коротких волн, приводящий к удалению границы дальней зоны, то есть к увеличению протяженности зоны Френеля и, как следствие, к увеличению числа объектов, попадающих в эту зону.

В литературе опубликовано уже немало работ, посвященных исследованию особенностей поля антенн в зоне Френеля [1-3]. Однако в большинстве из них приводятся результаты численных расчетов, что не в полной мере удовлетворяет потребности практики.

В работе получены аналитические выражения для основных параметров, характеризующих продольное распределение поля антенны в виде круглой апертуры с равномерным и спадающим амплитудными распределениями, сфокусированной как зону Френеля, так и в дальнюю зону.

Рассматривается плоская синфазная круглая апертура радиуса  $R$  с началом координат,



Получены аналитические выражения для расчета основных параметров, при различных расстояниях фокусировки – как в зоне Френеля, так и в дальней зоне. Приводятся графические зависимости параметров от расстояния фокусировки и высоты пьедестала, построенные по полученным приближенным формулам и по результатам численных расчетов. Сравнение с результатами численных расчетов показало, что полученные приближенные соотношения позволяют определить значения упомянутых параметров для любых значений расстояния фокусировки, лежащих как в зоне Френеля, так и в дальней зоне с погрешностью, не превышающей в худшем случае 7%. Результаты работы будут полезны при расчете поля апертурных антенн в виде круглой сфокусированной апертуры, а также сфокусированных антенных решеток, работающих в зоне Френеля.

**Ключевые слова:** зона Френеля, сфокусированные антенны, усиление фокусировки, глубина фокусировки, смещение максимума интенсивности.

### Литература

1. Hansen R.C. Microwave Scanning Antennas, Volume 1: Apertures, New York, Academic Press, 1964.
2. Hansen R.C. Focal Region Characteristics of Focused Array Antennas, IEEE Transactions on Antennas and Propagation, AP-33, 12, December 1985, pp.1328-1337.
3. Wang W., Gao H., Wu Y., Liu Y. Impact on Focal Parameters for Near-field-focused Aperture Antennas, Int J Numer Model., 2018, e2510, pp.1-13. <https://doi.org/10.1002/jnm.2510>.
4. Silver S. Microwave Antenna Theory and Design. McGraw-Yill, New York, 1949, 312 p.

### Longitudinal distribution of the field intensity of a circular aperture

In this paper, analytical expressions are obtained for calculating the main parameters characterizing the longitudinal distribution of the circular focused aperture field intensity with a relatively large diameter ( $2R/\lambda \geq 10$ ): the displacement of the intensity maximum relative to the focal point, focusing gain and depth of focus. Cases of uniform and decreasing amplitude distributions of the excitation field are considered. The found approximate relations make it possible to determine the values of the above parameters for any values of the longitudinal coordinate of the focal point, lying both in the Fresnel zone and in the far zone. Comparison with numerical calculations showed that the error in the obtained parameter values does not exceed 5%.

## АВТОМАТИЗАЦИЯ ОБРАБОТКИ ИНФОРМАЦИИ МЕТОДЫ ОТСЛЕЖИВАНИЯ ТРАНЗАКЦИЙ В БЛОКЧЕЙН-СИСТЕМАХ

**В.В. Дубина**

Харьковский национальный университет радиозлектроники, Харьков, Украина

e-mail: [valeriia.dubina@nure.ua](mailto:valeriia.dubina@nure.ua)

Современные информационные технологии прочно закрепились во многих областях человеческой деятельности. Сегодня множество аспектов нашей жизни хранится и отслеживается в базах данных, что делает взаимодействие с другими людьми и обращение к различным услугам более эффективным. Но, как следствие, наши персональные данные теперь все чаще попадают под угрозу несанкционированной обработки [2]. Именно поэтому вопрос обеспечения безопасности данных в информационной среде на сегодняшний день является чрезвычайно актуальным. Для этого необходимо постоянно совершенствовать существующие и исследовать новые идеи по внедрению механизмов защиты в сетях. Получившие широкое распространение технологии распределенного реестра, в том числе блокчейн, могут быть эффективно использованы для борьбы с возрастающим количеством угроз.

Блокчейн представляет собой базу данных в виде непрерывной цепочки блоков, содержащий информацию обо всех совершенных в системе транзакциях. Данные о переводах не зашифрованы, доступны всем пользователям и каждый может просмотреть их в любой момент времени. Это одна из главных свойств технологии – прозрачность. Кроме этого ей присущи: неизменность записанных данных и децентрализация, за счет которой информация хранится не на одном устройстве, а принадлежит всем пользователям сети. Применение технологии блокчейн позволяет автоматизировать транзакции в сети и повысить эффективность ее функционирования, не привлекая при этом третьей стороны. Данная система продолжает развиваться и становится все более популярной, все тщательнее исследуются ее свойства и возможности применения [1]. В качестве инструмента для управления данными и их безопасной обработки, блокчейн сегодня является наилучшим решением. Технология способна оказать огромное влияние в развитии многих сфер, что позволит достичь автоматизации различных процессов и услуг, и как следствие - значительной экономии ресурсов.

Одними из главных на сегодняшний день остается вопрос обеспечения надежного хранения информации и возможности отслеживания подозрительной активности и своевременной защиты пользователей в сети. Несмотря на большое количество преимуществ технологии блокчейн, проблема проведения незаконных операций является актуальной. Нарушители злоупотребляют криптовалютой для проведения различных финансовых

махинаций, торговли в Darkweb, а пользователи децентрализованных сетей сталкиваются с попытками несанкционированного доступа к персональным данным [4].

Таким образом, целями исследования определено:

- изучить принципы обработки данных в блокчейн сетях;
- проанализировать современные инструменты отслеживания транзакций и анализа блокчейн сетей и их возможности;
- определить перспективы развития технологии и рекомендации по ее применению.

На основе последних отчетов Internet Organised Crime Threat Assessment (ИОСТА) именно вымогатели в сетях остаются одной из наиболее актуальных угроз, как для государственных, так и для частных организаций в Европе и за ее пределами [4]. В связи с этим появилась необходимость в контроле за действиями в блокчейн сетях и усовершенствовании всех существующих в настоящее время аспектов киберзащиты. Из-за этого начал расти спрос на инструменты анализа сети с возможностью отслеживания истории транзакций, осуществленных пользователями. На данный момент можно выбирать среди коммерческих услуг и инструментов с открытым кодом.

На примере современных механизмов отслеживания транзакций рассмотрены методы анализа системы, выявления угроз и их устранения. Исследованы такие средства анализа блокчейн сетей, как: Blockchain Explorer, CryptoHound, Glassnode. Использование подобных инструментов с открытым кодом является удобным за счет их доступности, однако некоторые из них требуют большого количества времени для анализа отдельных участков сети и транзакций, поэтому проводить такую проверку вручную становится неэффективным. Тогда на помощь исследователям приходят именно коммерческие сервисы.

Также проведено исследование блокчейн транзакций с помощью платформы GraphSense. Это еще один инструмент с открытым программным кодом, разработанный австрийскими исследователями [3]. Система проводит анализ транзакций в сети в реальном времени, чтобы получить представление об их функциях и подробную статистику. Особое внимание уделяется выявлению так называемых аномалий, то есть идентификации тех транзакций, которые отклоняются от стандартных структур. Это позволяет выявлять и отслеживать потенциально вредоносные действия на ранних стадиях. Предоставляется возможность работать с такими криптовалютами, как: Bitcoin, Bitcoin Cash, Litecoin, Zcash и Ethereum. В итоге можно отметить, что данный инструмент является удобным в использовании, при этом он предлагает большое количество возможностей с высоким уровнем эффективности, позволяя его пользователям получать статистику по запросу в виде графиков и таблиц за достаточно короткое время. В перспективе, продолжая совершенствование платформы и обеспечивая растущий набор ее функций, GraphSense может стать хорошим инструментом для предприятий и организаций, занимающихся криптоактивами, для научных исследований, а также возможным решением возникающих проблем по соблюдению и регулированию безопасных взаимодействий в блокчейн сетях.

Результаты данной работы прежде всего полезны пользователям блокчейн-сетей, разработчикам приложений, основанных на технологии блокчейн, специалистам в сфере кибербезопасности.

### Литература

1. Свон М. Блокчейн: Схема новой экономики. Москва, 2017, 240 с.
2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: «Наука и техника», 2004, 384 с.
3. Haslhofer B. et al. GraphSense: A General-Purpose Cryptoasset Analytics Platform. 2021. 16 p. URL: <https://arxiv.org/abs/2102.13613v1>
4. Internet Organized Crime Threat Assessment (IOCTA) 2020. Europol: веб-сайт. URL: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020>

### **Automation of information processing methods for tracking transactions in blockchain systems**

The work is devoted to the research of the principles of data processing in the Blockchain technology. Particular attention is paid to the issue of ensuring reliable storage of information and the ability to track suspicious activity in the network. Due to the fact that all transfers are sent in an open form and everyone can view them at any time, there is a threat of dishonest actions of participants and attacks on the system. Methods of network analysis, detection and elimination of threats are proposed using the example of modern tools for tracking transactions as a way to solve existing problems associated with various manipulations in the network.

### **DBSCAN ALQORİTMİNİN TƏTBİQİ İLƏ BIG DATA - DA KÜY VERİLƏNLƏRİN AŞKARLANMASI**

#### **A. Fəxrəddinqızı**

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

e-mail: [aygul.fexreddin@gmail.com](mailto:aygul.fexreddin@gmail.com)

İnformasiya Kommunikasiya Texnologiyalarının (İKT) inkişafı rəqəmsal informasiyanın sürətli artımına və nəticədə külli miqdarda böyük ölçülü verilənlər konsepsiyasının meydana gəlməsinə səbəb olmuşdur. Bu səbəbdən böyük ölçülü verilənlər və onun mahiyyətini, analiz texnologiyalarının imkanlarını, təhlükəsizlik məsələlərini tədqiq etməyə ehtiyac yaranmışdır. Məqalədə böyük ölçülü verilənlərin analizindəki çatışmazlıqları aradan qaldırmaq üçün sıxlığa əsaslanan DBSCAN klasterləşdirmə alqoritmi analiz edilmişdir. Bu alqoritmin əsas xüsusiyyətlərindən biri böyük ölçülü verilənlərdə küy nöqtələri aşkar etməklə effektiv klasterin

yaradılmasından ibarətdir. Alqoritmin tətbiqi zamanı küy nöqtələri ehtiva edən real verilənlər bazalarından istifadə edilmişdir. Nizamlanmış rand indeksi, homogenlik, Davies-Bouldin indeksi və s. kimi qiymətləndirmə metrikalarının tətbiqi nəticələrinə əsasən, DBSCAN alqoritmi digər klasterləşdirmə alqoritmlərinə nisbətən küy nöqtələri aşkar etməkdə daha effektiv nəticə göstərmişdir.

### **Giriş**

XXI əsrin əvvəllərindən başlayaraq texnika və texnologiyalar – kompüterlər, mobil telefonlar, İnternet, sensor şəbəkələri, yerin süni peykləri, kosmik teleskoplar, bulud hesablamaları və s. vasitəsi ilə generasiya olunan rəqəmsal verilənlər hər il həndəsi silsilə ilə artmaqdadır. Nəticədə verilənlərin emalı, idarə olunması, saxlanması və istifadəsində yeni eranı əks etdirən “böyük ölçülü verilənlər” (ing. big data) konsepsiyası meydana çıxmışdır.

Big data fenomenal hadisə olaraq cəmiyyətin iqtisadi inkişafında inqilabi dəyişikliklərlə yanaşı, elmi ictimaiyyəti bir sıra problemlərlə üz-üzə qoymuş, yeni tədqiqat paradigması yaratmışdır. Bu verilənlərin emalı üçün yeni texnologiyalardan istifadə etmək zərurəti yaranmışdır. Başqa sözlə, big data termini həcm və müxtəliflik baxımından mürəkkəb olan məlumatları ifadə edir, lakin onları ənənəvi emal texnologiyaları vasitəsilə idarə etmək mümkün olmadığına görə əvvəlcədən təyin olunmuş real zaman rejimində yeni biliklərin əldə edilməsi çətinləşir. Bu da öz növbəsində verilənlərin məzmunundan asılı olaraq təhlükəsizlik baxımından müxtəlif problemlərə gətirib çıxara bilər [5]. Böyük ölçülü verilənlərin təhlükəsizliyini necə təmin etmək və gizliliyini qorumaq cari araşdırmalar mərhələsində ən aktual problemlərdən birinə çevrilmişdir. Həmçinin, məlumatların toplanması, saxlanması və istifadəsi zamanı fərdi məlumatların asanlıqla sızmasına və məlumatların klassifikasiyası zamanı çətinliklərə səbəb olur [1]. Klasterləşdirmə böyük ölçülü verilənlərin əsas təhlili üsullarından biridir. Xüsusilə də, klasterləşdirmənin əsas məqsədi verilənləri müəyyən xüsusiyyətlərə görə oxşar olduqları halda eyni qrupda təyin edərək, klasterlərə ayırmaqdır. Klasterlər fərqli ölçüdə, sıxlıqda və formada olduqda qrupların aşkarlanması problemi ortaya çıxır. Məqalədə DBSCAN klasterləşdirmə alqoritminin tətbiqi ilə eksperiment həyata keçirilir. Eksperimentin nəticələrinə əsasən müxtəlif qiymətləndirmə indeksləri vasitəsilə nəticələr qiymətləndirilir.

### **DBSCAN**

DBSCAN alqoritmi sabit radiuslu qonşuluqda yerləşən nöqtələrin sayını hesablayaraq sıxlığı qiymətləndirir və hər hansı iki nöqtə bir-birinin qonşuluğunda yerləşirsə, bu nöqtələri bir-birilə bağlı hesab edir. DBSCAN alqoritminin iki əsas parametri mövcuddur: *Eps* (Epsilon) - qonşuluqları təyin edən məsafə. İki nöqtə arasındakı məsafə  $\epsilon$ -dən az və ya bərabər olduqda qonşu hesab olunur. *MinPts* (Minimum Points) - klasteri təyin etmək üçün minimum məlumat nöqtələrinin sayı. Bu iki parametərə əsasən sıxlığa əsaslanan klasterləşdirmə alqoritmi üç fərqli nöqtələr tipinə ayrılır [2]:

- əsas nöqtələr (ing. *core points*), yəni sıx qonşuluqda yerləşən nöqtələr ( $|NEps(p)| \geq MinPts$ ); Qonşuluq radiusundakı *Eps* (Epsilon) ən azı *MinPts* (Minimum Points) nöqtəsindən ibarətdirsə, yəni qonşuluqdakı sıxlıq bəzi həddi keçməlidirsə, bu nöqtə *əsas nöqtə* adlanır.

- sərhəd nöqtələr (*ing. border points*), yəni hər hansı klasterə aid olan, ancaq sıx qonşuluqda yerləşməyən nöqtələr; bir nöqtə əsas nöqtədən əldə edilə biləndirsə və ətrafındakı sahədə *MinPts* nöqtəsindən az nöqtə varsa, bu nöqtə *sərhəd nöqtə* adlanır.

- küy nöqtələr (*ing. noise points*), yəni heç bir klasterə aid olmayan nöqtələr; əgər bir nöqtə əsas nöqtə deyilsə və hər hansı bir əsas nöqtədən əldə edilə bilən deyilsə, bu nöqtə *küy nöqtə* kimi qiymətləndirilir [4].

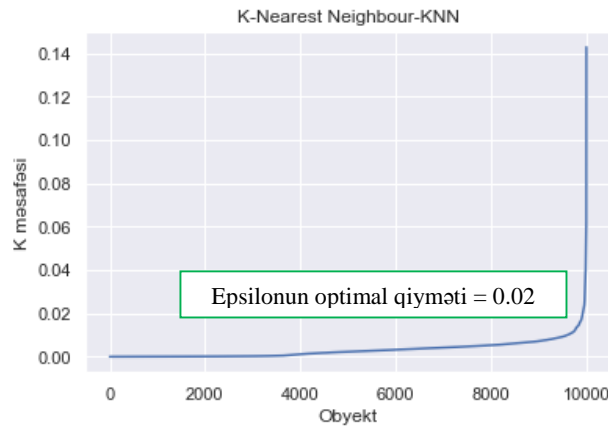
#### A. DBSCAN alqoritminin mərhələləri:

Yuxarıdakı anlayışlardan nəticə çıxararaq DBSCAN alqoritminin işləmə prosesini aşağıda kimi şərh edə bilərik [3]:

Alqoritm ixtiyari bir nöqtədən başlayır və qonşuluq məlumatları  $\varepsilon(Eps)$  parametrindən alınır. Bu nöqtə *MinPts* parametrinin  $\varepsilon$  qonşuluğunda yerləşirsə, klaster əmələ gətirir. Əks halda nöqtə küy nöqtə kimi işarələnir. Bu nöqtə sonradan fərqli bir nöqtənin  $\varepsilon$  qonşuluğunda yerləşə bilər və bununla da klasterin bir hissəsi ola bilər. Burada sıxlıq əldə edilə bilən və sıxlığa bağlı nöqtələr anlayışı vacibdir. Bir nöqtənin əsas nöqtə olduğu aşkar edilərsə,  $\varepsilon$  qonşuluğundakı nöqtələr də klaster hesab oluna bilər. Beləliklə,  $\varepsilon$  qonşuluğu içərisində tapılan bütün nöqtələr, əsas nöqtələdirsə, onda bu nöqtələr öz qonşuluğunda yerləşən nöqtələr ilə birlikdə əlavə olunurlar. Yuxarıdakı proses sıxlığa bağlı klaster tamamilə tapılana qədər davam edir. Proses yeni bir klasterin bir hissəsi ola bilər və ya küy nöqtələr kimi işarələnən yeni bir nöqtə ilə yenidən başlayır.

#### B. Eksperimentlər

Aşağıdakı eksperimentlərdə fərqli verilənlər bazası üçün ilkin klasterləşdirmə,  $k - NN$  metodu və DBSCAN alqoritminin tətbiqi ilə yekun qiymətləndirmə təsvir olunmuşdur.



Qeyd etmək lazımdır ki, qiymətləndirmə üçün istifadə edilmiş Davies-Bouldin indeksinin minimal, Bircinslik (Homogeneity) və Təmizlik (Purity) indeksinin isə maksimal qiyməti daha keyfiyyətli nəticəni ifadə edir. Cədvəl 1 - də sinifləndirilmiş verilənlər üçün əsasən Homogeneity indeksinə görə, sinifləndirilməmiş (ilk iki verilənlər bazası) verilənlərdə isə Davies-Bouldin indeksinə görə klasterlər yaradılır [6]. Əgər sinifləndirilmiş verilənlərdə Homogeneity və ya Purity indeksi bütün hallarda eynidirsə, onda burada da Davies-Bouldin indeksi nəzərə alınaraq, klaster yaradılır.

Cədvəl 1. Verilənlər bazasının və parametrlərin ətraflı təsviri qiyməti

| Verilənlər bazası               | Eps   | MinPts | Adjusted Rand index (ARI) | Silhouette score | Purity | Homogeneity | Davies-Bouldin index |
|---------------------------------|-------|--------|---------------------------|------------------|--------|-------------|----------------------|
| Churn<br>(10000 x 14)           | 0.01  | 10     | 0.019                     | -0.238           | 0.797  | 0.740       | 2.344                |
|                                 | 0.02  | 10     | -0.007                    | -0.311           | 0.796  | 0.860       | 5.759                |
|                                 | 0.02  | 8      | -0.006                    | -0.268           | 0.796  | 0.828       | 7.687                |
|                                 | 0.02  | 12     | -0.005                    | -0.278           | 0.796  | 0.816       | 6.753                |
| Online Shoppers<br>(12330 x 18) | 0.01  | 10     | -0.068                    | 0.578            | 0.855  | 0.961       | 1.043                |
|                                 | 0.01  | 8      | -0.068                    | 0.583            | 0.855  | 0.965       | 1.045                |
|                                 | 0.02  | 10     | -0.056                    | 0.787            | 0.855  | 0.967       | 1.412                |
|                                 | 0.009 | 10     | -0.072                    | 0.574            | 0.855  | 0.964       | 1.099                |
| Adult<br>(48842 x 15)           | 0.02  | 10     | 0.0                       | 0.631            | 1.0    | 1.0         | 0.988                |
|                                 | 0.03  | 10     | 0.0                       | 0.607            | 1.0    | 1.0         | 0.804                |
|                                 | 0.01  | 7      | 0.0                       | 0.580            | 1.0    | 1.0         | 1.411                |
|                                 | 0.01  | 12     | 0.0                       | 0.624            | 1.0    | 1.0         | 1.434                |
| Bank -marketing<br>(45211 x 17) | 0.02  | 12     | 0.011                     | 0.841            | 0.883  | 0.883       | 1.055                |
|                                 | 0.03  | 10     | 0.005                     | 0.834            | 0.883  | 0.941       | 1.208                |
|                                 | 0.01  | 10     | 0.025                     | 0.709            | 0.883  | 0.946       | 1.078                |
|                                 | 0.02  | 8      | 0.008                     | 0.709            | 0.883  | 0.816       | 1.904                |
| Diabetic<br>(101766 x 50)       | 0.02  | 12     | 0.0                       | 0.107            | 1.0    | 1.0         | 1.639                |
|                                 | 0.03  | 12     | 0.0                       | 0.311            | 1.0    | 1.0         | 0.995                |
|                                 | 0.02  | 14     | 0.0                       | 0.010            | 1.0    | 1.0         | 1.886                |
|                                 | 0.01  | 12     | 0.0                       | -0.503           | 1.0    | 1.0         | 1.586                |

**Nəticə.** Tədqiqat işində böyük ölçülü verilənlər konsepsiyası araşdırılmışdır, böyük ölçülü verilənlərin analizi üçün klasterləşdirmə alqoritmlərinin nəzəri cəhətdən müqayisəli analizi aparılmışdır. Böyük ölçülü verilənlərin analizi və küy (noise) nöqtələrin dəqiq aşkar edilməsi üçün sıxlığa əsaslanan DBSCAN alqoritmı tətbiq edilmiş və böyük ölçülü verilənlər üçün praktiki əhəmiyyəti müəyyən edilmişdir. DBSCAN alqoritminin qiymətləndirilməsində səmərəliliyin artırılması üçün müxtəlif metodlardan (Silhouette score, Adjusted Rand index, Purity index və Homogeneity index və s.) istifadə olunmuş və bu metodların nəticələrinə əsasən DBSCAN alqoritmı müxtəlif indekslərə görə yüksək nəticə vermişdir. Qeyd etdiyimiz kimi alqoritm əsas iki parametrlə (*Eps*, *MinPts*) seçilməsində həssas olduğuna baxmayaraq tədqiqat nəticəsində keyfiyyətli klasterlər əldə edilmişdir.

**Açar sözlər:** big data, sıxlığa əsaslanan klasterləşdirmə, DBSCAN alqoritmı.

### Ədəbiyyat

1. Alguliyev R.M., Imamverdiyev Y.N., Big data: big promises for information security, 2014 IEEE 8th International Conference on Application of Information and Communication Technologies, 2014, pp.1-4.

2. Clustering Algorithm with Noise. IEEE International Conference on Systems, Man, and Cybernetics, 2006.
3. Dharni C., Bnasal M., An improvement of DBSCAN Algorithm to analyze cluster for large datasets. 2013 IEEE International Conference in MOOC, Innovation and Technology in Education, 2013, pp.42-46.
4. Ester M., Kriegel H.P., Sander J., Xu X., A density-based algorithm for discovering clusters in large spatial databases with noise. ACM SIGKDD Conf. Knowl. Discovery Ad Data Mining, 1996, pp.226-231.
5. Fəxrəddinqızı A., Big data texnologiyalarında verilənlərin təhlükəsizliyinin əsas məsələləri. İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri, V respublika konfransı, 2019, s.226-228.
6. <https://archive.ics.uci.edu/ml/datasets.php>

### **Detection of noise points in big data with application of dbscan algorithm**

The development of information and communication technologies (ICT) has led to the rapid increase in digital information and the consequent emergence large amount of the concept of big data. Therefore, there is a need to study big data and its essence, the capabilities of analytics technologies, security issues. The article addresses the density-based clustering algorithm (DBSCAN) to overcome the shortcomings in the analysis of big data.

One of the main features of this algorithm is to create an effective cluster by detecting the noise points in big data. During the implementation of the algorithm, real databases containing noise points were used. Based on the results of applying evaluation metrics such as adjusted rand index, homogeneity, Davies-Bouldin index, etc. DBSCAN algorithm was more effective than other clustering algorithms in detecting noise points.

## **MÜASİR BANK SEKTORLARINDA KİBERTƏHLÜKƏSİZLİK STRATEGİYALARININ ANALİZİ**

**V.Ə. Qasimov, A.Ə. İsmayılov**

Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

e-mail: [vaqif.qasimov@aztu.edu.az](mailto:vaqif.qasimov@aztu.edu.az), [a.unudulmaz@mail.ru](mailto:a.unudulmaz@mail.ru)

**Giriş.** Bu gün bank sektoru kibertəhlükələrə qarşı həssas vəziyyətdədir. Bu, bir tərəfdən bankların informasiya infrastrukturalarında mövcud boşluqlara hədəflənən təhlükələrin aktivləşməsi, digər tərəfdən maliyyə sektorunda yeni texnoloji innovasiyaların tətbiqi ilə meydana çıxan kiberisklərlə səciyyələnir. Texnoloji infrastrukturda virtuallaşma, bulud texnologiyaları, suni intellekt və avtomatlaşdırılmış qərar qəbuletmə sistemləri, blokçeyn və digər innovativ həllərin tətbiqi və inteqrasiya olunması kibertəhlükə problemlərini həll etmir, əksinə biznesi maliyyə və reputasiya

itgiləri ilə təhdid edən yeni özünəxas riskləri ortaya qoyur [1, 2]. Bu risklər bank və biznes informasiyasının konfidensiallığı, tamlığı və əlçatanlığı kimi əsas üç meyarlarına təsir göstərir.

Xidmətin keyifyyətinin təkmillədirilməsi, potensial müştəri bazasının genişləndirilməsi, yeni çeşidli məhsulların ortaya qoyulması, maliyyə gəlirlərinin artırılması, təhlükəsizliyin idarə olunması kimi biznes hədəfləri artıq informasiya texnologiyalarının tətbiqi və təhlükəsizliyinin təmin olunması ilə birbaşa əlaqədardır. Bank sektorunun Kibertəhlükəsizlik üzrə başlıca zəiflikləri informasiya təhlükəsizliyi üzrə İdarəçiliyin, biznes məqsədləri ilə uzlaşan strategiyanın, proseslərinin, nəzarət çərçivəsinin, qayda və prosedurların, səlahiyyət bölgüsünün olmaması, informasiya təhlükəsizliyi üzrə peşəkar kadrlar qıtlığıdır. Sonun illərin təcrübələri və hadisələri bir daha sübut etdi ki, informasiya təhlükəsizliyinin təmin edilməsi zəncirinin ən zəif həlqəsi insanlar və davranışlardır. Kibertəhlükəsizliyin idarəedilməsi birdəfəyə tətbiq edilən proses deyil, davamlı idarə olunan proses olmalıdır. Kibertəhlükəsizliyin idarə olunması rəhbərliyin idarəetmə stilində və davranışlarında əks olunmalıdır ki, daxili nəzarət sistemi informasiyanın qorunmasına hədəflənsin. Aparıcı ölkələrin idarəetmə leksikonunda bu münasibəti “Tone at the top” adlandırırlar. Bank rəhbərliyinin davranışlarında bu yanşmanın hiss edilməməsi işçi kollektivin informasiya təhlükəsizliyinə hörmət və təmin etməsini sual altına qoyur. [3, 4, 5].

**Beynəlxalq Bank Sektorlarının Kibertəhlükəsizlik Strategiyaları.** Son on ildə bank sektorlarında və ya dövlət tərəfindən təsdiqlənmiş kiber müharibədə artım müşahidə olunur. Bu tendensiya 2010-cu ildə avadanlıqların sıradan çıxmasına səbəb olmaq üçün İranın uran santrifüj kompüterlərinə yerləşdirilmiş bir qurd olan Stuxnet ilə başladı. 2017-ci ildə Rusiyanın dəstəklədiyi bir hacker qrupu olan Sandworm, cəsarətlə Amerika şirkətlərindən Şərqi Avropa bank şəbəkələrinə qədər geniş bir hədəf hədəfinə çatdı.

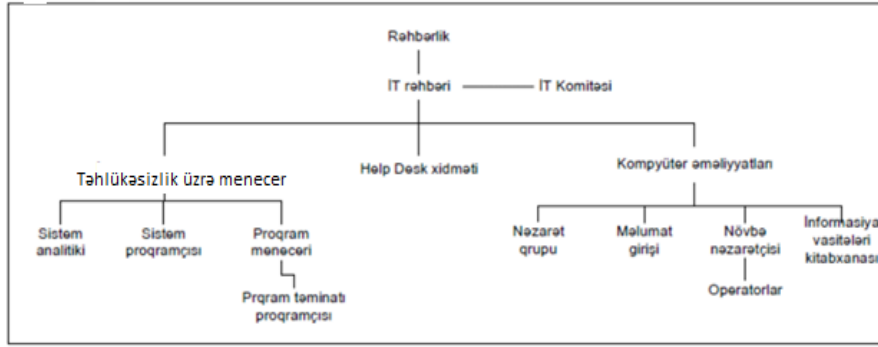
Artıq çoxları bir millətin virusları başqa bir ölkənin kompüter sistemlərinə qırdığı və ya birləşdirdiyi kiber müharibənin dünyada müharibələrin gətirdiyi sərhad olacağına inanır. Kiçik ölkələr və inkişaf etməkdə olan iqtisadiyyatlar ənənəvi qarşıdurmalarda iştirak etmək üçün resursları və ya siyasi dəstəyi olmadıqda bu marşruta müraciət edə bilirlər.

Gələcəkdə kiber təhlükəsizlik bankların infrastrukturunun əsas hissələrini - kiber müharibə zamanı hədəfləri cəlbədicə edəcəklərini - rəqəmsal müdaxiləyə daha davamlı istehsal yollarını tapmalı olacaqlar [6].

Merilend Bankının tədqiqatçısı Mişel Cukierin apardığı bir araşdırmaya görə, hakerlər o qədər çox olub ki, indi orta hesabla hər 39 saniyədə bir baş verir. Kiber hücumların əksəriyyəti, məlumat bazalarını və rəqəmsal ünvanları tarayan, istifadə etmək üçün zəifliklər axtaran avtomatlaşdırılmış skriptlərdən istifadə etməklə həyata keçirilir.

Hər hücumun ssenarisi texnoloji cəhətdən bilikli bir mütəxəssis tərəfindən yazılmalıdır və gələcəkdə onları icra etmək bacarığına və motivasiyasına sahib mütəxəssis sayının artacağına inanmaq üçün əsas var. İnkişaf etməkdə olan ölkələrdə bank standartları yaxşılaşır və texnoloji işçi qüvvəsinin kütləvi şəkildə genişlənməsinə səbəb olur [7].

Aşağıdakı diaqramda bank standartlarına nümunə üçün təşkilati sxemi təsvir edilmişdir:



**Bank sektorlarında kibertəhlükəsizlik strategiyalarının analiz üsulları.** Müasir bank sektorlarında kibertəhlükəsizlik strategiyalarının aşağıdakı dörd növ analiz üsulları var:

1. Çox faktorlu identifikasiya. Çox faktorlu identifikasiya (MFA), istifadəçinin iki və ya daha çox giriş etimadnaməsini təqdim etdikdən sonra əldə edildiyi bir identifikasiya üsuludur. Giriş etimadnaməsinə parollar, sancaqlar və ya barmaq izləri daxil ola bilər. MFA qurarkən, giriş məlumatlarının eyni mənbədən (yəni iki şifrədən) gəlmədiyinə əmin olun, çünki bu, təhlükəsizliyi zəiflədir.

2. Kiberrisiklərin qiymətləndirilməsi. Hansı risklərin işiniz üçün ən böyük təhlükə olduğunu qiymətləndirərək, aradan qaldırma səylərinə üstünlük verə və təhdidin azaldılmasını asanlaşdırma bilərsiniz. Bu, xərcləri və iş vaxtını azaldaraq məlumat pozuntusundan aktiv şəkildə qorunmağa imkan verir.

3. Kibersığorta. Kibersığorta - məlumatların pozulması halında müəssisələrin maliyyə cəhətdən qorunmasını təmin etməyə kömək edir və bu, kiber təhlükəsizlik strategiyasının vacib bir hissəsidir. Hüquqi xərcləri qarşılamaqla yanaşı, kiber sığorta daşıyıcıları da müştərilərə pozuntuları bildirirlər ki, təşkilatlar məlumatların pozulması qaydalarına riayət etsinlər. Bundan əlavə, kiber sığorta, zədələnmiş sistemləri düzəltmək və təhrif edilmiş məlumatları bərpa etmək üçün də ödəməyə kömək edəcək.

4. İşçilərin təlimi. İşçilər kibertəhlükəsizlik sistemlərindən düzgün istifadə etməyi öyrətdikdə sistemləri istismar olunan zəiflikləri aktiv şəkildə müəyyən edə və onların həll olunduğundan əmin ola bilərlər [8, 9].

**Nəticə.** İKT-nin müasir həyatın və inkişafın bütün sferalarını geniş şəkildə əhatə etməsi, global məkana və informasiyaya çıxışdakı sərhədləri aradan qaldırması, informasiya mübadilələrinin və əməliyyatların yüksək sürətini təmin etməklə yanaşı, ucuzluğu və əlyetərliliyi qısa bir zaman ərzində dünya əhalisinin təxminən yarısının istifadəçiyə çevrilməsi ilə nəticələnmişdir. Bütün bank sektorlarında isə kibercinayətlərin araşdırılmasının həyata keçirilməsi üçün yeni üsul və vasitələrlə yanaşı, onların realizəsində yeni metod və imkanların yaranmasına, habelə potensial kibercinayətkarlıq obyektlərinin sayının və miqyasının sürətlə artmasına gətirib çıxarmışdır.

Bir sıra Banklar kibertəhlükələri önləmək üçün güclü texniki-proqram vasitələri əldə etmişlər ki, bu alətlər daxildən və kənardan qaynaqlanan kiber riskləri minimallaşdırmağa imkan verir. Texnoloji yenilikləri daimi tətbiq edən təşkilat kimi Azərbaycan Respublikası Mərkəzi Bankı qeyd

edilə bilər. İT idarəçiliyi və kibertəhlükəsizliyin idarə edilməsi məsələləri Mərkəzi Bankın əməliyyat proseslərinə 10 ildən artıqdır ki, inteqrasiya edilməlidir. Bu sahədə COBIT5, ISO27001 standartları, SWIFT və aparıcı İnsitituların tövsiyələri əldə rəhbər tutulur. Dünyada qabaqcıl informasiya idarəetmə modeli hesab olunan 3 səviyyəli idarəetmə sistemini (İT idarəçiliyi, İnformasiya təhlükəsizliyi və Daxili Audit üzrə qarşılıqlı nəzarət fəaliyyətləri) istifadə edilir, nəzarət-monitoqing alətləri periodik təkmilləşdirilir [10].

Kiberməkanın səciyyəvi xüsusiyyətləri, habelə infrastrukturun, əsasən, özəl sektor və vətəndaşların əlində cəmlənməsi kibercinayətkarlıqla mübarizədə adekvat institusional strukturların, elmi-texniki və normativ-hüquqi bazanın formalaşdırılması və təkmilləşdirilməsi ilə yanaşı, dövlət, özəl sektor və vətəndaşlar arasında, həmçinin beynəlxalq səviyyədə tərəfdaşlığın və əməkdaşlığın genişləndirilməsini tələb edir. Adekvat mexanizmlərin, zəruri institutların, çoxtərəfli və beynəlxalq tərəfdaşlıq və əməkdaşlığın yerində olmaması isə kibercinayətkarlıqla mübarizəni daha da müəkkəbləşdirir və çətinləşdirir.

**Açar sözlər:** kibertəhlükəsizlik, informasiya təhlükəsizliyi, kiberməkan, kiberhücum, kibertəhlükəsizlik strategiyası.

### Ədəbiyyat

1. Olsen F., (2005), Input: IT security spending to catch its breath, Retrieved July 13, 2019 at URL: <http://www.fcw.com/article89546-07-13-05>
2. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Information, Part 2: Security Functional Requirements, Part 3: Security Assurance Requirements, Version 3.1 Revision 1, September 2010
3. Qasımov V.Ə. Kiberterrorçuluq – dünya dövlətlərinə yeni hədə kimi. Tədris vəsaiti, Bakı, 2006. 25 səh.
4. Qasımov V.Ə. İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq. Monoqrafiya. Bakı, Elm, 2007, 192 səh.
5. The ITU National Cybersecurity Strategy Guide. Geneva, 2012, 122 p.
6. OECD: Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies, OECD Digital Economy Papers, No.212, OECD Publishing. 2012.
7. Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2019, 253 p.
8. Sood A.K., Enbody R.J., Targeted Cyberattacks: A Superset of Advanced Persistent Threats, IEEE Security & Privacy, 2013, Vol. 11, No. 1, pp. 54-61.
9. Li F., Lai A., Ddl D., Evidence of Advanced Persistent Threat: A case study of malware for political espionage, Proc. of the 6th International Conference on Malicious and Unwanted Software, 2011, pp.102-109.
10. İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında Azərbaycan Respublikası Prezidentinin Fərmanı, 26 sentyabr 2012-ci il.

## **Analysis of cybersecurity strategies in modern banking sectors**

In modern times, cybersecurity becomes a strategic national problem that affects all layers of society. A fast, effective and effective fight against cyber aggregation requires the correct determination of national goals and priorities, the role and responsibility of the parties concerned, which must be achieved by the end of time. Cybersecurity strategies in the banking sector - one of the first steps in this direction. This article analyzes the existing cybersecurity strategies with the aim of revealing the previous experience in the development of cybersecurity strategies in the banking sector.

## **BIG DATA TƏHLÜKƏSİZLİYİ TEXNOLOGİYALARI: İSTİFADƏ DAİRƏSİ VƏ PROBLEMLƏRİ**

**V.Ə. Qasimov, D.A. Quluzadə, M.İ. Cavadova**

Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

e-mail: [vaqif.qasimov@aztu.edu.az](mailto:vaqif.qasimov@aztu.edu.az), [dilare.quluzade@aztu.edu.az](mailto:dilare.quluzade@aztu.edu.az)

[maryam.cavadova@aztu.edu.az](mailto:maryam.cavadova@aztu.edu.az)

Müasir dövrdə verilənlər bazası (VB), verilənlər bazası sistemləri (VBS), böyük verilənlər (Big Data) kimi anlayışlar insanların gündəlik fəaliyyətlərində rast gəldikləri və istifadə etdikləri informasiya saxlanması, emalı və təminatı sisteminə çevrilmişdir. Big data platformaları: böyük həcmli, müxtəlif strukturlu və yüksək sürətli əlçanlığa malik məhsul, əməkdaş, müştəri və s. məlumatları əhatə edir və belə platformaların tətbiqinin genişlənməsi ilə təhlükəsizlik və gizliliklə bağlı bəzi problemlər yaranır. Məqalədə Big Data təhlükəsizliyi, Big Data təhlükəsizliyi texnologiyaları, istifadə dairəsi, Big Data təhlükəsizliyi məsələlərinə baxılır.

Dövrün tələblərinə uyğun olaraq Big Data texnologiyaları, əlaqəsiz vesilənlər bazaları əksər müəssisələrin müraciət etdiyi texnologiyalardır. Eyni zamanda bu texnologiyalar təşkilatlar və müəssisələr üçün böyük fərsətlərə, həm də riskə malikdir. Kibertəhlükəsizlik baxımından Big Data-da məlumatları qorumaq və gələcək kibercinayətlərin qarşısını almaq üçün analitik və təhlükəsizlik həlləri baxımından yeni imkanlar yaradılsa da, məlumatların həcmünün böyüklüyü kibercinayətkarlara da qabaqcıl texnologiyalardan istifadə edərək çox sayda həssas və fərdi məlumatları əldə etmək imkanı verir.

Araşdırmalara əsasən 20.000 cihazı (fərdi kompüter, smartfon və server) olan orta ölçülü bir şəbəkədə 24 saat ərzində 50 TB-dan çox məlumat emal edilir ki, bu da öz növbəsində kibercinayətkarlar üçün hər saniyədə 5 Gbit-dən çox məlumatın oğurlanması, analiz edilməsi imkanı deməkdir [2].

Big Data təhlükəsizliyi həm məlumat, həm də analitik prosesləri qorumaq üçün istifadə olunan vasitə və tədbirlər kompleksi kimi başa düşülə bilər. Big Data təhlükəsizliyinin əsas məqsədi onların qiymətli məlumatlara zərər verə biləcək hücumlardan, oğurluqlardan və digər zərərli fəaliyyətlərdən qorunmasıdır.

Big Data təhlükəsizliyinin aşağıdakı əsas texnologiyalarını qeyd etmək olar:

- *Şifrələmə.* Verilənlərin şifrələnməsi ümumiyyətlə, məlumatların böyük həcmnin, müxtəlif üsullarla itifadəçi və ya maşın tərəfindən kodlanmasıdır. Şifrələmə vasitələri ilə birlikdə müxtəlif analitik alətlər məlumatları xüsusi formada formatlayır. Eyni zamanda əlaqəli verilənlər bazası idarəetmə sistemi (RDBMS), Hadoop Distributed File System (HDFS) və s. kimi xüsusi fayl sistemləri müxtəlif mənbələrdən alınan məlumatlara tətbiq olunur.

- *İstifadəçi Girişinə Nəzarət.* Bu mexanizmə əsas şəbəkə təhlükəsizliyi vasitələrindən biridir. Adətən, daha yüksək idarəetmə xərcləri olan şirkətlər onu tətbiq edir, şəbəkə səviyyəsində istifadəçi girişinə avtomatlaşdırılmış güclü nəzarət mexanizmi həyata keçirir. Big data platformasını daxili hücum qarşı qoruyan kompleks istifadəçi nəzarətini idarə edir [4].

- *Fiziki təhlükəsizlik.* Ümumiyyətlə, təkilatın məlumat bazası fiziki olaraq təşkilat daxilində yerləşdirilməlidir və ya bulud provayderinin məlumat mərkəzi etibarlılığı ciddi araşdırılmalıdır. Fiziki təhlükəsizlik sistemləri məlumat mərkəzinə və həssas sahələrə kənar şəxslərin fiziki olaraq girişinə nəzarət edir.

- *Mərkəzləşdirilmiş Açar İdarəetmə.* Uzun illərdir ən yaxşı təhlükəsizlik tətbiqetmələrindən biridir. Big data mühitlərində, xüsusən geniş coğrafi bölgüsü olanlarda tətbiq olunur. Mərkəzləşdirilmiş əsas idarəetmə adı altında ən yaxşı təcrübələr arasında siyasətə əsaslanan avtomatlaşdırma, tələbə uyğun açarların çatdırılması, qeydlər və əsas istifadədən əsas idarəetmə mücərrədləşdirilməsidir [1].

Big Data Təhlükəsizliyi istifadə dairəsini aşağıdakı kimi sistemləşdirmək olar:

- *Bulud təhlükəsizliyi monitorinqi:* Bulud texnologiyaları ümumiyyətlə bütün müəssisələr üçün daha səmərəli rabitə və artan gəlirlilik təklif edir. Bulud Təhlükəsizliyi monitorinqi, serverə həssas məlumatlar verir və eyni zamanda bir neçə müvafiq bulud platformasının yerləşdiyi infrastrukturunu izləyir.

- *Şəbəkə trafik analizi:* Trafik davamlı olaraq şəbəkənin və xaricində hərəkət edir. Əsas göstəriciləri yaratmaq və anomaliyaları aşkar etmək üçün istifadə olunur, bulud strukturu daxilində və xaricindəki trafikə təhlili üçün istifadə olunur.

- *Daxili təhlükələrin aşkarlanması:* Daxili (insayder) təhdidlər də ən az kibercinayətkarların hücumları qədər müəssisə üçün təhlükəlidir. Kibercinayətkar hər hansı bir zərərli proqram hücumu qədər təhlükəlidir, bəzi nadir hallarda bir daxili problem şəbəkəni məhv edə bilər. Təhlükəsizlik analitikasının köməyi ilə təşkilatlar daxili təhlükələri asanlıqla aşkarlaya bilərlər. Bu, anormal giriş vaxtları, qeyri-adi e-poçt istifadəsi və icazəsiz verilənlər bazasına giriş istəkləri kimi davranışlar əsasında müəyyənləşdirilir.

- *Təhlükə ovu (Threat Hunting):* Ümumiyyətlə, İT Təhlükəsizlik qrupu daha çox təhdid ovu ilə məşğul olur. İT infrastrukturuna hücum etməyə cəhd göstərən təhlükə və pozuntuların potensial göstəricilərini axtarırlar. Təhlükə ovu taktikaları hücumdan əvvəl potensial təhdidləri müəyyən etmək və təsnif etmək üçün əvvəllər toplanan təcrübələrə istinad edərək yeni təhdidləri müəyyən edə bilər.

- *İstifadəçilərin davranış analizi* Təşkilatın istifadəçiləri ümumiyyətlə hər zaman İT strukturu ilə əlaqə qururlar. Kibertəhlükəsizliyinizin uğurlu və ya uğursuz olmasına qərar verən, əsasən

istifadəçinin davranışdır. Buna görə istifadəçinin davranışını izləməyə ehtiyac var. Təhlükəsizlik analitikası işçilərin qeyri-adi davranışlarını izləyir. Beləliklə, bir daxili təhlükəni və ya zərərli bir hesabı aşkar etməyə kömək edir. Zərərli fəaliyyətləri əlaqələndirərək şübhəli nümunələri də aşkar edə bilər. Bu cür məşhur təhlükəsizlik analitikindən istifadə məsələsinə bir nümunə UEBA-dır və IT mühitində görünürlük təmin etməyə kömək edir.

▪ İcazəsiz məlumat axınının aşkarlanması İcazəsiz məlumat axını məlumatların oğurlanmasına və sızmasına səbəb ola bilər. Şifrəli rabitə məlumat sızıntısını aşkar etmək üçün istifadə olunur.

Big Data mühitinin yüksək sürətlə böyüməsini və bu sahədə yeni texnologiyaların yaranmasını nəzərə alsaq Big Data-da təhlükəsizlik problemlərinin çoxsaylı aspektlərini qeyd etmək olar. Ümumi olaraq bu problemlər aşağıdakı kimi sistemləşdirilir [6]:

Sistemə giriş nəzarətləri: hər bir təşkilatın tam təhlükəsiz bir sistemə sahib olması çox vacibdir və məlumatların mübadiləsi üçün icazə yalnız təsdiq edilmiş istifadəçilərə verilməlidir. Giriş nəzarəti hakerlər və təşkilatın məlumatlarına zərər vermək istəyən şəxslər tərəfindən hücumla məruz qalmayacaq şəkildə olmalıdır.

Qeyri-əlaqəli məlumat bazaları: NoSQL (Big data bazası: qeyri-əlaqəli verilənlər bazası) verilənlər bazası təhlükəsizlikdən daha çox performans və elastikliyə üstünlük verir. NoSQL verilənlər bazasını tətbiq edən təşkilatlar, verilənlər bazasını əlavə təhlükəsizlik tədbirləri ilə etibarlı bir mühitdə qurmalıdırlar.

Saxlanma: Big Data arxitekturasında məlumatlar bir neçə səviyyədə saxlanılır. Depolanma performans və maliyyət baxımından müxtəlif tələblərdən asılıdır. Məsələn, yüksək prioritetli məlumatlar ümumiyyətlə flash mühitdə saxlanılır.

Son nöqtələr (endpoint): Kibercinayətkarlar son nöqtələrdəki məlumatları manipulyasiya edə və yalan məlumatları kütləvi yayıma bilərlər. Gündəlik məlumatları son nöqtələrdən təhlil edən təhlükəsizlik həlləri, bu nöqtələrin həqiqiliyini təsdiqləməlidir.

Data Mining həlləri: Data Mining həlləri ümumiyyətlə iş strategiyalarını təklif edən bir model tapır.

**Nəticə.** Böyük məlumatların qorunmasında çoxsaylı problemləri qeyd edə bilərik. Hər bir təşkilat məlumatlarını Big Data mühitində- buludda saxladığı zaman xidmət təminatçısı ilə sıx işləməlidir. Təhdidlərin zamanında müəyyənəşdirilməsi və problemlərin operativ həlli xüsusi əhəmiyyət kəsb edir. Eyni zamanda təşkilatın məlumatlarının qorunmasında bütün təşkilat əməkdaşları cavabdehdir.

Big data platformasını yüksək və aşağı təhdidlərdən qorumaq, təşkilata uzun müddətə yaxşı xidmətlər göstərməyə imkan verəcəkdir. Getdikcə daha çox şirkət iş strategiyalarını təkmilləşdirmək üçün böyük məlumat analizi vasitələrindən istifadə edir. Bu, kiber cinayətkarlara böyük məlumat arxitekturasına hücum etmək üçün daha çox imkanlar verir. Beləliklə, böyük məlumat təhlükəsizliyi problemlərinin siyahısı artmağa davam edir

Big Data analizi vasitələri kifayət qədər məlumat bazası və statistiki məlumatlardan istifadə edərək yeni təhlükəsizlik strategiyaları təklif edə bilər. Məsələn, təhlükəsizlik kəşfiyyat vasitələri

fərqli sistemlərdə təhlükəsizlik məlumatlarının əlaqəsinə əsaslanaraq nəticələr çıxara bilər. Təhlükəsizliyi yenidən kəşf etmək bacarığı, daim inkişaf edən kiber hücumlar zamanı şəbəkələrin sağlamlığı üçün çox vacibdir.

**Açar sözlər:** Big Data, VB, VBS, Big Data təhlükəsizliyi.

### Ədəbiyyat

1. <https://techvidvan.com/tutorials/big-data-security/>
2. <https://onlinedegrees.sandiego.edu/threat-or-opportunity-big-data-and-cyber-security/>
3. <https://www.vamsitalkstech.com/cybersecurity/cybersecurity-the-killer-app-for-big-data-34/>
4. Security and Privacy Challenges in Big Data Era, August 2016, International Journal of Control Theory and Applications 9(43), pp.437-448.
5. IET Book Series on Big Data—Call for authors\ Security and Privacy for Big Data, Cloud Computing and Applications\ Edited by Wei Ren, Lizhe Wang, Kim-Kwang Raymond Choo and Fatos Xhafa.
6. <https://www.dataversity.net/big-data-security-challenges-and-solutions/>

### **Big data security technologies: use circle and problems**

In modern times, concepts such as database (VB), database systems (VBS), Big Data (Big Data) have become the system of information storage, processing and provision that people come across and use in their daily activities. Big data Platforms: product, employee, customer etc with large capacity, different structure and high speed measurement. it covers the data and with the expansion of the application of such platforms, some problems arise with security and Privacy. The article discusses Big Data Security, Big Data Security Technologies, scope of use, Big Data security issues.

## **İoT-DA KİBERTƏHLÜKƏSİZLİYİN TƏŞKİLİ VƏ KİBERRİSKLƏRİN İDARƏ OLUNMASI**

**V. Qasimov, M. Cavadova**

Azərbaycan Texniki Universiteti, Bakı, Azərbaycan.

e-mail: [vaqif.qasimov@aztu.edu.az](mailto:vaqif.qasimov@aztu.edu.az), [maryam.cavadova@aztu.edu.az](mailto:maryam.cavadova@aztu.edu.az)

Əşyaların İnterneti (IoT) anlayışı texnologiyaya yeni bir paradigma gətirdi. Bir-biri ilə əlaqə qurmağı və əməkdaşlıq etməyi bacaran qurğular və cihazlardan ibarət şəbəkənin əsası qoyuldu. IoT sistemlərinə daim artmaqda olan kiberhücumlar insanlar və təşkilatlar üçün bir sıra problemlər yaratdı. Kiberhücumların sürətlə artması ağıllı şəbəkələr, ətraf mühitin monitorinqi, xəstələrin monitorinq sistemləri, ağıllı istehsalat kimi sahələrdə IoT cihazlarının geniş tətbiqi ilə əlaqədardır. Cihazlar arasındakı əlaqənin dinamik və müvəqqəti xarakterli olması IoT-un təhlükəsizliyinin təşkili çətinləşdirir. Əvvəlki tədqiqatların əksəriyyəti IoT təhlükəsizliyinin təşkilinin texnoloji aspektlərinə

yönəlmişdir. Bununla birlikdə, IoT sistemlərindəki kompleks kibertəhlükəsizlik məsələlərinin həlli zamanı bütün aspektlərdə kiberrisiklərin idarə olunma problemi yaranır.

Dörd səviyyəli IoT kiberrisiklərin idarə olunması platforması, IoT təhlükəsizlik menecerlərinə sərfəli bir kiberrisiklərin idarəetmə planı hazırlamağa kömək üçün təklif olunur. Təklif olunan modeldə kiberrisikləri və onlara təsir edən əsas amilləri dörd sinfə ayırmaq mümkündür. Beləliklə, kiberrisik menecmenti fəaliyyəti mərhələli şəkildə təşkil edərək, heç bir kibertəhlükəsizlik məsələsini gözdən qaçırtmadan qiymətləndirə bilir. Şəkil 1-dən görüldüyü kimi biz IoT kiberrisik idarəetmə platformasını IoT kiber ekosistem, IoT kiber infrastruktur, IoT kiberrisik qiymətləndirmə səviyyəsindən və IoT kiber performans səviyyələrindən ibarət olan dörd mərhələyə ayıra bilərik.

|                               |
|-------------------------------|
| IoT kiber ekosistem           |
| IoT kiber infrastruktur       |
| IoT kiber risk qiymətləndirmə |
| IoT kiber performans          |

**Şəkil 1.** IoT kiberrisik idarəetmə platforması

Risk idarəetmə modeli IoT kiber ekosistem qatından başlayır ki, bu da ekosistem elementlərinin qiymətləndirilməsi aparılarkən təşkilat maraqlı tərəflərin dinamikasını və onlara verilən icazələri müəyyənləşdirir [1, s.7]. IoT kiber ekosistemi, IoT sistemləri ilə əməkdaşlıq edən və onlarla qarşılıqlı əlaqədə olan maraqlı tərəflərdən ibarətdir. Maraqlı tərəflər dedikdə IoT kibertəhlükəsizlik texnologiyası mütəxəsisləri, xarici müştərilər, rəqiblər, dövlət qurumları və standartlaşdırma təşkilatları nəzərdə tutulur. IoT kiber ekosistemindəki dəyişikliklər kibertəhlükəsizlik menecerlərinin diqqətindən yayınmamalıdır. IoT sistemlərinin qorunması və düzgün təhlükəsizlik addımlarını hazırlamaq üçün kiber təhlükəsizlik menecerləri üçün bu vacib amildir. Bir çox IoT menecerinin kifayət qədər təcrübəsinin olmaması IoT kibertəhlükəsizlik məsələlərinin inkişafına öz mənfi təsirini göstərir. Beləliklə, IoT menecerləri IoT texnologiyası inkişaf etdikcə baş verən yeniliklərdən, yeni texnologiyalardan (anında) xəbərdar olmalıdırlar. Kibertəhlükəsizlik texnologiyası inkişaf etdikcə, məlumatların ötürülməsinin təmin edilməsi, hücumların qarşısının alınması və məxfilik standartlarını qorumaq üçün IoT cihazlarına ən son texnologiyalar tətbiq edilir. Ən son texnologiya olan 5G, serversiz və duman hesablamının inkişafına əsasən IoT sistemləri müxtəlif kiberhücumlara qarşı daha yaxşı qoruna bilməlidirlər. Machine learning və süni intellekt ənənəvi metodlardan fərqli olaraq daha yüksək dəqiqliklə IoT sistemində real zamanda təhlükənin aşkarlanması, qarşısının alınması və bərpa tədbirlərini təmin edilməsini yerinə yetirə biləcək potensiala sahibdirlər. Təklif olunan IoT təhlükəsizlik platformaları, çoxsaylı istifadəçilərdən ibarət olan, heterogen cihazları və tətbiqləri birləşdirən təhlükəsiz IoT sistemini təqdim edə bilməlidir. IoT sistemində tətbiq edilən ən son yeniliklər istifadəçilər üçün əlçatan olmalıdır. IoT tətbiqlərinə əlavə olunan yeni xidmətlərdən istifadəçilərin və müştərilərin istifadə edə bilməsi IoT tətbiqlərinin müvəffəqiyyət əldə etməsi üçün şərtidir.

Son zamanlar aparılan araşdırmalar göstərir ki, IoT tətbiqlərinin asan istifadə olunması və faydalılığı istifadəçilər arasında müsbət qarşılır, ancaq məxfilik riski IoT tətbiqinin istifadəsinə mənfi təsir göstərir. Bu səbəbdən, IoT menecerləri IoT istifadəçilərini və müştərilərinin istəklərinin müəyyən etməli, tətbiqin istifadə üstünlüklərini, təhlükəsizlik və məxfiliklə bağlı istifadəçilərin narahatlıqlarından xəbərdar olmalıdırlar. Beləliklə, bundan sonra təhlükəsiz IoT modeli hazırlamaladırlar. Kiber ekosistem, iqtisadi mənfəət və ya digər çirkin məqsədlər üçün kibertəhdid yaradan müdaxilələr və hakerlərdən gələn təhlükələri nəzərdə saxlayır. Belə təhlükələr yarada biləcək rəqiblər qabaqcıl simsiz təhlükəsizlik protokolları və kriptografiyadan fəal istifadəedirlər. Beləliklə təşkilat yeni hücumlar təşkil edə biləcək hakerləri müəyyən edə bilmək üçün, onların sistemlərə hücum etmə hiylələrini və sistemə necə nüfuz etməsini, məlumatları oğurlamasını, zərərli proqram qurmasını və müdaxilə əməliyyatlarının təhlilinin aparılmasını yerinə yetirməlidir. IoT kiber ekosistem təbəqəsi ətraf mühiti periodik və ya davamlı olaraq izləyir, qiymətləndirir və əldə olunan informasiyanı müvafiq səviyyələrə çatdırır.

Sonrakı araşdırmalarda kiberrisiklərin idarə edilməsi planını hazırlayarkən təşkilatlar mövcud IoT kiber infrastrukturunu həm texnoloji, həm də idarəetmə baxımından qiymətləndirməlidir. IoT kiberrisik qiymətləndirməsəviyyəsi, IoT aktivlərini və xidmətlərini, zəifliklərini və kibertəhdidləri müəyyənləşdirir. Kibertəhdidləri və onların təsirlərini ölçür, prioritetləşdirir. IoT kiber performans qatında kiber texnologiyalar inkişaf etdirilir, monitoring və nəzarət fəaliyyətləri aparılır və davamlı təkmilləşdirmə işləri aparılır [2, s.697].

IoT sistemi ağıllı şəhər, ağıllı şəbəkə, ağıllı istehsalat, ağıllı sağlamlıq, sürücüsüz avtomobillər və pilotsuz təyyarələrin əsas hissədir. IoT sistemi inkişaf etdikcə bu şəbəkəyə qoşulan cihazların sayı sürətlə artır. Belə cihazların sayı artdıqca təhlükəsizlik riskləri də dəfələrlə artır. IoT sistemlərindəki təhlükəsizlik çatışmazlığı bədnəyyətliyə kritik infrastruktura və həssas məlumatlara giriş imkanlarını artırır. Bununla birlikdə, IoT kiberrisikləri idarəetmə platformasının olmaması, təşkilatların IoT kiberrisiklərin idarə olunmasını və qarşısının alınmasını çətinləşdirir.

**Açar sözlər:** Əşyaların İnterneti, kibertəhlükəsizlik, kiberrisiklərin idarə olunması.

### **Ədəbiyyat**

1. Lee I. The Internet of things for enterprises: An ecosystem, architecture, and IoT service business model. Internet Things Eng. Cyber Phys. Hum. Syst. 2019.
2. Malik, V., Singh, S. Security risk management in IoT environment. J. Discret. Math. Sci. Cryptogr, 2019ş

### **Organization cyber security and cyberrisk management in IoT**

Along with the growing threat of cyber attacks, cybersecurity has become one of the most important areas of the Internet of Things (IoT). The main goal of IoT cybersecurity is to reduce the security risk of users by protecting IoT applications and privacy. New cybersecurity technologies and methods have the best potential for IoT security. However, there are still shortcomings in IoT

cyberrisk management. This article examines IoT cyber security technologies and cyberrisk management platforms.

## **ANALYSIS THE MOST SIGNIFICANT RISKS IN TECHNOLOGY AND FINANCIAL SERVICES**

**A. Hasanov, E. Azizbeyov, G. Mirzayeva**

The Academy of Public Administration under the President of the Republic  
of Azerbaijan, Baku, Azerbaijan

e-mail: [eazizbayov@gmail.com](mailto:eazizbayov@gmail.com), [gulnar.mirzayeva@gmail.com](mailto:gulnar.mirzayeva@gmail.com)

Technology is a great enabler that, apart from it also presents a pervasive, potentially high-impact risk. Nowadays, cyber risk in the form of data theft, compromised accounts, destroyed files, or disabled is the main problem. Find the solution to problems and solutions is vital for the organization. Mostly, this organization is a financial institution. Financial institutions face risk from misalignment between business and strategies, management decisions that increase the cost and complexity of the IT environment, and mismatched. Sometimes, a financial company's technology may become obsolete, disrupted, or uncompetitive, with legacy systems hindering agility. Naturally, mergers and acquisitions can hopelessly complicate the organization's IT environmental fact that many management teams fail to budget for and address. Meanwhile, manage with the technology startups and disruptive financial technology ("FinTech") solutions are challenging the business models and processes at the core of many institutions, making swiftness of response a requirement for ongoing relevance and viability [2].

Some of the most significant risks in technology in financial services include:

1. Strategic risk of IT. 2. Cyber security and incident response risk. 3. IT resiliency and continuity risk. 4. Technology vendor and third-party risk. 5. Data management risk. 6. IT program execution risk. 7. Technology operations risk. 8. Risk of ineffective risk management.

1. Strategic risk of IT. In a rapidly changing world, risk emanating from an ineffective IT strategy stands among the top threats a financial institution faces.
2. Cyber security and incident response risk Cyber security and incident response risk. Nowadays, the many reports of cyber-attacks, data privacy breaches, and misconduct at major companies have pushed cyber security to the top of boards' agendas. Directors of the company need to understand management's view of cyber risks, the potential likelihood and impacts of risk events, and the steps taken to address the risks. It is possible practical to protect all digital assets equally; in addition to having foundational cyber capabilities across the institution.
3. IT resiliency and continuity risk. IT resiliency and continuity risk the organization's IT must be resiliency every financial problem and outages. An organization should have resilient standards and have to go toward the technology that supports the most critical business processes. In the

testing process, organizations have to especially for critical technology, must be rigorous, and verify that recovery plans will work.

4. Technology vendor and third-party risk Technology vendor and third-party risk. Vendor and third part starting new critical risk for company or business process. Proliferate in financial services, so do the risks. Indeed, the other parties' own technology generates new operational, financial, reputation risks to the institutions that use their services. However, in arrangements by standard forms of assurance provided by vendors, by check all processes, and testing gets reduce risk probably.
5. Data management risk. There is including huge information when we can imagine about data and data management. It is problematic for a company manages big data. In the business process, ineffective data management at a financial institution can open the way to financial fraud, accounting and regulatory reporting issues, and loss of stakeholders' trust. Therefore, every company has its own regulatory agencies. Regulatory agencies are expressing strong interest and they target manage big data. It is responsible for big data management capabilities, given that risk and capital management depend on reliable, accurate, and timely data. In addition, financial institutions are increasingly combining external data with internal data, adding new layers of complexity to data management and, potentially, new risks. Rigorous data management capabilities rest on data governance, policy, and procedures that support accuracy, reliability, and timeliness of data, and clarify data ownership, uses, and alteration. Controlled creation, transformation, storage, and disposal of data are central to the concept of big data integrity [1].
6. IT program execution risk. Execution risk analysis can use the same tools as other risk analyses. For example, a decision tree analysis lists out each potential project risk and the value it has on success and failure. Failure is a negative value in the decision tree. You create probabilities for each item or risk. You can apply this to execution risk by considering the probability of specific failures. For future is observed, a large financial institution will have multiple IT programs in development across organizational functions and geographic regions. In examples include enterprise resource planning (ERP), enterprise risk management (ERM), and customer relationship management (CRM) systems. These programs tracking risks, such as budget overruns, delays, and failure to deliver targeted business results.
7. Technology operations risk.  
Management should ensure that rigorous operational processes are in place to protect the integrity of the technology environment. IT needs to deliver services at levels agreed upon with the business, manage capacity, understand and manage its assets, comply with software license agreements, and effectively manage incidents and problems. Non-standard and complex architectures can hinder the ability to meet service performance objectives. A weak incident management process leads to untimely and inconsistent resolution of issues, and missed opportunities to strengthen processes [3].
8. Risk of ineffective risk management. Financial institutions traditionally pursue three lines of defense model to address risk. The first line of defense, product and process owners, identifies

and manages risk. The second line, frequently executed by risk and compliance functions, provides a risk management structure and independent oversight of the first line.

**Keywords:** risk management, big data, Cyber security, financial institution, IT resiliency.

### References

1. Cerchiello P., Giudici P., Big data analysis for financial risk management. Journal of Big Data, 2016, pp.3-18.
2. <https://www2.deloitte.com/us/en/pages/center-for-board-effectiveness/articles/information-technology-risks-financial-services.html>
3. <https://www.projectmanager.com/training/it-risk-management-strategies>

## BEYNƏLXALQ İNFORMASIYA TƏHLÜKƏSİZLİYİ SİSTEMİNDƏ PANDEMİYA ÖZƏLLİKLƏRİ: ZOOM VASİTƏSİ İLƏ DAĞIDICILIQ

**Ə.T. Həzərخانov, V.A. Neymətov**

Milli Aviasiya Akademiyası, Bakı, Azərbaycan

e-mail: [enver-xan@mail.ru](mailto:enver-xan@mail.ru), [neymvasif@mail.ru](mailto:neymvasif@mail.ru)

2 dekabr 2021-ci ildə Group-İB tərəfindən Qlobal təhlükələrin axtarışı və kəşfiyyatı üzrə növbəti veb-konfrans (GLOBAL threat hunting and intelligence conference) keçiriləcəkdir. Qısaca olaraq, adı CyberCrimeCon olan bu kimi veb-konfransların keçirilməsində əsas məqsəd beynəlxalq miqyasda informasiya təhlükəsizliyi sahəsində aparılmış tədqiqatlar, əldə olunmuş təqdirəlayiq nəticələr, tətbiq edilmiş yeniliklər, intellektualcasına dərinləşdirilmiş ekspertizalar haqqında qarşılıqlı praktiki və elmi-nəzəri mübadilələrin təşkil edilməsi, perspektivli sayıla biləcək əhəmiyyətli əməkdaşlıq tədbirlərinin müzakirə olunmasıdır [1].

Konfransın gündəliyinə daxil olan məruzələrin mövzularının müqayisəli təhlili əsasında beynəlxalq informasiya təhlükəsizliyi miqyasında qloballığı ilə seçilən aktual problemləri identifikasiya etmək mümkündür: High-tech (hərfi tərcüməsi: yüksək texnologiyalar) sahəsində intellektual kriminallığın inkişafı tendensiyaları; bank sektoruna kiberhücumlarda troyanların tətbiqinin genişləndirilməsi; Java seriallaşmasından informasiya təhlükəsizliyinə qarşı yarana biləcək hədələnmələr; pandemiya dövründə daha geniş tətbiq edilən və ən populyar proqram təminatı sistemlərindən birinə çevrilən Zoom videoçat platforması vasitəsi ilə informasiya təhlükəsizliyi sisteminin dağıdılması problemləri; İnternet şəbəkəsində intellektual mülkiyyətin qarət və məhv edilməsindən qorumaq üçün yaradılan informasiya təhlükəsizliyi sistemlərinə qarşı kiberhücumların aşkarlanıb aradan qaldırılması və s.

Yuxarıda sadalananların siyahısından pandemiya dövründə populyarlaşan Zoom videoçat platforması vasitəsi ilə informasiya təhlükəsizliyinin dağıdılmasından qorunmaq üçün yerinə yetirilən tədbirlərlə bağlı problemlərin Azərbaycanın həm təhsil sistemi cəmiyyəti, həm də texnokrat gəncliyi

üçün də aktualdır. Belə ki, Zoom videoçat (yaxud veb-konfrans platforması, bundan sonra qısaca VÇP) pandemiya dövründə əvvəlcə daha çox ali təhsildə onlayn dərslərin təşkilində tətbiq edildi. Əlavə olaraq, platforma ödənişsiz, olduqca rahat və cəld qoşulması ilə insanlar arasında online ünsiyyət və kütləvi tədbirlər vasitəsinə də çevrildi. Beləliklə, elektron ünsiyyət amili kimi, təkzibedilməz aktuallığını nəzərə alıb, tərəfimizdən müvafiq istiqamətlərdə statistik təhlillər, elmi araşdırmalar və tədqiqatlar aparılmışdır.

2011-ci ildə Ciscunun eks vitse-prezidenti Erik Yuan tərəfindən yaradılan Zoom VÇP ilk əvəllər yalnız korporativ müştərilərlə müqavilələrə malik olmuş, işəqəbuletmə zamanı distant müsabiqələrin keçirilməsində, əməkdaşların isə sadəcə qarşılıqlı ünsiyyəti üçün tətbiq edilirdi. 2014-cü ildə artıq 20 000 müəssisə ilə bağlanmış müqavilə əsasında 10 milyon istifadəçiyə malik idi. Nəhayət, pandemiya ərəfəsində, 2019-cu ildə kommersiya təyinatlı VÇP versiyalarının yaranışından sonra səhmləri 72% artaraq 16 milyard dollar civarında qiymətləndirilirdi [2].

Pandemiyanın elan olunduğu 2020-ci ilin mart ayının sonuna düşən statistik məlumatlara görə Zoom VÇP 200 milyonluq gündəlik auditoriyaya malik idi. Məhz, platformanın ödənişsiz versiyasının geniş imkanlı servisi və qoşulma sadəliyi Zoom VÇP-nin pandemiyanın ilk aylarında sürətlə populyarlaşmasına səbəb oldu.

Zoom VÇP-də informasiya təhlükəsizliyi ilə bağlı zaman-zaman meydana çıxmış problemlər tərəfimizdən araşdırılarkən, aşağıdakılar müəyyən edilmişdir:

1. 2019-cu ildə tədqiqatçı Conatan Leytsux VÇP-nin zəif tərəflərindən birini aşkarlayaraq, qeyd etmişdir ki, istənilən MacOS istifadəçisi istənilən sayt üzərindən Zoom zənglərinə qoşulub, veb-kameranı icazəsiz aktivləşdirə bilər [3]; Sonradan Apple, istifadəçilərini qorumaq üçün problemə müdaxilə etsə də, Zoom yaradıcıları problemi aradan qaldıra bildi.

2. Yenə həmin ilin sonunda Cequence startapçılar konfrans kodlarını bir-bir yoxlamaqla, Zoom zənglərinə qoşulmağı bacaran botlar yarada bilmişlər. Müxtəlif mənbələrin müqayisəli təhlili əsasında müəyyən etmək olmuşdur ki, müdaxiləyə imkan yaradan əsas səbəb odur ki, konfrans kodları (Meeting ID) qoruyucu şifrələnməyə malik deyil. VÇP yaradıcıları bu tip müdaxilələrin həqiqətən olub-olmadığı haqqında məlumatsız olduqlarını bildirsələr də, təhlükəsizlik səviyyəsini yüksəldəcəklərinə əmin etdirmişlər [4, 5].

3. Zoom VÇP-də mühafizə protokolu kimi TLS standartından istifadə edilir [6]. TLS, (Transport Layer Security- “nəqləmə səviyyəsində təhlükəsizlik) standartı əslində kriptografik alqoritmlə protokoldur və veb-brauzerlərdə HTTPS (Hyper Text Transfer Protocol Secure-hipermətnləri nəqləmənin mühazifəsi protokolu) təhlükəsizliyini təmin etmək üçün tətbiq edilir [7]. Praktiki olaraq, bu o deməkdir ki, istifadəçiyə ötürülən verilənlər şifrələnmiş formada onun istifadə etdiyi aparatda, yaxud cihazda qalır. Beləliklə, smartfonda olan və istifadəçiyə aid olan verilənlər hətta serverin sahibi üçün belə, əlçatmaz olur. Lakin, Zoom VÇP-nin serverində yerləşən informasiyalar hüquq-mühafizə orqanlarının müdaxiləsi üçün açıqdırlar, əlbəttə bu vəziyyətdən “texnokrat dələduzlar” məharətlə istifadə etmiş və nəticədə VÇP-nin informasiya təhlükəsizliyi sistemində arzu edilməz problemlər yaranmışdır.

Pandemiya dövründə Azərbaycan təhsil sistemində rəsmi olaraq, Microsoft Teams VÇP (yaxud, daha geniş anlamda veb-konfrans servisi) tətbiq edilsə də, Zoom istifadəçiləri də olduqca böyük auditoriyaya malik idilər. Bu mənada, Zoom VÇP-nin mühafizə sisteminin təkmilləşdirilməsinə aid tərəfimizdən formalaşdırılmış və aşağıda sadalanan təklifləri əhəmiyyətli hesab edirik:

1. Zoom mühafizə sistemində E2E (end-to-end encryption- hərfi tərcüməsi: obaşdan bubaşa şifrləmə) protokolunun tətbiq edilməsi. Bəzi informasiya portallarının iddialarına inansaq, bu protokol əksər VÇP üçün “qızıl standart” çevriləcəkdir. Mahiyyəti odur ki, bir istifadəçinin göndərdiyi informasiya şifrlənir və yalnız ünvanına yetişəndən sonra şifri açılır. Bu zaman, informasiya VÇP-nin serverinə qəbul edilərək ötürülməsində belə şifrlənmiş formada qalır, yəni heç server də onu oxuya bilmir. Bu, yuxarıda haqqında danışılan nəqləmə şifrlənməsi protokollarından daha etibarlıdır. Lakin, nəzərə almaq lazımdır ki, E2E-nin tətbiqi VÇP-nin serveri tərəfindən istifadəçiyə təklif edilən funksional imkanları nisbətən məhdudlaşdırıla bilər [8,9].

2. Bu günlərin son məlumatına görə, Zoom Video Communications şirkəti Facebook ilə birgə əməkdaşlıq çərçivəsində Whiteboard adlı, yeni interaktiv platformasının fəaliyyətinə start verəcək [10]. Xəbər portalında deyilir ki, Whiteboard real zaman miqyasında asinxron və müştərək işləməyə imkan verən virtual mərkəzə çevriləcəkdir. Daha çox müəssisələrarası elektron cəmiyyət üçün nəzərdə tutulan platformada istənilən cihaz üzərindən qarşılıqlı ünsiyyət və mübadilə təşkil etmək mümkün olacaqdır. Bu platforma əsasında gələcəkdə istifadəsi nəzərdə tutulmuş Horizon Workrooms platforması ünsiyyətdə olan insanların virtual reallıq formatında formalaşan bir otağa yığılmasını təmin edəcəkdir. Məlumdur ki, Facebook istifadəçiləri üçün informasiya təhlükəsizliyinin məsuliyyətinin bir hissəsi istifadəçilərin öhdəsinə verilir: şəxsi parolun mühafizəsi; şəxsi verilənlərin mənsəyi məlum olmayan şəbəkə sorğularından qorunması; akauntun fişinqdən qorunması və s. [10, 11]. Əgər Whiteboard Zoom funksiyalarını tamamilə özündə saxlayacaqsa, ola bilər ki, onun informasiya təhlükəsizliyinin səviyyəsi istifadəçinin şəxsi məsuliyyəti hesabına artırılmış olsun.

**Açar sözlər:** Zoom videoçat portalı, informasiya təhlükəsizliyi, TLS, HTTPS, E2E şifrləmə standartları, facebook, pandemiya.

## Ədəbiyyat

1. [https://cybercrimecon.com/ru/?utm\\_source=yandex&utm\\_campaign=ccc2021-ru](https://cybercrimecon.com/ru/?utm_source=yandex&utm_campaign=ccc2021-ru)
2. <https://explore.zoom.us/ru/about/>
3. <https://tjournal.ru/internet/157084-zoom-glavnoe-prilozhenie-epohi-pandemii-no-utechki-i-problemy-s-bezopasnostyu-sdelali-ego-samym-protivorechivym>
4. [https://www.gazeta.ru/tech/2020/04/01/13031095/zoom\\_danger.shtml?updated](https://www.gazeta.ru/tech/2020/04/01/13031095/zoom_danger.shtml?updated)
5. <https://habr.com/ru/company/pt/blog/459450/>
6. [https://explore.zoom.us/docs/doc/Zoom%20Encryption\\_RU.pdf](https://explore.zoom.us/docs/doc/Zoom%20Encryption_RU.pdf)
7. <https://techcrunch.com/2019/07/10/apple-silent-update-zoom-app/>

8. <https://www.comss.ru/page.php?id=2468>
9. <https://www.kaspersky.ru/blog/what-is-end-to-end-encryption/29075/>
10. <https://ria.ru/20210914/platforma-1749949670.html>.
11. <http://www.securrity.ru/articles/1081-facebook-bezopasnost-i-konfidencialnost.html>

### **Pandemy features in the international information security system: destruction by ZOOM**

Based on the presentation of the reasons for the high popularity of the Zoom platform at the beginning of the pandemic, the relevance of research on the levels of vulnerability of the platform from cyber attacks and fraud is justified. The transport data encryption protocols used in Zoom to ensure information security are explained. It is proposed to increase the level of security by using end-to-end data encryption, as well as by sharing responsibility with users.

## **AVIASIYA SİSTEMLƏRİNDƏ İNFORMASIYA TƏHLÜKƏSİZLİYİ**

**İ.M. İsmayılov, Ə.T. HəzərxaNov**

Milli Aviasiya Akademiyası, Bakı, Azərbaycan  
e-mail: [ismayil.maa@gmail.com](mailto:ismayil.maa@gmail.com), [enver-xan@mail.ru](mailto:enver-xan@mail.ru)

Havada hərəkətin avtomatlaşdırılmış idarəetmə sistemində (HHAİS) informasiya proseslərinin kütləvi avtomatlaşdırılması, informasiya resurslarının qiymətlərinin və əhəmiyyətinin artması ilə əlaqədar olaraq, kritik mühüm idarəetmə sistemlərində dövr edən informasiyanın etibarlı mühafizəsi çox ciddi problemə çevrilir. Problemin ciddiliyi barədə tək-cə o faktı qeyd etmək olar ki, qısa bir müddət ərzində (10 dəqiqədən bir az artıq) HHAİS-ə əlyətərliyi olan bir şəxs böyük bir hava limanının işini iflic vəziyyətə sala bilər. Bunun üçün HHAİS-in proqram təminatına proqram-virusun cəmi bir neçə onlarla kod sətirlərini daxil etmək kifayətdir. Əgər sistem informasiya mühafizəsinin xüsusi vasitələrinə malik olmazsa, bu yüz və minlərlə sərnişinlərin həyat fəaliyyəti üçün təhlükə törədə bilər.

Beləliklə, aeronaviqasiya sistemlərini və hava məkanı istifadəçilərini uçuşların intensivliyinin artması şəraitində zəruri informasiya ilə təmin edən avtomatlaşdırılmış sistemlərin, o cümlədən həmin sistemlərin tərkibinə daxil olan verilənlər bazasının mühafizəsi məsələləri aktual məsələ kimi irəli sürülür.

Verilənlər bazası şəbəkə təhlükəsizliyi tədbirləri kimi sayılan şəbəkəarası mühafizənin aparat-proqram vasitələri və şəbəkəyə müdaxilənin aşkarlanması sistemləri vasitəsilə xakkerlərdən qorunur. Şəbəkə təhlükəsizliyinin bu baxımdan qiymətli olmasına baxmayaraq, verilənlər bazası sistemlərinin təhlükəsizliyinin təmin edilməsi və onların içində olan proqramlar, funksiyalar və məlumatlar daha da əhəmiyyətli ola bilər. Belə ki, şəbəkələr getdikcə internetdən daha geniş istifadə üçün açılır və həmin şəbəkələrdən müxtəlif məqsədlər üçün istifadə edən istifadəçilərin sayı artır. Bundan əlavə, bazada olan məlumatlara girişin idarə olunması üçün sistem, proqram, funksiya və vasitələr, həmçinin

müvafiq identifikasiya, autentifikasiya və hüquqların idarə edilməsi funksiyalarını məhdudlaşdırmaq və bəzi hallarda səlahiyyətli istifadəçilər və administratorların hərəkətlərini qeyd etmək vacibdir [1].

HHAİS-də informasiyanın mühafizəsinin təmin olunması problemin kompleks həllinin mürəkkəbliyi ilə izah olunan spesifik xüsusiyyətə malik olması ilə əlaqədardır. Bu mürəkkəbliyə isə havada hərəkəti idarəetmə (HHİ) prosesinin verilənlər bazasının çoxşaxəli olması (aeronaviqasiya verilənlər bazası, uçuşlar barəsində informasiya sisteminin bazası, aeroport verilənlər bazası, resursların idarə olunması sisteminin bazası və s.) və onların hər birinin özünə məxsus xüsusiyyətlərə məxsus olmasından irəli gəlir. Qeyd olunanları nəzərə alaraq müasir dövrdə verilənlər bazasının mühafizəsinin ən mükəmməl və etibarlı sistemi sayılan ORACLE DATABASE sistemindən istifadə etməklə aviasiya verilənlər bazasında informasiyanın mühafizə sisteminin yaradılması prinsipləri tədqiq edilmişdir [2].

Verilənlərin təhlükəsizliyinin təmin edilməsi istiqamətində son illər irəliyə böyük addım kimi Oracle Database sistemini və onun əlavələrində rolların daxil edilməsini hesab etmək olar. Oracle-a qədər hər bir istifadəçiyə ona istifadə etməyə icazə verən verilənlər bazasının hər bir obyektinə əlyetərlik hüququnu aşkar şəkildə təqdim etmək lazım gəlirdi. Bu proses onun hesabına sadələşir ki, obyektlər yığımına əlyetərlik rollarla təqdim olunur, daha sonra isə bu roldan istifadə müvafiq şəxslərə verilir. Digər tərəfdən verilənlər bazası server informasiya idarəetmə problemlərinin həlli üçün əsasdır.



Şəkil.1

Verilənlər bazasının qorunması, verilənlər bazasında və onun içindəki obyektlərdə istifadəçi hərəkətlərinə icazə verilməsi və ya qadağan edilməsi deməkdir. Oracle məlumatların əldə edilməsini idarə etmək və verilənlər bazasının müxtəlif resurslarından istifadəni məhdudlaşdırmaq üçün təhlükəsizlik sxemləri və domenlərdən istifadə edir [4].

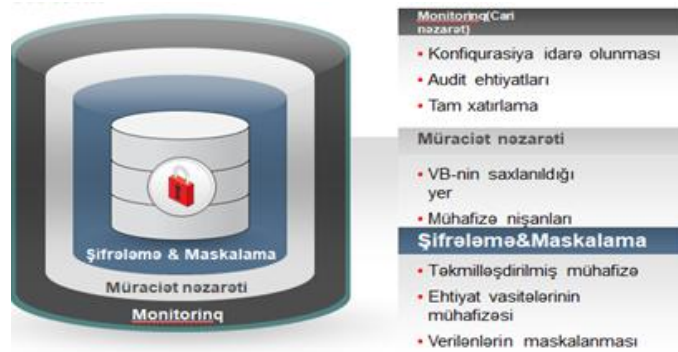
Oracle verilənlər bazasının təhlükəsizliyinin təmin edilməsi üzrə həllərin tərkibinə aşağıdakı proqram məhsulları daxildir (Şək.1).

Yuxarıda qeyd olunan analiz əsasında VBİS Oracle alətlər vasitəsilə verilənlər bazasının administratoru, şəbəkə administratoru, təhlükəsizlik siyasəti və istifadəçilərin rollarını

fərqləndirməklə aviasiya və aeronaviqasiya informasiyasının mühafizəsi, strategiyası, həmçinin VBİS Oracle-nin köməyi ilə verilənlərin şifrələnməsi və maskalanması məsələlərinin həlli təqdim olunmuşdur.

Aviasiya verilənlər bazasının ümumiləşdirilmiş proqram təminatına aşağıdakı altproqramlar daxildir: CREATE TABLE PLANE, CREATE TABLE AIRPORT, CREATE TABLE FLIGHT.

Konkret olaraq, qeyd olunan proqram təminatının əsas üstünlüklərindən istifadə edərək, VBİS Oracle əsasında layihələndirilən aviasiya verilənlər bazasının ümumiləşdirilmiş strukturu şəkil.2-də verilmişdir [3].



Şəkil.2

Nəticə olaraq məqalədə obyektlərin təhlükəsizliyinin təmin olunmasının ümumi sisteminin analizi əsasında və aeronaviqasiya informasiyasının mühafizəsi istiqamətində VBİS Oracle alətlər vasitəsilə aviasiya verilənlər bazasında informasiya təhlükəsizliyi sisteminin qurulması prinsipləri verilmişdir.

**Açar sözlər:** informasiyanın mühafizəsi, verilənlər bazası, verilənlər bazasının idarəetmə sistemi (VBİS), müasir informasiya texnologiyaları, müasir proqramlaşdırma dilləri.

### Ədəbiyyat

1. İsmailov I.M., Kodjayev A.E Data-Protection in aviation system. MAA Elmi məcmuələr, 2013, Cild 15, №4, s.51-55.
2. İsmailov I.M., Kodjayev A.E. Airline Reservation system. Труды международной научно-технической конференции Компьютерные системы и информационные технологии. Киев, 2014, с.12-13.
3. İsmayılov İ.M., Abbaslı O.E.. Aviasiya komplekslərində verilənlər bazasının mühafizə sisteminin yaradılması prinsipləri. MAA, Elmi Məcmuələr, Cild 20, №1, 2018, s.86-94.
4. Кайт Т. Oracle для профессионалов: архитектура, методики программирования и особенности версий 9i, 10g и 11g, 2-е издание Expert Oracle Database Architecture: Oracle Database Programming. - М.: Вильямс, 2011.

### **Information safety in aviation systems**

Any measures that should be taken for Air system data security purposes should also be considered at the database level, similar to hardware, network and operation system levels. Generally, companies buy a firewall product and think that they have already solved the problems related to security. Researches show that despite it is possible to take measures against external Air System attacks by the firewall products, no sufficient measures may be taken against internal attacks. In particular, no action related to protection of the data is executed on the server where the database operates.

## **İNFORMASIYA TƏHLÜKƏSİZLİYİNİN TƏMİNATINDA SÜNİ İNTELLEKTİN ROLU**

**E.N. İsrailova, A.M. Mustafayeva, A.M. Abdurrahmanova**

Mingəçevir Dövlət Universiteti, Mingəçevir, Azərbaycan

e-mail: [elmira.israfilova@mdu.edu.az](mailto:elmira.israfilova@mdu.edu.az), [aida.mustafayeva@mdu.edu.az](mailto:aida.mustafayeva@mdu.edu.az)

[asuda.abdurrahmanova@mdu.edu.az](mailto:asuda.abdurrahmanova@mdu.edu.az)

Dünyamızın informasiyalaşdırma yolu ilə fəal şəkildə irəliləməsi bəşəriyyət qarşısında, bir tərəfdən, yeni heyrətamiz imkanlar açır, digər tərəfdən isə, əvvəllər məlum olmayan yeni risklər yaradır. İnformasiya texnologiyalarının meydana gəlməsi nəticəsində bəzi insani qüsurlar, xüsusilə də şəxsi və ya kommersiya sirrinin pozulması ilə bağlı qüsurlar, yeni formalar alır, bu isə yeni müdafiə üsullarının yaradılmasını tələb edir.

Süni intellekt (Sİ) və maşın öyrənmə texnologiyalarının kibercinayətlərdən mühafizə sistemlərində istifadə edilməsi informasiya təhlükəsizliyinin əsas istiqamətlərindən birinə çevrilir. İnformasiya texnologiyaları mühitində insanlar və maşınlar arasında artan rəqabət, informasiya təhlükəsizliyi nöqtəyi-nəzərindən, daha çox diqqət mərkəzindədir. Lakin burada bir sıra suallar yaranır. İnformasiya təhlükəsizliyində Sİ geniş tətbiq tapıbmı? İnformasiya təhlükəsizliyinin təmini məsələlərində Sİ daha çox hansı sahələrdə istifadə olunur? Sİ texnologiyalarını kibercinayətkarlar öz məqsədləri üçün istifadə edə bilərmə? Bu sahədə istifadə olunan Sİ texnologiyalarının səhv etmə ehtimalı varmı? Bu suallara cavabların alınması aparılan tədqiqatın məqsədidir.

İnformasiya təhlükəsizliyi sahəsində Sİ-in tətbiqi 2000-ci illərin əvvəlində kifayət qədər sadə işlərdən başlayıb. O zaman zərərli faylların nümunələrinin sayı o qədər artmışdır ki, əl ilə və ya sadə avtomatlaşdırılmış təhlil əsasında məsələnin həlli mümkün deyildi. Nəticədə Sİ-in tətbiqi ilə virus analitiklərinin işini asanlaşdıran sistemlər qurulmuşdu. Həmin sistemlər zərərli kodda oxşarlıqları aşkarlayır və minimal əsilliyin təyin edilməsinə imkan verirdi. Müəyyən informasiya əsasında revers-mütəxəssislər və virus analitikləri bu və ya digər zərərli proqram təminatının təsnifatını aparırdı. Əslində, bu klasterləşmə və Big Data ilə (böyük məlumatlarla) iş idi [1].

Hazırda şəbəkədə yeni təhdidləri qeyd edə biləcək və ya hücumları proqnozlaşdıran böyük həcmdə informasiyanı təhlil edən qlobal şirkətlər mövcuddur. Bu şirkətlər verilənlər massivlərini

toplayan, Sİ texnologiyası ilə təhlil edən, qanunauyğunluqları aşkarlayan, verilənlərin klasterləşdirilməsini aparan və təhdidləri proqnozlaşdıran sistemlərə malikdir. Belə texnologiyalar olmadan böyük həcmli informasiyanın emalı praktiki olaraq mümkün deyil. Təbii olaraq burada neyron şəbəkələr və klasterləşmə çox geniş istifadə olunur. Sİ həmçinin açıq və qapalı mənbələrdən toplanmış verilənlərə görə təhdidlərin izlənilməsində fəal şəkildə tətbiq olunur. Beləliklə, informasiya təhlükəsizliyi sahəsində Sİ-in vəzifələri və tətbiq sferası son iki onillikdə artıb. Süni intellekt – kibertəhdidlərdən qorunmaq üçün effektiv bir köməkçidir [2]. Lakin Sİ, ilk növbədə, texnologiyadır və o, sistemlərin və məhsulların işlənməsi üçün tətbiq olunan texnologiyadır. Bu tip texnologiyalara maşın öyrədilməsi və kompüter görməsi, koqnitivistika, təbii dildə mətnlərin emalı, dərin öyrətmə və s. aiddir. Bu texnologiyalar bir çox sahələrdə istifadə olunur. Öz növbəsində, müxtəlif təyinatlı məhsullar daha səmərəli işləmək üçün Sİ texnologiyalarına müraciət edir.

Yüksək Texnologiyalar sənayesi bu gün Sİ texnologiyalarından istifadə edən çox sayda sistemlər təklif edir. Süni intellektin ümumi qəbul olunmuş tərifinə olmasa belə, hazırda bu sistemlər qlobal olaraq iki növə ayrılır: qərar qəbul edən sistemlər və qərarların qəbul edilməsinə dəstək sistemləri. Süni intellekt sinifinə böyük məlumatları emal edən sistemlər də daxildir. Bu məlumatların təhlili müəyyən qanunauyğunluqları və ya anomaliyaları aşkar etməyə imkan verir.

Təhlükəsizlik tələb olunan hər yerdə Sİ-nin istifadəsi müvafiq problemlərin həllində üstünlük təşkil edir. Məsələn, maliyyə sahəsinin müdafiəsində Sİ çox geniş tətbiq tapıb və öz effektivliyini sübut edib. Prinsipcə, təhlükəsizlik sistemləri bütün sahələrdə istifadə olunur, sadəcə olaraq Sİ texnologiyalarından istifadə etdikləri zaman bu sistemlər daha çox fayda verir [3].

İnformasiya təhlükəsizliyi sistemlərinə Sİ-in tətbiq edilməsi biznesin böyüklüyündən və ya kiçikliyindən asılı deyil. Məsələn, anomaliyaların aşkarlanması həm böyük, həm orta, həm də kiçik biznes üçün aktualdır. Mühafizə minimal səviyyədə belə hər zaman qurulmalıdır. Müasir dünyada təcavüzkarlar yalnız böyük məqsədləri deyil, kiçik şirkətləri, eləcə də fərdi istifadəçiləri də hədəfə alıb. Buna görə müasir təhlükəsizlik sistemlərinin və Sİ texnologiyalarından istifadə edən sistemlərin aktuallığı getdikcə artır. Prinsipcə, belə bir asılılığı qeyd etmək olar: təşkilata qoyulan təhlükəsizlik tələbi nə qədər ciddidirsə, həmin təşkilat üçün Sİ texnologiyalarının tətbiqi bir o qədər yüksəkdir. Təbii ki, təşkilatın rəqəmsallaşdırma səviyyəsi nə qədər yüksəksə, onun rəqəmsal aktivləri nə qədər çoxdursa, o, daha çox məlumat hasil edir və dəqiq emal olmadan onun mühafizəsi bir o qədər çətinləşir. Məhz bu zaman Sİ texnologiyalarının istifadəsi qaçılmazdır. Qlobal təhlükəsizlikdən, yəni bütöv sahələr və ya bütün dünya miqyasında təhdidlərin müəyyən edilməsindən söhbət getdikdə isə, süni intellekt, ümumiyyətlə, keçinmək mümkün deyil.

Qeyd etmək lazımdır ki, informasiya təhlükəsizliyi sistemlərində istifadə olunan Sİ-nin səhv qərar qəbul etmə ehtimalı da vardır. Müasir maşın öyrənməsi bir çox alqoritmlərdən ibarətdir. Belə ki, neyroşəbəkələrə bir çox ardıcıl maşın öyrənmə alqoritmləri daxildir. Parametrləri nəzərə almaqla əvvəlcə elə bir ardıcılıq, alqoritmlər dəsti təyin olunmalıdır ki, mümkün qədər az səhvlər olsun. Neyron şəbəkələr üçün hər hansı bir maşın öyrənmə texnologiyasının tətbiqi müsbət və mənfi cəhətlərə malikdir. Müsbət cəhəti alqoritmlərə əl ilə əlavələr etmədən işləməsi və məsələnin həllini daha çox resurs xərci olmadan mümkün etməsidir. Mənfi cəhət ondan ibarətdir ki, standart alqoritmik

sistemlərdən fərqli olaraq, yaranmış səhvin mənbəyini tapmaq və onu düzəltmək çox çətindir. Neyroşəbəkənin bir yerdə düzgün, digərində isə səhv reaksiya verməsinin səbəbinin təyin edilməsi çox çətindir. Məhz bu məqam maşın öyrənməsinə əsaslanan mühafizə sistemlərinin istismar xüsusiyyətini təşkil edir [4].

Sİ böyük üstünlüklər verir, buna görə təcavüzkarlar onu öz məqsədləri üçün daha səmərəli istifadə edirlər, bu texnologiyalara fəal yiyələnirlər. Hakerlər tərəfindən maşın öyrənmə texnologiyalarının istifadəsinin ilk nümunəsi, skriptlərə və botlara qarşı qorunmaq üçün lazım olan “kapça”dan (kompüterləri və insanları fərqləndirmək üçün tam avtomatlaşdırılmış açıq Turing testi) uğurla keçməsidir. Maşın öyrənmə texnologiyaları həm şəkillərin hasili, həm də onların tanınmasına imkan verir. Kibercinayətkarlar tərəfindən Sİ-nin tətbiqinin yeni bir nümunəsi leqal istifadəçilərin impersonifikasiyası, yəni digər istifadəçi adından kodun yerinə yetirilməsi üçün səs və videonun hasilidir. Ümumiyyətlə, səs saxtalaşdırılması texnologiyası bir müddətdir ki mövcuddur. Maşın öyrənməsi cinayətkarlara yeni imkanlar yaradır, bu səbəbdən də bu cür avtorizasiya artıq tamamilə etibarlı hesab edilə bilməz. Beləliklə, Sİ-nin tətbiqi texnologiyaları kibercinayətkarların öz maraqları naminə istifadə etdikləri əsas vasitələrdən birinə çevrilmişdir [5].

Gələcəkdə süni intellekt texnologiyaları əsasında informasiya təhlükəsizliyi sistemləri yeni imkanlarla zənginləşəcək. Qlobal səviyyədə şirkətləri və bütün sahələri yeni təhlükələrə hazırlayan sistemlər inkişaf edəcək. Böyük ehtimalla təşkilatın bütün təhlükəsizlik sistemlərini birləşdirən süni intellekt texnologiyaları bir insanın iştirakı olmadan hadisələrin hərtərəfli təhlilini aparıb, potensial təhlükələrin qarşısını almaq üçün qərarlar qəbul edəcək. Bir müddət sonra, təhlükəsizliyin təmin edilməsi mərkəzlərində insanın iştirakı minimuma endiriləcək, yəni funksiyaların əksəriyyətini kompüter öz üzərinə götürəcəkdir.

**Açar sözlər:** informasiya təhlükəsizliyi, süni intellekt, neyron şəbəkə, maşın öyrənməsi.

### Ədəbiyyat

1. Шабанов А. Применение технологий искусственного интеллекта в информационной безопасности <https://www.anti-malware.ru>
2. Фишман А. Искусственный интеллект: возможности и угрозы <https://www.it-world.ru>
3. Какие отрасли искусственный интеллект изменит до неузнаваемости? <https://nangs.org/news/it>
4. Рассел С., Норвиг П. Искусственный интеллект: современный подход. Изд-во Williams, 2019, 1480 с.
5. Кибербезопасность 2019-2020. Тренды и прогнозы <https://www.ptsecurity.com>

### **The role of artificial intelligence in ensuring information security**

In the context of information security in recent decades, the tasks and application spheres of artificial intelligence have increased rapidly. Such a rapid increase in the role of artificial intelligence in the field of information security makes it necessary to analyze a wide range of issues related to its application in this area. The purpose of the research work is to investigate these issues.

## IMPROVEMENTS ON POLYNOMIAL MULTIPLICATION IN NTRU PRIME

Melike Karatay<sup>1</sup>, Erdem Alkim<sup>2</sup>, Urfat Nuriyev<sup>1,3</sup>

<sup>1</sup>Ege University, İzmir, Turkey

<sup>2</sup>Dokuz Eylül University, İzmir, Turkey

<sup>3</sup>Institute of Control Systems of ANAS, Baku, Azerbaijan

e-mail: [karataymlk9@gmail.com](mailto:karataymlk9@gmail.com), [erdemalkim@gmail.com](mailto:erdemalkim@gmail.com)

[urfat.nuriyev@ege.edu.tr](mailto:urfat.nuriyev@ege.edu.tr)

The cryptographic protocols that are used today are mostly based on hard problems such as Factorization and discrete logarithm. In 1994, P. W. Shor proposed an algorithm to solve these problems in polynomial time in quantum computers [7]. Because of the recent development on building big enough quantum computers, the National Institute of Standards and Technologies (NIST) in the United States started a project to standardize new cryptographic protocols that should be secure enough even after quantum computers are used to solve underlying problems [3]. After 4 years of progress in the project, 7 candidates were selected as finalists [6]. From the beginning, the implementation performance was one of the main considerations of the project [3, 6], hence this paper proposes an improvement on the implementation of the NTRU Prime key encapsulation mechanism (KEM) [2] which is one of the finalists. NTRU Prime's key generation, encapsulation and decapsulation algorithms are given in Algorithm 1., 2., and 3..

|  |  |
|--|--|
| Algorithm 1 . NTRU LPRime Key Generation: LPRKeyGen()                            |  |
| Output: $Return ((S, A), (a, S, A, p))$ .  |  |
| 1: $s \xleftarrow{S} Seeds$  | 5: $A \leftarrow Round(aG)$                    |
| 2: $G \xleftarrow{S} Generator(S)$ ,   | 6: $p \leftarrow Short$                        |
| 3: $a \leftarrow Short$  | 7: $Return (S, A, (a, S, A, p))$               |
| 4: $aG \leftarrow a \cdot G \in R/q$   |  |
| Algorithm 2 . NTRU LPRime Encapsulation: LPREncap(S,A)                           |  |
| Input: $pk = (S, A)$   |  |
| Output: $C = (C, HashSession(1, r, C))$ .  |  |
| 1: $r \xleftarrow{S} \{0,1\}^l$  | 6: $c \leftarrow Round(bG)$                    |
| 2: $G \leftarrow Generator(S)$ ,   | 7: $T \leftarrow Encode(bA, r)$                |
| 3: $b \leftarrow HashShort(r)$   | 8: $C \leftarrow (c, T, HashConfirm(S, A))$    |
| 4: $bG \leftarrow b \cdot G \in R/q$   | 9: $return (C, HashSession(1, r, C))$          |
| 5: $bA \leftarrow b \cdot A \in R/q$   |  |
| Algorithm 3 . NTRU LPRime Decapsulation: LPRDecap(C, (a,S,A,p))                  |  |
| Input: $C = (c, T, \gamma)$ , $sk = (a, S, A, p)$                                |  |
| Output: $HashSession(1, r, C)$ if $C' == C$ , otherwise $HashSession(0, p, C)$ . |  |
| 1: $aB \leftarrow a \cdot c \in R/q$   | 7: $c' \leftarrow Round(bG')$                  |
| 2: $r' \leftarrow Decode(aB, T)$   | 8: $T' \leftarrow Encode(bA', r')$             |
| 3: $G \leftarrow Generator(S)$   | 9: $C' \leftarrow (c', T', HashConfirm(S, A))$ |
| 4: $b' \leftarrow HashShort(r')$   | 10: $return (C == C)$                          |
| 5: $bG' \leftarrow b' \cdot G \in R/q$   | $? HashSession(1, r', C)$                      |
| 6: $bA' \leftarrow b' \cdot A \in R/q$   | $: HashSession(0, p, C)$                       |

NTRU Prime KEM is using a polynomial ring for its arithmetic operations which is in the form of  $R/q = \mathbb{Z}_q/(X^p - X - 1)$ . The authors proposed different  $p$ 's and  $q$ 's for different security considerations. Recently, Alkim et al compared different optimizations on the implementation of the protocol and demonstrated their results in a selected parameter set of NTRU Prime scheme [1]. The main optimization they proposed was to perform polynomial multiplication in a bigger ring that can allow them to use Number Theoretic Transform (NTT) to reduce multiplication complexity. They showed that if they can perform multiplication in  $\mathbb{Z}_{q'}/(X^n - 1)$  where  $n > 2p$  and a proper  $q'$  exist, then they can improve implementation efficiency by performing multiplications in this ring and perform additional polynomial reduction after multiplication.

In this paper, we show that instead of performing multiplication in  $\mathbb{Z}_{q'}/(X^n - 1)$ , one can use much smaller two rings namely  $\mathbb{Z}_{q'}/(X^m - 1)$  and  $\mathbb{Z}_{q'}/(X^m - c)$  where  $m > p$  then construct the desired result in  $\mathbb{Z}_q/(X^p - X - 1)$ . It can be seen that if the input polynomials  $a$  and  $b$  has a degree less than  $m$ , then  $(1/(c - 1)) \times ((a \times b \bmod X^m - c) - (a \times b \bmod X^m - 1))$  gives the coefficient of  $X^m$  to the  $X^{2p-2}$  of the resulting polynomial. Then one can compute the first  $m$  coefficients of the resulting polynomial with subtracting them from the multiplication modulo  $X^m - 1$ . This observation let us compute the result of  $a \times b$  with computing two multiplications in two different polynomial rings. The multiplication in  $\mathbb{Z}_{q'}/(X^m - 1)$  is a natural candidate of NTT based multiplication. On the other hand, to be able to use NTT based algorithm in  $\mathbb{Z}_{q'}/(X^m - c)$  we need to find  $m$ th root of  $c$  in  $\mathbb{Z}_{q'}$  but unlike NTT this root doesn't need to be a primitive root [5].

Since we would like compare our results with [7], where only  $q = 4591$ ,  $p = 761$  is implemented, we select their  $\mathbb{Z}_{4591}/(X^{1620} - 1)$  implementation. The implementation uses degree 270 NTT and 6-degree polynomial multiplications instead computing the NTT all the way down to the coefficient-wise multiplication. This technique, called in-complete NTT, used in efficient implementation of lattice-based cryptography [4]. Then we reduced NTT degree to 135 to perform multiplications in  $\mathbb{Z}_{4591}/(X^{810} - 1)$  and  $\mathbb{Z}_{4591}/(X^{810} + 1)$  since the degree of the NTT is an odd number  $-1^{135} = -1$ .

Performing two halved size NTT's instead of one big NTT has actually no performance implications since the first layer of the NTT can be seen as the preparation of the polynomial in both rings and then other layers have exactly same amount of calculations. But if one can find  $m$ -th root of  $c$  with a small order, then one can remove multiplication with 1 to increase efficiency of the multiplication and reduce memory usage. For an odd degree NTT, we were able to use -1 for  $c$ . Hence the preparation of the polynomials requires only 405 multiplication with -1 instead 810 multiplication with arbitrary numbers modulo  $q$ . In addition to this, the implementation uses signed integers, thus multiplication with -1 doesn't require any modular reduction.

In Table 1, the performance results for ntrulpr761 is given for our implementation and the results from [1]. Since we are computing a smaller degree NTT, our method needs to precompute 399 integers in modulo  $q$  while the old method requires 801 integers are precomputed in modulo  $q$ . Results show that for selected parameter the proposed method is %4 faster in polynomial multiplication which

yields about %3 faster implementations for all tree steps of key encapsulation mechanism, namely key generation, encapsulation and decapsulation.

**Table 1.** Cycle counts for selected primitives on ARM Cortex M4 microprocessor

| ntrulpr761 | Polymul | KeyGen | Encap   | Decap   |
|------------|---------|--------|---------|---------|
| [1]        | 185010  | 752560 | 1348563 | 1479239 |
| Our work   | 178961  | 746507 | 1338070 | 1462565 |

For simplicity, we have selected one of the most simple implementation in [1], but, including the other mixed radix implementation in their paper there are number of other parameters we think our method can improve implementation efficiency. We left those implementations as a future work.

**Keywords:** Lattice-based Cryptography, NTT, NTRU Prime.

### References

1. Alkim E., Cheng D.Y.L., Chung C.M.M., Evkan H., Huang, L.W.L., Hwang V., ... & Yang B. Y. (2021). Polynomial Multiplication in NTRU Prime. IACR Transactions on Cryptographic Hardware and Embedded Systems, 217-238.
2. Bernstein D.J., Chuengsatiansup C., Lange T., & van Vredendaal C. (2019). NTRU Prime: round 2. Post-Quantum Cryptography Standardization Project. NIST.
3. Chen L., Chen L., Jordan S., Liu Y.K., Moody D., Peralta R., ... & Smith-Tone D. (2016). Report on post-quantum cryptography (Vol. 12). US Department of Commerce, National Institute of Standards and Technology.
4. Chung C.M.M., Hwang V., Kannwischer M.J., Seiler G., Shih C.J., & Yang B.Y. (2021). NTT Multiplication for NTT-unfriendly Rings. IACR Transactions on Cryptographic Hardware and Embedded Systems, 159-188.
5. Crandall R., Fagin B. (1994). Discrete weighted transforms and large-integer arithmetic. Mathematics of computation, 62(205), 305-324.
6. Moody D., Alagic G., Apon D.C., Cooper D.A., Dang Q.H., Kelsey J.M., ... & Alperin-Sheriff, J. (2020). Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process.
7. Shor P.W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). IEEE.

## MACHINE LEARNING APPLICATIONS FOR ANOMALY DETECTION

Melike Karatay<sup>1</sup>, Emrah Emirtekin<sup>1</sup>

<sup>1</sup>Ege University, İzmir, Turkey

e-mail: [karataymlk9@gmail.com](mailto:karataymlk9@gmail.com), [eemirtekin@gmail.com](mailto:eemirtekin@gmail.com)

**Abstract.** The rapid development of technology causes the rapid development of many problems as well as the advantages it provides to people. Cyber security vulnerabilities are at the forefront of these problems. Any vulnerability in cyber security creates great threats to systems. Intrusion detection or prevention systems (IDS/IPS) are created to prevent cyber attacks. IDS/IPS can be signature-based or anomaly-based. While anomaly-based intrusion detection systems are frequently used to protect cyber mechanisms, these systems are developed using either machine learning or deep learning. In this paper, machine learning and deep learning models that benefit from IDS/IPS developed to detect anomalies in a cyber system were investigated.

### 1 Introduction

We use electronic device technologies in almost all of our daily lives. Mobile phones, computers and smart homes, which are now a part of our lives, can be given as examples of these technologies. In addition to making our lives easier, these technologies are all connected to the Internet and cyber threats are increasing day by day on devices connected to the Internet. Intrusion detection or prevention systems (IDS/IPS), firewall and vulnerability scanners have been developed to prevent cyber attacks.

Even if we think that all measures are taken to protect against cyber attacks, cyber attacks are developing day by day with technology. Intrusion Detection or Prevention Systems are the name given to security technologies created to detect and prevent these cyber attacks. In order for IDS/IPS to understand that an incoming attack is an attack, this attack must have been made before. For this reason, it may not prevent newly created attacks. In order to prevent this, with the development of machine learning and deep learning methods in recent years, machine learning and deep learning methods are frequently used in IDS/IPS.

The aim of this work is to examine machine learning and deep learning models used in cyber attack prevention systems such as IDS/IPS. When machine learning and deep learning methods are used, inferences are made about the efficiency of the systems used to prevent cyber attacks. After, it was compared with systems that do not use machine learning and deep learning.

### 2 Anomaly detection

Identification of rare items, events, or observations that raise suspicion by differing significantly from most anomaly data. According to [1], it is defined as the detection of those that are significantly different from other observations in the sample, while according to [2] it is defined as observations that do not conform to the data set characteristic and deviate significantly from other

observations in the data set. In the literature, anomalies are also known as outliers, novelties, noises, deviations and exceptions. Anomaly can also be defined as the patterns in the data that appear infrequently in a certain period, contain different features, carry a certain meaning, and do not conform to a well-defined concept of normal behavior. There may be deviations from the normal during the process. The reason for this is the abnormal situations encountered. These deviations cause observations to be obtained that are different from the expected observation value. Basically, we can express the problem as follows; the lack of a definition that allows us to evaluate how similar two data points are, and it is unknown how a data point differs from other points in the data set.

Since removing the outliers that negatively affect the quality of the data set from the data set will be important for the reliability of the results of the statistical analyzes to be performed, it is necessary to correctly identify the outliers in the data set and remove them from the data set [3]. Today, it has become very easy to detect anomalies in large data sets as of the point where technology has come. However, although abnormal conditions are rarely observed, they can have negative consequences when they occur. Examples include credit card fraud, cyber-attack, terrorist activities, or disruption of a system. The more important the technology is in preventing the situations in the samples, the more important the methods and techniques used in anomaly detection are. In general, machine learning and deep learning methods are used extensively in anomaly detection.

### **3 Use of machine learning in anomaly detection**

Most of the new systems proposed in the literature for detecting cyber attacks or problems are artificial intelligence-based anomaly detection systems. Anomaly detection in networks often uses behavioral artificial intelligence algorithms. In other words, networks are monitored for a long time and then anomaly situations occurring on the network are detected by these software. To summarize the relationship between cyber security and anomaly detection, artificial intelligence, which learns all the behaviors on the cyber network, maps the system and automatically detects and calculates the risks of network anomalies bypassing the firewall or antivirus software in the slightest anomaly behavior that is not suitable for the operation of the system. notify the system administrator.

While detecting anomaly on a cyber network, trace records (LOG), packets and streams are examined. While examining these flows, zero-day attacks and bot network detection, which normal security systems cannot do, can be detected by anomaly detection systems. In such attacks, as in other cyber attacks, the anomaly detection system generates an alarm to the system administrator.

Cyber security is an important issue in every area where the internet is used. For this reason, anomaly detection is a technology that we need in every part of our lives. For example, anomaly detection occupies an important place in terms of the safety and efficiency of industrial processes. Machine learning methods are frequently used to make anomaly detection fast and safe. Decision trees, a machine learning method used in anomaly detection, are suitable for use in industrial applications [6].

Another area where anomaly detection is used is the Internet of Things (IoT), as mentioned at the beginning. Anomaly detection methods are frequently used in the field of the Internet of Things.

In this area, anomaly detection in the environments is made using especially LSTM-based models [4]. Such machine learning-based systems also assist in correcting errors in anomaly detection. Of course, the accuracy and cleaning of the data set makes machine learning methods work more accurately. In general, when the recent studies are examined, the use of machine learning methods for anomaly detection is especially on wireless technologies and IoT. In machine learning methods, almost all methods, specially artificial neural networks and decision trees, have been used in anomaly detection.

In addition to machine learning methods used to detect anomalies, deep learning methods are also frequently used. In recent years, there are many studies on this subject [5]. Developments in deep learning methods have also improved the use of deep learning in anomaly detection. Anomaly detection systems created by using deep learning methods now work much more accurately and efficiently [7].

**Conclusion.** It is pointless to rely only on methods such as firewall or IDS/IPS in cyber systems. For this reason, it is recommended to get support from other systems in order to detect anomalies in the systems and to use these protection methods together if necessary. Another solution is to trust that the system used is truly reliable. In addition to reliability, the system used must perform well. With the development of machine learning and deep learning methods, the use of machine learning and deep learning methods for anomaly detection is a very popular application.

**Keywords :** Deep Learning, Machine Learning, Anomaly Detection.

### References

1. Grubbs F.E. (1969). Procedures for detecting outlying observations in samples. *Technometrics*, 11(1), 1-21.
2. Hawkins D.M. (1980). *Identification of outliers* (Vol. 11). London: Chapman and Hall.
3. Leroy, A.M., & Rousseeuw, P.J. (1987). *Robust regression and outlier detection*. Wiley series in probability and mathematical statistics.
4. Liu Y., Pang Z., Karlsson M., Gong, S. (2020). Anomaly detection based on machine learning in IoT-based vertical plant wall for indoor climate control. *Building and Environment*, 183, 107212.
5. Pang, G., Shen, C., Cao, L., & Hengel, A. V. D. (2021). Deep learning for anomaly detection: A review. *ACM Computing Surveys (CSUR)*, 54(2), 1-38.
6. Quatrini, E., Costantino, F., Di Gravio, G., & Patriarca, R. (2020). Machine learning for anomaly detection and process phase classification to improve safety and maintenance activities. *Journal of Manufacturing Systems*, 56, 117-132.
7. Wang, R., Nie, K., Wang, T., Yang, Y., & Long, B. (2020, January). Deep learning for anomaly detection. In *Proceedings of the 13th International Conference on Web Search and Data Mining* (pp. 894-896).

## NEW NUMBER SYSTEM, ITS CRYPTOGRAPHY AND DATA COMPRESSION APPLICATIONS

**N.A. Khankishiyeva**

Ege University, İzmir, Turkey

e-mail: [nargizkhankishiyeva@gmail.com](mailto:nargizkhankishiyeva@gmail.com)

### I. Number Systems

Number systems are divided in two categories:

- 1) **Non-positional:** In this type of number system a value of the symbols doesn't depend on their positions: Maya, Roman, Kaktovik, Cystercian numerals
- 2) **Positional:** In this type of number system a value of the symbols depends on their positions: Babylonian, Decimal, Binary, Octal, Hexadecimal number system and so on.

### II. The New Number System (Nuriyev Number System)

The number system  $N^k$  ( $k = 1, 2, \dots$ ) proposed below is non-positional number system.

There is no zero in this system. Here  $k$  is the base. There is only one one-digit number in  $N^1$  for

$k=1$ : 1. Here '0' means '1+'.  $(1)_N^1 = 1$ ,  $(0)_N^1 = 1+$ ,  $(01)_N^1 = 1 + 1 = 2$ ,  $(001)_N^1 = 1 + 1 + 1 = 3 \dots$  Numbers are represented in  $N^2$  ( $k=2$ ) system like following:  $(01)_N^2 = 1_{10}$ ,  $(10)_N^2 = 2_{10}$ ,  $(11)_N^2 = 3_{10}$ ,  $(00)_N^2 = (3+)_{10}$ ,  $(0001)_N^2 = 4_{10}$ ,  $(0010)_N^2 = 5_{10}$ ,  $(0011)_N^2 = 6_{10}$ ,  $(0000)_N^2 = (6+)_{10}$ . In this way all numbers can be described in  $N^k$  system. As a result, the general formula for the numbers in  $N^k$  system [1] is:

$$\left( \underbrace{\underbrace{0 \dots 0}_k \underbrace{0 \dots 0}_k \dots \underbrace{a_{k-1} \dots a_0}_k}_{m} \right)_N^k = \left( \left( \frac{m}{k} - 1 \right) \cdot (2^k - 1) + (a_{k-1} \cdot 2^{k-1} + \dots a_1 \cdot 2^1 + a_0) \right).$$

### III. Arithmetic operations on the new number system

**Addition:** Let's add two numbers with the length of  $l$  and  $m$ . Addition process is done by dividing the numbers by  $k$  places.

- a) First, let's look at the bits above and below in the first  $k$  digits and the carry number on them: If both are 0, let's write 0 below and move on. If both are 0 and there is a carry, or one is 0 and the other is 1 and no carry, then write 1 and continue. If both are 1 and there is no carry, or one is 1 and the other is 0 and there is one carry, then write 0 down and give one carry for the next digit. If both are 1, and the carry is one bit then write one below and add one carry to the next digit.
- b) For the  $(k+1)$ th digits let's look at the bits above and below and the carry number on them: If both are 0 and have a carry, or one is 0 and the other is 1 and no carry, then write  $k$  bits of zeros and add  $(\underbrace{00 \dots 0}_k 1)$  to the previous  $k$  digits and continue. If one is 1 and the other is 0 and there is a carry,

then add  $2k$  of zeros below and add  $(\underbrace{00 \dots 0}_k 1)$  twice to the previous  $k$  digits and continue.

c) Let's look at the zero bits above and below in the next  $k$  digits: If both are zero, let's add two zeros. If one is zero and other is absent, let's add a zero.

**Subtraction:** Let's say we need to subtract a number (length  $m$ ) from a number (length  $l$ ). Subtraction is done by dividing the numbers into  $k$  digits. a)

In the first  $k$  digits let's look at the bits above and below: If both are 0, write 0 to the result and continue. If there is 1 above and 0 below, 1 is written below. If there is a 0 above and 1 below, then 1 is written to the result and one bit is subtracted from the next bit of minuend.

b) In the next  $k$  digits: the above and below bits are checked, if both are 0, nothing is written below. If the bit above is 0, if there is no bit below, write 0 to the result and continue. If there is 1 to be subtracted from the previous operation,  $k$  zeros are subtracted from minuend and  $(\underbrace{00 \dots 0}_k 1)$  is

subtracted from the result in  $k$  digits.

**Multiplication:** Let's multiply two numbers of length  $l$  and  $m$ . Let's call the result product. Except the first  $k$  digits, the zeros of multiplicand and multiplier are replaced by 1 bit. a)

First, look at the bits above and below. Every bit of the number below is taken and multiplied by all bits of the number above. The result of each multiplication is written by shifting one bit to the left.

Due to do addition operation the product is divided into  $k$  bits column. Then starting from the left column, the addition process is done one under the other. Addition is done separately for each column.

If there  $k$  of 1 in the columns those are replaced with  $k$  of zeros and  $k$  of zeros added to the product.

b) After the addition process is completed within the column, if there is any carry, the carry is added to the result in the same column and the addition process is continued until the carry is 0, and  $k$  of 0 are added to the product each time as much as the carry ones.

If the carry is 0, the value found at the end of the column is added to the next column and  $k$  of 0 is added to the product by the same value.

If the result of the operation in the column is  $k$  of 1,  $k$  of 0 is added to the product. The last result found in the last column is written to the multiplication as it is.

**Division:** Division on the new number system is done with the following algorithms: Suppose that a number with the length of  $l$  need to be divided by the number with the length of  $m$ .

$\underbrace{0 \dots 0}_k \underbrace{0 \dots 0}_k \dots \underbrace{a_{k-1} \dots a_0}_k$  is dividend and  $\underbrace{0 \dots 0}_k \underbrace{0 \dots 0}_k \dots \underbrace{b_{k-1} \dots b_0}_k$  is divisor.

a) Except of the first  $k$  digit of the divisor and dividend number, zeros are replaced by 1. Division starts from the left and progresses in each step by the length of the divisor.

b) Since the numbers consist of 0 and 1, the quotient is either 1 or it doesn't exist. If there is a divisor in the first  $m$  digits, 1 is written to the quotient and if it is still greater than the divisor in the same  $m$  digits the division process is continued, and the quotients are added to each other. If there is any remaining after the  $m$ -step operation is done, it is added to the last digit.

#### IV. New number system's applications

**Nuriyev Data Compression:** For the compression of binary images, coding methods have been developed that enable the data image to be expressed with fewer bits. One of these methods is

NDC [2]. The basis of this method is based on coding the frequency numbers of the repeated data by writing the equivalent of this numbers in the NNS [1]. The application of this number system in data compression is given in paper [2].

**Cryptology:** It is the science that encrypts and sends information according to a certain rule in order to ensure a secure flow of information between two institutions. One of these encryption methods was proposed by Nuriyev et al [3]. Encryption scheme: This scheme consists of repeatedly encoding the repeated bit numbers of information in different bases of the NNS number system. For example, if encryption is done in the number systems, respectively, the encryption/decryption key would be 324. This key is sent to the other party securely with the RSA encryption scheme. Detailed information about this encryption method is given [3].

**Keywords:** NNS number system, Cryptology, Data Compression.

### References

1. Nuriyev U., Nuriyeva F., Sadık T., On a New Number System, Proceeding of the International Conference on Computer Science and Engineering, (UBMK 2016), Namık Kemal University, Tekirdağ, Turkey, October 20-23, 2016, pp. 825-827.
2. Tanır D., Nuriyeva F., (2017), İkili Görüntülerin Kayıpsız Sıkıştırılması için Yeni Bir Yöntem, International Artificial Intelligence and Data Processing Symposium, Malatya, Turkey, September 16-17, (IEEE Xplore Digital Library).
3. Nuriyeva F., Karatay, M. On the analysis of an encryption scheme, Theoretical and Applied Aspects of Program Systems Development, 04-08 December 2017, Kiev, Ukraine.

## АНТЕННАЯ СИСТЕМА КОМПЛЕКСА ПАССИВНОЙ РАДИОПЕЛЕНГАЦИИ БПЛА

**В.Г. Лихограй, Д.В. Грецких, А. Шербина**

Харьковский национальный университет радиоэлектроники, Харьков, Украина

e-mail: [vasyl.lykhograi@nure.ua](mailto:vasyl.lykhograi@nure.ua)

Беспилотные летающие аппараты (БПЛА, UAV - Unmanned Aerial Vehicles) получили широкое распространение и применение во многих областях человеческой деятельности. Они могут выполнять как целый ряд полезных функций, но также могут нести значительную физическую или информационную угрозу в военной сфере, хозяйственной деятельности или личной жизни человека [1 - 3].

Специфические свойства и преимущества БПЛА - относительно невысокая стоимость, разнообразие выполняемых функций, высокая оперативность подготовки к применению, экономичность и простота в эксплуатации, трудности контроля приводят к повышению безнаказанности и массовости противоправных действий с их использованием.

Актуальной соответствию с этим является задача получения достаточно полной оперативной информации о БПЛА с помощью специальных технических средств и обеспечения высокой скорости и эффективности адекватных действий на возникающие и существующие вызовы и угрозы с их использованием.

В соответствии с этим возникают задачи выявления, оценки координат и параметров движения (в частности оценки угловых координат - пеленга), а также распознавания класса БПЛА по их радио излучению. Современное оборудование радиомониторинга и радиопеленгации должно обеспечивать надежную и точную разрешение на источник радиоизлучения (БПЛА) в диапазонах его рабочих частот (ISM 2400 МГц). Одним из важнейших элементов системы радиомониторинга и радиопеленгации является его антенная система (АС).

Итак целью работы является разработка пеленгационной АС диапазона ISM 2400 МГц для работы в составе комплексов пассивной радиопеленгации БПЛА.

Современные БПЛА имеют небольшие размеры, а значит низкий уровень заметности: они изготавливаются из композитных материалов, имеют малую эффективную поверхность рассеивания в радиодиапазоне, их двигатели излучают мало тепла. Соответственно возникают задачи выявления, оценки координат и параметров движения (в частности оценки угловых координат - пеленга), а также распознавания класса БПЛА по их радио излучению.

Информация для обнаружения и последующей пеленгации БПЛА может быть получена путем приема специальными средствами отраженной и излучаемой энергии во всех диапазонах спектра электромагнитных и акустических волн. БПЛА присущи демаскирующие признаки, которые выделяют их в окружающей среде, делая заметными для наблюдения. Степень его заметности определяется в радиочастотном, инфракрасном (ИК), видимом и акустическом диапазонах.

БПЛА могут быть выявлены средствами радиотехнической разведки путем приема и анализа радиосигналов линий связи и управления, радиолокационных высотомеров, постановщиков активных помех и радиолокационных станций. Этим методом можно установить направление на БПЛА. Точность определения повышается при увеличении времени наблюдения. Некоторые НЧ линии связи могут быть обнаружены на значительных расстояниях. Излучения бортовых РЛС и постановка активных помех БПЛА могут быть обнаружены на еще больших расстояниях. Этот метод требует минимального оборудования и позволяет быстро определить пеленг цели при дальнейшей выдачи целеуказания на средства оптического или ИК наблюдения. Большая часть операций радиоуправления БПЛА осуществляется в нелицензируемом ISM диапазоне полос частот 2,4 ГГц или 5,8 ГГц, однако используются и другие полосы частот, включая 433 МГц и 4,3 ГГц.

В качестве примера разработки средств радиоэлектронного обнаружения и подавления БПЛА можно привести примеры станций радиоразведки и постановки помех ARDRONIS фирмы «Rohde & Schwarz», (Германия) [2] и системы пассивной локации БПЛА «Drone Detector» компании «Aaronia» (Германия) [3].

Современные антенные система радиопеленгаторов состоят из нескольких антенных подсистем, в частности пеленгационной АС реализованы как кольцевые антенные решетки (АР), которые имеют многоярусную структуру, где для наиболее оптимальной настройки апертуры антенны под рабочую полосу частот используются широкополосные (ШС) антенные элементы или узкополосные с изменяемой электрической длиной (с реконфигурацией) для антенны мониторинга преимущественно используются ШС антенны.

Антенные системы, используемые в аппаратуре мониторинга БПЛА, должны обеспечивать работу в широкой полосе частот, прием сигналов достаточно низкого уровня для возможности дальнейшей их обработки и возможности обеспечения разрешения с близкими угловым координатам и в то же время иметь приемлемые габариты и массу.

В докладе приведены результаты разработки макета шести элементной кольцевой АР диапазона ISM 2400 МГц для комплекса пассивной радиопеленгации БПЛА (рис. 1).

В качестве антенного элемента кольцевой АР избран микрополосковых патч с линейной поляризацией, настроенный на центральную частоту 2400 МГц. Для управления положением диаграммы направленности в АС использовано антенный переключатель типа BGS16GA14. Период опроса антенных элементов переключателя BGS16GA14, зависит от скорости передвижения БПЛА, направления его перемещения в пространстве, эффективной площади БПЛА, ТТХ приемника и способа обработки сигналов в нем и составляет 2-5 с.

**Keywords:** UAV, ISM, passive radio reconnaissance.

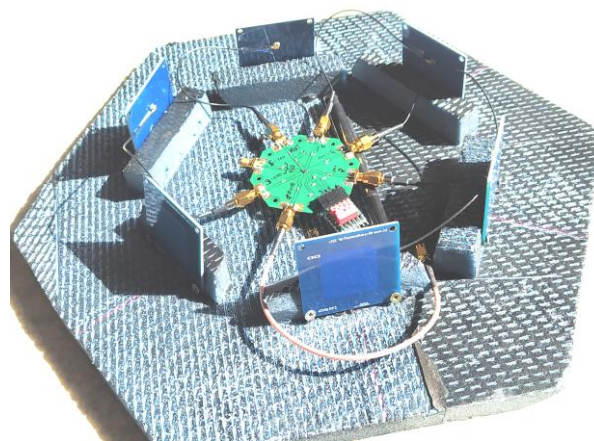


Рис. 1

## References

1. Карташов В.М., Олейников В.Н., Шейко С.А., Бабкин С.И., Корытцев И.В., Зубков О.В. Особенности обнаружения и распознавания малых беспилотных летательных аппаратов. «Радіотехніка» Всеукраїнський міжвідомчий науково-технічний збірник 2018, № 195, с.235-243.
2. Rohde & Schwarz [Электронный ресурс]. – режим доступа: [https://scdn.rohde-schwarz.com/ur/pws/dl\\_downloads/dl\\_common\\_library/dl\\_brochures\\_and\\_datasheets/pdf\\_1/A](https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/A)

[RDRONIS\\_bro\\_ru\\_5214-7035-18\\_v0600.pdf](#) 26.11.2020. Заголовок с экрана: R&S ARDRONIS Противодействие радиоуправляемым дронам.

3. Sernia инжиниринг: Каталог товаров [Электронный ресурс]. – режим доступа: [https://sernia.ru/news/2017/reshenie\\_dlya\\_radionablyudeniya\\_i\\_avtomaticheskogo\\_otslezhivaniya\\_ia\\_traektorii\\_dronov/](https://sernia.ru/news/2017/reshenie_dlya_radionablyudeniya_i_avtomaticheskogo_otslezhivaniya_ia_traektorii_dronov/) 26.11.2020. Заголовок с экрана: Решение для радионаблюдения и автоматического отслеживания траектории дронов

### **Antenna system of UAV's passive radio reconnaissance**

The paper considers the results of development and design of an antenna system in the ISM 2400 MHz band for a UAV passive radio direction-finding complex.

### **АНАЛИЗ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ LPWAN СЕТЕЙ ДЛЯ ПОСТРОЕНИЯ РАДИОЗАКЛАДНЫХ УСТРОЙСТВ**

**Ю.В. Лыков, А.А. Паниотова, А.А. Лыкова, Э.А. Костенко**

Харьковский национальный университет радиоэлектроники, Харьков, Украина

e-mail: [yurii.lykov@nure.ua](mailto:yurii.lykov@nure.ua)

За последнее десятилетие появился ещё один спектр протоколов и технологий, которые отвечают коммуникационным требованиям IoT (Internet of Things) – маломощные глобальные сети (LPWAN). LPWAN для IoT нужен был для замены Wi-Fi, который хорошо закрепился в потребительских сетях, предлагая взамен радиопокрытие на большой площади через базовые станции, а также через механизмы адаптации скорости передачи, мощности передачи, модуляции, рабочих циклов и т.п., оптимизируя очень низкое потребление энергии конечных устройств.

LoRa (LoRa Alliance) або LoRaWAN - один из таких протоколов LPWAN. LoRa нацелен на развертывание конечных устройства имеющих ограниченный источник энергии (например, от батареи), когда не требуется передавать более нескольких байт и где трафик данных может инициироваться или с конца - от устройства (например, когда конечное устройство является датчиком) или сервером, который желает установить связь с конечным устройством (например, когда оконечное устройство является исполнительным механизмом). Особенность LoRa, работающий на дальних расстояниях, делает его интересным кандидатом на технологию передачи в гражданских инфраструктурах (таких как мониторинг состояния здоровья, интеллектуальное измерение, мониторинг окружающей среды и т.д.), в промышленных приложениях, а также может применяться и злоумышленниками для организации канала утечки информации.

Ещё одна популярная технология LPWAN – Sigfox. Первая сеть Sigfox была развернута во Франции в 2012 году, а к 2014 году было обеспечено общенациональное покрытие страны. Политика Sigfox подразумевает предоставление открытой информации о необходимом для

построения сети аппаратном обеспечении (базовых станциях и модулях), при этом программное обеспечение является закрытым и продается операторам как услуга [2]. В настоящее время Sigfox присутствует в более чем 70 странах.

Общее для этих двух технологий является большая дальность действия (до нескольких десятков км на открытой местности и до нескольких км в городе) и хорошая энергоэффективность (работа от батарейки больше года). Данные значения параметров являются одними из основных при выборе технологии при организации технических каналов утечки информации. Для того чтобы оценить сценарии использования LPWAN протоколов в организации каналов утечки информации необходимо определить возможную пропускную способность, которая для обеспечения малого энергопотребления и большой ёмкости сети, значительно ограничена. На рис.1 приведены максимальные значения пропускной способности канала LoRaWAN для различных параметров сообщения.

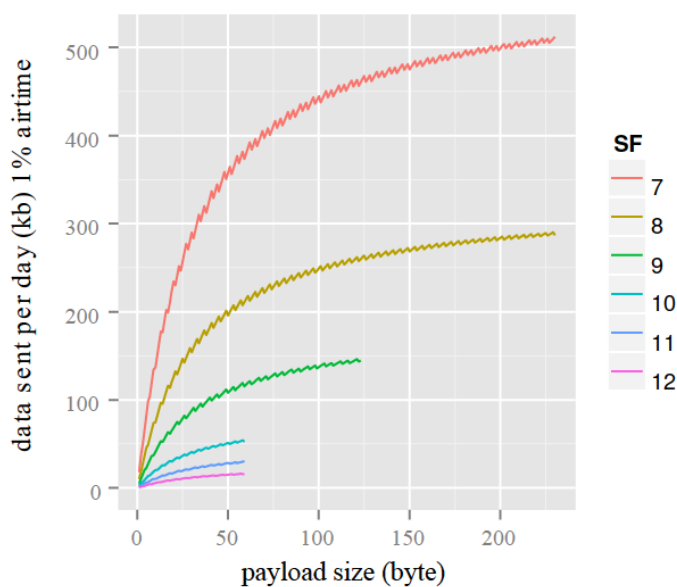


Рисунок 1. Пропускная способность канала для разных значений SF [1]

Следует отметить, что пропускная способность канала получено с учетом ограничения в ЕС ETSI EN300.220 для протокола LoRaWAN на процент времени передачи данных в эфир. Для разных стран это ограничение составляет следующие значения: 0,1%, 1% или 10%. Для Украины и Азербайджана действуют рекомендации CEPT Rec. 70-03 согласно которым процент времени в эфире (*Duty Cycle*) для конечного узла должен составлять не более 1%.

Для протокола Sigfox максимальная пропускная способность в сутки для одного конечного устройства составляет 1.7кВ (140 сообщений по 12 байт).

Пожалуй, наиболее удачным применением технологии LoRaWAN и Sigfox для организации канала утечки злоумышленником будет перехвата текста вводимого потенциальной жертвой на клавиатуре. Путем подмены клавиатуры на такую же с уже установленным закладным устройством злоумышленник сможет перехватить весь текст, вводимый в том числе и пароли. Текстовый трафик генерирующий обычный пользователь в сутки достаточно небольшой (20КБ для 10 страниц текста) и значительно меньше ограничения пропускной способности LoRaWAN канала. При использовании протокола Sigfox возможно передача текста объемом около 1 страницы. Несколько повысить объемы передаваемой текстовой информации можно путем применения алгоритмов сжатия.

Согласно [3] объем файла записи речи в формате .mp3 длиной в 1 минуту со скоростью 56 кб/с составляет 420КВ, такую запись злоумышленник сможет передать по LoRaWAN сети один раз в сутки, не нарушая нормы и не привлекая дополнительное внимание со стороны служб регуляторов в сфере частотного ресурса. Кроме того, при использовании собственного шлюза для обеспечения канала, злоумышленник может и нарушить и эти нормы и выйти на пропускную способность 5МБ / сутки и более.

Дополнительно для уменьшения трафика злоумышленник может использовать VOX (VAS) системы активирующих запись только при наличии голоса. Далее запись оцифровывается и кодируется кодеком (mp3, CELP, Speex или др.) разбивается на равные части с размером 200 байт и передается в эфир. То есть теоретически небольшие аудио файлы можно передавать по сети LoRaWAN и закладное устройство использующее эту технологию может использоваться для подслушивания разговоров.

Возможности протокола Sigfox для организации утечки речевой информации значительно ограничены из-за низкой пропускной способности.

Следует отметить, что каким бы ни было применение сетей LoRaWAN и Sigfox для организации канала утечки информации они имеют следующие преимущества:

- высокая энергоэффективность (большая автономность), что может позволить с одной стороны монтаж закладки еще на этапе реконструкции / ремонта здания, а с другой закладка может иметь малые габариты, так как основным фактором для современной закладки сдерживающим уменьшения габаритов являются элементы питания;

- высокая скрытность в радиозфире, что обусловлено не большой мощностью передатчика (менее 25 мВт)

- значительная длина канала утечки (до нескольких километров в условиях города), что позволит находиться злоумышленнику на безопасном расстоянии от объекта наблюдения.

Поэтому существует реальная опасность применения LPWAN сетей для организации технических каналов утечки информации, требующая разработки мероприятий по предотвращению данной угрозы.

**Ключевые слова:** LPWAN, LORAWAN, SIGFOX, радиозакладное устройство, утечка информации, пропускная способность.

### Литература

1. Blenn N., Kuipers F. LoRaWAN in the wild: Measurements from the things network. arXiv 2017, arXiv:1706.03086.
2. SigFox [(accessed on 19 September 2021)] Available online: <https://iot.ru/wiki/sigfox>
3. Audio codec calculation [(accessed on 19 September 2021)] Available online: <http://abcibc.com/computer-notebook-gadget.php?art=4>

## **Analysis of the possibility of using lpwan networks for spy/listening devices creation**

Recently, LPWAN networks have become widespread. The report examines the main threats to information security that can be organized using LPWAN networks. The two most popular technologies Sigfox and LoRaWAN are considered. Possible scenarios of using LPWAN for organizing information leakage channels are given.

## **АНАЛИЗ ВОЗМОЖНОСТИ ПЕРЕХВАТА ВИБРОАКУСТИЧЕСКОЙ ИНФОРМАЦИИ ПУТЕМ ЕЕ ПЕРЕХВАТА С ПОМОЩЬЮ ДАТЧИКОВ СМАРТФОНА**

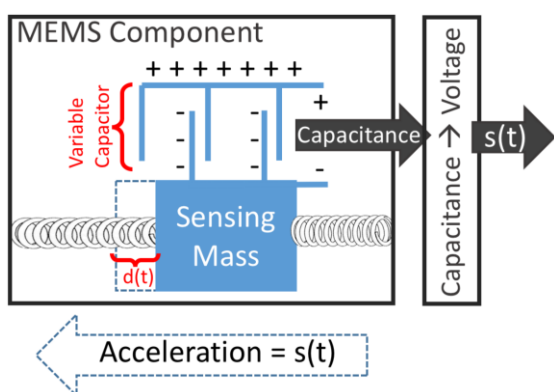
**Ю.В. Лыков, И.В. Хрипко, А.А. Лыкова**

Харьковский национальный университет радиоэлектроники, Харьков, Украина  
e-mail: [yurii.lykov@nure.ua](mailto:yurii.lykov@nure.ua)

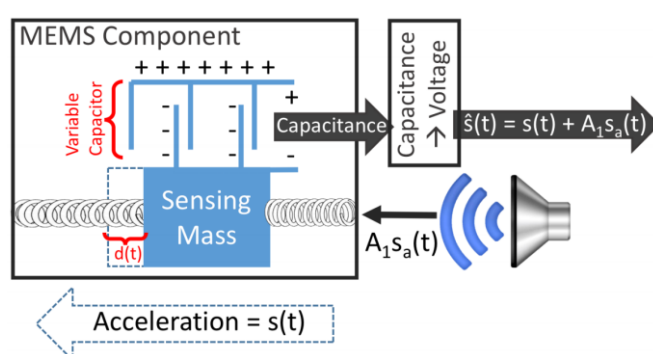
В современном мире тяжело найти человека, который не использует повседневно свой смартфон. Производители постоянно расширяют возможности мобильных устройств. Для этого современные модели имеют множество датчиков таких как: инфракрасный дальномер, акселерометр и гироскоп, датчик сенсорного экрана, фотокамера, магнитометр и барометр, датчик отпечатков пальцев и др. Неограниченный доступ к показаниям датчиков на большинстве современных мобильных платформах (например, ОС Android) - известная уязвимость безопасности, которая по существу делает их датчиками нулевого разрешения. В данной работе основное внимание уделено рассмотрению уязвимости через акселерометр и гироскоп смартфона (датчики движения). В работах [1-5] данные полученные с акселерометра и гироскопа были использованы для кейлоггера рядом расположенной клавиатуры, перехвата графического и цифрового пин-кода смартфона, определения местоположения пользователя с выключенным GPS, запись разговора в помещении, в котором расположен смартфон.

Поскольку операционная система Android имеет долю рынка 73% (в Украине и в Азербайджане близко 85%) [6] во всем мире, эта уязвимость системы безопасности имеет чрезвычайно большое значение, особенно с точки зрения конфиденциальности речевой информации. Поэтому важно понять, как пользователи воспринимают подобные угрозы. Интересным является то, насколько эффективно проинформированные пользователи мобильных и переносных устройств о разных угрозах, связанных с датчиками движения (относительно других угроз конфиденциальности), предпринимают контрмеры. В данной работе рассмотрена возможность использования акселерометра смартфона для прослушивания разговоров в помещении и те трудности с которыми может столкнуться злоумышленник при реализации этой угрозы.

Принцип работы датчиков движения (акселерометров и гироскопов) основан на измерении смещения инерционной массы относительно корпуса  $d(t)$  и преобразовании его в пропорциональный электрический сигнал  $s(t)$ . Емкостной метод преобразования измеренного перемещения является наиболее точным и надежным, поэтому емкостные акселерометры получили широкое распространение. Структура емкостного акселерометра состоит из различных пластин, одни из которых являются стационарными, а другие свободно перемещаются внутри корпуса, величина емкости зависит от расстояния между ними. Емкости включены в контур резонансного генератора (рис. 1). Под влиянием силы ускорения емкость конденсатора меняется [7]. Под действием внешних акустических колебаний сигнал на выходе акселерометра содержит и акустическую составляющую (рис.2).



**Рисунок 1.** Функциональная схема MEMS акселерометра [8]



**Рисунок 2.** Модель канала утечки через MEMS акселерометр смартфона [8]

Частота дискретизации - это скорость преобразования сигнала в цифровой вид. В соответствии с теоремой дискретизации Найквиста частота дискретизации  $f$  позволяет нам реконструировать сигналы на частотах  $f/2$ . Следовательно, более высокая частота дискретизации позволяет нам более точно реконструировать звуковой сигнал. Однако большинство сенсоров движения поддерживают частоты дискретизации от 600 Гц до 1600 Гц [9]. Более того, все мобильные операционные системы значительно ограничивают частоту дискретизации до 200 Гц - для уменьшения энергопотребления (но с помощью Sensor Kinetics можно обойти ограничение до 400 Гц). Кроме того, некоторые наборы инструментов браузера дополнительно ограничивают частоту дискретизации.

В табл. 1 обобщены результаты экспериментального исследования, в котором измерялись максимальные частоты дискретизации, разрешенные в последних версиях Android в разных режимах работы телефона.

**Таблица 1.** Ограничение частоты дискретизации датчиков движения в ОС Android

| Режим   | Частота дискретизации, Гц |
|---|---------------------------|
| Быстрый (максимально допустимый программно)                           | 400                       |
| Игровой   | 50                        |
| UI (при использовании приложений, которые требуют показания датчиков) | 25                        |
| Режим ожидания  | 15                        |

Как видно из табл. 1, частота дискретизации датчиков движения может принимать значения не больше 400 Гц. Это позволяет непосредственно воспринимать звуковые сигналы до 200 Гц. Алиасинг - это явление, при котором синусоидальное колебание с частотой  $f$ , дискретизированное с частотой  $f_s$ , имеет результирующие выборки, которые невозможно отличить от другого синусоидального колебания с частотой  $|f - N \cdot f_s|$ , для любого целого числа  $N$ . Значения, которые отвечают  $N \neq 0$ , называются изображениями или алиасами частоты  $f$ . В целом нежелательное явление, здесь алиасинг позволяет фиксировать звуковые сигналы с частотами, которые превышают 200 Гц, тем самым получать больше информации из показаний сенсоров движения.

В работе проведено экспериментальное исследование чувствительности датчиков движения в нескольких смартфонах. Полученные значения чувствительности лежат в диапазоне от 65 дБ до 77 дБ. В ходе эксперимента также было установлено и влияние ориентации смартфона по отношению к источнику звука на чувствительность датчика, что вероятнее всего обусловлено различным взаимодействием поверхности на которой располагался смартфон с звуковой волной. В подвешенном состоянии чувствительность датчиков движения имеют слабовыраженную направленность.

В следующем экспериментальном исследовании было проведено измерение разборчивости речи с закрытым словарём с помощью ПО автоматического распознавания речи Sphinx. Полученные значения разборчивости для разных тестовых сигналов и речевых моделей смартфонов составил от 9% до 40%. При этом гендер диктора распознавался с вероятностью 60-80%.

Кроме того следует иметь в виду, что есть программы, направленные на определение шаблона местопребывания пользователя на основе окружающего шума, выявленного его смартфоном, например, ресторана, улицы, офиса и др.[10]. Некоторые демаскирующие звуки достаточно громки и могут иметь четкий отпечаток в диапазоне низких частот, чтобы их можно было идентифицировать с помощью гироскопа, например железнодорожный вокзал, торговый центр, шоссе и метро и т.д. Это может позволить злоумышленнику получить больше информации о жертве, получив сведения о местонахождении пользователя.

### **Выводы**

Показано, что акустический сигнал, измеренный акселерометром, может раскрыть информацию об окружающей среде телефона, например, о том, кто говорит в комнате, и, в определенной степени, о чём идет речь. Полученная разборчивость слов с ограниченным словарём достигает 40%, распознавание гендера - до 80%. Дальнейшая работа над низкочастотной обработкой сигналов этого типа должна еще больше повысить качество информации, изъятая из гироскопа и акселерометра. Эта работа демонстрирует неожиданную угрозу, вызванную неограниченным доступом к гироскопу: программы и активное веб-содержимое, которое работает на телефоне, могут подслушивать звуковые сигналы включая

разговор, вблизи телефона. Рассмотрены некоторые контрмеры для защиты от утечки конфиденциальной информации через датчики смартфонов, а именно:

- ФНЧ, реализованный программно и/или аппаратно;
- обновление системы разрешений ОС;
- вибро и/или акустическая маскировка;
- приглушение (демпфирование) вибраций.

Общий вывод заключается в том, что доступ ко всем датчикам должен контролироваться системой разрешений, возможно, разграничивая низкую и высокую частоту дискретизации.

**Ключевые слова:** смартфон, акселерометр, гироскоп, утечка информации, разборчивость речи.

### Литература

1. <https://habr.com/ru/post/130759/>
2. <https://habr.com/ru/post/126806/>
3. <https://crypto.stanford.edu/gyrophone/files/gyromic.pdf>
4. <http://www.news.gatech.edu/2011/10/17/georgia-tech-turns-iphone-spiphone>
5. <https://geektimes.ru/post/251018/>
6. Mobile Operating System Market Share Worldwide <http://gs.statcounter.com/os - market - share/mobile/>, 2021.
7. <https://russianelectronics.ru/mems-datchiki-dvizheniya-ot-stmicroelectronics-akselerometry-i-giroskopy/>
8. <https://spqrmlab1.github.io/papers/trippel-IEEE-oaklawn-walnut-2017.pdf>
9. [https://datasheet.lcsc.com/szlcsc/1911041207\\_Bosch-Sensortec-BMI120\\_C437657.pdf](https://datasheet.lcsc.com/szlcsc/1911041207_Bosch-Sensortec-BMI120_C437657.pdf)
10. Rossi M., Feese S., Amft O., Braune N., Martis S., Troster, G. Ambientsense: A real-time ambient sound recognition system for smartphones. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2013 IEEE International Conference on (2013), IEEE, pp. 230–235.

#### **Analysis of the possibility of intercepting acoustic information by intercepting it with the use of smartphone sensors**

Unlimited access to the data of sensors on modern mobile platforms is well-known vulnerability of safety that essentially does their as the sensors of a zero permission. In this work, basic attention is spared to consideration of vulnerability through an accelerometer and gyroscope of smartphone (sensors of motion).

## IMPLEMENTATION OF LATTICE-BASED IDENTIFICATION SCHEMES IN C

**A. Murzaeva, S. Akleylek**

Ondokuz Mayıs University, Samsun, Turkey

e-mail: [azhar.murzaeva@bil.omu.edu.tr](mailto:azhar.murzaeva@bil.omu.edu.tr)

In 1982, Feynman proposed the idea of a quantum computer that is about to come true [2]. Classical computers work with two 0 and 1 states, while quantum computers use the ‘qubits’ that contain more than two states at a time, making them exponentially faster in performing computations [7]. Big companies such as IBM, Microsoft, and Google are in the race of its development: IBM claims to develop a one million-qubit quantum computer by 2030 [3]. Thus, upcoming quantum computers threaten the security and privacy of the current widely-used cryptosystems. For instance, the prime factorization problem, which is used as the main underlying problem in many contemporary cryptosystems, is going to be solved by Shor’s algorithm on quantum computers in polynomial time [10]. Also, the emergence of technology trends such as cloud computing, which provides real-time computing services to dozens of companies and their users, and the Internet of Things technology, which aims to connect machines to machines, shows the need for strengthening the current cryptosystems. Therefore, the ineffectiveness of traditional public key cryptography against quantum computers led to the standardization of post-quantum cryptography [8].

The results of NIST’s (National Institute of Standards and Technology) standardization project show that among the post-quantum cryptography approaches, the lattice-based cryptography is the most promising candidate [9] [7]. Also, the fact that many fundamental problems in lattices are supposed to be hard against quantum computers attracted many researchers to design and develop lattice-based cryptosystems. During this study, from these cryptosystems, the identification schemes were considered. Since identification schemes are the basis of identification and signature schemes [1], they play an important role in the digital signatures that are widely used in government, healthcare, financial and other services today. The purpose of this study is to develop an open-source library for lattice-based identification schemes, which will provide convenience in the implementation of any newly designed identification scheme. The low-level C language that is used for the implementation of computationally hard systems is selected.

We perform the implementation of lattice-based identification scheme proposed by Kawachi [5], Soysaldi [12], Silva [11], Xagawa and Tanaka [13], and Lyubashevsky [6]. These schemes are based on different hard problems in lattices. For example, we describe the identification scheme itself and its implementation by reviewing LWE-based (Learning With Errors) Silva’s scheme given in Figure 1.

Identification is defined as the process of identifying uniquely a user of a system or an application [4], which prevents impersonation. If to think about the standard client-server structure, interacting parties must pass through the identification step before transmitting the data between

them. There are two basic entities in an identification scheme: the Prover and the Verifier parties. So, let the client be the Prover and let the server be the Verifier. First of all, the public and private parameters are computed in the Key Generation stage, as shown in Figure 1. Then, by using these keys, the Prover computes commitments (in Figure 1, they are defined as  $c_1$ ,  $c_2$ , and  $c_3$ ). In its turn, the Verifier generates and sends a challenge. Depending on the challenge, the Prover reveals some parameters. Using these parameters, the Verifier performs some computations and checks the results. Thus, a server can identify its client.

**KeyGen:**

$$A \xleftarrow{\$} \mathbb{F}_q^{n \times m}, s \xleftarrow{\$} \mathbb{F}_q^m, e \xleftarrow{\$} \mathbb{F}_q^n,$$

$$b = As + e$$

$$p = hw(e)$$

**Prover:**

$$u \xleftarrow{\$} \mathbb{F}_q^m, r_1 \xleftarrow{\$} \mathbb{F}_q^n, r_2 \xleftarrow{\$} \mathbb{F}_q^n, r_3 \xleftarrow{\$} \mathbb{F}_q^n,$$

$$\gamma \xleftarrow{\$} \mathbb{F}_q^m, \gamma \neq 0, \forall i \in 1 \dots m, \Sigma \xleftarrow{\$} \mathbb{S}_n,$$

$$c_1 \leftarrow Com(\Pi_{\gamma, \Sigma}; r_1)$$

$$c_2 \leftarrow Com(\Pi_{\gamma, \Sigma}(A(u+s)); r_2)$$

$$c_3 \leftarrow Com(\Pi_{\gamma, \Sigma}(Au+b); r_3)$$

If  $c=1$ :

$$resp = (r_1, r_2, (u+s), \Pi_{\gamma, \Sigma})$$

If  $c=2$ :

$$resp = (r_2, r_3, \Pi_{\gamma, \Sigma}(A(u+s)), \Pi_{\gamma, \Sigma}(e))$$

If  $c=3$ :

$$resp = (r_1, r_3, \Pi_{\gamma, \Sigma}, u)$$

**Verifier:**

$$\xrightarrow{c_1, c_2, c_3}$$

$$\xleftarrow{c} c \xleftarrow{\$} \{1, 2, 3\}$$

$$\xrightarrow{resp}$$

If  $c=1$ :

$$\text{check } c_1 \stackrel{?}{=} Com(\Pi_{\gamma, \Sigma}, r_1) \text{ and}$$

$$c_2 \stackrel{?}{=} Com(\Pi_{\gamma, \Sigma}(A(u+s)), r_2)$$

If  $c=2$ :

$$\text{check } c_2 \stackrel{?}{=} Com(\Pi_{\gamma, \Sigma}(A(u+s)), r_2) \text{ and}$$

$$c_3 \stackrel{?}{=} Com(\Pi_{\gamma, \Sigma}(A(u+s)) + \Pi_{\gamma, \Sigma}(e)),$$

$$hw(\Pi_{\gamma, \Sigma}(e)) \stackrel{?}{=} p$$

If  $c=3$ :

$$\text{check } c_1 \stackrel{?}{=} Com(\Pi_{\gamma, \Sigma}, r_1) \text{ and}$$

$$c_3 \stackrel{?}{=} Com(\Pi_{\gamma, \Sigma}(Au+b); r_3)$$

Figure 1 demonstrates Silva's identification scheme in detail, while its implementation's source code is given in Figure 2. In that piece of code, the abovementioned steps of the identification process are called as functions.

```

printf("----- Silva's ID Scheme -----\n");
printf("start Key Generation...\n");
keygen(matrix_A, sk_s, pk_b, errors);
printf("finish Key Generation.\n");

printf("Prover (Compute commitments) ...\n");
p_coms(coms_ptr, r1, r2, r3, u, us, aus, matrix_A, sk_s, pk_b, errors);

printf("Verifier (Generate challenge) ...\n");
ch = v_challenge();

printf("Challenge: %d\n", ch);
printf("Prover (Send some parameters) ...\n");
p_params(params_ptr, ch, r1, r2, r3, u, us, aus, errors);

printf("Verifier (Check the truthfulness) ...\n");
result = v_check(coms_ptr, params_ptr, ch, matrix_A, pk_b);

```

**Figure 2.** Main functions of Silva's identification scheme

Like Silva's scheme is based on LWE problem in lattices, all other considered schemes are based on different lattice problems. The LWE problem in Silva's scheme is used during the key generation step, and its source code is demonstrated in Figure 3.

```

// b = As + e
vectorMultiplyMatrix(temp_y, sk_s, N, M, matrix_A);
modVector(temp_y, N, Q);
addVectors(pk_b, temp_y, errors, N);
modVector(pk_b, N, Q);

```

**Figure 3.** The LWE problem in Silva's identification scheme

The remaining identification schemes designed by Kawachi [5], Soysaldi [12], Xagawa and Tanaka [13], and Lyubashevsky[6] are also implemented the way we described Silva's scheme. All common functions used in these schemes are gathered in one common file, which can be included as an external library.

**Keywords:** lattice-based identification schemes, implementaion of lattice-based identification schemes, library for lattice-based identification schemes.

## References

1. Akleyek S., Soysaldi M. (2018). A novel 3-pass identification scheme and signature scheme based on multivariate quadratic polynomials. Turkish Journal of Mathematics. doi:10.3906/mat-1803-92
2. Feynman R.P. (1982). Simulating Physics with Computers. International Journal of Theoretical Physics.

3. Hackett R. (2020). IBM plans a huge leap in superfast quantum computing by 2023. <https://fortune.com/2020/09/15/ibm-quantum-computer-1-million-qubits-by-2030/>
4. IBM (2021). Identification and authentication. <https://www.ibm.com/docs/en/ibm-mq/7.5?topic=mechanisms-identification-authentication>
5. Kawachi A., Tanaka K., Xagawa K. (2008). Concurrently Secure Identification Schemes Based on the Worst-Case Hardness of Lattice Problems, J. Advances in Cryptology - ASIACRYPT 2008, 372–389.
6. Lyubashevsky V. (2009). Fiat-Shamir With Aborts: Applications to lattice and factoring-based signatures, Advances in Cryptology –ASIACRYPT 2009, Lecture Notes in Computer Science; Springer Berlin Heidelberg, 598–616.
7. National Security Agency (2021). Quantum Computing and Post-Quantum Cryptography. [https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/Quantum\\_FAQs\\_20210804.PDF](https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/Quantum_FAQs_20210804.PDF)
8. NIST (2016). Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. <https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms>
9. NIST (2020). Post-Quantum Cryptography: Round 3 Submissions. <https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions>
10. Shor P.W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J Comput. , 26(5) , 1484-1509.
11. Silva R., Campello A., Dahab R. (2011). LWE-based identification schemes, CoRR, abs/1109.0631.
12. Soysaldi M., Akleyek S. (2019). A new 3-pass Zero-knowledge Lattice-based Identification Scheme, 4th International Conference on Computer Science and Engineering (UBMK) 2019.
13. Xagawa K. and Tanaka K. (2009). Zero-Knowledge Protocols for NTRU: Application to Identification and Proof of Plaintext Knowledge, Lecture Notes in Computer Science, 198-213.

## İDARƏETMƏ PROSESİNDƏ VERİLƏNLƏR BAZASININ TƏHLÜKƏSİZLİYİ

**Ş.İ. Mustafayeva**

Azərbaycan Respublikasının Prezidenti yanında Dövlət İdarəçilik Akademiyası,

Bakı, Azərbaycan

e-mail: [shemus26@yandex.ru](mailto:shemus26@yandex.ru)

Hal-hazırda verilənlərin generasiya sürəti çox yüksəkdir. Buna görə də bu cür verilənlərin saxlanması və idarə olunması verilənlər bazası sistemində aparılır. Konfidensiallığın və verilənlər bazasında saxlanılan informasiyanın mühafizəsi verilənlər bazasının təhlükəsizliyi adlanır. O verilənlər bazasının ixtiyari növ icazəsiz və ya qanunsuz girişin təmin olunması ilə yanaşı ixtiyari səviyyəli hücumun qarşısını alır [7].

### **Verilənlər bazası hücumları**

Hücumlar aşağıdakı kateqoriyalar üzrə bölünür:

1. Birbaşa hücumlar – hücum bilavasitə bütöv verilənlərə yönləndirilsə bu birbaşa hücum adlanır.
2. Dolaylı hücumlar. Burada məqsəd verilənlər haqda informasiyanı digər predmetlərin (obyektlərin) köməyiylə toplamaqdır.

Onlar bu üsulla təsnifləşdirilir:

1. Aktiv hücumlar – bu cür hücumlarda verilənlər bazasının aktual dəyəri dəyişdirilir.
2. Passiv hücumlar – bu cür hücumlarda ancaq hücum edən verilənlər bazasında verilənlərə dəyişiklik etmədən nəzarət edir. Bunu üç üsulla etmək mümkündür:
  - statik sızma – bəd niyyətli nəzarətçi verilənlər bazası haqqında informasiya əldə etmək üçün verilənlər bazası haqqında açıq mətn dəyərlərinə sahib olur;
  - dinamik sızma – bədniiyyətli hücumçu təyin olunmuş zaman ərzində açıq mətn dəyərləri haqda informasiya almaq üçün verilənlər bazasında dəyişikliklərə nəzarət edir.
  - əlaqə sızması – təcavüzkar verilənlər bazasının dəyərini indeks dəyərinin mövqeyi üzrə dəyərlərini birləşdirir [1].

### **Verilənlər bazası təhdidləri**

Təhdidlər aşağıdakı kimi təsnif edilmişdir:

- həddən artıq imtiyazlar;
- imtiyazdan sui-istifadə;
- imtiyazın icazəsiz yüksəldilməsi;
- platforma zəiflikləri;
- SQL injeksiyası;
- xidmətdən imtina;
- ehtiyat nüsxə [6], [3].

### **Web təhlükəsizlik təhdidləri**

1. AJAX təhlükəsizliyi – AJAX (asinxron JavaScript və XML) . Bu asinxron əlaqəni dəstəkləyir.
  - AJAX təhlükəsizliyi (Server tərəf) – AJAX əsaslı Web əsaslı tətbiqlər server təhlükəsizlik sxemlərindən də istifadə edir.
    - AJAX təhlükəsizliyi (Kliyənt tərəf) – JavaScript kodlar istifadəçi kimi ixtiyari tərəfə və hakərə görünə bilər.
2. Saytlarası skriptlər – saytlarası skriptlər dinamik veb səhifələrə kimliyi təsdiqlənməyən girişlər olduqda baş verir [4].

### **Verilənlər bazası hücumlarının nəzarət üsulları**

Bəzi təhlükəsizlik siyasəti ilə müşayiət olunan nəzarət hüquqları sistemə birbaşa girişə cavab verir. O ən çox konfidensial informasiyaya girişə məhdudiyət qoyur.

Giriş nəzarətini aşağıdakı kimi ayırmaq olar:

1. İstəyə bağlı giriş nəzarəti - bu vasitə subyekt və ya qrupların məxsus olduğu şəxsiyyət əsasında obyektlərə girişin məhdudlaşdırılmasıdır.
2. Məcburi giriş nəzarəti – bu təhlükəsizlik mexanizmi fayla qadağa qoymaq və ya icazə vermək üçün resurs sahibinin imkanlarına məhdudiyyət qoyur.
3. İstifadəçi identifikasiyası və autentifikasiyası – təhlükəsizliklə bağlı mühüm tələblərdən biri verilənlər bazasına giriş etmək üçün qeydiyyatdan keçmiş istifadəçi özünün yaratdığı istifadəçiləri resurslara giriş etməmişdən öncə onları müəyyən etmək lazımdır [2].

### **Hesabat və audit**

Bu verilənlərin fiziki bütövlüyünün qarşısını almaq üçün istifadə olunur. Bütün uğurlu və uğursuz cəhdlərin jurnalı audit jurnalı faylında görünür. Auditin müxtəlif üsulları mövcuddur:

1. Hesabatlar audit: SQL auditini aparmağa icazə verir. Onların təsir etdiyi obyektə görə deyil, təsdiqin tipinə görə təsdiq olunur;
2. İmtiyaz audit: o ancaq müəyyən olunmuş tipi yoxlayır. Bu tip güclü sistem imtiyazlarının istifadə olunmasına icazə verir;
3. Sxemin obyekt audit: həmişə verilənlər bazasının bütün istifadəçilərinə tətbiq olunan bir və doğru təyin olunmuş sxem obyektinin göstərilmiş təsdiq tipini yoxlayır;
4. Ətraflı audit: auditin keçirilməsi sütunlara girişin və ya dəyişdirilməsinin əsasında icazə verilir. Auditin bir qədər ətraflı səviyyəsi olub verilənlərə giriş və məzmunu əsasında aparılır;
5. Şifrələmə. Bu informasiyanın “Şifrələnmiş mətn”ə çevrilməsi əsasında baş verib verilənlər bazasında saxlanılır. Kodun açarı olan istifadəçi tərəfindən bu informasiya oxuna bilən olacaq. Şifrələmənin üstünlüyü ondan ibarətdir ki, hətta təcavüzkar tərəfindən bu informasiya əlçatan olduqda belə artıq kod şəklində olan məlumat ona lazım olmayacaq [5], [3].

### **Son istifadə olunan verilənlər bazası. Təhlükəsizlik metodları**

- Kriptografiyanın köməyi ilə verilənlər bazasının mühafizəsi.  
Qarışıq kriptografiya verilənlər bazasının şifrələnməsini mühafizəsiz şəbəkədə saxlənmiş şəkildə əhatə edir.
- Verilənlər bazasının stenoqrafiyanın köməyi ilə mühafizəsi.

O şifrələnmiş verilənləri heç kəsin görməməsi üçün gizləyir və heç kəs bilmir ki, onlar mövcuddur. Stenoqrafiyada verilənlər izafi dəyərlərdə istifadə olunan alqoritmlərlə şifrələnir. Müxtəlif metodlar istifadə olunur: stenoqrafiya, videostenoqrafiya, IP dataqramma.

**Açar sözlər:** VB, VBİS, SQL, verilənlərin mühafizəsi, verilənlərin təhlükəsizliyi.

### **Ədəbiyyat**

1. Брюхомицкий Ю.А., Кобилев М.А., Обеспечение безопасности систем баз данных MySQL, Таганрог 2014.
2. Скакун В.В., Защита информации в базах данных и экспертных системах, Минск: БГУ, 2015, 140 с.

3. Потапов А.Е., Манухина Д.В., Соломатина А.С., Бад-маев А.И., Яковлев А.В., Нилова А.С. Безопасность локальных баз данных на примере SQL Server Compact, Вестн. Тамбов. ун-та. Серия: Естественные и технические науки. 2014. № 3. С. 915-917.
4. Муравьев С., Дворянкин С., Насенков И. СУБД: проблема выбора, Открытые системы.СУБД, 2015.
5. Советов Б.Я., Цехановский В.В., Чертовской В.Д. Базы Данных 3-е изд., пер. и доп. Учебник для прикладного бакалавриата, М.:Издательство Юрайт, 2019, 420с. URL: <https://urait.ru/book/bazy-dannyh-431947>
6. Rohilla S., Mittal P.K. Database Security: Threads and Challenges. Intern. Journ. of Advanced Research in Computer Science and Software Engineering, 2013, vol. 3, iss. 5, pp. 810-813.

### **Security of the database in the management process**

At the end of the article, we can conclude that a number of objects are used to ensure the security of the data in the database. These objects are the objects of the database and provide different levels of security. In addition, threats and methods to eliminate them are shown.

Data protection issues are very important for the security of today's corporate systems. The article is devoted to the current situation in the field of information security under management. Database management systems (DBMS) consider information security tools and methods. DBMS that support SQL have special facilities that provide security.

## **MÜASİR PROQRAM-TEXNİKİ, TƏŞKİLATİ METODLAR VƏ İNFORMASIYANIN QORUNMASI VASİTƏLƏRİ**

**N. Müzəffərli, L. Ağamaliyeva**

Azərbaycan Universiteti, Bakı, Azərbaycan

e-mail: [latifa.aghamaliyeva@au.edu.az](mailto:latifa.aghamaliyeva@au.edu.az)

İnformasiya bu gün – mühüm və əhəmiyyətli bir qaynaqdır və onun itkisi xoşagəlməz hallarla nəticələnə bilər. Məxfi şirkət məlumatlarının itirilməsi maliyyə itkisi təhlükəsi daşıyır, çünki əldə edilən məlumatlar rəqiblər və ya hakerlər tərəfindən istifadə edilə bilər. Bu cür arzuolunmaz halların qarşısını almaq üçün bütün firmalar və təşkilatlar məlumatların qorunması üsullarından istifadə edirlər.

İnformasiya sistemlərinin təhlükəsizliyi bir ixtisas kimi informasiya sistemləri sahəsində çalışan mütəxəssislər və proqramçılar tərəfindən öyrənilir. Bununla birlikdə, gizli məlumatlarla işləyən hər kəs informasiya təhlükəsi növlərini və qorunma texnologiyalarını bilməlidir.

Hakerlər məlumatların oğurlanması üçün xüsusi olaraq hazırlanmış proqramlardan istifadə edərək qurğulara birbaşa daxil olmaqla və ya uzaqdan hücum etməklə həyata keçirə biləcəkləri əməlləri əvvəlcədən planlaşdırırlar.

Hakerlərin hücumlarından başqa, firmalar tez -tez proqram və aparatların nasazlığı səbəbindən məlumat itkisi ilə üzləşirlər. Bu halda gizli materiallar müdaxilə edənlərin əlinə düşür, ancaq itirilir və ya çox uzun müddət ərzində bərpa olunur. Kompüter sistemlərində xətlər aşağıdakı səbəblərdən meydana gələ bilər: hard disklərin sıradan çıxması səbəbilə məlumat itkisi, proqramda baş verən səhvlər, zədələnmə və ya digər aparat nasazlıqları səbəbindən məlumat itkisi.

Məlumatların qorunması texnologiyaları, məlumatların sızmasını və itirilməsinin qarşısını alan müasir metodların istifadəsinə əsaslanır. Bu gün yeddi əsas qoruma üsulu (metodu) istifadə olunur: maneə, maskalanma, şifrələmə mexanizmləri, tənzimləmə, girişin idarəedilməsi, təzyiqlər. Yuxarıda qeyd edilən metodların hamısı, məlumatların mühafizəsi üçün effektiv texnologiya qurmağa yönəldilmişdir ki, bunun sayəsində də kənd səhlənkərliliyi nəticəsində baş verən itkilər aradan qaldırılır və müxtəlif növ təhdidlər uğurla dəf edilir.

Maneə metodu dedikdə informasiya sistemlərinin fiziki qorunma üsulu nəzərdə tutulur ki, bu da müdaxilə edənlərin qorunan əraziyə girməsinə imkan vermir.

Məlumatı qorumağın başqa bir metodu olan maskalanma - məlumatların kənar şəxslər tərəfindən qəbul edilməsi mümkün olmayan bir formaya çevrilməsini metodudur. Şifrəni açmaq üçün prinsipi bilmək lazımdır.

Şifrələmə mexanizmləri - məlumatın kriptografik bağlanmasıdır. Bu qorunma üsulu həm maqnit daşıyıcılarında məlumatların işlənməsində, həm də saxlanılmasında istifadə olunur. Uzun məsafəli ünsiyyət kanalları üzərindən məlumat ötürərkən, bu üsul yeganə etibarlı üsuldur.

Giriş nəzarəti bütün informasiya texnologiyaları qaynaqlarının istifadəsini tənzimləyir və müxtəlif yollarla informasiyaya icazəsiz girişin qarşısını alır. Giriş nəzarəti aşağıdakı təhlükəsizlik xüsusiyyətləri daxildir:

- sistemin istifadəçilərinin, personalının və resurslarının identifikasiya edilməsi (hər bir obyektə fərdi identifikator təyin edilməsi);
- təqdim etdiyi identifikator tərəfindən obyektin və ya subyektin tanınması (identifikasiyası);
- səlahiyyətlərin yoxlaması (həftənin gününün, saatının, tələb olunan mənbələrin və prosedurların müəyyən edilmiş qaydalara uyğunluğunu yoxlamaq);
- müəyyən edilmiş qaydalar çərçivəsində iş şəraiti yaratmaq; qorunan mənbələrə edilən müraciətlərin qeydiyyatı;
- icazəsiz hərəkətlərə cəhd zamanı cavab (siqnal, işlərin dayanması, sorğunun rədd edilməsi və s.).

Tənzimləmə - xüsusi təlimatların tətbiq edilməsini əhatə edən informasiya sistemlərinin qorunmasının ən vacib üsuludur? Bu da qorunan məlumatlarla bütün manipulyasiyaları həyata keçirilməyə imkan verir.

Məlumatların qorunması üsulları müəyyən vasitələrdən istifadə etməyi nəzərdə tutur. Gizli məlumatların itirilməsinin və sızmasının qarşısını almaq üçün aşağıdakı vasitələrdən istifadə olunur: fiziki, proqram təminatı və aparat, təşkilati, qanunvericilik, psixoloji.

Məlumatın qorunmasının fiziki vasitələri, kənar şəxslərin qorunan əraziyə girməsinə maneə törədir. Fiziki maneələrin əsas və ən qədim vasitəsi möhkəm qapılar, etibarlı kilidlərdir. Məlumatın

qorunmasını gücləndirmək üçün giriş məntəqələri istifadə olunur, bu da insanlar (mühafizəçilər) və ya xüsusi sistemlər tərəfindən həyata keçirilir. Məlumat itkisinin qarşısını almaq üçün hətta yanğından mühafizə sisteminin quraşdırılması da məsləhət görülür. Fiziki üsullar həm kağız, həm də elektron daşıyıcılarda olan məlumatları qorumaq üçün istifadə olunur.

Proqram və aparat təminatı üsulları - müasir informasiya sistemlərinin təhlükəsizliyinin təmin edilməsində əvəzolunmaz bir komponentdir. Aparat üsulları məlumatların işlənməsi üçün aparatlara daxil olan qurğularla təmsil olunur. Proqram təminatı - haker hücumlarını dəf edən proqramlardır. Həmçinin, proqram sistemlərinə itirilmiş məlumatları bərpa edə bilən proqram sistemləri də daxildir. Avadanlıq və proqramlar kompleksinin köməyi ilə itkilərin qarşısını almaq məqsədilə məlumatların ehtiyat nüsxəsi çıxarılır.

Təşkilati vasitələr bir neçə qoruma üsulu ilə əlaqələndirilir: tənzimləmə, idarəetmə, məcbur etmə. Təşkilati vasitələrə vəzifə təlimatlarının hazırlanması, işçilərlə söhbətlər, cərimələr və təşviqlər daxildir. Təşkilat vasitələrindən səmərəli istifadə etdikdə müəssisə işçiləri qorunan məlumatlarla işləmə texnologiyasına yaxşı yiyələnir, vəzifələrini dəqiq yerinə yetirir və qeyri-dəqiq məlumatların təqdim olunması, məlumatların sızması və ya itirilməsindən məsuliyyət daşıyırlar.

Qanunvericilik vasitələri - qorunan məlumatlara çıxışı olan insanların fəaliyyətini tənzimləyən və məxfi məlumatların itirilməsinə və ya oğurlanmasına görə məsuliyyət ölçüsünü təyin edən normativ hüquqi aktlar toplusudur. Azərbaycan Respublikasında bu istiqamətdə işlər fəal şəkildə aparılır.

Psixoloji müdafiə vasitələri - məlumatların təhlükəsizliyi və həqiqiliyinə işçilərin şəxsi marağını yaratmaq üçün tədbirlər kompleksidir. Rəhbərlər işçilər arasında şəxsi motivasiya yaratmaq üçün müxtəlif təşviq növlərindən istifadə edirlər. Hər bir işçinin özünü sistemin vacib bir hissəsi kimi hiss etməsi və müəssisənin uğuru ilə maraqlanması kimi korporativ mədəniyyət quruculuğu da psixoloji vasitələrə aiddir.

Beləliklə, belə bir nəticəyə gələ bilərik ki, məlumatların qorunması, xüsusən də hüquq-mühafizə orqanları üçün aktual problemdir, çünki “kənar əllərə” keçən (hətta qeyri-hərbi xarakterli) məlumatlar təhlükə yarada bilər. Məhz bu səbəbdən məlumatların qorunması üçün bir çox üsul və vasitələr hazırlanmışdır.

Son on ildə informasiya ən qiymətli mənbələrdən birinə çevrilmişdir və onun qorunması üçün yeni üsul və metodlar hazırlanır.

### **Ədəbiyyat**

1. Əliquliyev R.M., İmamverdiyev Y.N., Mahmudov R.Ş., İformasiya təhlükəsizliyinin multidissiplinar elmi-nəzəri problemləri, İformasiya cəmiyyəti problemləri, 2017, №2, 32–43.
2. Niyazov X. İformasiya azadlığı və informasiya təhlükəsizliyi: milli təhlükəsizlik kontekstində. İformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 14 may 2015-ci il.
3. İformasiya təhlükəsizliyi, Dərslük, Bakı, “İqtisad Universiteti” nəşriyyatı, 2016, 384 səh.

## **MODELING AND SELECTION OF OPTIMAL PARAMETERS OF SECURITY GATEWAYS TO PROTECT INDUSTRIAL EQUIPMENT FROM CYBERATTACKS**

**I. Nevludov, M.A. Omarov, S. Novoselov**

Kharkiv National University of Radio Electronics, Department of Computer-Integrated Technologies, Automation and Mechatronics, Kharkiv, Ukraine

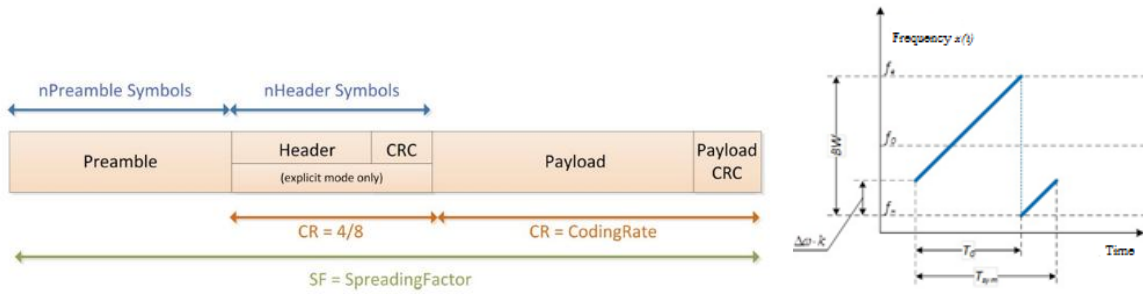
Automated control systems of technological process (ACS TP) are an integral part of almost any production process in modern enterprises. As a rule, ACS TPs have higher levels of risk compared to corporate information systems. It is worth noting the current trend of implementing the concept of Industry 4.0 in enterprises and the widespread use of wireless networks. Industrial Internet of Things (IIoT) is a system of integrated computer networks and connected industrial (production) facilities with built-in sensors and software for data collection and exchange, with the possibility of remote control and management in an automated mode, without human intervention [1].

The industry uses a variety of equipment that requires separate communication channels to exchange information. Depending on the type of equipment and application, the network transmits different amounts of data. Depending on the type of network, special equipment is used. Gateways, routers, and routers are used in high-load, high-volume networks.

Gateways in IoT networks provide the connection of devices and data analytics to IoT devices, which usually do not have these capabilities. Any gateway can use IoT modules to perform analysis or pre-processing before sending messages from slave devices to the Internet of Things. Gateways in IoT networks provide secure connection of devices and data analytics to IoT devices, which usually do not have these capabilities [2]. There are three patterns for using an IoT device as a gateway: transparency, protocol conversion, and authentication conversion.

To model the operation of the gateway, it is necessary to determine the principle of packet transmission. The total transmission time and power consumption depend on the change of the module parameters responsible for the transmission and reception modes. By changing these parameters, you can choose the optimal mode of operation of the LoRa module to solve the problem and set the module to the minimum level of energy consumption, which will provide maximum operating time of the device from autonomous power supply [3, 4].

To organize messaging at the physical level, data blocks are transmitted between the end device (End Node) and the LoRa gateway (Gateway). The general view of the LoRa package is shown in Figure 1 and consists of three elements [4]: preamble; optional title; payload.



**Fig. 1.** The structure of the data packet of the LoRa package and example of the dependence of the frequency of the radio signal on time for the data frame

Next, we will simulate different options for building a data package in order to determine the optimal format for a particular task. The receiver performs the preamble detection process, which is periodically restarted. For this reason, the length of the preamble must be set identical to the length of the preamble of the transmitter. If the preamble length is unknown or can vary, the maximum preamble length must be programmed on the receiver side.

Depending on the selected mode of operation of the LoRa module, two types of headers are available: explicit mode; implicit mode. The principle of transmitting the information symbols of the physical layer data block using the broadband radio signal LoRa is the frequency shift

$$e^{j \cdot \Delta\omega \cdot k \cdot t}$$

relative to the reference signal

$$e^{j \cdot (\omega_n \cdot t + \mu \cdot t^2)},$$

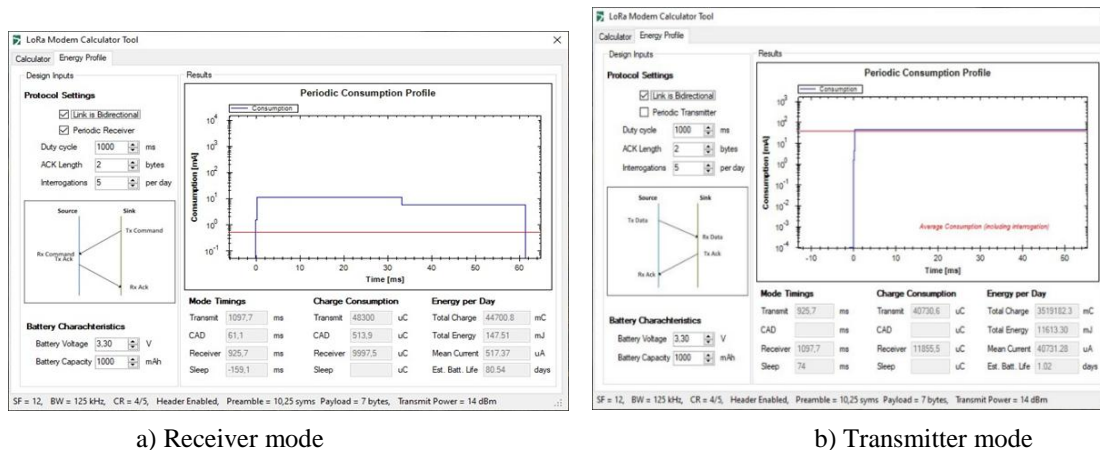
where  $k = 0, 1, 2, \dots, 2SF$  - information symbol, dimension SF bits [4].

Thus, the function  $x(t)$  is written as follows:

$$\chi(t) = \begin{cases} A_0 \cdot \cos\left(\omega_H \cdot t + \Delta\omega \cdot k \cdot t + \frac{\mu}{2} \cdot t^2\right), & 0 \leq t < T_0 \\ A_0 \cdot \cos\left(\omega_H \cdot t + \Delta\omega \cdot k \cdot t - BW \cdot t + \frac{\mu}{2} \cdot t^2\right), & 0 \leq t < T_0 \end{cases} \quad (1)$$

where  $BW$  is the width of the spectrum of the radio signal;  $k = 0, 1, 2, \dots, 2SF$  - information symbol, dimension SF bits;  $T_{sym} = 2SF / BW$  - duration of the radio signal;  $\mu = BW / T_{sym}$  - rate of change of radio signal frequency;  $t$  is the transmission time of the data unit;  $\omega_H$  is the frequency of the radio signal. Figure 2 shows the simulation result in LoRa Modem Calculator for Periodic Receiver mode. and Transmitter mode.

Based on the analysis of the data exchange protocol, we can conclude that to reduce power consumption and reduce airtime, you can make a variable frame length. For example, you only need 4 bytes to control the availability of a device (remove empty data fields and cell addresses from the log). By reducing the length of the data field, we reduce the time spent on the air from 925.7 to 761.86 ms. The current consumption does not decrease. Thus, we need to find other parameters that will allow us to extend the battery life.



**Fig. 2.** The simulation result in LoRa Modem Calculator

As a result of these studies, the LoRa Modem Calculator was used to determine the values of the parameters at which the maximum energy efficiency and speed of the protective gateway are achieved. The simulation results showed that the condition in the air up to 1% of the time of the active cycle for the size of the data field, the size of the data field Payload = 7 or 4 meet the following parameters: Spreading factor = 6;  $BW \geq 250$  kHz; header field is missing; no checksum field;  $CR = 4/5$ . Thus, a methodology and software scripts were developed to automate the determination of the optimal configuration of the IoT gateway operating modes.

**Keywords:** Cybersecurity, LoRaWAN, IoT, Security Gateways, Industrial Control Systems.

### References

1. Boyes H., Hallaq B., Cunningham J., Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in industry*, 101, 1-12.
2. Snitkin S. Unidirectional Security Gateways Reduce Risk of Industrial Cyber Attacks. <https://www.arcweb.com/blog/unidirectional-security-gateways-reduce-risk-industrial-cyber-attacks> [accessed Sep 12 2021].
3. Novoselov S., Donskov O., Distributed Local Positioning System Using DWM1000 Location Chip, 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, 2017, pp. 489-492.
4. Novoselov S., Sychova O., Tesliuk S., Development of the Method Local Navigation of Mobile Robot a Based on the Tags with QR Code and Wireless Sensor Network, 2019 IEEE XVth International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH), Polyana, Ukraine, 2019, pp. 46-51.

## APACHE HADOOP PLATFORMASI: BÖYÜK HƏCMLİ VERİLƏNLƏRİN EMALI ÜÇÜN MÜASİR YANAŞMA

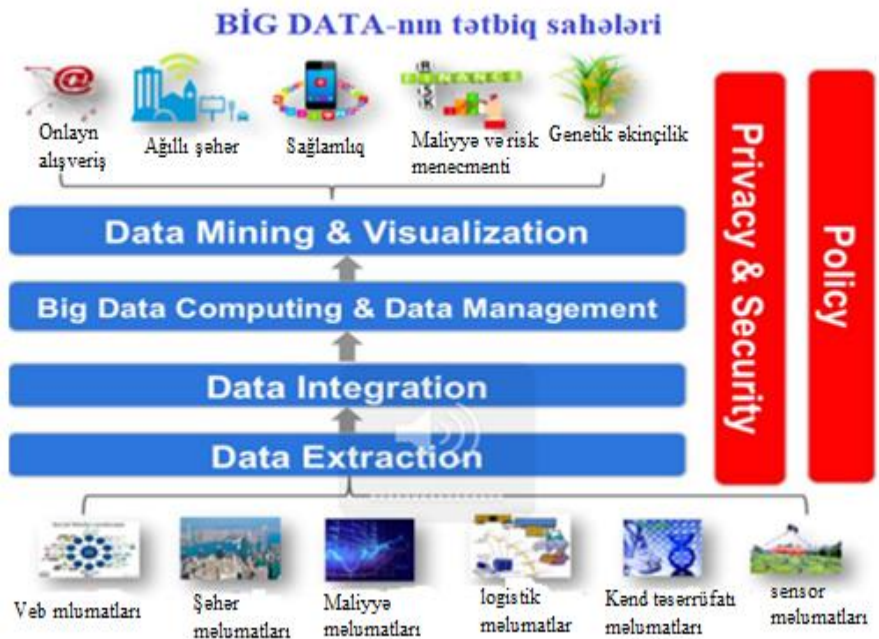
V.A. Nuriyeva

Mingəçevir Dövlət Universiteti, Mingəçevir Azərbaycan

e-mail: [valida.nuriyeva@mdu.edu.az](mailto:valida.nuriyeva@mdu.edu.az)

XX əsrin sonlarında informasiya və kompüter texnologiyalarının sürətli inkişafı böyük həcmli məlumatların ortaya çıxmasına və bu məlumatların müəyyən strukturlaşdırılmış formada bazalarda toplanmasına səbəb oldu. Zaman keçdikcə bu məlumatların tez-tez yenilənməsinə və fərqli mənbələrdən daxil olan məlumatların emalına tələbat artmışdır. Bu məqsədlə, mütəxəssislər böyük həcmli verilənlərin emalı texnologiyalarını - Big Data texnologiyalarını işləyib, informasiya texnologiyaları bazarına inteqrasiya etdilər [1-6].

Big Data texnologiyası – praktikada verilənlərin emalı (toplanması, çeşidlənməsi, strukturlaşdırılması, ötürülməsi və s.) və təhlilini paylanmış şəkildə həyata keçirən xidmətlər toplusunu təqdim edir: həcmlik; sürətlilik; müxtəliflilik; etibarlılıq. Verilənlərin həcmi - illər boyu toplanan məlumatların paylanmış verilənlər bazasında saxlanılmasının və təhlilini əks etdirir. Sürət-verilənlərin internet üzərindən sorğu ünvanına çatdırılmasını əks etdirir. Müxtəliflik – verilənlərin predmet sahələri üzrə emalını əks etdirir. Etibarlılıq - müasir texnologiyaların tətbiqi ilə keyfiyyətli və dəqiq məlumatların emalını əks etdirir. Big Data texnologiyalarının həll etdiyi problemləri 4 istiqamət üzrə qruplaşdırmaq olar (şəkil 1):



Şəkil 1. BIG DATA-nın tətbiq sahələri

1. DATA Mining & Visualization (Məlumatların emalı və vizuallaşdırılması);
2. BIG DATA computing & DATA management (BIG DATA hesablama və DATA idarə edilməsi);
3. DATA İntegration (Verilənlərin inteqrasiyası);
4. DATA Extraction (Verilənlərin eksportu (çıxarılması)).

Şəkil 1-də qeyd olunan istiqamətlər üzrə tətbiq olunan sahələr təsvir olunmuşdur: bazar vəziyyətinin proqnozlaşdırılması; smart (ağıllı şəhər) şəhərin idarə olunması; genetik kodlaşdırma; logistik, maliyyə, sensor verilənlərin idarə olunması; qərarların qəbulu; marketing və satışın optimallaşdırılması [4].

Beləliklə, Big Data texnologiyaları böyük həcmli və səmərəli məlumatların çeşidlənməsi, üsul və metodları, strukturlaşdırılmış və strukturlaşdırılmamış məlumatların işlənməsini nəzərdə tutduğundan, analitik şirkətlərin verdiyi proqnoza görə gələcəkdə dünyadakı məlumatların miqdarı 40 ZB (1ZB =  $10^{21}$  bayt) səviyyəsinə çatması planlaşdırılırki, bu da yer kürəsinin hər bir sakini üçün 5200 GB məlumat (mətn sənədləri, şəkillər, videolar, maşın kodları, cədvəllər və s.) qəbul etməsinə imkan verəcəkdir [5]. Big Data texnologiyalarının inkişaf perspektivlərindən biri nəinki böyük həcmli və müxtəlif tərkibli məlumatlarla işləmək, həm də emal olunmuş məlumatlar üzərindən praktiki biliklər əsasında gəlir əldə etməkdir. Bu məqsədlə geniş auditoriya qazanmış Apache Hadoop modeli çoxlu sayda məlumatı emal etmək üçün aşağıdakı komponentlərdən ibarət səmərəli sistem hesab olunur: MapReduce; HDFS; Hbase; ZooKeeper; Pig; Hive; Avro [1].

MapReduce - predmet sahəsi üzrə tapşırıqları bölməklə böyük miqdarda məlumatların paralel işlənməsi üçün hazırlanmış bir proqram modelidir. MapReduce Google tərəfindən icad edilmişdir. Böyük həcmli məlumat anbarında axtarış sistemləri üçün Veb indeksləşdirilməsini sadələşdirir [3].

HDFS - Kataloqlar və fayllar iyerarxiyasını formalaşdırır. Bu proqramın köməyiylə fayllar bloklara bölünür (128 MB).

Hbase – HDFS bazasında paylanmış məlumatlar açarlar üzrə qiymətləndirilməsini realizə edir.

ZooKeeper - Paylanmış tapşırıqlar üçün paylanmış koordinasiya xidmətini realizə edir.

Pig və Hive - Böyük məlumat siniflərini təhlil etmək üçün bir platformadır.

Avro - Məlumatların seriallaşdırılması sistemini realizə edir [6].

Təhlildən görüldüyü kimi, Hadoop platformasında problem həllərin üstünlükləri əhəmiyyətli dərəcədə çoxdur:

- məlumatların işlənməsi üçün vaxtın azaldılması;
- avadanlığın xərcinin azaldılması;
- müqavimətin artması texnologiyada nasazlığa davamlı bir həll qurmağa imkan verməsi;
- xətti miqyaslılıq;
- strukturlaşdırılmamış məlumatlarla işləmək.

Qeyd olunan üstünlüklərdən əlavə olaraq bu texnologiya predmet sahələri üzrə strukturlaşdırılmış kompleks fayllarla işlənmə imkanına malikdir. Bu da yeni imkanların və ideyaların ortaya çıxması üçün ən optimal vasitə hesab olunur.

**Açar sözlər:** Big Data, böyük məlumatlar, proqnozlaşdırma, rəqabət üstünlüyü, strukturlaşdırılmamış məlumatlar, Hadoop platforması,

#### *Ədəbiyyat*

1. Sadıqova A. Big Data texnologiyalarında istifadə olunan proqram təminatı, Proqram mühəndisliyinin aktual elmi-praktiki problemləri. Bakı, 2017.
2. Əliquliyev R.M., Hacırahimova M.Ş., Əliyeva A.S. Big Data-nın aktual elmi-nəzəri problemləri, İnformasiya cəmiyyəti problemləri, 2016.
3. Murthy, A., Eadline, D. (2014). Apache Hadoop YARN: moving beyond MapReduce and batch processing with Apache Hadoop 2. Pearson Education.
4. Артемов С. Big Data: новые возможности для растущего бизнеса. URL: <http://www.pcweek.ru/upload/iblock/d05/jet-big-data.pdf>
5. Gantz J., Reinsel D. (2012). The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east. IDC iView: IDC Analyze the future, 2007(2012), 1-16.
6. What is Apache Hadoop? URL: <http://hortonworks.com/hadoop/>

#### **Apache Hadoop PLATFORM: a modern approach to the processing of large volumes of data**

In the digital society, the processing of large volumes of data has led to a revolution in the application of modern scientific approaches. Thus, the rapid response to requests in problem areas has opened the way to the use of modern approaches – technologies that allow large data analysts to minimize the loss of time, which is the biggest problem. The main purpose of data processing is to determine the most effective way of analysis of modern data processing is to technologies for large volumes of data. The analysis identified the advantages and capabilities of the Hadoop platform and determined that it meets the requirements of the modern era.

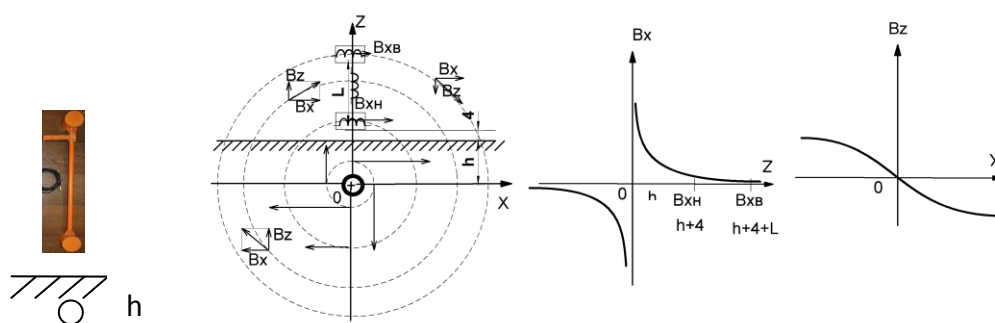
## МЕТОДИКА КАЛИБРОВКИ ПРИБОРОВ ДЛЯ ПОИСКА СКРЫТЫХ КАБЕЛЕЙ

**В.И. Огарь**

Харьковский национальный университет радиоэлектроники. Харьков, Украина

e-mail: [valeriy.ogar@nure.ua](mailto:valeriy.ogar@nure.ua)

Для определения места расположения кабелей, в т.ч. для технической защиты информации от утечки, используются трассоискатели. Некоторые из них имеют функцию измерения глубины залегания кабеля. Они используют мощный генератор, подключенный к линии, три приёмных ферритовые антенны, приёмник и процессор с индикатором глубины.



**Рис.1.** Размещение антенн и силовые линии магнитного поля проводника

Две горизонтальные антенны расположены на расстоянии 70 см сверху и внизу штанги. Вертикальная антенна (на рис.1 расположенная в штанге), позволяет размещать горизонтальные антенны точно над кабелем, при этом сигнал  $B_z$  равен нулю, а при смещении вправо или влево по оси  $X$  изменяет знак, что отражается на индикаторе. Составляющая  $B_x$  магнитного поля проводника обратно пропорциональна расстоянию от кабеля  $B_x = \frac{\mu_0 I}{2\pi \cdot z}$ .

Измеряя сигналы, пропорциональные индукции поля верхней горизонтальной катушке (индукция  $B_{xV}$ ) и нижней (индукция  $B_{xH}$ ), с учётом высоты нижней антенны 4 см над землёй, глубина залегания кабеля  $d$  (см) вычисляется процессором по формуле

$$d = \frac{B_{xV} \cdot 70}{B_{xH} - B_{xV}} - 4 \quad (1)$$

Одним из вопросов работы с трассоискателями является методика калибровки измерений глубины залегания кабелей. Фирма Radiodetection в методике калибровки использует кабель длиной 50 м, подвешенный на высоте 0,5 м, подключенный к выходу генератора поисковых сигналов. Второй выход генератора и противоположный конец кабеля заземляют. Показания измеренной глубины должны соответствовать расстоянию между

кабелем и измерительными антеннами трассоискателя. Этот метод наиболее точен, но для него необходим большой полигон, свободный от побочных электромагнитных полей и невозможен в лабораторных условиях.

Другие производители для калибровки подают на вход приёмника напряжения, имитирующие сигналы, полученные от антенн. Для этого необходимо устройство с понижающим трансформатором в экранированном корпусе, которое не поставляется.

Для калибровки трассоискателей предложено использовать короткую катушку, подключенную к поисковому генератору, и измерение показаний трассоискателем глубин на известных расстояниях от неё с соответствующим перерасчётом.

Зависимость составляющей индукции магнитного поля  $B_x$  одного витка катушки с радиусом  $R$  и током  $I$ , определяется интегралом [1], и при  $x=0, y=0$  в точке  $z_1$  на оси  $z$

$$B_x(x_1, y_1, z_1) = \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{R(R - y_1 \cdot \sin \varphi - z_1 \cdot \cos \varphi)}{[(z_1 - R \cdot \cos \varphi)^2 + (y_1 - R \cdot \sin \varphi)^2 + (x_1 - x)^2]^{3/2}} d\varphi = \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{R(R - z_1 \cdot \cos \varphi)}{((z_1 - R \cdot \cos \varphi)^2 + R^2 \cdot \sin^2 \varphi)^{3/2}} d\varphi = \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{(R^2 - z_1 \cdot R \cdot \cos \varphi)}{((z_1 - 2R \cdot z_1 \cos \varphi + R^2)^{3/2}} d\varphi$$

Этот интеграл вычисляем числовыми методами в программе Mathcad в дискретных точках для радиуса катушки  $R=10,5$  см на расстояниях  $Z$  через 1 см (рис.2).

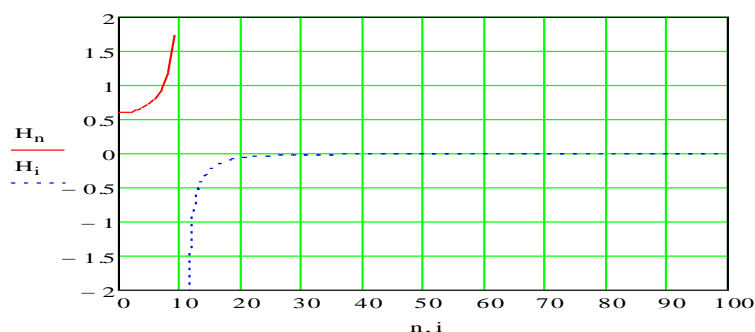


Рис.2. Зависимость индукции магнитного поля от расстояния от центра катушки

Видно, что магнитное поле сбоку торца катушки имеет конфигурацию, аналогичную линиям поля прямого проводника (рис.3), и с расстоянием от края катушки ослабевает сильнее (от  $\sim 1/z^3$  до  $\sim 1/z^2$ ). Это и позволяет проводить измерения в условиях лаборатории.

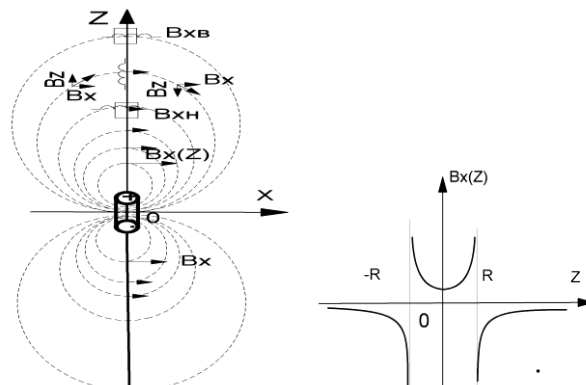


Рис.3. Силовые линии магнитного поля катушки с током и зависимость составляющей  $B_x$  от расстояния до центра катушки

Вычислив в дискретных точках значения сигнала на расстоянии  $z = h$  от края катушки, для нижней антенны  $V_{хн} = V(h)$  и для верхней антенны  $V_{в} = (h + 70)$  с помощью формулы (1), получаем таблицу зависимости показаний глубины  $d$  от действительных расстояний нижней антенны от края катушки  $(h+4)$  в см. Далее по показаниям трассоискателя  $d$  и таблице определяют расчётное значение глубины  $h_{расч}$ . Отклонение (погрешность) результатов измерения глубины залегания трассоискателем  $\Delta h$  определяют по формуле

$$\Delta h = h_{расч} - h, \quad (2)$$

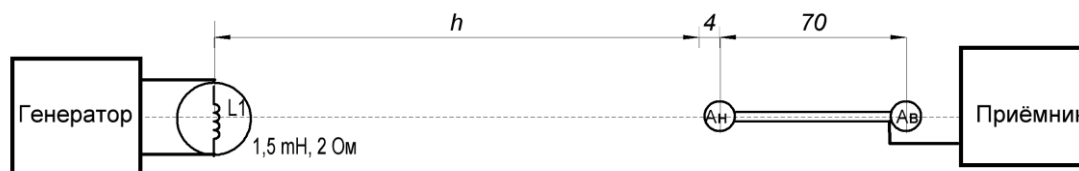


Рис.4. Стенд и схема калибровки трассоискателя

В эксперименте для частоты генератора около 1 кГц использовалась катушка радиусом 11,5 см, содержащая 60 витков провода. Катушку располагают на стенде (рис.4). Погрешность измерений глубины залегания кабеля не превысила 5%.

**Ключевые слова:** трассоискатели, антенна, калибровка, катушка.

### Литература

1. Shibaji B., Siddhartha Shankar P., Partha B., Sabyasachi M. (2013). Pulsed magnetic field measurement outside finite length solenoid: experimental results & mathematical verification. Journal of Electromagnetic Analysis and Applications, Vol.5 No.10, Article ID:38528, [DOI:10.4236/jemaa.2013.510059](https://doi.org/10.4236/jemaa.2013.510059)

### Method of calibration of instruments for finding hidden cables

The report proposes a method for calibrating cable depth meters. The Radiodetection calibration method uses a 50 m long, 0.5 m high cable connected to the output of the search signal generator. Measurement error is defined as the difference between the locator readings and the actual distance between the cable and the tracker antennas. This method is the most accurate, but requires a large area free of parasitic electromagnetic fields.

It is recommended to use the short coil magnetic field for calibration. The dependence of the magnetic field strength on the distance to the coil is determined numerically in the Mathcad program and, accordingly, the dependence of the readings on the real distance. The deviation of the calculated value from the actual value does not exceed 5%.

## ВЫБОР ТЕХНИЧЕСКИХ ПАРАМЕТРОВ СРЕДСТВ ДИСТАНЦИОННОЙ АКУСТИЧЕСКОЙ РАЗВЕДКИ

А.Н. Олейников, И.Н. Чигирев

Харьковский национальный университет радиоэлектроники. Харьков, Украина

e-mail: [anatoly.oleynikov@nure.ua](mailto:anatoly.oleynikov@nure.ua)

В настоящее время самыми распространенными средствами ведения дистанционной акустической разведки являются узконаправленные микрофоны, чаще всего в виде микрофонных решеток (МР), и лазерные системы акустической разведки. Современные успехи в области применения средств акустической разведки опираются на результаты, которые были достигнуты в области съема акустической информации в течение XX века.

Совершенствование технических параметров узконаправленных микрофонов условно можно разделить на три этапа: начальный этап («механический»), этап *аналоговой обработки сигналов* и этап *цифровой обработки речевой информации*. На начальном этапе (в ходе первой мировой войны) дистанционный прием звука применялся с использованием довольно громоздких механических конструкций для приема акустических колебаний с целью обнаружения летательных аппаратов и определения положения артиллерийских батарей. Основными типами узконаправленных микрофонов на втором этапе стали системы с параболическим отражателем и трубчатые микрофоны. В тоже время были разработаны первые микрофонные решетки, однако они обладали ограниченными возможностями и весьма сложной реализацией. Кроме того были разработаны основы обработки сигналов в системах в виде решеток построенных из единичных элементов (антенн или микрофонов). Наконец, третьим этапом развития узконаправленных микрофонов (начиная с 90-х годов) стало применение средств цифровой обработки сигналов (ЦОС). С развитием ЦОС МР стали применяться для решения широкого круга задач, связанных с обработкой речевых сигналов. Мощным дополнительным импульсом к расширению сферы применения МР явилась разработка и серийный выпуск цифровых микроэлектромеханических систем МЭМС (Microelectromechanical systems MEMS) микрофонов. Все технологии извлечения речевой информации в МР строятся на основе алгоритмов ЦОС. Применение ЦОС значительно расширяет функциональные возможности узконаправленных микрофонов [1-3]

Основополагающими характеристиками средств акустической разведки, влияющими на дальность разведывательного контакта при использовании узконаправленных микрофонов, является значение индекса направленности (ИН)  $Q$  в диапазоне частот речевого сигнала и их максимально применимая рабочая частота.

Индекс направленности микрофона может быть рассчитан по формуле:

$$Q = 10 * \lg \left( \frac{2}{\int_0^\pi R^2(\theta) * \sin(\theta) d\theta} \right),$$

В первой части доклада проводится обоснование выбора параметров узконаправленных микрофонов с аналоговой обработкой сигналов на основе исследования их характеристик и сравнительного анализа. При одинаковых габаритных размерах сравниваются характеристики и индексы направленности узконаправленных микрофонов типа линейной группы и плоской решётки микрофонов, трубчатого микрофона органного типа и рефлекторного микрофон в диапазоне частот речевого сигнала.

| № | Тип узконаправленного микрофона                 | Формула для расчёта характеристики направленности узконаправленного микрофона   |
|---|---|---|
| 1 | Линейная группа микрофонов (плоская решётка)[1] | $R(\Theta) = \frac{\sin(\frac{n * \pi * d}{\lambda} * \sin \Theta)}{n * \sin(\frac{\pi * d}{\lambda} * \sin \Theta)}$             |
| 2 | Трубчатый микрофон органного типа[1]            | $R(\Theta) = \frac{\sin(\frac{n * \pi * d}{\lambda} * (1 - \cos \Theta))}{n * \sin(\frac{\pi * d}{\lambda} * (1 - \cos \Theta))}$ |
| 3 | Рефлекторный микрофон[4]                        | $R(\Theta) = \frac{2 * J_1(\psi)}{\psi}, \text{ где } \psi = \frac{2 * \pi}{\lambda} \rho_0 * \sin \Theta$                        |

Эффективность применения микрофонов оценивается путём расчёта разборчивости речи, на которую влияют как энергетические характеристики сигнала, полученного на выходе средства акустической разведки, так и характер изменения зависимости индекса направленности микрофона от частоты для речевого диапазона.

Во второй части доклада рассматриваются особенности характеристик МР использующих разные алгоритмы ЦОС для базового элемента МР состоящего из двух микрофонов: алгоритм сверхнаправленности, алгоритм задержки и суммирования, алгоритм дифференциальной микрофонной решетки.

Большим недостатком алгоритма дифференциальной микрофонной решетки является спад индекса направленности с увеличением частоты. На более высоких частотах дифференциальная решетка уступает алгоритму задержки и суммирования. Алгоритм сверхнаправленности объединяет преимущества двух алгоритмов: 1) дифференциального; 2) задержки и суммирования. На низких частотах используется более эффективный дифференциальный алгоритм, а на более высокой частоте используется алгоритм задержки и суммирования. Оптимальной структурой микрофонной решетки для получения максимального индекса направленности является алгоритм сверхнаправленности. На низких частотах алгоритм задержки и суммирования ведет себя как ненаправленный микрофон, в то время дифференциальный имеет форму кардиоиды. Также можно получить диаграмму направленности в виде гиперкардиоиды при использовании оптимального фильтра. На низкой частоте характеристики направленности дифференциальной решетки и алгоритма сверхнаправленности совпадают, но с ростом частоты алгоритм задержки и суммирования

показывает результаты лучше, чем дифференциальный. Алгоритм сверхнаправленности позволяет получить максимально значение индекса направленности. [4]

**Ключевые слова:** акустическая разведка, узконаправленные микрофоны, аналоговая обработка сигналов, индекс направленности, микроэлектромеханические системы, алгоритмы цифровой обработки сигналов, эффективность, разборчивость речи.

### Литература

1. Олейников А.Н., Войтенко А.О. Сравнительная характеристика параметров узконаправленных микрофонов. «Радиотехника» Всеукраинский межведомственный научно-технический сборник, 2013, Вып. № 173. с. 224-231.
2. Столбов М.Б. Применение микрофонных решеток для дистанционного сбора речевой информации. Научно-технический вестник информационных технологий, механики и оптики, 2015, Т. 15. No 4, с. 661–675.
3. Антіпов І.Є., Олейніков А.М., Ликов Ю.В. та інші. Засоби та системи технічного захисту інформації: Навчальний посібник для студентів ЗВО / Харків: ХНУРЕ, 2019, 216 с.
4. Buck M., Rößler M. First order differential microphone arrays for automotive applications. Proc. 7th International Workshop on Acoustic Echo and Noise Control, IWAENC. Darmstadt, Germany, 2001, pp. 19–22.

### Selection of technical means parameters of acoustic reconnaissance

The report substantiates the choice of the parameters of narrow-beam microphones with analog and digital signal processing on the basis of a study of their characteristics and comparative analysis. With the same overall dimensions, the characteristics and directivity indices of narrowly directed microphones of the following type are compared: a linear group and a flat array of microphones, a tubular microphone of an organ type and a reflex microphone. For the basic element of the microphone array, consisting of two microphones, the features of the characteristics of microphone arrays using different algorithms for digital signal processing are investigated: superdirectional algorithm, delay and summation algorithm, differential microphone array algorithm. The effectiveness of the use of microphones is assessed by speech intelligibility.

## ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ МЕТОДОВ И СРЕДСТВ ПОДАВЛЕНИЯ НЕСАНКЦИОНИРОВАННОЙ ЗАПИСИ РЕЧИ

**А. Олейников, В. Пулавский, И. Чигирев**

Харьковский национальный университет радиоэлектроники. Харьков, Украина

e-mail: [anatoly.oleynikov@nure.ua](mailto:anatoly.oleynikov@nure.ua)

Подавление несанкционированной записи речи на диктофон может осуществляться акустическим, ультразвуковым и электромагнитным методами [1, 2].

*Акустический* метод в его традиционной интерпретации основан на постановке пространственной акустической помехи в направлении возможного расположения записывающего устройства. Акустическая помеха подается постоянно и присутствует вне зависимости наличия или отсутствия речевого сигнала, что производит отрицательное психологическое воздействие на собеседников, вызывая их раздражение. Увеличение амплитуды акустической помехи не повышает эффективность защиты, так как приводит к самопроизвольному увеличению громкости разговора со стороны обоих собеседников. По этим причинам акустический метод противодействия несанкционированной записи на диктофон считался малоэффективным.

Задача *электромагнитных* подавителей состоит в наведении на случайных антеннах диктофона, в качестве которых выступают дорожки на печатной плате и элементы схемы, высокочастотного помехового сигнала. Наведенный высокочастотный помеховый сигнал детектируется на нелинейных элементах диктофона и проникает в его звуковой тракт, что приводит к существенному искажению полезного сигнала.

Средства *ультразвукового* подавления излучают мощные ультразвуковые колебания (УЗК). Современные диктофоны оснащаются, как правило, электретными микрофонами верхняя граница полосы пропускания которых составляет 25-27 кГц и попадает в ультразвуковой диапазон частот. Применяют одночастотные и двухчастотные ультразвуковые подаватели, достоинства и недостатки которых приводятся в докладе

Системы ультразвукового подавления оказываются неэффективными, если микрофон записывающего устройства защищен специальным тканым материалом (или находится в кармане одежды), имеют ультразвуковые фильтры или применен микрофон звукового диапазона.

Показано, что если тип записывающего средства априорно не известен, то общим недостатком всех рассматриваемых методов является отсутствие гарантированного подавления несанкционированной записи речи.

Для существенного повышения эффективности подавления предложено **адаптировать акустический метод с учетом** особенностей распространения акустических колебаний в воздухе и психофизического восприятия звуков ухом человека, а именно:

1- расстояние между источником акустической помехи и местом вероятного расположения диктофона необходимо свести до минимума и сделать его в несколько раз меньше, чем расстояние между источником речи и диктофоном ;

2- формировать акустическую помеху на основе речи собеседников. Такая речеподобная помеха оказывается коррелированной во времени с речью, что позволяет избавиться от отрицательного психологического воздействия помехи на собеседников в моменты тишины в паузах между фразами и не поддается фильтрации, так как занимает ту же полосу частот, что и речевой сигнал. Помеха присутствует только в моменты наличия речевого сигнала и отсутствует в паузах. . Затрудняется возможность получения копии помехи для проведения очистки.

3- существенно улучшить технические параметры акустической системы для излучения речеподобной помехи применив **электростатическую акустическую систему** излучения помехи, приблизив спектральные характеристики помехи к голосам собеседников и уменьшив величину коэффициента гармоник, отказавшись от использования традиционных электродинамических излучателей. Кроме того сужение диаграммы направленности электростатической акустической системы при одинаковой излучающей мощности приведет к увеличению плотности потока мощности помехового сигнала, что повышает эффективность подавления несанкционированной записи речи.

Для оценки эффективности помехи, сформированной электростатическим излучателем, был проведён эксперимент по сравнению её зоны подавления с зоной подавления колонки с динамическим излучателем. Для эксперимента использовался электростатический излучатель с размерами сторон 25см на 34см. в условиях открытого пространства. Схема экспериментальной установки изображена на рисунке 1.

Электростатический излучатель воспроизводил речеподобную помеху сформированную из речи человека с уровнем 65 дБ на расстоянии 1 метр. Акустические измерения производились сертифицированным микрофоном Behringer ECM8000 с нормированной частотной характеристикой и круговой диаграммой направленности. Колонка формировала человеческую речь. Зона подавления определялась по разборчивости речи на фоне помехи при различных углах  $\alpha$  и дальности  $l$  с использованием метода экспертной оценки. Для демонстрации преимущества предложенного метода на рисунке 2 изображены зоны подавления при формировании помехи электростатическим излучателем (красная кривая) и электродинамической колонкой. (синяя кривая)

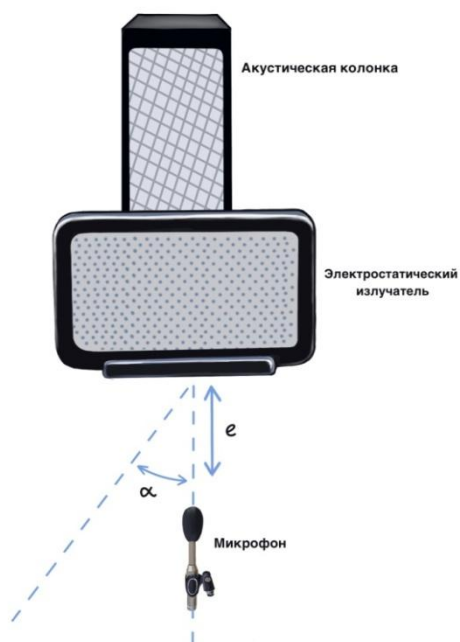


Рисунок 1

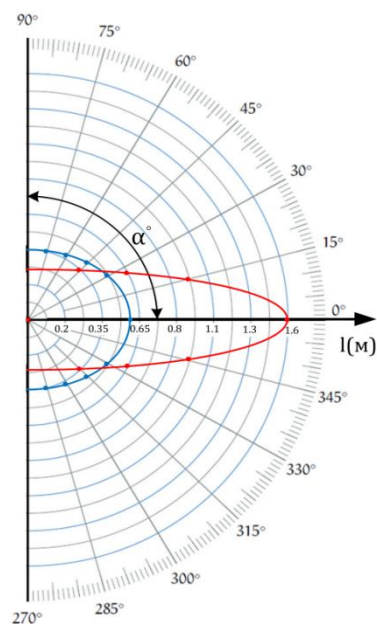


Рисунок 2

Предложенный адаптированный акустический метод будет одинаково эффективен для любых типов записывающих устройств, так как помеха формируется по функциональному каналу – акустическому.

**Ключевые слова:** речь, несанкционированная запись, методы подавления, электростатическая акустическая система, эффективность.

### Литература

1. 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.
2. 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.

### **Increasing the efficiency of methods and means of suppressing unauthorized speech recording**

The report analyzes the effectiveness of suppression of unauthorized speech recording using acoustic, electromagnetic and ultrasonic countermeasures. For a significant increase in the efficiency of suppression, it is proposed to adapt the acoustic method taking into account the peculiarities of the propagation of acoustic vibrations in the air and the psychophysical perception of sounds by the human ear. The results of experimental studies of a suppressor with an electrostatic emitter are presented.

## АНАЛИЗ БЕЗОПАСНОСТИ АТОМАРНЫХ ОБМЕНОВ МЕЖДУ BITCOIN И LITECOIN

**В.В. Просолов**

Харьковский национальный университет радиоэлектроники, Харьков, Украина

e-mail: [vladyslav.prosolov@nure.ua](mailto:vladyslav.prosolov@nure.ua)

Несмотря на повышенную волатильность, криптовалютный рынок развивается и постоянно пополняется новыми цифровыми активами. На 2021 их количество достигло более 6000, большая часть из которых в различном процентном соотношении находится в портфелях криптовалютных инвесторов и трейдеров.

Повышенное предложение создает потребность в обмене криптовалюты. До недавнего времени он осуществлялся с помощью посредников - криптовалютных бирж или обменников. Но это подразумевает комиссию и дополнительные расходы на конвертацию.

Атомарный обмен - это процесс, в котором два человека, владеющие двумя разными типами криптовалюты, осуществляют транзакцию, в которой они меняют определенную сумму каждой валюты, равной сумме, которую обменивает другой.

Конвертация криптовалюты посредством реализации атомарного обмена осуществляется с помощью так называемых хешированных контрактов с временной блокировкой (Hash Time Locked Contracts, HTLC).

Чтобы сделка была осуществлена, участники открывают секретные коды в блокчейне, которые до этого были известны только владельцу криптовалюты. Вторым дополнительным условием является установка двух блокчейнов криптовалюты, которые будут участвовать в обмене [1].

HTLC не перегружает основную сеть, что позволяет сделать перевод мгновенным, в отличие от аналогичной операции на бирже или у других посредников. Это временный смарт контракт. В течение заранее установленного срока оба участника должны подтвердить операцию с помощью специально сгенерированного платежного поручения. Без этого перевод не состоится, что сводит риски кражи денег к нулю. Если один из участников не предоставит подтверждение перевода в установленные сроки, то средства автоматически возвращаются [2].

Рассмотрим преимущества атомарных обменов. Прежде всего, при торговле через атомарные обмены всегда только пользователь имеет доступ к своим личным ключам и, следовательно, к своим монетам и токенам. Нет необходимости передавать контроль над своими средствами третьей стороне.

Во-вторых, атомарные обмены устроены таким образом, что обмен или происходит, и обе стороны получают желаемые средства, или вообще ничего не происходит, и обе стороны сохраняют средства, с которыми они начали (за вычетом очень небольшой комиссии за

транзакцию для получателя). Атомарные обмены делают торговлю цифровыми активами максимально безопасной.

В-третьих, атомарные обмены намного дешевле торговли на централизованных биржах. Большинство централизованных бирж взимают относительно высокие комиссии, обычно 0,2% от каждой транзакции, для каждой стороны в сделке. Большинство централизованных бирж взимают комиссию и за снятие средств. А также за то, что возвращают контроль над вашими средствами.

И последнее, но не менее важное: атомарные свопы позволяют торговать между более широким спектром монет и токенов. Например, AtomicDEX, децентрализованная биржа Komodo, ликвидировала разрыв между монетами на основе протокола биткойнов и токенами ERC-20 на основе Ethereum.

Например, пользователь может торговать непосредственно с альткойна на основе BTC на токен ERC-20, или наоборот. Прежде чем платформа Komodo сделала это возможным, трейдеру пришлось бы сделать несколько обменов, чтобы получить тот же результат. В процессе торговли использовались бы альткойны на основе BTC -> биткойнов -> Эфир -> токен ERC-20 с комиссией за каждую из трех транзакций.

Однако, в использовании атомарных обменов есть и ряд недостатков. Обмен на централизованной бирже может занимать секунды, в то время как проведение одного атомарного обмена зависит от платформ и участников процесса и может занимать достаточно длительное время. Например, гарантированный обмен может быть проведен не менее чем за 2 часа (время полного подтверждения 2-х блоков в Bitcoin и 2-х блоков в Litecoin) и это при условии, что стороны действуют быстро. Верхний предел проведения обмена в нашем случае - 12 часов. Следующим ограничением является высокая комиссия за проведение обмена. Для обмена каждому участнику нужно провести две транзакции: одну в сети Bitcoin и одну в Litecoin, а это, как известно, не самые дешевые с точки зрения комиссии системы. На той же централизованной бирже комиссия может составлять несколько центов за обмен. Еще одним ограничением является необходимость самостоятельного поиска стороны для взаимодействия. Децентрализованные биржи помогают решить эту проблему, но все равно скорость согласования заказов на них гораздо ниже, чем на централизованных. Также к ограничениям можно отнести невозможность проведения атомарных обменов с участием фиатных валют. Отдельно стоит упомянуть о риске потери монет в результате сложно написанного смарт-контракта. Если пользователь не провел аудит смарт-контракта транзакции, которая была отправлена в сеть, он может потерять свои деньги и данную транзакцию невозможно будет отменить.

Атомарные обмены имеют дополнительные преимущества в безопасности владения криптовалютой и обмену их между собой. Что делают их более интересными для тех, кто хочет максимально самостоятельно контролировать свои средства и уровень безопасности их хранения.

**Ключевые слова:** BTC/LTC, Атомарный Обмен, Bitcoin, Litecoin, криптовалюта.

### Литература

1. Кравченко П., Скрябин Б., Курбатов А., Дубинина О. Блокчейн и децентрализованные системы: учеб. пособие для студ. заведений высш. образования: в 3 частях. Ч. 3, Харьков: 2020, 305 с.
2. Frankenfield J. Cryptocurrency. Hashed Timelock Contract (HTLC) [Электронный ресурс], Investopedia, 2021, Режим доступа: <https://www.investopedia.com/terms/h/hashed-timelock-contract.asp>

### Safety analysis of atomic swap between bitcoin and litecoin

The work is devoted to the analysis of atomic swaps in cryptocurrency. An exchange between a pair of BITCOIN / LITCOIN is considered, which is implemented on the basis of Hash Time Locked Contracts (HTLC). Such exchange method allows users to have complete control over their funds and reduce transfer fees. This provides better protection for storing and exchanging cryptocurrencies, but requires more skill and attention from the user during transactions.

## IoT TEXNOLOGİYASINA YÖNƏLMİŞ “MIRAI” KİBERHÜCUMU VƏ ONDAN MÜHAFİZƏNİN TƏŞKİLİ

V. Qasimov, C. İsmayılov

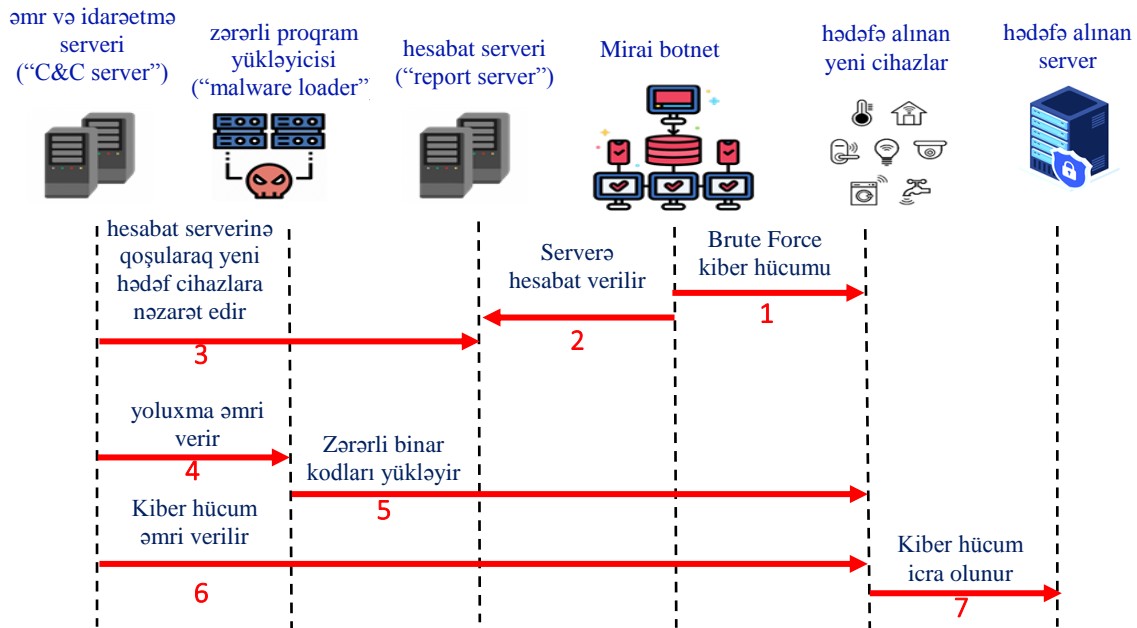
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

e-mail: [vaqif.qasimov@aztu.edu.az](mailto:vaqif.qasimov@aztu.edu.az), [jalal.ismayil@aztu.edu.az](mailto:jalal.ismayil@aztu.edu.az)

**Giriş.** Müasir dövrdə insanların IoT texnologiyasından istifadəyə olan zərurət getdikcə artmaqdadır. Lakin IoT əsasında işləyən ağıllı cihazların təhlükəsizliyi, eləcə də onların topladığı verilənlərin gizliliyi məsələsi istifadəçilərin böyük narahatlığına səbəb olur. Belə ki, bu verilənlərin müxtəlif növ zərərli proqram vasitələri ilə əldə olunması mümkündür. Belə zərərli proqram vasitələrindən biri də “Mirai” proqram vasitəsidir.

Mirai (digər adı ilə “Dyn Attack”) - Telnet protokolunu dəstəkləyən IoT cihazlarında, cihazın ilkin istifadəçi adı və şifrəsindən istifadə etməklə cihazın hesabına daxil olmağa çalışan zərərli proqram vasitəsidir. Hər hansısa bir cihaza yoluxan bu zərərli proqram vasitəsi, yoluxmadan sonra, başqa yeni cihazlara yoluxmaq üçün onları axtarmağa başlayır. Mirai zərərli proqram vasitəsinə yoluxan digər cihazlar, onun, yəni "Mirai Botnet"-in tərkib hissəsinə çevrilirlər. Daha sonra kiber cinayətkarlar, bu cihazların vasitəsi ilə hədəfdə olan serveri çökdürmək üçün DDoS ("Distributed Denial of Services Attack" - paylanmış xidmətlərdən imtina hücumu) kiber hücumunu həyata keçirirlər. Mirai zərərli proqram vasitəsi, əsasən, IP-kameraları, “Raspberry PI” cihazlarını, marşrutizatorları və digər ağıllı cihazları (sensorlar) hədəf alırlar [1,2].

“Mirai Botnet” zərərli proqram vasitəsinin əsas məqsədi, düzgün konfigurasiya edilməmiş cihazlara yoluxmaq və “bot” və ya “botmaster” tərəfindən əmr qəbul edərək, DDoS hücumunu həyata keçirməkdən ibarətdir (şəkil 1).



Şəkil 1. “Mirai” zərərli proqram vasitəsinin iş prinsipinin arxitektura təsviri

Bu proses aşağıdakı kimi icra olunur [3,4]:

1) “Mirai”, 23 və ya 2323 nömrəli TCP əlaqə portları vasitəsilə təsadüfi olaraq IP ünvanları yoxlayır. “Mirai Bot”, düzgün konfigurasiya edilməmiş cihazların ilkin identifikasiya məlumatlarını əldə etmək üçün onlara “brute force” kiber hücumunu həyata keçirir. Qeyd edək ki, “Mirai” zərərli proqram vasitəsində kodlaşdırılmış 62 sayda ehtimallı identifikasiya məlumatları (cihazın adı və şifrəsi) mövcuddur.

2) “Mirai Bot”, cihazın identifikasiya məlumatlarını əldə etdikdən sonra onun xarakteristikalarını fərqli bir əlaqə portu ilə “report server”-ə ötürür.

3) Bot meneceri, C&C (“command and control”) serveri vasitəsilə “report server”-lə əlaqə quraraq, hədəfdə olan yeni cihazlara nəzarət edir.

4) Bot meneceri, zərərli proqram yükləyicisinə (“malware loader”), hədəfdə olan yeni cihazlara yoluxmaq üçün yoluxma əmrini (“infect command”) verir.

5) Zərərli proqram yükləyicisi (“malware loader”), hədəfdə olan cihazda seans başlayır və onun xarakteristikalarına uyğun olan zərərli binar kodları (“malicious binary”) Wget ([www.gnu.org/software](http://www.gnu.org/software)) vasitəsi ilə ona yükləyir və quraşdırır. Zərərli proqram vasitəsi cihaza quraşdırıldıqdan sonra “Mirai”, özünü digər zərərli proqram vasitələrindən qorumaq məqsədilə port 22 (SSH), port 23 (TELNET) və port 80 (HTTP) əlaqə portlarını bağlayır.

6) Bot meneceri, “C&C server” ilə kiber hücumun növü, müddəti və bot nümunələri, eləcə də hədəfdə olan serverin IP ünvanları kimi parametrlərdən ibarət əmr ilə bütün botlara hədəfdə olan serverə hücum etmək əmri verir.

7) Botlar tərəfindən hədəfdə olan serverə kiber hücum (məs. DDoS kiber hücumu) həyata keçirilir.

#### **“Mirai” zərərli proqram vasitəsindən mühafizənin təşkili.**

“Mirai” zərərli proqram vasitəsindən mühafizənin təşkil etmək üçün aşağıdakı qaydalara riayət etmək lazımdır [5]:

- Şəbəkəyə qoşulan hər bir cihazın təhlükəsizlik parametrləri uyğun qaydada nizamlanmalıdır.
- Satın alınan IoT cihazının proqram interfeysinə daxil olmaq üçün istifadə olunan cari istidadəçi adını və parolu (*məsələn, ID: admin., password: admin*) dəyişdirmək lazımdır. IoT cihazlarında autentifikasiyadan istifadə edilməlidir.
- IoT cihazları ilə VEM arasında verilənlərin mübadiləsinin təhlükəsiz şəkildə yerinə yetirilməsi üçün şəbəkələrarası qoruyucu ekrandan (“firewall”) istifadə edilməlidir.
- IoT cihazları üçün nəzərdə tutulmuş proqram yeniləmələrini vaxtında yükləmək lazımdır. Qeyd etmək lazımdır ki, bu yeniləmələri yükləməzdən əvvəl, onun haqqında məlumat əldə etmək lazımdır.

**Nəticə.** Statistik göstəricilərə əsasən, hal-hazırda dünyada çox sayda IoT cihazları mövcuddur və gələcəkdə bu cihazların sayının sürətlə artacağı gözlənilir. Kibercinayətkarların, IoT cihazlarının topladığı verilənlərin gizliliyinin açmaq, həmçinin, bu cihazlardan istifadə etməklə, hədəf serverə DDoS kiber hücumunu həyata keçirmək istəkləri, gələcəkdə, IoT texnologiyasının təhlükəsizliyi məsələsinin daha aktual bir hala gələcəyini göstərir. Ona görə də IoT texnologiyasının təhlükəsizliyi daim diqqət mərkəzində saxlanılmalıdır.

**Açar sözlər:** Əşyaların interneti, kiberhücum, Mirai, təhlükəsizlik.

#### **Ədəbiyyat**

1. <https://www.iotforall.com/iot-attacks-hacker-motivation>
2. <https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities>
3. Burair S.H., Manickam S., Alieya K. Internet of Things botnet (mirai): a systematic review. Sci. Int. (Lahore), 31(4), 2019, 607-616.
4. Koliass C., Kambourakis G., Stavrou A., & Voas J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.
5. <https://www.trendmicro.com/vinfo/fr/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions>

## "Mirai" cyber attack on IOT technology and its protection

As with other technologies, the issue of security in IoT technology is a serious concern for users. There are various types of malware aimed at smart devices, one of which is Mirai. This article will discuss the creation of Mirai, its working principle and the organization of protection against Mirai malware.

## İNFORMASYA SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİN PROQRAM VASİTƏLƏRİ

**M.Ə. Salmanova**

Azərbaycan Dövlət İqtisad Universiteti (UNEC), Bakı, Azərbaycan

e-amil: [mahila.salmanova@mail.ru](mailto:mahila.salmanova@mail.ru)

İnternetin geniş istifadəsi informasiya sistemlərində təhlükəsizliyə diqqəti artırmayı tələb edir. İnformasiya sistemlərində məxfiliyi, tamlığı və əlyətənliyi təmin etmək üçün bir çox təhlükəsizlik vasitələri və layihəsi hazırlanıb və hazırlanmaqdadır.

İnformasiya təhlükəsizliyinin bütün dünyada qəbul edilən üç əsas prinsipi var:

- məxfilik
- tamlıq
- əlyətənlik

Müxtəlif informasiya təhdidlərinin davamlı böyüməsinə və dinamik inkişafına baxmayaraq, hələ də qorunma metodları mövcuddur.

Fiziki qorunma informasiya təhlükəsizliyinin birinci mərhələsidir. Buraya icazəsiz istifadəçilər üçün girişin məhdudlaşdırılması və xüsusilə də server bölməsinə daxil olmaq üçün giriş sistemi daxildir. İnformasiyanın qorunmasının əsas səviyyəsi kompüter viruslarını bloklayan proqramlar (antivirus proqramları), şübhəli yazışmaları süzəcdən keçirmək üçün sistemlərdir. Ümumiyyətlə kompüter sistemində və şəbəkəsində istifadə olunan vacib informasiyaları qorunması üçün onun mütləq şəkildə ehtiyat nüsxəsi yaradılmalıdır. Əsas nüsxə və ehtiyat nüsxə ilə bərabər yüksək səviyyədə şifrələnməlidir [2].

İnformasiya sisteminin mühafizə edilməsinin ən vacib şərtlərindən biri onun aparat və proqram təminatının sazlığının pozulması və işinin dayanması hallarından mühafizə edilməsidir. Burada prosessor, yaddaş qurğuları, periferiya qurğuları və daxili proqramlar sistemi dayanmalardan mühafizə etmək üçün əsas rol oynayırlar.

Proqram təminatı əgər sistemdəki elementlərin etibarlılıq dərəcəsi yüksək deyilsə o zaman daha vacib mühafizə vasitəsinə çevrilir. Etibarlılıq dərəcəsi o zaman yüksək olur ki, sistem lazımı əməliyyatları tam dəqiqliklə və lazımı vaxtda yerinə yetirə bilsin. Prosesin avtomatlaşdırıla bilmə dərəcəsi və onun izlənməsinin təşkil olunması ilə isə proqram təminatının etibarlılıq dərəcəsi təyin olunur.

İnformasiya təhlükəsizliyi sahəsində yaşanan təhlükəsizlik pozuntularının artan hissəsi şəbəkələrdən və sistemlərdən tətbiqetmələrə və hətta verilənlər bazalarına keçməkdir. Təhlükəsiz

mühitlərdə institusional və ya fərdi qaydada iş aparmaq ehtiyacı və istəyi gündən-günə artır və istifadə olunan proqram təminatının təhlükəsizliyi informasiya təhlükəsizliyinin təmin edilməsində əsas rol oynayır [1].

Informasiyanın qorunması üçün informasiyanın qorunması interfeysi anlayışı mövcuddur. Bu informasiyanın mühafizəsinin aparat və proqram təminatını özündə birləşdirir, onlar arasında əlaqəni izah edir.

Məxfi olan informasiyanın sızmasının, yayılmasının və eyni zamanda bu informasiyaya səlahiyyətsiz şəxslərin giriş imkanının məhdudlaşdırılması informasiya mühafizəsinin aparat vasitələrinin əsas məqsədidir.

İnformasiya sistemində təhlükəsizliyi təmin etmək üçün də bir çox təhlükəsizlik modelləri mövcuddur:

- Çoxsəviyyəli qəfəs modelləri
- Müdaxilə edilə bilməyən modellər
- İnformasiya axını modeli və s.

İnformasiya təhlükəsizliyini təmin etmək üçün bir çox tədqiqatlar aparılır. Bu tədqiqatlar ümumiyyətlə bütün sistemi əhatə edir. Təhlükəsizlik divarlarını quraşdırmaq, müdaxiləni aşkarlama sistemlərini qurmaq, etibarlı rabitə protokollarını təmin etmək və zərərli kodlara qarşı proqramdan istifadə kimi həllər ola bilər. Lakin bütün bu araşdırmalardan sonra da sistemdə təcavüzkarların faydalana biləcəyi zəifliklər ola bilər. Bu boşluqlar müxtəlif təhlükəsizlik vasitələrindən istifadə edilərək aşkar edilə və lazımi tədbirlər görülməlidir. Təhlükəsizliyi təmin edən aparat proqram vasitələri sistemi izləmək imkanı da təklif edir. Mövcud aparat vasitələri ümumiyyətlə kompüter sistemlərinə hücum etmək üçün hazırlanmışdır. Buradakı əsas fikir sistemin təcavüzkarlar qarşısında zəifliklərini aşkarlamaq və lazımi tədbirləri görməkdir [3].

Yaxşı bir təhlükəsizlik aparat-proqram vasitəsi istifadəçilərin işini çətinləşdirməməli, istifadəçilər arasında heç bir uyğunsuzluq yaratmamalı və istifadəçilərin işinə heç bir problem yaratmamalıdır. Vasitələr istifadəçilərin və sistem administratorlarının əməl edə biləcəyi və tətbiq edə biləcəyi, kifayət qədər güclü olan və onların bu vasitələri tətbiq etməsini asanlaşdıran qaydalardan ibarət olmalıdır. Təhlükəsizlik tədbirləri üçün aparat-proqram qurulmasını həyata keçirən təşkilatlar və ya şirkətlərbunu tətbiq etmək üçün inzibati və texniki səlahiyyətlərlə malik olmalıdır.

Ümumiyyətlə, informasiya və kompüter sistemlərində nə qədər təhlükəsizlik tədbirləri görülsə də, riskləri sifirə endirmək mümkün olmadığını bilmək lazımdır. Görüləcək ən əsas tədbirlər risklərə qarşı daimi xəbərdarlıq etmək, təhlükəsizlik siyasətlərini yaratmaq və istifadə etmək, proseslərin performansını davamlı izləmək və təsiretmə ehtimalını minimuma endirməkdir. İnformasiya təhlükəsizliyinin təmini üçün təhlükəsizlik siyasəti tətbiq olunmalıdır.

**Açar sözlər:** informasiya, informasiya sistemləri təhlükəsi, internet, təhlükəsizlik.

## Ədəbiyyat

1. Arms W., WTEC Principles of Digital Libraries, 2018.
2. Audrey A., Enrico F., Information Security Issues in a Digital Library Environment, 2018.
3. Balayev R.Ə., Əlizadə M.N. İntellektual sistemlər və texnologiyalar. Bakı, MSV Nəşr, 2016.

### Information system security software

In parallel with the extraordinary developments in the world of information technology and systems, the importance of information systems security for individuals, institutions and organizations is growing. The security program used for this purpose is of great importance in the protection of systems belonging to individual enterprises and organizations. Thus, active security policies, useful security tools, and various security measures that are important in the security of information systems are presented, as well as the basic security strategies required in person or as an organization.

### HARD PROBLEMS IN LATTICE-BASED CRYPTOGRAPHY: X-LWE

**K. Seyhan<sup>1</sup>, S. Akleyek<sup>1</sup>, E. Kılıç<sup>1</sup>, Y. Oruç<sup>2</sup>**

<sup>1</sup>Department of Computer Engineering, Ondokuz Mayıs University, Samsun, Turkey

<sup>2</sup>Rönesans Holding, Ankara, Turkey

e-amil: [kubra.seyhan@bil.omu.edu.tr](mailto:kubra.seyhan@bil.omu.edu.tr), [sedat.akleyek@bil.omu.edu.tr](mailto:sedat.akleyek@bil.omu.edu.tr), [erdal.kilic@bil.omu.edu.tr](mailto:erdal.kilic@bil.omu.edu.tr)  
[yalcin.oruc@ronesans.com](mailto:yalcin.oruc@ronesans.com)

**Abstract.** This paper explains the basic idea of the new hard lattice problem for designing a post-quantum secure public-key cryptosystem. The components in the proposed problem will provide the reusable key feature for post-quantum secure key exchange protocols.

#### 1. Introduction

Diffie and Hellman introduced the public-key cryptography concept in the 1970s. Key exchange (KE) protocols allow the sharing of the secret key to be used in symmetric ciphers. At the same time, authentication and non-repudiation are guaranteed with digital signature schemes. Traditional public key cryptosystems Diffie-Hellman (DH) KE protocol and Digital Signature Algorithm (DSA) scheme are based on discrete logarithm problem (DLP) hardness assumption. The RSA encryption/key encapsulation protocol is based on the integer factorization problem (IFP). In contrast, the ECDSA digital signature and ECDH KE protocols are based on the hardness assumption of the elliptic curve DLP problem. In other words, with the power of today's computational systems, it is not possible to solve these problems in polynomial time [5]. Shor algorithm proposed in 1994 is a solution proposal for DLP and IFP problems in polynomial time in quantum computers. Therefore, in the presence of large-scale quantum computers, these cryptosystems that allow secure communication will become insecure. This situation has revealed the necessity of creating secure

public-key cryptosystems even in the presence of quantum computers. The families of post-quantum secure cryptosystems are classified as lattice, code, hash, multivariate polynomial, isogenies and other systems. The lattice-based cryptosystem family has been one of the most promising candidates for cryptosystem classes. Some of the important features of lattice-based cryptosystems are as follows: worst-case hardness guarantees, relatively efficient implementations, excellent simplicity, and strong security proofs. In this context, the design components of lattice-based KE protocols, similar to the traditional DH KE protocol, are given in Figure 1 [1]. The main framework of the scheme is described in Figure 1. In this framework, DLP has been replaced by the learning with errors (LWE) problem. The security of this scheme is guaranteed by the fact that hard lattice problems cannot be solved in polynomial time, even in the presence of quantum computers. Lattice-based hard problems and new hard problems that can be proposed by reducing the hardness assumptions are essential for proposing quantum secure cryptosystems.

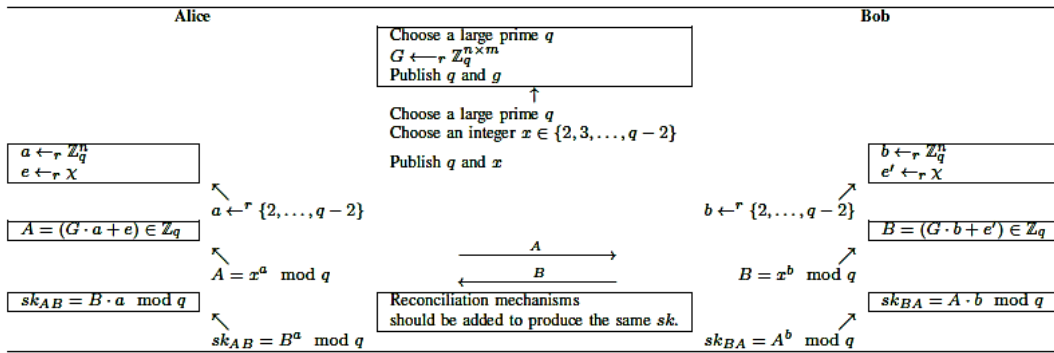


Figure 1. Framework of DH-Like Lattice-Based Key Exchange Protocol

## 2. Hard Problems Based on LWE

This section explains the LWE problem, its derivatives, and the proposed new hard problem widely used in lattice-based cryptosystem design. The symbols used in the paper and their meanings are as follows:  $R$ : Real numbers,  $Z$ : Integers,  $R$ : Polynomial ring,  $p, q \in Z^+$ , prime modulus such that  $q > p$ ,  $Z_q$ : Integers in mod  $q$  denoted by  $\{0, \dots, q - 1\}$ ,  $a \in Z_q^n$ :  $n$ -dimensional vector whose elements are selected from mod  $q$ ,  $\chi$ : Discrete Gaussian distribution defined on integers with width  $\alpha \cdot q$  such that  $\alpha < 1$ ,  $\kappa$ : security parameter,  $\chi_{\alpha_1}$  and  $\chi_{\alpha_2}$  discrete Gaussian distributions with standard deviations of  $\alpha_1$  and  $\alpha_2$  such that  $\frac{\alpha_1}{\alpha_2} = 2^{\omega(\log \kappa)}$  and  $\alpha_2 \leq \alpha_1$ ,  $\chi_\gamma$ : Discrete Gaussian distribution with standard deviation  $\gamma = \sqrt{\alpha_1^2 + \alpha_2^2}$ ,  $Z[x]$ : A set of polynomials with integer coefficients,  $R \in Z[x]/(\ )$ : Ring of polynomials with integer coefficients  $(a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}, \forall a_i \in Z)$ ,  $R_q$ : Ring of integer polynomials whose coefficients are in mod  $q$ ,  $M = R^d$ : For  $\forall m_i \in R$ , module algebraic structure consisting of  $d$ -dimensional ring elements denoted by  $m = (m_0, \dots, m_{q-1}) \in M$ .

**Definition 1. (R)LWE [2]:** Let  $s \in Z_q^n$  be a vector,  $a_i \in Z_q^n$  be random value, and the error term  $e_i \leftarrow \chi$ . Then, LWE distribution is defined as follows:  $(a_i, b_i = s \cdot a_i + e_i \text{ mod } q) \in Z_q^n \times Z_q$ . The hardness of the LWE problem is expressed in problems based on the worst-case hardness. The

hardness of the LWE problem based on the average-case hardness when specific parameter conditions are taken into account is expressed by the  $GapSVP_\gamma$  and  $SIVP_\gamma$ . In addition, by changing the algebraic structure used in the LWE problem, ring-LWE, module-LWE problems are defined.

The methods used to achieve reconciliation on the shared secret key in KE protocols based on (R)LWE-like problems can leak information about the static secret key of the parties. The pasteurization method proposed in [2] requires additional components to prevent information leakage about the secret key. The reusable key property will allow efficient public-key cryptosystem design by adding these additional components to the hard problem structure. This feature will improve the key generation phase, where the most time is spent in cryptosystem design. In this context, the new lattice-based hard problem is proposed in Definition 2.

**Definition 2. Extended-LWE (X-LWE):** Let  $n$  be integer,  $q = q(n) \leq poly(n)$  be a prime,  $H: \chi_\gamma \rightarrow \chi_{\alpha_1}$  be a one-way function,  $s \leftarrow^r \chi_{\alpha_2}$ ,  $a \leftarrow^r R_q$ , and  $e \leftarrow^r \chi_\gamma$ . Then, X-LWE distribution is defined as follows:  $(a, b = a(s + H(e)) + e) \in R_q \times R_q$ .

In the X-LWE problem,  $(s' = s + H(e))$  consists of two parts containing the secret key  $s$  and the error term  $e$ , the output of the one-way function. This structure is obtained by adding the components of the pasteurization method to the construction of the problem. It is thought that the secret key will provide the reusable key property with the small number of multiplication and addition operations in the KE schemes of the problem. In this way, secure keys that can be used in symmetric cryptosystems will be obtained by using the same secret key more than once [3,4].

### 3. Conclusion

This paper explains the basic idea of the new lattice-based hard problem, called X-LWE, which can be used in the security of post-quantum secure KE schemes and includes a reusable key feature. In the future, the security of the proposed problem will be explained by reducing the hardness assumption of the basic hard lattice problems depending on the parameter selection limits.

**Keywords:** post-quantum cryptography, lattice-based cryptography, LWE.

### References

1. Akleylek S., Seyhan K. (2019). Kuantum Bilgisayarlar Sonrası Güvenilir Kafes Tabanlı Kriptosistem Temellerine Giriş, Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık Cilt II, 1st ed. Ankara, Türkiye: Grafiker Yayınları, ch. 5, pp.172-209.
2. Ding J., Branco P., Schmitt K. (2019). Key Exchange and Authenticated Key Exchange with Reusable Keys Based on RLWE Assumption, IACR Cryptol. ePrint Arch., 2019, 665.
3. Akleylek S., Seyhan K. (2020). A Probably Secure Bi-GISIS Based Modified AKE Scheme With Reusable Keys, in IEEE Access, vol. 8, pp. 26210-26222.
4. Seyhan K., Nguyen T.N., Akleylek S., Cengiz K., Islam S.H. (2021). Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security, In JISA, 58, 102788.
5. Paar C., Pelzl J. (2009). Understanding Cryptography: A Textbook for Students and Practitioners, 1st ed., Springer, pp. 205-233.

## ОБ ОДНОМ ПОДХОДЕ ПО ОБНАРУЖЕНИЮ АНОМАЛИЙ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ НА ОСНОВЕ АКУСТИЧЕСКИХ СИГНАЛОВ

Л.В. Сухостат

Институт Информационных Технологий Национальной Академии Наук Азербайджана

Баку, Азербайджан

e-mail: [lsuhostat@hotmail.com](mailto:lsuhostat@hotmail.com)

**Аннотация.** Развитие Индустрии 4.0 привело к появлению новых технологий для эффективного и надежного мониторинга киберфизических систем. Современные киберфизические системы – сложные архитектуры с неоднородными сенсорными системами разной природы. Для обеспечения безопасности таких систем важно раннее обнаружение неисправностей. В статье предлагается подход на основе глубокого обучения и алгоритма XGBoost для обнаружения аномалий в акустических сигналах устройств киберфизических систем.

### Введение

Аномальное состояние киберфизической системы (КФС) может быть вызвано кибератаками, неисправными компонентами, неправильной конфигурацией или их комбинацией [1, 3]. Злоумышленник вмешивается в КФС, чтобы манипулировать показаниями сенсоров или исполнительных механизмов, что приводит к аномальной работе системы. Обнаружение аномалий в КФС важно, поскольку необнаруженные отказы могут привести к критическим повреждениям. Их обнаружение может повысить надежность оборудования КФС и снизить затраты на эксплуатацию и техническое обслуживание.

В статье предлагается подход к обнаружению аномалий в акустических сигналах КФС на основе глубокого обучения и алгоритма XGBoost. Рассматриваются изображения спектрограммы и скалограммы акустических сигналов. Применение XGBoost обеспечивает высокую производительность и требует небольших вычислительных ресурсов.

### Предлагаемый подход

Предлагаемый подход состоит из следующих этапов: предварительная обработка, извлечение признаков с помощью глубокой нейронной сети, объединение признаков и классификация на основе алгоритма XGBoost [2]. Скалограмма на основе вейвлет-преобразования и спектрограмма на основе кратковременного преобразования Фурье (КПФ), извлекаются из акустических сигналов. КПФ разбивает сигнал на несколько перекрывающихся блоков, умножая их на оконную функцию Хеннинга:

$$\Theta(\omega, \tau) = \int_{-\infty}^{+\infty} \theta(t) \sigma(t - \tau) e^{-i2\pi\omega t} dt, \quad (1)$$

где  $\sigma$  – оконная функция.

А вейвлет Морле учитывается в вейвлет-преобразовании для получения более информативных изображений:

$$\psi(t) = e^{-\beta^2 t^2 / 2} \cos(\pi t), \quad (2)$$

где  $\beta$  – параметр, который управляет формой материнского вейвлета.

Затем визуальные представления сигналов размером 128x128x3 отправляются в глубокую нейронную сеть. В статье рассматриваются следующие предварительно обученные глубокие нейронные сети: Xception, MobileNet, DenseNet и InceptionV3.

Полностью связанный слой рассматривается как вектор признаков с использованием предварительно обученной модели. Результаты объединяются для извлечения информации о различных признаках и уменьшения ошибки распознавания. Общий размер вектора признаков составляет 1x1024. Затем он подается на классификатор XGBoost [2]. В основе данного алгоритма лежит оптимизация значения целевой функции, которая определяется как

$$\tilde{y}_i = \sum_{k=1}^K \phi_k(x_i), \quad \phi_k \in \Phi, \quad (3)$$

где  $K$  – количество деревьев решений,  $\phi_k$  – оценка листьев независимого дерева, а  $\Phi$  – пространство дерева регрессии. В этом случае функция потерь определяется как

$$L(\phi_t) \approx \sum_{j=1}^T \left[ \left( \sum_{i \in I_j} g_i \right) w_j + \frac{1}{2} \left( \sum_{i \in I_j} h_i + \lambda \right) w_j^2 \right] + \gamma P, \quad (4)$$

где  $P$  – количество вершин листьев,  $w$  – оценка на каждом листе,  $\gamma$  и  $\lambda$  являются константами для управления степенью регуляризации,  $g_i$  – первая производная, а  $h_i$  – вторая производная функции потерь соответственно. Для XGBoost скорость обучения составляет 0,001, количество деревьев равно 100, максимальная глубина дерева 6,  $\gamma=0$  и  $\lambda=1$ .

### Результаты экспериментов

В этой статье эксперименты проводятся на Python 2.7.13 с использованием различных библиотек, включая Tensorflow, Librosa и Keras. Использовался процессор Intel Xeon (R) X5670 @ 2,93 ГГц \* 24 с 24 ГБ оперативной памяти.

Набор данных МИМII (Malfunctioning Industrial Machine Investigation and Inspection) о работе КФС в нормальных и аномальных условиях эксплуатации рассматривается для оценки предлагаемого подхода [4]. МИМII включает звуки четырех различных типов машин: клапаны, насосы, вентиляторы и направляющие. Аудиосигналы были получены с частотой дискретизации 16 кГц. МИМII содержит восемь отдельных каналов для каждого сегмента. Он состоит из 26092 «нормальных» и 6065 аномальных звуковых сегментов.

Результаты экспериментов показаны в Таблице. Сравнение различных глубоких нейронных моделей показало, что Densenet+XGBoost превзошел другие рассматриваемые модели при обнаружении аномалий от сигналов устройств КФС в соответствии с метрикой F-мера. Модели Inception+XGBoost, Xception+XGBoost и Densenet+XGBoost хорошо проявили

себя для «Направляющих», используя метрики precision и recall. Несмотря на это Densenet+XGBoost показал лучшую производительность для всех типов устройств.

**Таблица.** Оценка производительности предлагаемого подхода

| Метод             | Метрика   | Устройство |       |              |        |
|-------------------|-----------|------------|-------|--------------|--------|
|                   |           | Вентилятор | Насос | Направляющие | Клапан |
| Inception+XGBoost | Recall    | 87.0       | 95.0  | 98.0         | 100    |
|                   | Precision | 89.1       | 87.9  | 100          | 94.3   |
|                   | F-measure | 92.3       | 90.6  | 98.1         | 96.3   |
| Xception+XGBoost  | Recall    | 100        | 88.0  | 98.0         | 100    |
|                   | Precision | 84.2       | 100   | 100          | 92.6   |
|                   | F-measure | 96.8       | 92.8  | 98.1         | 95.3   |
| Mobilenet+XGBoost | Recall    | 96.0       | 88.0  | 94.0         | 100    |
|                   | Precision | 78.7       | 95.7  | 100          | 96.2   |
|                   | F-measure | 92.0       | 90.9  | 96.1         | 97.2   |
| Densenet+XGBoost  | Recall    | 99.9       | 96.0  | 98.0         | 100    |
|                   | Precision | 87.0       | 100   | 100          | 97.1   |
|                   | F-measure | 98.2       | 97.1  | 98.1         | 97.7   |

**Заключение.** Проблема обнаружения аномалий в КФС решается на основе акустических сигналов. В работе предложен подход с применением глубокого обучения и классификатора XGBoost. Результаты экспериментов на наборе данных MIMII показали эффективность предложенного подхода и могут помочь специалистам в диагностике неисправностей оборудования с целью обеспечения безопасности КФС.

**Ключевые слова:** обнаружение аномалий, XGBoost, акустический сигнал, киберфизическая система.

### Литература

1. Ahmed S.M., Zhou J. Challenges and opportunities in CPS security: a physics-based perspective. IEEE Security & Privacy, 2020, Vol. 18, No. 6, pp. 14-22.
2. Chen T., Guestrin C. XGBoost: a scalable tree boosting system. Proc. 22<sup>nd</sup> ACM SIGKDD International Conference, 2016, pp. 785-794.
3. Langner R. Stuxnet: dissecting a cyberwarfare weapon. IEEE Security & Privacy, 2011, Vol. 9, No. 3, pp. 49-51.
4. Purohit H., Tanabe R., Ichige K., Endo T., Nikaido Y., Suefusa K., Kawaguchi Y. MIMII dataset: sound dataset for malfunctioning industrial machine investigation and inspection. Proc. 4<sup>th</sup> Workshop on Detection and Classification of Acoustic Scenes and Events, 2019, pp. 209-213.

## **An approach for detecting anomalies in cyber-physical systems based on acoustic signals**

Industry 4.0 has led to the emergence of new technologies for efficient and reliable monitoring of cyber-physical systems. Modern cyber-physical systems are complex architectures with heterogeneous sensory systems of different nature. Early detection of faults is essential to ensure the security of such systems. The paper proposes a deep learning approach with the XGBoost algorithm for detecting anomalies in acoustic signals from devices of cyber-physical systems.

## **ABOUT SOME APPROACHES FOR DETECTING VULNERABILITIES IN WEB APPLICATIONS**

**V. Strukov, V. Gudilin**

Cybersecurity and DATA Technologies Department, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine,

e-mail: [struk\\_vm@ukr.net](mailto:struk_vm@ukr.net), [vgudilin7@gmail.com](mailto:vgudilin7@gmail.com)

The architecture of modern web applications and tool systems for their development is built in such a way that it allows having of vulnerabilities in the final product that can be used by intruders to unauthorized impact on web applications. These problems are due to various reasons: the commands features of the web application development tool systems, backdoors, the poor quality of web application testing, the large size of the application code, etc.

According to the results of studies by information security experts of the Carnegie Mellon Institute, there are about seven bugs related to vulnerabilities in one thousand lines of code [1]. This applies to programs that has been tested and released for use. If the Windows operating system has five million lines of code and the Linux operating system has four million, we can easily guess how many operating system vulnerabilities exist that could be exploited by attackers.

The Positive Technologies study, which consisted of sixteen thousand automated scans using special software, sixty in-depth program analyzes, showed that eighty-three percent of web applications have dangerous security bugs for all system and seventy-eight percent have problems that can lead to a security breach in the future. Experts have calculated that the possibility of a security breach with the worm computer viruses is from fifteen to twenty percent [2].

These statistics makes it clear that creators of sites do not care about checking programs for vulnerabilities. They care more about the breadth of the site's capabilities. The site that has great functionality has a more intricate code. Consequently, a lot of web applications are not security enough.

The experimental technique helps to detect security bugs in web applications and correct code that contains it, earlier than a hacker can detect such problems. The techniques proposed by the

authors helps the security specialists, system administrators or developers to perform effectively a security audit even when time is really short.

Experimental investigation of web application security is an effective technique for assessing computer systems for vulnerabilities. The aim of the investigation is to prove that the site is safe or unsafe, simulating a real attack. The essence of the experiment is that, a security expert operates like a real hacker to harm computer systems. The technique helps to detect web application security bugs faster, than attacker will detect the problems and use them for illegal activity.

Site security bugs can cause to site malfunctioning, getting access to user accounts, stealing personal information or confidential data, getting control to the corporation's computer systems.

Experimental investigation of web application security technique helps to detect security bugs and quickly fix them [3].

The presentation contains analyses of the most dangerous and popular types of web vulnerabilities used by attackers to hack sites: web injections and security misconfigurations of the web applications. It had been performed a short write-up of the security audit, developed advices to specialists who conduct security audit on security bugs and vulnerabilities efficient search.

Experimental part of the paper contains the author's write-ups of the audits of four real organization's sites.

As a result of investigation it was discovered bugs, that have different level of danger for all company's systems: SQL-injection, security misconfiguration of the AWS S3 service and HTML injection. The dangerous vulnerability was identified in the web application of one organization. Exploiting SQL injection vulnerability it was managed to take control over dedicated machines where the developers of the site kept the site. Also it was managed to execute privilege escalation attack on the servers.

The authors handed over description of detecting the vulnerabilities on their sites for protection company's cybersecurity.

The authors proposed techniques and general methodology of site security problems detecting for using by cybersecurity experts in their work.

No hardware or software may not provide full protection for the organization cybersecurity. Intrusion detection systems and intrusion prevention systems must be in place to protect the organization's systems. But the most important thing is a calendar experimental investigation of the system security.

Summing up, the proposed methodology for detection vulnerabilities helps to save time for finding security bugs. The time is all that a hacker needs to hack an application, because almost all systems are computationally save, which means can be cracked in polynomial time.

However, it is worth noting, that cybersecurity protection should be like as a set of protective measures. This severity can be achieved if, in addition to the proposed methodology of experimental audit of the web application security, the cybersecurity experts use a detal search of the mistakes in the code.

Thus, the following results were obtained in scientific work:

1) The confirmation of theoretical conclusions of experts of the Carnegie Mellon Institute about the presence of vulnerabilities in the tested industrial web applications based on experimental research.

2) The confirmation of the effectiveness of the method of experimental investigation of web application security.

3) For the first time specific mechanisms and tools for detecting certain types in vulnerabilities of web applications, and methods of their implementation are proposed by the authors.

4) In the course of the research the authors received concrete practically significant results - concrete vulnerabilities of really functioning sites was detected.

5) The results of the study were used to improve the cybersecurity system of the real sites.

6) The results obtained by the author can be used in the educational process for classes in the discipline «Security audit of computer systems and networks», «Cybersecurity».

**Keywords:** vulnerability, web-injection, cybersecurity, privilege escalation, security bugs.

### References

1. S. McDonnell, Code complete, 2nd ed. Redmond: Microsoft Press, 2004.
2. Positive technologies. Web application vulnerabilities.  
ptsecurity.com. <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Vulnerabilities-2019-rus.pdf> (accessed Sep 12, 2021).
3. Sharan L.S., Effective penetration testing approach for modern web application vulnerabilities, International journal of computer applications, vol. 181, no. 22, 2018, pp. 44–50.

## THE OVERVIEW OF CYBER RESILIENCE APPROACH USING TRAFFIC ENGINEERING FAST REROUTE FEATURES

**O. Yeremenko, A. Mersni, A. Akulynichev**

Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

[oleksandra.yeremenko.ua@ieee.org](mailto:oleksandra.yeremenko.ua@ieee.org), [amal.mersni.ua@ieee.org](mailto:amal.mersni.ua@ieee.org), [artem.akulynichev@nure.ua](mailto:artem.akulynichev@nure.ua)

The research is dedicated to evaluating and developing a method for assuring cyber resilience based on Traffic Engineering Fast ReRoute with the assistance of Traffic Policing mechanism. The suggested approach is founded on a mathematical model defined by multipath routing conditions and modified flow conservation conditions. Additionally, it considers traffic policing at the network edge and conditions for protecting (reserving) the link, node, and network bandwidth, all of which are tailored to meet cyber resilience needs. The proposed solution has the advantage of recasting the problem as a linear optimization. The numerical example demonstrates the model's operability and the adequacy of the findings acquired using it.

Modern communication networks demand technological solutions to provide cyber resilience against network attacks, compromises, etc. Only the suitable reserve capacity can identify these repercussions [1-5]. When compromising a network element, such as a link, a node, or even an entire network segment, a network reserve with sufficient bandwidth is necessary.

Assuring a network's cyber resilience is a difficult task. The study reveals that using Fast ReRouting (FRR) effectively can improve the network's cyber resilience [5-8]. The network can respond operationally (in tens of milliseconds) to possible service issues. However, this requires resource redundancy, as well as rapid computation and the use of backup routes. Such routes do not share a network element with the main working path. However, enhancing the cyber resilience of an infocommunication network via resource reservation always has a detrimental effect on the overall Quality of Service (QoS) level [9-10]. Consequently, strengthening the cyber resilience of an infocommunication network by reserving network resources inevitably reduces overall QoS. This is especially true when the network's resources, notably bandwidth, are insufficient to perform a particular protective system that may cause network overload.

Thus, to avoid network congestion induced by applying cyber resilience principles, two things must be ensured during Fast ReRouting [11, 12]. Firstly, the balanced use of available network resources on the Traffic Engineering principles should be implemented. Secondly, priorities of limiting (policing) traffic at the network edge may be applied.

Therefore, the pertinent scientific and practical task is developing of novel approaches for ensuring the cyber resilience of communication networks following the requirements for network resilience, security, and QoS when using traffic management technologies such as Traffic Engineering and Traffic Policing in conjunction with the means of Fast ReRouting in the event of a network element failure.

In modeling the cyber resilience strategy based on Traffic Engineering Fast ReRoute, the network structure is represented by a graph. The nodes of the graph are network routers, and the communication links connecting these routers are edges. The presented approach is based on a mathematical model that incorporates conditions for multipath routing, updated flow conservation conditions that account for network edge Traffic Policing, and link, node, and network bandwidth protection (reservation) conditions. The advantage of the suggested method is that it recasts the Traffic Engineering Fast ReRoute under the Traffic Policing (TE-FRR-TP) task as an optimization problem. The optimality criterion is defined as the minimum of a linear function that sums the use of dynamically managed upper bound of network links utilization under the Traffic Engineering requirements. The linearity of the formulated optimization problem is intended to reduce the computational complexity associated with calculating the routing variables that determine the primary and backup paths.

The work proposes a cyber resilience approach based on Traffic Engineering Fast ReRoute with policing. The study's results on various numerical network topologies supported the proposed cyber resilience approach's efficacy and suitability. It is worth noting that providing cyber resilience necessitates the involvement of extra network resources, both topological (links, nodes) and

functional (bandwidth of network elements). Thus, the innovation and primary benefits of the proposed approach are as follows. First, it is advocated to coordinate the effective (balanced) usage of network resources according to the TE-FRR principles to avoid network overload while ensuring cyber resilience. Second, it is proposed to implement Traffic Policing at the network edge, both in primary and backup routes, prioritizing the flows into account. The developed model is a continuation and improvement of previously known approaches to load balancing during Fast ReRouting [12] and traffic policing [13].

**Keywords:** Cyber Resilience, Traffic Engineering, Fast ReRoute, Traffic Policing, Bandwidth Protection.

### References

1. Linkov I., Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In *Cyber resilience of systems and networks* (pp. 1-25). Springer, Cham.
2. Stallings W., *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Addison-Wesley Professional, 2018.
3. Galinec D., Steingartner W., Combining cybersecurity and cyber defense to achieve cyber resilience, in *Proc. 2017 IEEE 14th International Scientific Conference on Informatics*, November 2017, pp. 87-93.
4. Björck F., Henkel M., Stirna J., Zdravkovic J., *Cyber resilience—fundamentals for a definition*. New contributions in information systems and technologies, Springer, Cham, 2015, pp. 311-316.
5. White M.B. *Computer Networking: The Complete Guide to Understanding Wireless Technology, Network Security, Computer Architecture and Communications Systems (Including Cisco, CCNA and CCENT)*. CreateSpace Independent Publishing Platform, 2018.
6. Monge A.S., Szarkowicz K.G. *MPLS in the SDN Era: Interoperable Scenarios to Make Networks Scale to New Services*. O'Reilly Media, 2016.
7. Al-shawi M., Laurent A. *Designing for Cisco Network Service Architectures (ARCH) Foundation Learning Guide: CCDP ARCH 300-320*. 4th edition, Cisco Press, 2017.
8. Rak J., Papadimitriou D., Niedermayer H., Romero P. Information-driven network resilience: Research challenges and perspectives. *Optical Switching and Networking*, vol. 23, part 2, January 2017, pp. 156-178.
9. Lemeshko O., Yevdokymenko M., Yeremenko O., Mersni A., Segeč P., Papán J., Quality of Service Protection Scheme under Fast ReRoute and Traffic Policing Based on Tensor Model of Multiservice Network, 2019 International Conference on Information and Digital Technologies (IDT), 2019, pp. 288-295, doi: 10.1109/DT.2019.8813675.
10. Mersni, A., Ilyashenko, Vavenko T., Complex optimality criterion for load balancing with multipath routing in telecommunications networks of nonuniform topology, 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2017, pp. 100-104, doi: 10.1109/CADSM.2017.7916095.

11. Lemeshko O., Yeremenko O. Linear optimization model of MPLS Traffic Engineering Fast ReRoute for link, node, and bandwidth protection, in Proc. 2018 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 20-24 February 2018, pp. 1009-1013.
12. Lemeshko O., Garkusha S.V., Yeremenko O.S., Hailan A.M., Policy-based QoS Management Model for Multiservice Networks, in Proc. 2015 International Siberian Conference on Control and Communications (SIBCON), 21-23 May 2015, pp. 1-4.
13. Lemeshko A.V., Evseeva O.Yu., Garkusha S.V. Research on Tensor Model of Multipath Routing in Telecommunication Network with Support of Service Quality by Greate Number of Indices. Telecommunications and Radio Engineering, Vol. 73, Iss. 15, 2014, pp. 1339-1360.