COMPUTER SIMULATION OF DECENTRALIZED NETWORK

M. M. Magzom, S. E. Nyssanbayeva, M. N. Kalimoldayev

The Institute of Information and Computational Technologies
050010, Almaty, Republic of Kazakhstan

УДК 004.056.5

This paperis dedicated to the development of a software system for computer modeling (simulation) of a decentralized network with the ability to perform calculations on distributed nodes.The results of the creation of a such simulation system for decentralized computer networks are discussed. This system is used during research and implementation of different cryptographic algorithms based on modular arithmetic.

In decentralized networks, there are no dedicated servers, and each node (peer) acts like a client and a server. Unlike the client-server architecture, such an organization allows to keep the working capacity of network at any number and any combination of available nodes. Considering the steady growth in the number of applications, users and devices in these networks, issues of ensuring information security in such networks are particularly relevant.

Cryptographic means of information protection can be used to solve the problems of confidentiality and authentication during the interaction in the network. Encryption of the data flow between decentralized network nodes allows not only to protect the data itself, but also to hide the fact that network connection has taken place.

The main tasks of cryptographic protection of information in decentralized networks are the following: data encryption to ensure confidentiality during storage and transmission over the network between nodes; the usage of hash functions to control the integrity of data; usage of message authentication codes and electronic digital signatures for message authentication. An important task for this type of networks is to provide cryptographic protection of information during data transmission through communication channels and during storage.

During the research and development of cryptographic systems based on modular arithmetic in the Laboratory of Information Security of the Institute of Information and Computational Technologies, it was important to investigate possibility and efficiency of usage of the developed symmetric and asymmetric cryptographic algorithms in network data transmission. For this reason, the work on the development and implementation of a simulation system of decentralized networks is carried out.

The analysis of existing programs for simulating peer-to-peer networks is performed. The typical requirements for these systems such as workflow architecture, usability, scalability, statistics, portabilitywere evaluated. It was shown, that the most of the simulation systems, which are available from the open sources, are obsolete and do not allow to run network simulation on distributed nodes. According to it, a new simulation system has been developed.

The developed system includes the following components: topologydesign and monitoring system; node process manager; computing process instance. First the component of topology design creates a network topology based on the specified parameters. Based the created topology process managers create instances of processes that simulate the operation of individual nodes. Building a node manager in a separate component allows to distribute the process of creating and managing nodes to different computers. Each process performs calculations and acts like a separate network node. A process is

assigned a unique identifier and a lambda function that will be executed by the process and simulate the calculation process. Processes can exchange data through this protocol by using an arbitrary form of messages, the content of which depends on specifications in the processes of the lambda functions. The system uses an event-based workflow, that is, a state change causes corresponding events in related objects. The network monitoring component receives every status message from nodes in the network.

The system is implemented in the JavaScript language using the Node.js and AngularJS web platforms. Processes are interconnected by passing a message through the HTTP protocol by using WebSocket technology.

The structural and protocol design of the system is discussed. The proposed structure of the system allows users to apply their own encryption algorithms and security protocols to the simulation process. The developed system of decentralized network simulation has a feature of working on distributed nodes, for example on different computers, either physical or virtual. This feature makes the developed simulation system a useful tool during research and implementation of different cryptographic algorithms based on modular arithmetic. This gives an opportunity to evaluate efficiency of different cryptographic schemes in a network flow.

Key words: decentralized networks, network simulation, information security, computer modeling.

References

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2009; 2017. [El. Res.]. `http://www.bitcoin.org/bitcoin.pdf`

2. Bocek T., Peric D., Hecht F., Hausheer D., Stiller B. PeerVote: A Decentralized Voting Mechanism for P2P Collaboration Systems. In: Sadre R., Pras A. (eds) Scalability of Networks and Services. AIMS 2009. Lecture Notes in Computer Science. Springer; Berlin; Heidelberg, 2009. Vol. 5637.

3. Risson J., Moors T. Survey of Research Towards Robust Peer-to-Peer Networks: Search Methods. Technical Report, University of New South Wales. Sydney; Australia, 2004.

4. Kurose J., Ross K. Computer Networking: A Top-Down Approach Featuring the Internet. Addison-Wesley, 2005.

5. Status of the UC-Berkeley SETI Efforts, Korpela, et al. // Instruments, Methods, and Missions for Astrobiology XIV. Proc. SPIE 8152. 2011. Vol. 14. P. 1–8.

6. Ethereum: a platform for smart contracts. [El. Res.]. `https://www.ethereum.org/`

7. Biyashev R. G., Nyssanbayeva S. E., Begimbayeva Ye. Ye., Magzom M. M. Modification of the Cryptographic Algorithms, Developed on the Basis of Nonpositional Polynomial Notations // Proceedings of the International Conference on Circuits, Systems, Signal Processing, Communications and Computers (CSSCC 2015). Vienna, 2015. P. 170–176.

8. Biyashev R. G., Nyssanbayeva S. E., Begimbayeva Ye. Ye., Magzom M. M. Building modified modular cryptographic systems // International Journal of Applied Mathematics and Informatics. 2015. Vol. 9. P. 103–109.

9. Biyashev R., Kalimoldayev M., Nyssanbayeva S., Magzom M. Development of an encryption algorithm based on nonpositional polynomial notations // Proceedings of the International Conference on Advanced Materials Science and Environmental Engineering (AMSEE 2016). Chiang Mai; Thailand, 2016. P. 243–245.

10. Bailes J., Templeton G. Managing P2P security // Communications of the ACM 47. 2004. Vol. 47, N 9. P. 95–98.

11. Schoder D., Fischbach K. Core Concepts in Peer-to-Peer (P2P) Networking. [El. Res.]. `http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf`

12. Naoumov N., Ross K. Exploiting P2P Systems for DDoS Attacks. International Workshop on Peer-to-Peer Information Management. 2006. [El. Res.]. http://cis.poly.edu/~ross/papers/p2pddos.pdf

Introduction. Decentralized (p2p — „peer-to peer“) computer network is a method of building an architecture of computer network in which all end nodes (network users) have equal rights and act as providers and consumers of network services simultaneously. For the first time, the phrase „peer-to-peer“ was used in 1984 in the development of architecture of the Advanced Peer to Peer Networking (APPN) of IBM company.In such networks, there are no dedicated servers, and each node (peer) acts like a client and a server. Unlike the client-server architecture, such an organization allows to keep the working capacity of network at any number and any combination of available nodes. According to the steady growth in the number of applications, users and devices in these networks [1–6], issues of ensuring information security in such networks are particularly relevant.

In the Laboratory of Information Security of the Institute of Information and Computational Technologies the research and development of the cryptographic systems based on modular arithmetic is conducted [7–9]. During the research, it is important to investigate possibility and efficiency of usage of the developed symmetric and asymmetric cryptographic algorithms during network data transmission. For this reason, the work on the development and implementation of a simulation system of decentralized networks is carried out.

In this paper, we discuss some results of the creation of a simulation system for decentralized computer networks and development of cryptographic means of information security in such networks.

Some types of security issues in decentralized networks are [10–12]:

— Distributed DoS attacks. In P2P networks, attackers can use the nature of the requests between nodes to overload the network;

— A P2P network routing table poisoning. Because P2P network nodes must somehow discover other network members, for example, based on a centralized directory or a distributed table, an attacker can insert a large number of invalid records into such a directory. Fictitious elements in the index can slow down the query time or produce invalid query results.

— Confidentiality and authentication;

— Content validations.

Cryptographic means of information protection can be used to solve the problems of confidentiality and authentication. Encryption of the data flow between P2P nodes allows not only to protect the data itself, but also to hide the fact that P2P connection has taken place.

The main tasks of cryptographic protection of information in such systems are: data encryption to ensure confidentiality during storage and transmission over the network between nodes; the usage of hash functions to control the integrity of data; usage of message authentication codes and electronic digital signatures for message authentication.

Considering the widespread distribution of portable and embed devices (for instance, such as „smart“ watches, electricity meters, various sensors with Internet connection, etc.), it is necessary to take into account that many devices in the network may have small processing power, work from internal power sources and be limited in memory capacities.

1. Development of system for computer simulation of a decentralized. The analysis of existing programs for simulating peer-to-peer networks is performed. The typical requirements for such systems wereevaluated: workflow architecture, usability, scalability,

Table 1

Popular modelling platforms for p2p networks

Name	Workflow	Execution	Last update
Peersim	Cycle and Event based	On one computer	2008
P2PSim	Event based	On one computer	2002
Neurogrid	Event based	On one computer	2002

```
1: procedure BuildNodes(N)
2:     nodes = []
3:     for each integer i in N do
4:         x = random();
5:         y = random();
6:         node = {x, y}
7:         nodes[] = node
8:     end for
9:     Return nodes
10: end procedure
```

Fig. 1. Networks node location algorithm

```
1: procedure WireNodes(N, nodes, maxDistance)
2:     wire = [];
3:     for each integer i in N do
4:         for each integer j in N do
5:             d = distance(nodes[i], nodes[j])
6:             if d < maxDistance then wire[] = nodes[i], nodes[j]
7:             end if
8:         end for
9:     end for
10:    Return wire
11: end procedure
```

Fig. 2. Networks node connection algorithm

statistics, portability. In order to test existing simulating systems, the latest available version of them was downloaded. Each simulator was evaluated on the basis of mentioned requirements.

Table 1 shows a comparison of the most popular platforms among the tested systems.

As could be seen from the table, the most of the simulation systems, which are available from the open sources, are obsolete and do not allow to run network simulation on distributed nodes. According to it, a new simulation system has been developed.

The developed system includes the following components:

— Topology and monitoring design system. The task of the component is to create a network topology based on the specified parameters, to receive status messages from nodes in the network. The network topology is defined by the input parameters and implemented by algorithms, illustrated in fig. 1 and fig. 2.

An example of a topology with the ability to highlight nodes (based on the library vis.js) is shown in fig. 3.

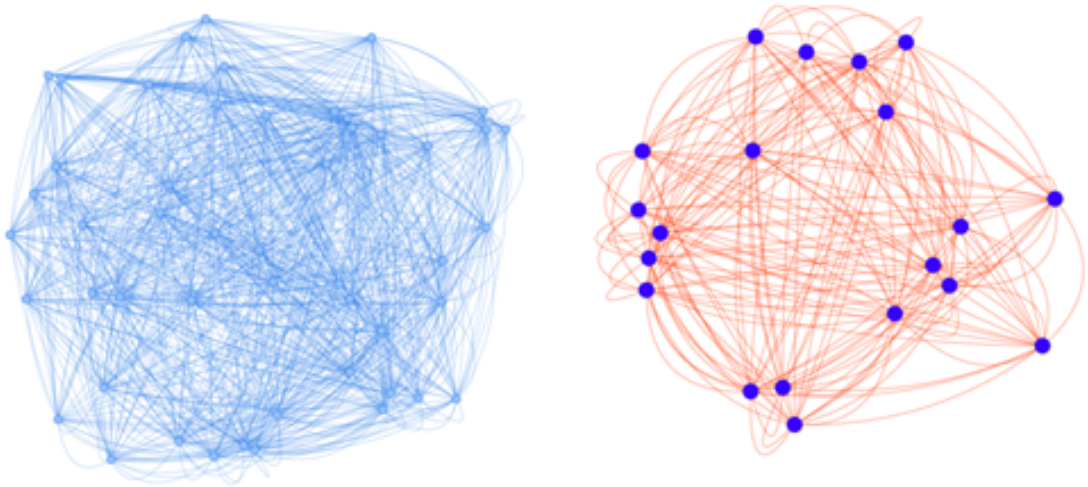


Fig. 3. Different topologies created in the system

— A node process manager. This component, after receiving information about the network topology, creates instances of processes that simulate the operation of individual nodes. Building a node manager in a separate component allows to distribute the process of creating and managing nodes to different computers.

— A computing process instance. This is a process that performs calculations and acts like a separate network node. Each process is assigned a unique identifier and a lambda function that will be executed by the process and simulate the calculation process.

The interaction scheme of these components is shown in fig. 4. Processes are interconnected by passing a message through the HTTP protocol by using WebSocket technology. Processes can exchange data through this protocol by using an arbitrary form of messages, the content of which depends on specifications in the processes of the lambda functions.

This program uses an event-based workflow, that is, a state change causes corresponding events in related objects. These events can be: connection, disconnection of nodes in the network, receiving messages from neighboring nodes, sending messages from the control system, and others.

Consider the structure of the main messages on the network:

— Request information about neighboring nodes. It is sent by a node that has just connected to the simulated network. This message is used for the nodes added manually to the simulated network.

```
{
  "node_id": "123",
  "domain": "routing",
  "type": "getTable"
}
```

— Connection notification. It is distributed by a node to all known „neighbors“.

```
{
  "node_id": "123",
  "domain": "announce",
```

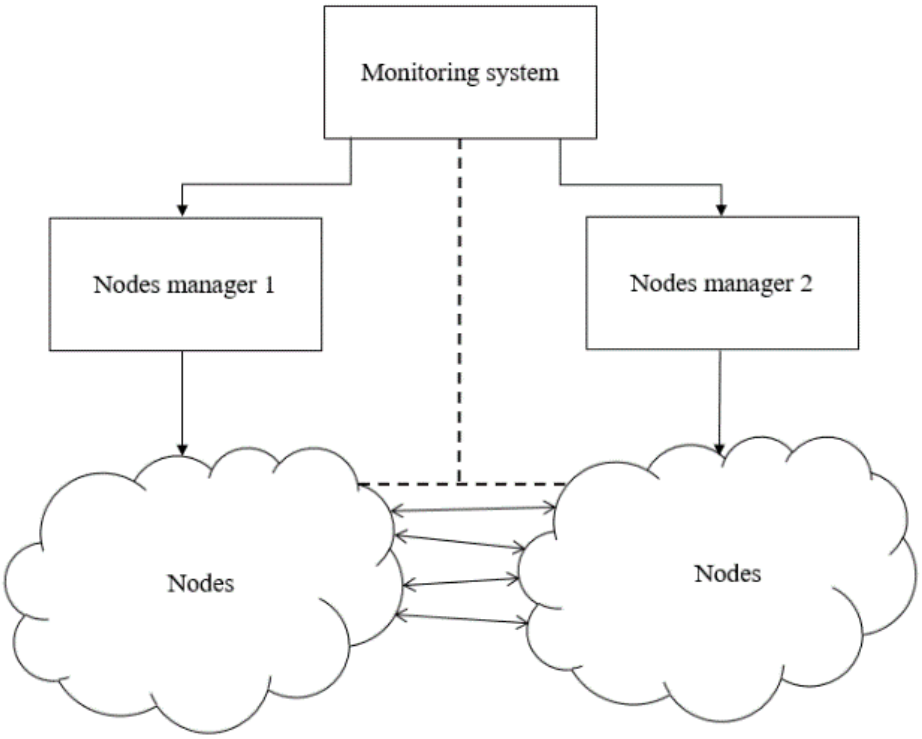


Fig. 4. The interaction the components of the developed simulation system

```
  "type": "connected",
  "data": {
    "address": "10.0.0.150",
    "port": "1017"
    }
}
```

— Update of the status. It is distributed by a node to all known „neighbors“ and the monitoring system.

```
{
  "node_id": "123",
  "domain": "status",
  "type": "update",
  "data": {
      ...
     }
}
```

Each message specifies the identifier of the sender (field node_id), the category of the message (the domain field) and the type of the message (type field). The content of the data field of data varies depending on the category and type of the message.

The system is implemented in the JavaScript language using the Node.js and AngularJS web platforms.

The screen of the topology modelling system is shown in fig. 5.

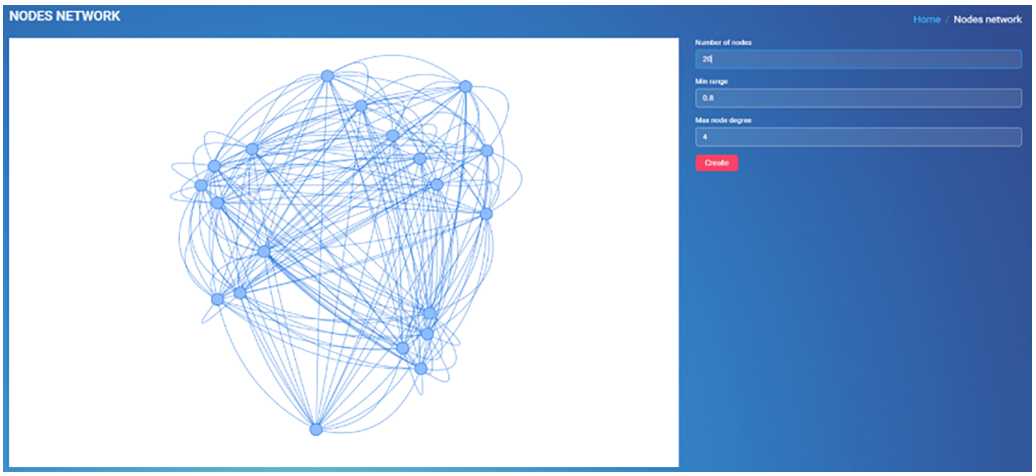


Fig. 5. Topology creation component

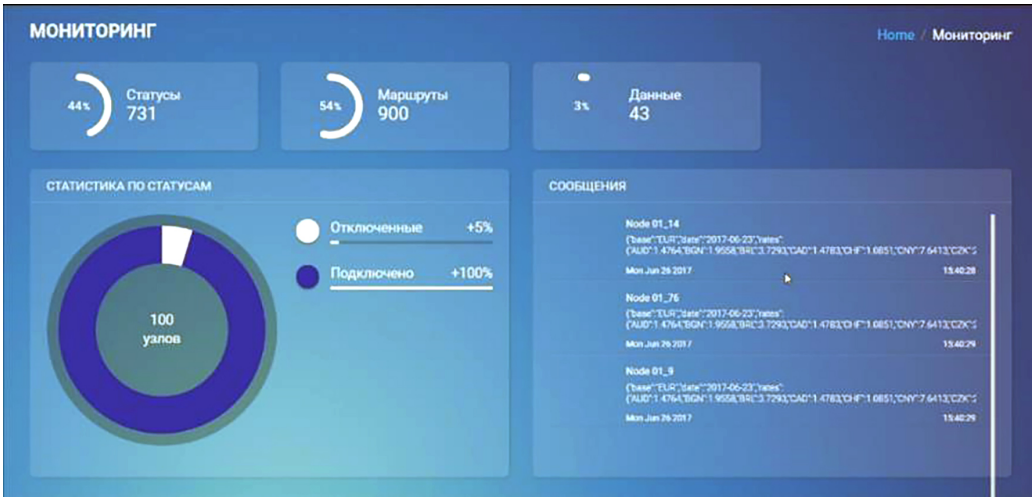


Fig. 6. Messages in the monitoring component

The monitoring system allows to gather status update messages from the network nodes. Based on these messages the monitoring system can create reports on nodes statistics. The screen of the component is shown in fig. 6.

The use of the standard and popular Node.js platform makes it possible to run nodes of the modelling network on both physical and virtual machines, or the Docker container, and also interact with hardware nodes to simulate IoT devices (example in fig. 7).

Conclusion. In this article, the results of the research on development of a decentralized network simulation system is discussed. An important task for this type of networks is to provide cryptographic protection of information during data transmission through communication channels and storage. The developed system of decentralized network simulation has a feature of working on distributed nodes, for example on different computers, either physical or virtual. The proposed structure of the system allows users to apply their own encryption algorithms and security protocols to the simulation process. This gives an opportunity to evaluate efficiency of different cryptographic schemes in a network flow.

Fig. 7. Example of usage of Docker containers and IoT devices in simulation process

References

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2009; 2017. [El. Res.]. http://www.bitcoin.org/bitcoin.pdf

2. Bocek T., Peric D., Hecht F., Hausheer D., Stiller B. PeerVote: A Decentralized Voting Mechanism for P2P Collaboration Systems. In: Sadre R., Pras A. (eds) Scalability of Networks and Services. AIMS 2009. Lecture Notes in Computer Science. Springer; Berlin; Heidelberg, 2009. Vol. 5637.

3. Risson J., Moors T. Survey of Research Towards Robust Peer-to-Peer Networks: Search Methods. Technical Report, University of New South Wales. Sydney; Australia, 2004.

4. Kurose J., Ross K. Computer Networking: A Top-Down Approach Featuring the Internet. Addison-Wesley, 2005.

5. Status of the UC-Berkeley SETI Efforts, Korpela, et al. // Instruments, Methods, and Missions for Astrobiology XIV. Proc. SPIE 8152. 2011. Vol. 14. P. 1–8.

6. Ethereum: a platform for smart contracts. [El. Res.]. https://www.ethereum.org/

7. Biyashev R. G., Nyssanbayeva S. E., Begimbayeva Ye. Ye., Magzom M. M. Modification of the Cryptographic Algorithms, Developed on the Basis of Nonpositional Polynomial Notations // Proceedings of the International Conference on Circuits, Systems, Signal Processing, Communications and Computers (CSSCC 2015). Vienna, 2015. P. 170–176.

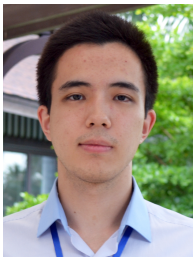
8. Biyashev R. G., Nyssanbayeva S. E., Begimbayeva Ye. Ye., Magzom M. M. Building modified modular cryptographic systems // International Journal of Applied Mathematics and Informatics. 2015. Vol. 9. P. 103–109.

9. Biyashev R., Kalimoldayev M., Nyssanbayeva S., Magzom M. Development of an encryption algorithm based on nonpositional polynomial notations // Proceedings of the International Conference on Advanced Materials Science and Environmental Engineering (AMSEE 2016). Chiang Mai; Thailand, 2016. P. 243–245.

10. Bailes J., Templeton G. Managing P2P security // Communications of the ACM 47. 2004. Vol. 47, N 9. P. 95–98.

11. Schoder D., Fischbach K. Core Concepts in Peer-to-Peer (P2P) Networking. [El. Res.]. http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf

12. Naoumov N., Ross K. Exploiting P2P Systems for DDoS Attacks. International Workshop on Peer-to-Peer Information Management. 2006. [El. Res.]. http://cis.poly.edu/~ross/papers/p2pddos.pdf



Магзом Мирас Мухтарулы — младший научный сотрудник Лаборатории информационной безопасности Института информационных и вычислительных технологий КН МОН РК, г. Алма-Ата, Республика Казахстан; PhD докторант; тел.: +77078878246.

Мирас Магзом получил степень магистра технических наук по специальности „Вычислительная техника и программное обеспечение“ в 2014 году в Алматинском университете энергетики и связи. С 2014 года проходит обучение по совместной программе PhD в Институте информационных и вычислительных технологий МОН РК и Казахском национальном университете им. Аль-Фараби по специальности „Вычислительная техника и программное обеспечение“. С 2015 года работает в лаборатории информационной безопасности Института информационных и вычислительных технологий.

Miras Magzom received his M.S. degree in Computer Science in 2014 from Almaty University of Power Engineering and Telecommunications. Since 2014 studies PhD in Computer Science by the joint program in Institute of Informational and Computational Technologiesof Ministry of Education and Science of the Republic of Kazakhstan and Al-Farabi Kazakh National University. Since 2015 works in the Laboratory of Informational Security in Institute of Informational and Computational Technologies.

Нысанбаева Сауле Еркебулановна — главный научный сотрудник Лаборатории информационной безопасности Института информационных и вычислительных технологий КН МОН РК, г. Алма-Ата, Республика Казахстан; доктор технических наук, ассоциированный профессор; тел.: +77017743730.

Сауле Нысанбаева окончила механико-математический факультет Казахского Государственного Университета им. С. М. Кирова (КазГУ, г. Алма-Ата) в 1971 году. В 1986 году защитила кандидатскую диссертацию по специальности 01.04.14 „Математическое моделирование тепловых режимов кристаллизации переохлажденных жидкостей“ на соискание ученой степени кандидата физико-математических наук. В 2009 г. защитила диссертацию „Разработка и исследование криптографических систем на базе непозиционных полиномиальных систем“ на соискание ученой степени доктора технических наук. С октября 1971 года работала в КазГУ на кафедре прикладной математики и в проблемной лаборатории математического моделирования. С февраля 1994 года по август 2001 года работала в Институте проблем информатики и управления (ныне Институт информационных и вычислительных технологий) Министерства образования и науки Республики Казахстан ученым секретарем. С декабря 2003 года — сотрудник лаборатории информационной безопасности ИПИУ. Тематика научных исследований — разработка и исследование алгоритмов и средств криптографической защиты информации с использованием модулярной арифметики, хранимой и распространяемой в инфо-коммуникационных системах.

Saule Nyssanbayeva graduated from the Mechanics and Mathematics Faculty of the Kazakh State University named after S.M. Kirov in 1971.In 1986, she received her candidate degree on speciality 01.04.14 „Mathematical modeling of the thermal modes of crystallization of super cooled liquids“. In 2009 she defended her thesis „Research and development of cryptographic systems based on nonpositional polynomial systems“ and received a degree of Doctor of Technical Sciences. Since October 1971, she worked in the Kazakh State University in the chair of applied mathematics and in the laboratory of mathematical modeling. From February 1994 to August 2001, she worked as a scientific secretary at the Institute of Problems of Informatics and Control (now the Institute of Informational and Computational Technologies) of Ministry of Education and Science of the Republic of Kazakhstan. Since December 2003 — researcher in the information security laboratory. Subject of research — development and analysis of algorithms and means of cryptographic protection of information using modular arithmetic.

Калимолдаев Максат Нурадилович — д-р физ.-мат. наук, академик НАН РК, директор Института информационных и вычислительных технологий КН МОН РК, e-mail: mnk@ipic.kz;

Максат Нурадилович Калимолдаев окончил факультет механики и прикладной математики Казахского государственного университета им. С. М. Кирова в 1980 году. В 1990 году защитил кандидатскую диссертацию на тему „Исследование динамики многомерных фазовых систем“ в КазГУ им. аль-Фараби.

В 2000 году защитил докторскую диссертацию по специальности 05.13.16 — „Применение вычислительной техники, математического моделирования и математических методов в научных исследованиях“ на тему „Устойчивость и математическое моделирование нелинейных многомерных фазовых систем“.

С 1982 года работал в КазГУ им. Кирова (затем был переименован в КазГУ им. аль-Фараби) от ст. лаборанта до профессора кафедры информационных систем. В 2001–2003 гг. работал в должностях начальника управления и зам. директора Департамента науки Министерства образования и науки РК. В 2003–2005 гг. — первый зам. Председателя ВАК.

С 2008 года по настоящее время — генеральный директор Института информационных и вычислительных технологий (бывший Институт проблем информатики и управления). Им опубликовано около 200 работ, в т. ч. 4 монографии и 5 учебных пособий для вузов.

Академик НАН РК. Под его руководством защищены 3 докторских, 16 кандидатских диссертаций на соискание ученых степеней кандидатов физико-математических, технических и педагогических наук и 1 доктор PhD.

М. Н. Калимолдаев является ведущим специалистом в области математического моделирования и теории управления. В сферу его научных интересов входят разработка математических моделей для исследования устойчивости, стабилизации, управляемости и оптимальности фазовых (электроэнергетических), технических и экономических систем; проблемы разработки синтеза и распознавания казахской речи; защита информации и теория принятия решений; робототехника.

Kalimoldayev Maksat Nuradilovich graduated from the faculty of Mechanics and Applied mathematics of the Kazakh State University named after S. M. Kirov in 1980. In 1990 he defended his candidate dissertation work on the theme „Study of the dynamics of multidimensional phase systems“ at Kazakh State University named after S. M. Kirov.

In 2000 he defended his doctoral dissertation work on the specialty 05.13.16- application of computing science, mathematical modeling and mathematical methods in scientific researches on the theme „Stability and Mathematical modeling of nonlinear multidimensional phase systems“.

Since 1982 he worked at Kazakh State University named after S. M. Kirov (then it was renamed into the Kazakh State University named after al-Farabi) from senior laboratory assistant to the Professor of the Department of Information systems. 2001–2003 he worked as head and deputy director of the Science Department of the Ministry of Education and Science of the Republic of Kazakhstan. 2003–2005 he was the 1st Vice Chairman of the Higher Attestation Commission.

From 2008 to present, he has been a Director General of the Institute of Information and Computational Technologies (former Institute of problems of Informatics and Control).

M. N. Kalimoldayev is the author of over 200 research papers including 4 monographs and 5 study guides for universities and high school graduate. He is a corresponding member of National Academy of Sciences of Kazakhstan. Under his leadership 3 doctors and 16 candidates of physical and mathematical, technical and pedagogical sciences and 1 PhD were prepared.

M. N. Kalimoldayev is a leading specialist in the field of mathematical modeling and control theory. His areas of research interests include: development of mathematical models to study the stability, stabilization, controllability and optimality phase (electrical), technical and economic systems; problems of development of synthesis and recognition of Kazakh speech; protection of information and decision theory; robotics.

Дата поступления — 28.07.2017