Intellectual Technologies on Transport No 3

Интеллектуальные технологии на транспорте № 3

Санкт-Петербург
St. Petersburg
2018

Интеллектуальные технологии на транспорте
№ 3, 2018

Сетевой электронный научный журнал, свободно распространяемый через Интернет.
Публикуются статьи на русском и английском языках с результатами исследований и практических достижений в области интеллектуальных технологий и сопутствующих им научных исследований.

Журнал основан в 2015 году.

Учредитель и издатель

Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I» (ФГБОУ ВО ПГУПС)

Адрес редакции
190031, Санкт-Петербург, Московский пр., 9, ауд. 1–210
e-mail: itt-pgups@yandex.ru, сайт: http://itt-pgups.ru

ISSN 2413-2527

Журнал зарегистрирован Федеральной службой по надзору в сфере связи и массовых коммуникаций, свидетельство ЭЛ № ФС77-61707 от 07 мая 2015 г.

Журнал зарегистрирован в Российском индексе научного цитирования (РИНЦ).

Intellectual Technologies on Transport
Issue № 3, 2018

Network electronic scientific journal, open access. It publishes articles in Russian and English with the results of research and practical achievements in the field of intelligent technologies and associated research

Founded in 2015

Founder and Publisher

Federal State Educational Institution of Higher Education
«Emperor Alexander I Petersburg State Transport University»

Editorial adress
190031, St. Petersburg, Moskovskiy pr., 9, aud. 1–210
e-mail: itt-pgups@yandex.ru, http://itt-pgups.ru

ISSN 2413-2527

The journal is registered by the Federal Service for Supervision of Communications and Mass Media, EL no. FS77-61707 testimony from May 7, 2015

The journal is registered in the Russian Science Citation Index (RSCI)

Содержание

Contents

Key Differences between Traditional and Software Defined Networks

V.V. Jakovlev, Zh.M. Berkinbayeva
Emperor Alexander I St. Petersburg
State Transport University
St. Petersburg, Russia
jakovlev@pgups.ru, berkinbayeva.zhanniyet@gmail.com

Angel Fernandez del Campo
Universidad Politécnica de Madrid
Madrid, Spain
afc@dit.upm.es

Abstract. **Traditional data networks are complex and difficult to manage because the implementation of a global network policy should be generated separately for each network device, which includes risks associated with incorrect configurations. Software defined networks allow you to manage the network with software that eliminates the need for manual debugging or changing the settings of network equipment, and this in turn reduces the workload of IT specialists. The network control is performed in an automatic mode with the help of intelligent control algorithms. The article considers the comparison of traditional networks (TN) and software defined networks (SDN), their advantages in using and describing how to work and how to start creating a SDN that is completely different from today's principles of creating data transmission networks, will also be described the disadvantages of the SDN, which supports versatility and flexibility.**

Keywords: **traditional networks, software defined networks, network and telecommunication, data centers, virtual machine, information technology, communication network, computer network, control system.**

INTRODUCTION

Networks are built using switches routers and other devices that have become extremely complex because they are implementing an increasing number of complex distributed protocols, standardized by IETF [1], (today the number of active protocols and their versions exceeds 600) and use proprietary interfaces inside. In such circumstances, researchers cannot drive the experiments they need on a functioning network, operators cannot quickly enter new services for their users, the network hardware manufacturers cannot innovate to meet customer demands. Supporting and managing a complex network infrastructure today is more art than engineering.

The growth of network attacks, viruses, and other network threats suggests that security issues still have no durable solutions, and that computer and telecommunications networks are the object of national security. Increasing the number and heterogeneity of content the development of services and the extent of their coverage has led to a change in the paradigm of the organization of Computation in society: to the place of client-server computing organization came, the data processing centers (DPC) and cloud computing, and the file systems and databases have been transformed into a data storage network (DSN).

The term Software Definition Network (SDN) is not new. The first work and studies on this topic have been emerging since 1995 [2]. Technology came in response to the needs of distributed computing, the use of network technologies in clouds (where the number of routers to manage can reach several tens of thousands), the emergence of large date centres, the beginning of Internet virtualization [3]. In fact, it's a new architecture that changes the organization of traditional data networks. In SDN networks, the core functions of switches and routers have been moved to the central Network ' controller, which simplifies both the application of network policies and the monitoring of network status. With this approach, the transmitting devices are responsible only for the transfer of data, based on the flow table, which is built by a centralized network controller that interacts with the transmitting device [4].

THE PROBLEMS OF MODERN COMPUTER NETWORKS AND THE KEY PRINCIPLES OF CREATION OF THE SDN NETWORKS

Computer networks and the Internet, as a fundamental infrastructure, are a strategic factor in the development of modern information technologies. However, the architecture of the global Internet, whose foundations were laid in the late 1960s and 1970s, is outdated and is not always able to respond adequately and effectively to the new needs of society. The increase in the number and diversity of mobile devices and the development of various wireless communications technologies have resulted in the number of users exceeding the number of fixed-link networks today. However, the growth of mobile power is boosting the computational capacity of applications, which in turn requires increased bandwidth. The volume of mobile traffic is growing exponentially, and traffic patterns are becoming more diversified. According to the leading network hardware manufacturers, traffic doubles every nine months, which in the next few years will increase the load by several orders. According to forecasts of the Cisco forecasts that the volume of traffic will quadruple over the next five years, with mobile traffic double yearly.

The modern computer networks consist of many separate network elements that perform specific functions: routers, switches, load balancing, NAT (Network Address Translation) [1], firewalls. SDN technology proposes to abandon such a trend in the development of computer networks by making the transition from individual network elements and the network as platforms in general to programmable entities. With the help of applications, you can optimize transport streams to find the shortest path, as it is done by the modern distributed routing protocols, and optimize the network to make maximum use of connections, make mobility of devices seamless or create different domains for different users.

To understand why writing routing protocols is so difficult, let's take a look at how routing is working in today's networks. Networks are created from target devices (personal computer and server) and intermediate devices connected to the cable system. The packet arrives at one port, the router checks it, and sends it through the port, which will make the package one step closer to the destination. Each router periodically polls the neighbours to which networks it is connected, and each neighbour collects that information and uses it to create a structure for all networks. Although routers share topological data among themselves, each of them performs a route calculation independently. Even if two neighbouring routers calculate the same results in a network topology, they will not pass overlapping results to each other. Because each processor cycle requires a certain amount of power, this duplication is not efficient. Implementing complex routing algorithms requires large processing power on devices. Each router individually is a costly device that performs the same computation as all others, just to get a slightly different result. Large networks require large computations. When an enterprise grows, the network increases, and each router must be updated to handle the additional calculations. The types and number of ports on the router do not change, but the processor does not have sufficient power to execute the algorithms. Sometimes it is sufficient to supplement the memory of random access, but it is often necessary to replace the processor unit with a more expensive one. This is a good business model for network providers: If you purchase enough routers, you should purchase updates and upgrade your hardware on a regular basis. In this case, these processors can only be obtained from these network providers because they are specialized, proprietary processors.

For today, the number of actually (actively) used protocols is more than 600, and this figure not finite. So, we can single out the following problems of modern computer networks [5]:

• scientific and technical – can't be controlled today and to safely foresee behavior of such difficult objects as wide computer networks;

• economic – networks are expensive, difficult and require for the service of highly qualified specialists;

• development problems – in the architecture of modern networks, there are available barriers to experimentation and the creation of new services.

The answer to the crisis of computer networks was the emergence of a fundamentally new approach to their construction - software defined networks (SDN).

ARCHITECTURE FOR SDN

The concept of a new network architecture of software-defined networks was proposed in 2007 by the staff of Stanford University [6]. Since then, the SDN networks have developed mainly in the Stanford and Berkeley scientific laboratory, and no one has tried them on an industrially significant scale. The researches initiated by them found support not only in the academic circles, in universities worldwide, but also were actively perceived more than four tens by the leading vendors of a network equipment and the large IT companies which formed Open Networking Foundation in March, 2011. Interest of the leading IT companies is caused by the fact that as practical approbation showed, PKS approach allows to increase efficiency of a network equipment for 25%-30%, to lower costs of operation of networks more than by 30%, to turn control of networks from art into engineering, it is essential to increase safety, to programmatically create new services and to quickly load them in a network equipment. Implementation of this approach, first of all, should have a significant impact on the network of data centers, corporate networks, WAN [7], cellular and home networks.

Researchers from Stanford and Berkeley assumed that on the computer networks it is possible to separate functions of control and data transfer.

Open Networking Foundation (ONF) [8] – the group which is most of all associated with development and standardization of SDN. According to ONF, «software defined networks (SDN) is a new architecture which is dynamic, controlled, effective on expenses and the adaptive that does it ideal for the dynamic modern applications requiring high throughput. This architecture disconnects the network control and transmission functions, which allows you to make control of the network directly programmable, and the underlying infrastructure to allocate for applications and network services. The OpenFlow protocol is the main element needed to create SDN solutions».

Figure 1 shows the architecture of SDN, as it is seen by ONF.

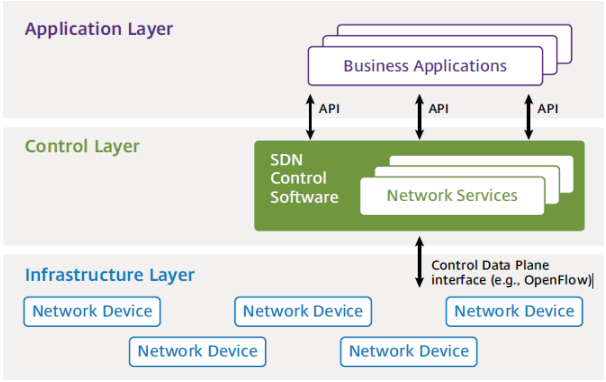


Fig. 1. Architecture of SDN. Source ONF

Some of the basic concepts that are part of the SDN system architecture, shown in figure 1, are described below.

Business applications

Applications which are used by directly finite users. Opportunities include carrying out videoconferences, management of a chain of deliveries and management of relationship with clients.

Network services and services of safety

The functionality allowing business applications to work effectively and safely. Opportunities include ADC, WOC [9] and function of safety, such as firewalls, IDS/IPS [10] and ensuring protection against DDoS [11].

SDN switch

In a pure SDN switch, all the management functions of a traditional switch (i.e. the routing protocols used for creation of information bases on routing) are performed in the central controller. The functionality of the switch is entirely limited to the data plane.

Hybrid Switch

In a hybrid switch, SDN technologies and traditional switch protocols work at the same time. The network manager

can configure the SDN controller to detect and control specific traffic flows, while traditional distributed network protocols continue to direct the rest of the traffic over the network.

The origin of this technology was associated with several points.

• Traditional architecture networks are proprietary, closed for research and almost any changes from outside. Equipment of different manufacturers often with each other poorly compatible.

• The growth of traffic in a geometric progression and the thesis that the network of the current architecture can not cope with it at the required level of quality.

• Increase in the number of protocols and their stacks in the network. Researchers from Stanford and Berkeley suggested that in computer networks it is possible to separate the functions of control and data transmission.

Hybrid network

The hybrid network is a network on which traditional switches and the switches SDN (whether they are the pure switches SDN or hybrid switches) work in the same environment.

As can be seen in figures 1 and 2 in architecture of SDN of a network it is possible to select three levels [11]:

• The infrastructure layer including a set of network devices (switches and transmission channels).

• The control layer including network operating system which provides for applications a set of network services and the program interface (API) for control of network devices and a network.

• Layer of network applications for flexible and effective management of a network.

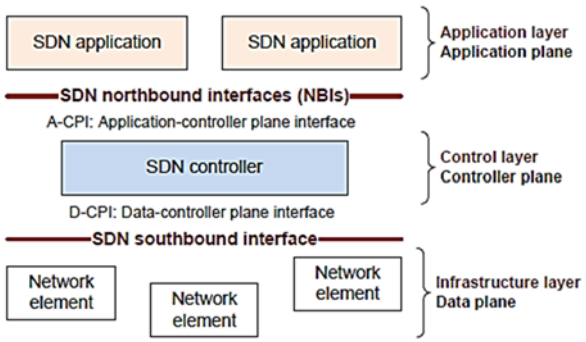


Fig. 2. Location of the North and South interfaces

Northbound API interface

According to figure 2, the northbound API interface is an interface which serves for interpretation of business logic in network instructions. By means of Northbound API of a business application can transfer information to the SDN controller for the subsequent programming of a network. The interface allows administrators to select flexibly network resources, based on application requirements, abstracting network infrastructure.

Southbound API interface

According to figure 2, the southbound API interface is an interface that provides an communication between the control layer and a infrastructure layer. The most famous interaction protocol is OpenFlow.

Part of the confusion associated with SDN is that many vendors do not fully agree with the definition of SDN submitted by ONF. For example, while some vendors consider OpenFlow to be the main element of their SDN solutions, other vendors are still thinking about the approach to OpenFlow. Another reason for the confusion is the disagreement over what constitutes the infrastructure layer. According to ONF, the infrastructure layer is a wide range of physical and virtual switches and routers. As described above, one of the current approaches to realizing networked virtualization is based on an architecture similar to that shown in figure 1, but including only virtual switches and routers.

The OpenFlow protocol, the first version of which was created in 2008, is the first SDN protocol and at the moment the standard «de facto» for SDN solutions on the basis of open technologies. OpenFlow describes the principles of interaction between the SDN controller (Control Plane) and network devices (Data Plane). The Open Networking Foundation (ONF) organization is responsible for the standardization of the protocol.

Vulnerabilities in the SDN architecture

Architecture of SDN, assuming significantly other approach to implementation of network infrastructure, it isn't deprived of potential vulnerabilities from the point of view of information security. The need to separate the access of network applications when working with the controller, the issues of authentication and authorization when running applications with the controller are just a few of the security aspects that have to be taken into account when designing SDN networks.

The controller as a key component in the management of the entire SDN infrastructure is the most vulnerable element, an attack on which can lead to consequences that are critical for the entire infrastructure [12]. Separation of access of network applications when working with the SDN controller is an actual problem of delimiting the areas of responsibility of network applications. The situation, when any network application is able to change the flow-tables of any switch controlled by this controller, does not meet modern information security requirements. Different types of applications require different levels of access, and the more detailed the limitations of each application (in accordance with the nature of the task), especially the network will be reliable. Different models of division of access can be applied to the decision of this task, for example, role, mandatory and discretionary, and also combinations of these models taking into account specifics of securable infrastructure.

Variations of such attacks as «failure in service», substitution of the controller, etc. remain the main threats arising from the network devices working by the principle of the program-configured network. Transfer of a «analytical» component of a network on the controller naturally transfers emphasis of many attacks from a network equipment to the providing functioning of the software network: the controller of a network and network applications addressing the controller [13].

The most simple and at the same time effective method of disrupting the integrity of the SDN network is attacks of type «failure in service». Danger of the attack follows from the algorithm of operation of the SDN switch when receiving an unknown (i.e. not suitable under the rules which are available

in the flow-table) a packet. In such situation two options are possible:

• The packet entirely goes to the controller for the analysis.

• The packet remains in the memory of the switch, only the packet headers are sent to the controller.

Both methods leave a wide field for the attacker to effectively implement the failure in service by generating a stream of different packets in the SDN network. Consider the network reaction in both of the above cases:

1. The switch starts forming a large number of messages to transfer unknown packets to the controller. The processor resources of the switch are consumed, the memory consumption is increased. Memory is especially strongly spent if the switch buffers packets and sends the controller only their titles.

2. The flow of packets from the switch to the controller loads the communication channel between the controller and the switch. If the communication environment is shared, then all the switches can experience a decrease in the speed of delivery of messages. Increased influence on the communication channel will be provided in the situation when the switch sends packets for the analysis entirely.

3. The controller accepts and processes a flow of messages, spending processor time and memory of the environment of execution. Formation of message queues will force legitimate messages to expect of queue and will reduce efficiency of making a decision on a network.

4. The controller generates a flow of different messages in response to requests of the attacked switch. The resources of the communication channel between the switch and the controllers are consumed.

5. The switch accepts commands from the controller and executes them, spending resources of the processor and memory. If commands comprise creation of new rules of tables of flows, then there is their avalanche increase, time of check of each new packet according to the table increases, expenditures on service of such table grow, and also possible overflowing of tables of flows is. As a result implementation of the attack can lead to the following consequences:

• Exhaustion of resources of the switch. Legitimate packets or generally won't be processed by this network point, or their processing will be followed by time delays.

• The communication link between the controller and the switch will not provide delivery of control messages when the data streams are loaded.

• The controller will be overloaded with incoming requests and will not be able to process control messages caused by legitimate traffic.

COMPRATION OF SDN WITH TRADITIONAL NETWORKS

The modern routers solve two main objectives: data transfer (forwarding) – advance of a packet from input port on a certain output port, and data management – processing of a packet and making decision on, where it to route, on the basis of a current status of the router. Thus, within all network it is possible to select the transmission level of data consisting of data transmission media (communication lines, the channel-forming equipment, routers and switches), and the control level with statuses of data transmission media.

The development of routers was on the way of convergence and «splicing» of the two levels, hardware acceleration, improvement of a software and implementation of new functional capabilities for an increase in speed of decision-making on routings of each packet. But at the same time the level of control remained enough primitive, leaning on the difficult distributed algorithms of routing and intricate instructions for configuring and setup of a network. It is necessary to mark, that the software of routers realizing control level remained proprietary and closed for developers, researchers and network operators.

In approach of SDN it was offered to separate the control layer and the data transmission layer. In the figure 3 it is provided comparing of traditional networks with the SDN networks.

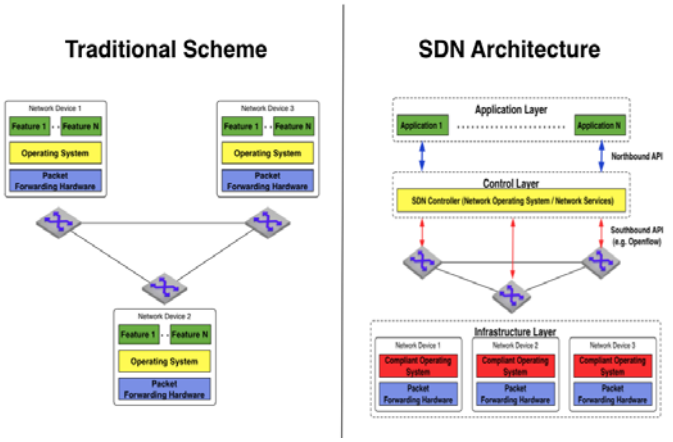


Fig. 3. Comparison of traditional networks with SDN networks

Following table 1 describes difference between traditional and software defined networking types [14].

TABLE 1. Difference between traditional and software defined networks

Traditional Networking	Software Defined Networking
They are static and inflexible networks. They are not useful for new business ventures. They possess little agility and flexibility	They are programmable networks during time as well as at later stage based on change in the requirements. They help new business ventures through flexibility, agility and virtualization
They are hardware appliances	They are configured using open software
They have distributed control plane	They have logically centralized control plane
They use custom ASICs[15] and FPGAs[16]	They use merchant silicon
They work using protocols	They use APIs to configure as per need

Traditional data networks

With the traditional approach to network technologies, most of the network functionality is implemented in a special device, for example, a switch, a router, an application delivery controller. In addition to this, inside of special device the most functions is implemented on a special hardware, for example ASIC [17] (specialized integrated circuit).

Some key characteristics of this approach to the development of network devices:

• ASIC, providing network functionality, develop slowly;

• the development of ASIC functionality is under the control of the vendor of the device;

• devices are proprietary;

• each device is configured individually;

The organizations using network technologies are under the increasing pressure: demand from them to be more effective and flexible, than it is possible in case of traditional approach to data networks. One of the reasons for this pressure is the widespread use of server virtualization. As part of server virtualization, virtual machines (VM) dynamically move between servers in a matter of seconds or minutes. However if relocation of VM crosses boundary of the 3rd layer of a network stack, then for realignment of a network for the purpose of support of VM on its new place several days or even can be required weeks. Sometimes it is difficult to determine what exactly a flexible network means. In view of the above, if the network reconfiguration to support VM migration takes weeks, then such of the network is not at all flexible.

Transition to the software

As it was marked, the traditional data communication network is substantially oriented on the hardware. However in the last several years use of the virtualized network devices and the growing interest in Software Defined Data processing Centers (SDDC)[18] led to increase in trust to the network functionality based on the software. For example, in the middle – the end of the 2000th network devices, such as controllers of optimization of data transfer on a wide area network Optimization Controller (WAN, WOC)[6] and Application Delivery Controller, ADC[9], were specialized physical devices. It means that such functions as encoding / decoding and processing of TCP flows, were executed by means of the hardware intended especially for execution of these functions. Due to the growing need for more flexibility now functionality of WOC or ADC, as a rule, is provided with the software working at the universal server or at VM.

SDDC can be considered as the complete antithesis of the traditional network of data-processing centers described above. For example, one of key characteristics of software defined data-processing center is that all infrastructure of data-processing center is virtualized and is provided in the form of service. Another key characteristic is that the automated control of data center applications and services is provided by a policy-based management system.

Potential opportunities

One of characteristics which often is associated with any fundamentally new approach to technologies is existence of confusion concerning opportunities which are given by this new approach. In order to successfully evaluate and apply a new approach to technology, such as SDN, IT organizations need to determine what opportunity or capabilities are important for the organization, best implemented through this approach.

After all discussions connected to SDN over the past few years the most probable set of opportunities which SDN can provide was defined:

• support of dynamic relocation, replication and distribution of the virtual resources;

• facilitation of administrative loading in case of a configuration and a provisioning of functionality, such as quality of service and safety;

• easier deployment and scaling of network functionality;

• regulation of a traffic thanks to open network transparency;

• more effective management of network resources;

• reduction of operating costs;

• faster development of network functionality based on the life cycle of software development;

• the ability of applications to dynamically request services from the network;

• Implementation of more effective safety functions;

• simplification.

According to ONF the architecture of SDN is:

• Directly programmable: control over a network is directly programmable as it is separated from transmission functions.

• Flexible: separation of monitoring from transmission allows administrators to regulate dynamically a flow of a network traffic according to permanently the changing needs.

• Centrally managed: network intelligence (logically) centralized in software-based SDN controllers that preserve the global appearance of the network, representing a single logical switch for applications and policies.

• Software configurable: SDN allows network managers to configure, manage, protect and optimize network resources very quickly, thanks to dynamic, automated SDN programs that they can create themselves, because the programs do not depend on proprietary software.

• Based on open standards and vendor-independent: implementation of SDN in accordance with open standards leads to simplification of the structure and operation of the network, since the instructions are provided by SDN controllers, rather than multiple devices and protocols from different vendors.

ADVANTAGES OF SDN

Thus, the architecture of SDN and the offered centralized approach gives the following advantages in comparison with traditional networks with distributed data transmission control:

Programmability and flexibility of network management, the considerable simplification of a possibility of modification of network management due to creation of new applications or the modification existing control automation and administrations by networks.

• Adaptability of management of network, that is an opportunity to change behavior and a status of the network in real time taking into account the changing operating conditions and adapt to them, adapt to the changing needs of users of networks due to creation of new network applications and services. The development of network applications requires much less time in comparison with a manual reconfiguration of all network is required.

• Independence from hardware and proprietary software for network hardware manufacturers.

• The ability to independently deploy the control level and the level of data transfer.

• The possibility of independent scaling of the control level and the level of data transfer.

• Improving reliability by reducing the amount of distributed state for management. Instead of existing distributed protocols that operate on each node of the network, each of them

supports a database of distributed copies of channel states in each node, however such information can be collected centrally in one place – on the controller. Thus, such a centralized database will contain much less uncoordinated information, and such approach will allow to reduce probability of cycles on a network.

• Simplify the structure and logic of network devices, because now they do not need to process a huge number of standards and protocols, and it is enough to execute only the instructions received from the controller.

• Reducing the cost of switches and the network infrastructure as a whole by making the «brains of routers» in the controller.

Thus, the SDN approach allows to significantly automate and simplify network management due to the possibility of their «programming», allowing to build flexible scalable networks that can easily adapt to changing operating conditions and user needs.

Conclusion

The benefits of the SDN concept are obvious. It is centralized management, monitoring and independence from a specific manufacturer's technology, and easier upgrading and maintenance of the network. The SDN architecture significantly alters the structure of the network, and therefore new security threats are emerging due to the vulnerabilities of individual infrastructure components. In addition, most of the threats associated with traditional data networks are critical in the same or greater degree in the context of SDN networks. On the other hand, the SDN architecture offers opportunities for innovation in the development of security instruments. A combination of centralized network management and programmability improves network security.

References

1. Cisco Systems, Inc. IP Addressing: NAT Configuration Guide. Available at:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/12-4t/nat-12-4t-book.pdf.

2. Calvert K., Bhattacharjee S., Zegura E., Sterbenz J., Active Networks, *Proc. IFIP-TC6 4th International Working Conference*, *IWAN,* Zurich, 2002, pp. 72–78.

3. Diego K., Fernando MV R., P Esteves V., Christian E. R., Siamak A., Steve U. Software-defined networking : A comprehensive survey. *Proc. IEEE*, 103(1), Lisbon, 2015, pp. 14–76.

4. Jakovlev V. V., Berkinbayeva Zh. M., Angel Fernandez del Campo. Application of the OpenFlow protocol based on the Mininet network emulator with the installation of a Floodlight controller. *Intellectual Technologies on Transport [Intellektual'nye tekhnologii na transporte]***.** 2018. No. 2. pp. 5–12.

5. Software-Defined Networking (SDN) Definition. Available at: https://www.opennetworking.org/sdn-resources/sdn-definition

6. Chuan L., Eric P., Donald R., Tom Zh. WAN Optimiza-tion Controller Technologies, *EMC Techbooks*, 2015, № H8076.7, pp. 32–71.

7. Introduction to WAN Protocols Protocols. Available at: http://www.cisco.com/networkers/nw01/pres/preso/WANand MultiserviceTechnologies/WMS-101.pdf

8. Open Networking Fundation. SDN Architecture Overview. Available at https://www.opennetworking.org

9. Brand Leader Report. Application Delivery Controller. URL: https://www.citrix.com.

10. Namiot D.E. Application Level Interfaces in SDN [Interfeysy prikladnogo urovnya v sdn] // *Modern Information Technology and IT-education [Sovremennye informatsionnye tekhnologii i IT-obrazovanie]*, vol. 2, no. 11, 2015, pp. 26–30.

11. SDN security: A survey. Available at: http://iranarze.ir/wp-content/uploads/2017/08/7602-English-IranArze.pdf

12. Kevin B., Jean C., Chris S. Openflow vulnerability assessment, *Proc. In Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, HotSDN '13, New York, 2013, pp. 151–152.

13. Seungwon Sh., Guofei Gu. Attacking software-defined networks: A first feasibility study, *Proc. In Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, HotSDN '13, New York, 2013, pp. 165–166.

14. Traditional vs Software Defined Networking. Available at: http://www.rfwireless-world.com/Terminology/traditional-networking-vs-software-defined-networking.html.

15. Elaine Rhodes. ASIC BASICS: An Introduction to Developing Application Specific Integrated Circuits. 2005. 62 p.

16. Guan-Lin Wu. Introduction to FPGA [www]. Available at: http://cc.ee.ntu.edu.tw/~jhjiang/instruction/courses/fall11-cvsd/LN13-FPGA.pdf.

17. Tewksbury S.K. Application-Specific Integrated Circuits (ASICS), *Technical report of Microelectronic Systems Research Center,* West Virginia, 1996, pp. 8–11.

18. VMware, Software-Defined Data Center. Capabilities and Outcomes.Available at: http://www.vmware.com.

Основные отличия между традиционными и программно-конфигурируемыми сетями

В.В. Яковлев, Ж.М. Беркинбаева
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, РФ
jakovlev@pgups.ru,
berkinbayeva.zhanniyet@gmail.com

Ангел Фернандез дел Кампо
Мадридский политехнический университет
Мадрид, Испания
afc@dit.upm.es

Аннотация. **Традиционные сети передачи данных сложны и трудны в управлении, при этом глобальная сетевая политика должна формироваться отдельно для каждого сетевого устройства, а это связано с риском неправильной конфигурации. Программно-конфигурируемые сети (ПКС) позволяют управлять сетью с помощью программного обеспечения, которое избавляет от необходимости ручной отладки или изменения настроек сетевого оборудования, что в свою очередь уменьшает рабочую нагрузку IT-специалистов. Сетевое управление происходит в автоматическом режиме с помощью интеллектуальных алгоритмов контроля.**

В статье проводится сравнение традиционных сетей (ТС) и программно-конфигурируемых сетей (ПКС), преимущества их использования и описание того, как работать и как создавать ПКС, которые существенно отличаются от ТС. Кроме того, описаны недостатки ПКС.

Ключевые слова: **традиционные сети, программно-конфигурируемые сети, сети и телекоммуникации, центры обработки данных, виртуальная машина, информационные технологии, сеть связи, компьютерная сеть, система управления.**

Литература

1. Cisco Systems, Inc. IP Addressing: NAT Configuration Guide. Available at: https://www.cisco.com/c/en/us/td/docs /ios-xml/ios/ipaddr_nat/configuration/12-4t/nat-12-4t-book.pdf.

2. Calvert K., Bhattacharjee S., Zegura E., Sterbenz J., Active Networks, *Proc. IFIP-TC6 4th International Working Conference*, *IWAN,* Zurich, 2002, pp. 72–78.

3. Diego K., Fernando MV R., P Esteves V., Christian E. R., Siamak A., Steve U. Software-defined networking : A comprehensive survey. *Proc. IEEE*, 103(1), Lisbon, 2015, pp. 14–76.

4. Jakovlev V. V., Berkinbayeva Zh. M., Angel Fernandez del Campo. Application of the OpenFlow protocol based on the Mininet network emulator with the installation of a Floodlight controller // Интеллектуальные технологии на транспорте. – 2018. № 2. – С. 5–12.

5. Software-Defined Networking (SDN) Definition. Available at: https://www.opennetworking.org/sdn-resources/sdn-definition

6. Chuan L., Eric P., Donald R., Tom Zh. WAN Optimization Controller Technologies, *EMC Techbooks*, 2015, № H8076.7, pp. 32–71.

7. Introduction to WAN Protocols Protocols. Available at: http://www.cisco.com/networkers/nw01/pres/preso/WANand MultiserviceTechnologies/WMS-101.pdf

8. Open Networking Fundation. SDN Architecture Overview. Available at https://www.opennetworking.org

9. Brand Leader Report. Application Delivery Controller. URL: https://www.citrix.com.

10. Намиот Д.Е. Интерфейсы прикладного уровня в SDN // Современные информационные технологии и ИТ-образование, Т. 2, № 11, 2015, с. 26–30.

11. Sdn security: A survey. Available at: http://iranarze.ir/wp-content/uploads/2017/08/7602-English-IranArze.pdf

12. Kevin B., Jean C., Chris S. Openflow vulnerability assessment, *Proc. In Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, HotSDN ’13, New York, 2013, pp. 151–152.

13. Seungwon Sh., Guofei Gu. Attacking software-defined networks: A first feasibility study, *Proc. In Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, HotSDN ’13, New York, 2013, pp. 165–166.

14. Traditional vs Software Defined Networking. Available at: http://www.rfwireless-world.com/Terminology/traditional-networking-vs-software-defined-networking.html.

15. Elaine Rhodes. ASIC BASICS: An Introduction to Developing Application Specific Integrated Circuits. 2005. 62 p.

16. Guan-Lin Wu. Introduction to FPGA [www]. Available at: http://cc.ee.ntu.edu.tw/~jhjiang/instruction/courses/fall11-cvsd/LN13-FPGA.pdf.

17. Tewksbury S.K. Application-Specific Integrated Circuits (ASICS), *Technical report of Microelectronic Systems Research Center,* West Virginia, 1996, pp. 8–11.

18. VMware, Software-Defined Data Center. Capabilities and Outcomes.Available at: http://www.vmware.com.

Направления развития корпоративной информационной системы компании «Узбекистон Темир Йуллари»

Ф.И. Кушназаров
ООО Интернет научно-технологическая компания «ВЭЙБИ»
Шанхай, Китай
k.farruh@bk.ru

В.Г. Бабина
Ташкентский институт инженеров
железнодорожного транспорта
Ташкент, Узбекистан
victory2610@mail.ru

Аннотация. **В настоящее время железнодорожная транспортная система страны претерпевает существенные качественные изменения в связи с усилением конкуренции со стороны других видов транспорта. В статье рассмотрены основные этапы развития корпоративной информационной системы (КИС) железнодорожной компании АО «Узбекистон Темир Йуллари» в условиях развивающихся рыночных отношений. Эти обстоятельства выдвигают принципиально новые требования к КИС транспортно-промышленных корпораций и международных транспортных консорциумов, а также требуют адекватного формирования планов на будущее развитие транспортной отрасли в целом.**

Ключевые слова: **КИС, АСУ, СПД, бизнес-процессы, информационные технологии, уровни зрелости предприятия.**

Введение

В современном мире адекватное и динамичное реагирование на события является одним из основополагающих параметров развития компании. При этом наиболее значимым фактором является необходимость обработки все возрастающих объемов данных, что требует создания и поддержки соответствующих информационных ресурсов в составе корпоративной вычислительной инфраструктуры предприятия (вычислительные машины, сети передачи данных, соответствующее программное обеспечение, мобильные и веб-приложения, комплекты разработки, диагностики и мониторинга и др.).

В настоящее время актуальной для крупных корпораций, к числу которых относится АО «Узбекистон Темир Йуллари», является тема повышения отдачи от информационных технологий (ИТ), обеспечения их соответствия требованиям бизнеса. Во взаимоотношениях ИТ и бизнеса в последнее время стали проявляться две важные тенденции. С одной стороны, широко внедряемые приложения автоматизации бизнес-процессов и поддерживающие их технологии (информационные сети, сервисы, системы хранения данных, программные средства промежуточного слоя, СУБД, обработка больших объемов данных и т. д.) стали неотъемлемой частью повседневной работы предприятий. С другой стороны, приходит понимание того, что главная роль ИТ-инфраструктуры состоит в обеспечении эффективности бизнеса (сокращение оперативных затрат и повышение прибыльности компании).

В области ИТ-управления активно внедряется новая методология управления бизнес-сервисами BSM (Business Service Management), основная идея которой состоит в установлении более тесной связи между бизнес-процессами и компонентами ИТ-инфраструктуры компании.

При этом параметры качества такого бизнес-сервиса и результаты их измерения должны формулироваться в терминах бизнеса, а не на языке информационных технологий. Например, данные о задержке в сети, загрузке процессорных мощностей серверов или уровне доступности приложения необходимо трансформировать в число обработанных заказов, длительность цикла разработок, объем продаж и полученной прибыли и т. п. Соответствующая инструментальная поддержка обеспечивается в настоящее время наличием средств широкого класса проприетарных аналитических платформ, реализующих концепцию BABOK (Business Analysis Body of Knowledge), как свода знаний по бизнес-анализу. Причем при внедрении BSM и BABOK необходимо определить уровень зрелости корпо-рации со стороны информационных систем.

Определение уровня зрелости корпорации

При формировании планов развития КИС компании необходимо разработать стратегию ее развития. Для этого прежде всего следует провести оценку текущего состояния развития компании в целом, в том числе эффективности уже внедренных компьютерных и мобильных технологий. Необходимо оценить, насколько достигнутый уровень технологий обработки и анализа данных удовлетворяет современным требованиям по взаимодействию с пассажиропотоками и грузопотоками на всех участках, а также выявить потенциальные точки взаимодействия на основе анализа аналогичных практик в других железнодорожных компаниях, перспективных с точки зрения развития железнодорожной индустрии в целом.

После этого должна быть разработана бизнес-стратегия развития КИС на ограниченный контрольный период. Проект должен включать формирование перечня потенциальных инициатив, а также оценку необходимого уровня инвестиций в инновационные технологии.

На основе стратегии должны быть разработаны этапы развития данных технологий, включающие план с описанием инициатив, целей их достижения, необходимого бюджета, основных мероприятий, сроков и ответственных за реализацию лиц.

Известные конфигурации КИС часто классифицируют как [1]: автоматизированную систему управления, систему поддержки принятия решений, сеть передачи данных, систему сбора данных, информационно-аналитическую систему, информационно-поисковую систему, систему управления ресурсами и т. д.

В условиях АО «Узбекистон Темир Йуллари» рассматриваемый подход концептуально следует закрепить в нормативном документе. В этом документе должен быть указан один из базовых принципов создания эффективной КИС – единое информационное пространство (интеграция в единую автоматическую систему управления, регламент модификации в инфосреде компании и др.)

Необходимость создания КИС для управления ресурсами всех подразделений АО «Узбекистон Темир Йуллари» возникнет в процессе структурной реформы железнодорожной отрасли, для улучшения бизнес-деятельности компании и утилизации дотационных частей компании.

По данным ежегодного отчета консалтинговой компании Standish Group о состоянии дел в программной индустрии, около 24 % проектов корпоративных информационных систем (ИТ-проектов) заканчивается провалом, 44 % ИТ-проектов испытывают различные трудности (превышения бюджета, сроков и т. д.), и только 32 % проектов можно считать успешными [2].

Как известно, архитектура в общем случае – это концепция сложного объекта, определяющая состав, функции и взаимосвязь его компонентов. В качестве сложного объекта в данном случае выступает собственно КИС, в ее общей архитектуре можно выделить следующие составляющие:

- сетевая архитектура;
- программно-аппаратная архитектура;
- информационная архитектура;
- функциональная архитектура.

Перед тем как приступить к внедрению проекта КИС, эксперты рекомендуют оценить уровень зрелости предприятия. Одной из самых известных моделей для оценки зрелости является 5-уровневая модель, представленная в табл. 1.

Развитие КИС

При принятии решения о целесообразности создания КИС полезной является следующая рекомендация: нецелесообразно внедрять мощную современную технологию, если уровень зрелости предприятия не соответствует уровню этой технологии.

Можно рассмотреть комплексную модель CMMI for Development (Capability Maturity Model Integration for Development – Интеграция модели зрелости возможностей для развития) для оценивания зрелости процессов разработки программного обеспечения [3]. CMMI – набор моделей (методологий) совершенствования процессов в организациях разных размеров и видов деятельности. CMMI содержит набор рекомендаций в виде практик, реализация которых, по мнению разработчиков модели, позволяет реализовать цели, необходимые для полной реализации определённых областей деятельности.

Одним из параметров зрелости предприятия является система резервного копирования, которая также необходима для обеспечения непрерывности бизнеса. По данным компании Gartner, среди компаний, пострадавших от катастроф и переживших крупную необратимую потерю корпоративных данных, 43 % не смогли продолжить свою деятельность [4].

ТАБЛИЦА 1. Характеристика уровней зрелости предприятий

Уровень зрелости	**Характеристика уровня**
1	Начальный уровень Отсутствуют внутренние регулирующие документы. Действия не документируются, бизнес-знания не отделены от работников (знания пропадают при увольнении работников). Бизнес-процессы в компании не описаны и не классифицированы. Деятельность компании непрозрачна даже для основного персонала
2	Управляемый уровень Есть внутренние стандарты, описывающие основные бизнес-процессы компании. Возникает повторяемость: выполнение новых проектов основывается на опыте выполнения предыдущих проектов
3	Устоявшийся уровень В компании задокументированы и стандартизированы все бизнес-процессы. Система управления оказывается отделенной от персонала компании, т. е. появляется внутренний «свод законов». Эти законы распространяются на весь персонал компании
4	Измеряемый уровень В компании вводится количественная система оценки эффективности бизнес-процессов. Используется некоторая система оценки работы персонала, например система ключевых показателей. Обе системы оценки синхронизированы между собой – эффективная деятельность компании приводит к стимулированию персонала
5	Уровень совершенствования На основе анализа количественных показателей в компании проводится корректировка (реинжиниринг) бизнес-процессов. Коррекции отражаются во внутренних документах. Процесс коррекции носит постоянный, системный характер

Рассмотрев теоретические основы построения эффективных КИС, приходится констатировать, что типичная информационная среда предприятия – это, как правило, несколько программных систем, разрабатывавшихся в разное время разными разработчиками на разных платформах в соответствии с тем пониманием бизнес-процессов, которое существовало в соответствующее разработке время. Часть из них была разработана внутри предприятия, часть – приобретена как тиражированный продукт, однако все они обычно задействованы и их функционирование критично для предприятия.

Проблема заключается в том, что эти приложения – отдельные технологические «островки», независимые друг от друга, с отдельными, часто несопоставимыми данными «об одном и том же», с отсутствием технической документации и, следовательно, невозможностью развития. Кроме того, такие приложения обычно слабо взаимосвязаны или вообще не связаны друг с другом. При выборе программной оболочки желательно придерживаться определенных правил (табл. 2).

ТАБЛИЦА 2. Критерии выбора программной оболочки КИС

№ п/п	Обобщенные критерии	Частные критерии
1	Рейтинг производителя КИС	1. Длительность присутствия на рынке КИС 2. Количество внедрений (число клиентов) 3. Возможность ухода с рынка (надежность, финансовая устойчивость разработчика) 4. Система поставщиков (развитость, число поставщиков)
2	Функционал КИС	Широта функционала, число модулей (вариант: каждый частный критерий – одна из желаемых функций сверх обязательного набора поддерживаемых функций)
3	Поддержка поставщиком	1. Предоставление новых версий программных средств на регулярной основе 2. Помощь при модернизации 3. Уровень технической поддержки (оперативность, выезд к клиенту и пр.) 4. Информирование о проблемах и модернизациях, осуществляемых другими клиентами 5. Организация обучения персонала клиентов
4	Качество документации	1. Полнота документации 2. Понятность, простота использования, качество перевода 3. Простота внесения изменений в документацию при модернизации системы
5	Адаптация, модернизация, развитие	1. Простота настройки и внесения исправлений 2. Гибкость, открытость (простота внесения изменений и расширения функциональности) 3. Масштабируемость (возможность увеличения производительности без существенных изменений программных средств системы) 4. Простота интеграции с другими системами (в том числе с ранее созданными на предприятии)
6	Эксплуатационные характеристики	1. Легкость установки системы 2. Простота администрирования 3. Простота работы пользователя (в том числе наличие средств помощи пользователю) 4. Оперативность восстановления при сбоях 5. Формирование сообщений о сбоях, документирование сбоев, наличие опций и инструкций по устранению последствий сбоев 6. Полнота и качество средств защиты информации
7	Финансовые показатели	1. Затраты на обучение персонала 2. Эксплуатационные затраты (включая затраты на обновление лицензий, передачу данных по каналам связи, модернизацию, оплату персонала, приобретение дополнительных модулей и т. д.) 3. Стоимость приобретения 4. Стоимость технической поддержки (вариант «Совокупная стоимость владения»: сумма прямых (стоимость оборудования, лицензий, затраты на эксплуатацию, модернизацию и т. д.) и косвенных (затраты на административный аппарат, коммутационные услуги и т. д.) затрат за период жизненного цикла системы (т. е. с момента ее приобретения до прекращения эксплуатации)

При оценке качества и тестировании программного обеспечения используются следующие методы [5]:

- тестирование программного обеспечения и измерение количественных показателей качества;
- определение показателей качества с помощью математических моделей;
- анализ проектной документации и исходного кода для выявления их свойств.

Внедрение ITSM (IT Service Management – управление ИТ-услугами) можно разделить на условные этапы [6]:

Обследование. Проводится анализ ИТ-инфраструктуры и бизнес-процессов.

Проектирование. Разработка логического и физического (прототипа) проекта системы автоматизации и обучения сотрудников, план ввода решения в эксплуатацию.

Опытная эксплуатация. ITSM тестируется на основе созданных конкретных документов бизнес-процесса и системы АСУ.

Основным информационно-технологическим средством АО «Узбекистон темир йуллари» является Автоматизированная система оперативного управления перевозками (АСОУП), разработанная ОАО «РЖД» [3]. Дорожная АСОУП базируется на системе SAP/3, которая не только использовала опыт предшествующих систем, но и обеспечивала их взаимодействие, позволяла сделать шаг к объединению всех систем оперативного управления в единую многоуровневую отраслевую автоматизированную систему управления грузовыми перевозками.

В состав АСОУП входят следующие эксплуатируемые системы и комплексы задач [7]:

- автоматизированная система пономерного учета контроля дислокации, анализа использования и регулирования вагонного парка (ДИСПАРК);
- автоматизированная система управления тяговыми ресурсами (ДИСТПС), включающая оперативный контроль наличия, состояния и дислокации локомотивов грузового движения и организацию их подвода на техническое обслуживание (ОКДЛ-1), дислокацию и работу локомотивных бригад грузового движения (ОКДБ-1);
- автоматизированная информационная система организации перевозок грузов по безбумажной технологии с использованием электронной накладной (АИС ЭДВ);
- «Грузовой Экспресс» в части ведения подсистем контроля погрузки экспортных грузов в адрес портов и пограничных переходов и информационного взаимодействия между автоматизированными системами регионов припортовых, пограничных станций и регионов примыкания к крупным промышленным комплексам;
- система оперативного пономерного контроля погрузки и выгрузки вагонов, включая распределение по типам и категориям годности (ОКПВ);
- автоматизированный банк данных инвентарного парка вагонов железных дорог и вагонов, принадлежащих предприятиям и другим организациям (ЛБД-ПВ);
- информационная система определения собственника вагонов (СОСВЛГ);
- автоматизированная система контроля за использованием и продвижением контейнеров (ДИСКОН).

В состав АСОУП входит около 6000 программ. АСОУП обеспечила выдачу оперативным работникам

станций и управлений дорог комплекса технологических документов по каждому поезду. Она стала фундаментом для создания ряда новых автоматизированных систем и комплексов задач в системе управления перевозочным процессом.

Направления дальнейших исследований

Возникает необходимость создания исследовательского проекта пошагового перехода КИС на уровень зрелости 5 (табл. 1), при этом следует уделять большее внимание полносвязанности и централизованности системы.

В качестве одной из перспективных возможностей рассматривается создание программного обеспечения с доступом через REST и SOAP [8]. Данное программное обеспечение будет работать в виде облачного сервиса на приватном сетевом пространстве корпорации и, следовательно, будет иметь единое окно выхода на все подсистемы с определением уровнем доступа пользователей относительно местоположения и должности. Например, у оператора, находящегося на станции, будет более детальный вид станции, чем у оператора в диспетчерском центре.

Ожидается обработка огромного количества данных, в связи с этим возникает необходимость применения технологии больших данных (Big Data) с динамической отчетной системой в онлайн-режиме и минимальными задержками [9].

В связи с этим возникнет необходимость создания подразделения BI (Business intelligence), работающего с большими данными, интерпретирующего большое количество данных, моделирующего исход различных вариантов действий и отслеживающего результаты принятия решений [10, 11].

Так как создание таких систем требует больших вложений (человеко-часов и денежных), планируется создание имитационной модели на базе лаборатории ТашИИТа (Ташкентского института инженеров транспорта). Таким образом, внедрение данной системы станет возможным после оценки ее эффективности и производительности на имитационной модели путем математического моделирования.

Одним из перспективных направлений развития железнодорожного транспорта является переход на цифровую железную дорогу. Цифровая железная дорога – это целый комплекс информационно-аналитических систем, систем управления перевозочным процессом, систем управления вокзальными комплексами, интеллектуальных систем для тягового подвижного состава и т. д. По мнению авторов, ключевыми факторами цифровой железной дороги являются следующие технологии: обработка больших данных, внедрение искусственного интеллекта (ИИ) и блокчейн-механизмов для безопасности.

Источниками больших данных могут быть данные, полученные с датчиков, расположенных на транспортных средствах (локомотивах, вагонах, контейнерах и т. д.), – это перспективный источник информации в железнодорожной отрасли [12].

Еще один потенциальный вариант – данные с мобильных приложений, которыми пользуются машинисты и наземные операторы, а также запросы на грузовое бронирование, получаемые от клиентов. Кроме того, день за днем появляются новые источники данных, которые могут быть использованы как часть инфраструктуры цифровой железной дороги.

Перечисленные выше данные могут служить хорошими исходными данными для ИИ, так как использование ИИ избавляет людей от рутинных работ и уменьшает в разы влияние человеческого фактора, которое в большинстве случаев снижает уровень безопасности транспортной системы.

Также блокчейн-механизм будет обеспечивать безопасность и прозрачность цифровой железной дороги.

Заключение

Существенная задача, стоящая перед компанией, – разработка собственной КИС. Имеется два пути ее осуществления:

1) разработка собственного продукта с нуля, при этом необходимо иметь высококвалицированных разработчиков системы. Такая КИС будет рассчитана на эксплуатацию в течение нескольких десятков лет с необходимым обновлением в определенные сроки;

2) внедрение продуктов ведущих вендоров, таких как SAP, IBM, EMS, 1С др.

В эпоху развития информационных технологий разработка и развитие КИС является необходимым условием дальнейшего существования компании. В данной работе представлен перечень мероприятий для создания, поддержки и планомерного развития таких информационных систем.

Литература

1. Борчанинов М.Г. Корпоративные информационные системы на железнодорожном транспорте / М.Г. Борчанинов, Э.К. Лецкий, В.В. Яковлев. – М. : ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2013. – 116 с.

2. CHAOS Summary 2009 report The Standish Group. – Boston, Massachusetts, April 23, 2009: www.standishgroup.com/newsroom/chaos_2009.php.

3. SCAMPI Upgrade Team. Standard CMMI Appraisal Method for Process Improvement (SCAMPI) A Version 1.3: Method Definition Document. Carnegie Mellon University Software Engineering Institute. March 2011. – P. 37–45.

4. Russell D., DiCenzo C. Gartner RAS Core Research Note G00142739. MarketScope, 2006. – P. 55–58.

5. Лецкий Э.К. Проектирование информационных систем на железнодорожном транспорте. – М. : Маршрут, 2003. – 83 с.

6. Brenner, M. Classifying ITIL Processes – A Taxonomy under Tool Support Aspects. Munich Network Management Team University of Munich IEEE. 2006.

7. Лецкий Э.К. Информационные технологии на железнодорожном транспорте : учебник для вузов ж.-д. транспорта / Э.К. Лецкий, В.И. Панкратов, В.В. Яковлев. – М. : УМК МПС России, 2000. – 444 с.

8. Кушназаров Ф.И. Сравнение производительности протоколов доступа к облачным ресурсам / Ф.И. Кушназаров, В.В. Яковлев, О.А. Турдиев // Известия Петербургского университета путей сообщения. – Вып. 4(45). – 2015. – с. 117–123.

9. Goepfert J., Glennon M., etc. IDC's Worldwide Semiannual Big Data and Analytics Spending Guide Taxonomy, https://www.idc.com/getdoc.jsp?containerId=US43625215.

10. Luhn H.P. A Business Intelligence System. IBM Journal of Research and Development (Volume: 2, Issue: 4, Oct. 1958). – P. 314–319.

11. Gartner Says Worldwide Business Intelligence, CPM and Analytic Applications/Performance Management Software Market Grew Seven Percent in 2012. https://www.gartner.com/newsroom/id/2507915.

12. Куприяновский В.П. Цифровая железная дорога – прогнозы, инновации, проекты / В.П. Куприяновский, Г.В. Суконников, П.М. Бубнов и др. // International Journal of Open Information Technologies. – Vol. 4, no. 9. – 2016. – 34–43 с.

Directions of Development of the Corporate Information System of the Company «Uzbekiston Temir Yullari»

F.I. Kushnazarov
Internet Scientific Company «Weibi»
Shanghai, China
K.farruh@bk.ru

V.G. Babina
Tashkent Railway Engineering Institute
Tashkent, Uzbekistan
victory2610@mail.ru

Abstract. **The transport system is currently undergoing qualitative changes, connections with a large competition of different types of transport. In this paper discussed the ways of developing the corporate information system (CIS) of the railway company, as an example took JSC «Uzbekistan Temir Yullari». The ways of development of CIS are considered in the conditions of developing market relations, which sharply affects the productivity of transport. These circumstances put forward fundamentally new requirements for corporate information systems of transport-industrial corporations and international transport consortia also require the correct forming of plans for the future development of whole transport industry.**

Keywords: **CIS, automatic control systems, computing networks, business processes, information technologies, maturity levels of enterprises.**

REFERENCES

1. Borchaninov M.G. Corporate Information Systems in Railway Transport / Borchaninov M.G., Letsky E.K., Yakovlev V.V. – Moscow: «Educational and Methodological Center for Education in Railway Transport». – 2013. – 116 p.

2. CHAOS Summary 2009 report The Standish Group, Boston, Massachusetts, April 23, 2009: www.standishgroup.com/newsroom/chaos_2009.php.

3. «Standard CMMI Appraisal Method for Process Improvement (SCAMPI) A Version 1.3: Method Definition Document». Carnegie Mellon University Software Engineering Institute. – March 2011, p. 37–45.

4. Russell D., DiCenzo C. Gartner RAS Core Research Note G00142739. MarketScope, 2006, p. 55–58.

5. Letsky E.K. Information Technologies in Railway Transport: / Letsky E.K., Pankratov V.I., Yakovlev V.V. // Textbook. For higher educational institution in railway transports – Moscow: UMK MPS of Russia, 2000. – 444 p.

6. «Brenner, M. Classifying ITIL Processes – A Taxonomy under Tool Support Aspects». Munich Network Management Team University of Munich IEEE. – 2006, p. 55–58.

7. Letsky E.K. Designing information systems in rail transport – Moscow: Marshrut, 2003. – 83 p.

8. Kushnazarov F.I Comparing the performance of access protocols to cloud resources./ Kushnazarov F.I, Yakovlev V.V, Turdiev O.A. // Izvestia of the St. Petersburg State Transport University, issue 4 (45) 2015, p. 117-123.

9. Woo, Benjamin et al. IDC's Worldwide Big Data Taxonomy . International Data Corporation (1 October 2011).

10. H. P. Luhn. A Business Intelligence System. IBM Journal of Research and Development (Volume: 2, Issue: 4, Oct. 1958). – P. 314–319.

11. Gartner Says Worldwide Business Intelligence, CPM and Analytic Applications/Performance Management Software Market Grew Seven Percent in 2012. https://www.gartner.com/newsroom/id/2507915.

12. Kupriyanovsky V.P. Digital Railroad – forecasts, innovations, and projects / Kupriyanovsky V.P., Sukonnikov G.V., Bubnov P.M., Sinyagov S.A., Namiot. D.E. // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 4, no. 9, 2016, pp. 34–43.

Исследование коэффициента готовности сложных технических комплексов с помощью имитационной модели, разработанной в среде Stateflow пакета MatLab

И.В. Дорожко, А.Л. Копейка
Военно-космическая академия имени А.Ф. Можайского
Санкт-Петербург, Россия
Doroghko-Igor@yandex.ru

Аннотация. **Работа посвящена исследованию зависимости показателей надежности и контроля (диагностирования) сложных технических комплексов. В статье представлена имитационная модель оценивания комплексного показателя надежности (коэффициента готовности) с учетом показателей контроля и диагностирования сложных технических комплексов, разработанная с помощью среды моделирования Stateflow программного пакета Matlab. Адекватность разработанной имитационной модели подтверждается аналитическими расчетами. Разработанная имитационная модель позволяет вычислять коэффициент готовности с учетом режимов эксплуатации, т. е. для нестационарных процессов, у которых параметры могут меняться со временем. В отличие от аналитической модели имитационную модель можно расширить с учетом всех возможных видов технического состояния объекта, избегая громоздких формул.**

Ключевые слова: **надежность, контроль, диагностирование, коэффициент готовности, достоверность, ошибки, марковский процесс, имитационная модель.**

Введение

В настоящее время при предъявлении требований и расчете показателей надежности сложных технических комплексов практически не рассматривается влияние показателей контроля и диагностирования. Хотя связь этих показателей представляется очевидной и интуитивно понятной, существующие оценки влияния показателей контроля и диагностирования на показатели надежности объекта носят, как правило, качественный характер, без конкретных аналитических зависимостей и математических моделей.

Современные структурно сложные комплексы имеют в своем составе встроенные средства аппаратного и программного контроля и диагностирования. В технических заданиях (ТЗ) на выполнение опытно-конструкторских работ по созданию (модернизации) сложных технических комплексов присутствуют в обязательном порядке разделы «Требования надежности» и «Требования к диагностическому обеспечению».

В разделе «Требования надежности», как правило, приводятся требуемые значения вероятности безотказной работы комплекса, коэффициента готовности, максимального времени восстановления и т. д. В разделе «Требования к диагностическому обеспечению» в большинстве случаев указывается требуемая глубина диагностирования (например, до сменного модуля), приводятся допустимые значения ошибок 1-го и 2-го рода при контроле технического состояния, требуемые значения достоверности и периодичности диагностирования, которые влияют на показатели надежности сложных технических комплексов. Следовательно, разработка и исследование имитационных и аналитических моделей, связывающих показатели надежности и диагностирования, является важной и актуальной задачей.

Модель марковского процесса, связывающая коэффициент готовности и достоверность диагностирования сложных технических комплексов

На рисунке 1 изображена схема графа состояний, представляющего собой описание марковского процесса перехода из одного состояния в другое. Модель подробно рассмотрена в работах [1, 2] и позволяет связать коэффициент готовности и достоверность контроля сложных технических комплексов. Достоверность диагностирования при этом оценивалась условной вероятностью пребывания объекта в некотором виде технического состояния при условии, что система диагностирования зафиксировала именно этот вид технического состояния [3, 4]. В качестве показателя надежности был выбран комплексный показатель надежности – коэффициент готовности [5–8], который имеет особую важность для многих сложных технических комплексов (ракетно-космических, авиационных, морских, железнодорожных), а также комплексов атомной энергетики и др.

В качестве состояний марковского процесса выступают работоспособное и неработоспособное состояния объекта (S_0, $\overline{S_0}$), в которых контроль не проводится (т. е. «рабочий режим»), а также состояния, при которых производится контроль: R_1, R_3 – состояния, при которых проводится контроль с достоверным результатом (S_0^*/S_0 – система

контроля фиксирует работоспособное состояние S_0^*, при этом объект действительно работоспособен S_0, $\overline{S_0^*}/\overline{S_0}$ – система контроля обнаруживает неработоспособное состояние $\overline{S_0^*}$, при этом объект действительно неработоспособен $\overline{S_0}$); R_2, R_4 – состояния, при которых проводится контроль с ошибочным результатом ($\overline{S_0^*}/S_0$ – система контроля обнаруживает неработоспособное состояние $\overline{S_0^*}$, при этом объект работоспособен S_0, $S_0^*/\overline{S_0}$ – система контроля фиксирует работоспособное состояние S_0^*, при этом объект неработоспособен $\overline{S_0}$).

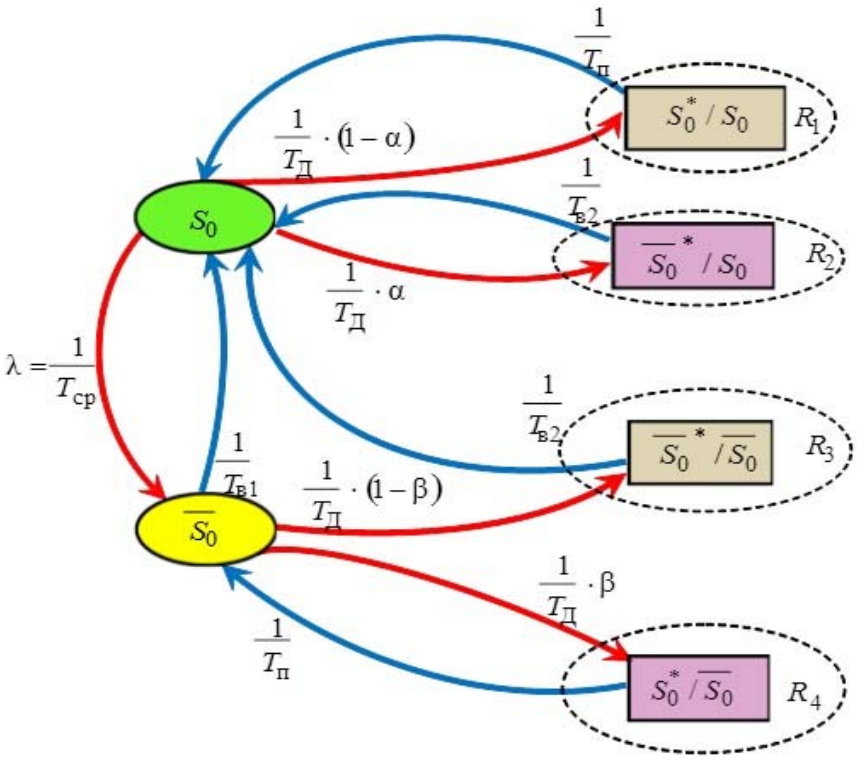


Рис. 1. Схема марковского процесса, связывающая показатели надежности и контроля

На рисунке 1 также введены следующие обозначения: α, β – вероятности ошибок контроля (ошибок 1-го и 2-го рода); $T_{СР}$ – средняя наработка на отказ; $T_Д$ – периодичность контроля; $T_{В1}$ – среднее время восстановления без применения средств контроля (т. е. предполагается, что объект можно восстановить даже при отсутствии или отказе средств контроля, например, с помощью последовательной замены блоков до тех пор, пока система не станет работоспособной. Очевидно, что на это могут потребоваться значительное время и ресурсы. Если без контроля объект не может быть восстановлен, то $T_{В1} \to \infty$); $T_{В2}$ – среднее время восстановления с учетом контроля; $T_П$ – средняя продолжительность перевода объекта из режима контроля в рабочий режим (если контроль происходит параллельно с работой объекта (функциональный контроль), то $T_П = 0$, но если производится тестовый контроль, при котором объект последовательно переводится из режима контроля в рабочий режим и обратно, то необходимо учитывать $T_П$).

Данная модель имеет следующие преимущества:

– учет достоверности результатов диагностирования (через вероятности ошибок результатов диагностирования);

– возможность рассмотрения предельных случаев: отсутствие контроля (диагностирования) и наличие постоянного контроля (диагностирования);

– возможность рассмотрения тестового ($T_П \neq 0$) и функционального диагностирования ($T_П = 0$).

Исследование зависимости коэффициента готовности от показателей контроля сложных технических комплексов

По графу состояний (см. рис. 1) опишем марковский процесс системой дифференциальных уравнений:

$$\begin{cases} -\left(\frac{1}{T_Д}+\frac{1}{T_{СР}}\right)\cdot P_{S_0}(t)+\frac{1}{T_{В1}}\cdot P_{\overline{S_0}}(t)+\frac{1}{T_П}\cdot P_{R_1}(t)+\frac{1}{T_{В2}}\cdot\left(P_{R_2}(t)+P_{R_3}(t)\right)=\frac{d\left(P_{S_0}(t)\right)}{dt}; \\ \frac{1}{T_{СР}}\cdot P_{S_0}(t)-\left(\frac{1}{T_Д}+\frac{1}{T_{В1}}\right)\cdot P_{\overline{S_0}}(t)+\frac{1}{T_П}\cdot P_{R_4}(t)=\frac{d\left(P_{\overline{S_0}}(t)\right)}{dt}; \\ \frac{1-\alpha}{T_Д}\cdot P_{S_0}(t)-\frac{1}{T_П}\cdot P_{R_1}(t)=\frac{d\left(P_{R_1}(t)\right)}{dt}; \\ \frac{\alpha}{T_Д}\cdot P_{S_0}(t)-\frac{1}{T_{В2}}\cdot P_{R_2}(t)=\frac{d\left(P_{R_2}(t)\right)}{dt}; \\ \frac{1-\beta}{T_Д}\cdot P_{\overline{S_0}}(t)-\frac{1}{T_{В2}}\cdot P_{R_3}(t)=\frac{d\left(P_{R_3}(t)\right)}{dt}; \\ \frac{\beta}{T_Д}\cdot P_{\overline{S_0}}(t)-\frac{1}{T_П}\cdot P_{R_4}(t)=\frac{d\left(P_{R_4}(t)\right)}{dt}. \end{cases} \quad (1)$$

В стационарном режиме Марковский процесс можно описать системой алгебраических уравнений (2):

$$\begin{cases} -\left(\frac{1}{T_Д}+\frac{1}{T_{СР}}\right)\cdot P_{S_0}+\frac{1}{T_{В1}}\cdot P_{\overline{S_0}}+\frac{1}{T_П}\cdot P_{R_1}+\frac{1}{T_{В2}}\cdot\left(P_{R_2}+P_{R_3}\right)=0; \\ \frac{1}{T_{СР}}\cdot P_{S_0}-\left(\frac{1}{T_Д}+\frac{1}{T_{В1}}\right)\cdot P_{\overline{S_0}}+\frac{1}{T_П}\cdot P_{R_4}=0; \\ \frac{1-\alpha}{T_Д}\cdot P_{S_0}-\frac{1}{T_П}\cdot P_{R_1}=0; \\ \frac{\alpha}{T_Д}\cdot P_{S_0}-\frac{1}{T_{В2}}\cdot P_{R_2}=0; \\ \frac{1-\beta}{T_Д}\cdot P_{\overline{S_0}}-\frac{1}{T_{В2}}\cdot P_{R_3}=0; \\ \frac{\beta}{T_Д}\cdot P_{\overline{S_0}}-\frac{1}{T_П}\cdot P_{R_4}=0. \end{cases} \quad (2)$$

Для однозначного решения систем уравнений (1) и (2) добавим нормирующие суммы $P_{S_0}(t)+P_{\overline{S_0}}(t)+P_{R_1}(t)+P_{R_2}(t)+P_{R_3}(t)+P_{R_4}(t)=1$ и $P_{S_0}+P_{\overline{S_0}}+P_{R_1}+P_{R_2}+P_{R_3}+P_{R_4}=1$, соответственно образуется полная группа событий, так как система может находиться в шести состояниях: S_0 – объект работоспособен, диагностирование не производится, $\overline{S_0}$ – объект неработоспособен, диагностирование не производится, R_1 – объект работоспособен, диагностирование производится, технический диагноз «работоспособен», R_2 – объект неработоспособен, диагностирование производится, технический диагноз «работоспособен», R_3 – объект неработоспособен, диагностирование производится, технический диагноз «неработоспособен», R_4 – объект неработоспособен, диагностирование производится, технический диагноз «работоспособен». Решение системы уравнений (2) в символьном виде относительно P_{S_0}, $P_{\overline{S_0}}$, P_{R_1}, P_{R_2}, P_{R_3}, P_{R_4} позволяет получить аналитическое выражение для коэффициента готовности: $K_Г = P_{S_0} =$

$$= \frac{T_{СР}\cdot T_Д\cdot\left(T_{В1}\cdot(1-\beta)+T_Д\right)}{T_{СР}\cdot T_{В1}\cdot(1-\beta)\cdot\left(T_{В2}\cdot\alpha+T_П\cdot(1-\alpha)\right)+T_{СР}\cdot T_Д\cdot\left(T_П\cdot(1-\alpha)+T_{В1}\cdot(1-\beta)\right)+T_Д\cdot\left(T_{В1}\cdot T_{В2}\cdot(1-\beta)+T_Д\cdot(T_{СР}+T_{В1})+T_{СР}\cdot T_{В2}\cdot\alpha+T_П\cdot T_{В1}\cdot\beta\right)}. \quad (3)$$

Если рассматривается функциональное диагностирование, то $T_{\text{П}} = 0$ и формула (3) примет следующий вид:

$$K_{\text{Г}} = \frac{T_{\text{СР}} \cdot T_{\text{Д}} \cdot \left(T_{\text{В1}} \cdot (1-\beta) + T_{\text{Д}}\right)}{T_{\text{СР}} \cdot T_{\text{В1}} \cdot (1-\beta) \cdot T_{\text{В2}} \cdot \alpha + T_{\text{СР}} \cdot T_{\text{Д}} \cdot T_{\text{В1}} \cdot (1-\beta) + T_{\text{Д}} \cdot \left(T_{\text{В1}} \cdot T_{\text{В2}} \cdot (1-\beta) + T_{\text{Д}} \cdot (T_{\text{СР}} + T_{\text{В1}}) + T_{\text{СР}} \cdot T_{\text{В2}} \cdot \alpha\right)}. \quad (4)$$

Если рассматривается тестовое диагностирование без ошибок ($\alpha = 0, \beta = 0$), то формула (3) примет такой вид:

$$K_{\text{Г}} = \frac{T_{\text{СР}} \cdot T_{\text{Д}} \cdot \left(T_{\text{В1}} + T_{\text{Д}}\right)}{T_{\text{СР}} \cdot T_{\text{В1}} \cdot T_{\text{П}} + T_{\text{СР}} \cdot T_{\text{Д}} \cdot \left(T_{\text{П}} + T_{\text{В1}}\right) + T_{\text{Д}} \cdot \left(T_{\text{В1}} \cdot T_{\text{В2}} + T_{\text{Д}} \cdot (T_{\text{СР}} + T_{\text{В1}})\right)}. \quad (5)$$

Если рассматривается функциональное диагностирование без ошибок ($\alpha = 0$, $\beta = 0$, $T_{\text{П}} = 0$), то формула (3) примет вид:

$$K_{\text{Г}} = \frac{T_{\text{СР}} \cdot \left(T_{\text{В1}} + T_{\text{Д}}\right)}{T_{\text{СР}} \cdot T_{\text{В1}} + T_{\text{В1}} \cdot T_{\text{В2}} + T_{\text{Д}} \cdot T_{\text{СР}} + T_{\text{Д}} \cdot T_{\text{В1}}} = \frac{T_{\text{СР}}}{T_{\text{СР}} + T_{\text{В1}} \cdot \dfrac{T_{\text{В2}} + T_{\text{Д}}}{\left(T_{\text{В1}} + T_{\text{Д}}\right)}}. \quad (6)$$

Если диагностирование вообще не учитывать (т. е. $T_{\text{Д}} \to \infty$), то получим известную из теории надежности систем формулу [5–8]:

$$K_{\text{Г}} = \frac{T_{\text{СР}}}{T_{\text{СР}} + T_{\text{В1}}}. \quad (7)$$

Имитационная модель для оценивания показателей надежности сложных технических комплексов с учетом показателей контроля

Для построения моделей, подобных изображенной на рис. 1, может успешно применяться среда Stateflow, входящая в состав последних версий программного продукта Matlab [9, 10]. На рис. 2 представлена схема имитационной модели, построенная в среде Stateflow пакета Matlab.

Рассмотрим связь матрицы интенсивностей переходов и матрицы вероятностей переходов в марковских процессах. Для этого получим дифференциальное уравнение, описывающее марковский процесс, используя уравнение Колмогорова–Чепмена, в следующем виде:

$P(t + \Delta t) = P(t) \cdot \mathbf{P}$, где $\mathbf{P}$ – матрица вероятностей переходов;

$P(t + \Delta t) - P(t) = P(t) \cdot \mathbf{P} - P(t)$;

$\dfrac{P(t + \Delta t) - P(t)}{\Delta t} = \dfrac{P(t) - (\mathbf{P} - \mathbf{E})}{\Delta t}$, где $\mathbf{E}$ – единичная матрица;

$\dot{P}(t) = P(t) \cdot \mathbf{A}$, где $\mathbf{A}$ – матрица интенсивностей переходов, $\mathbf{A} = \dfrac{\mathbf{P} - \mathbf{E}}{\Delta t}$.

Следовательно, $\mathbf{P} = \mathbf{A} \cdot \Delta t + \mathbf{E}$.

Для построения графа, входящего в блок «Chart» (рис. 2), от матрицы интенсивностей переходов из систем уравнений (1) и (2) перейдем к матрице вероятностей переходов:

$$\mathbf{A} = \begin{bmatrix} -\left(\frac{1}{T_{\text{Д}}} + \frac{1}{T_{\text{СР}}}\right) & \frac{1}{T_{\text{СР}}} & \frac{1-\alpha}{T_{\text{Д}}} & \frac{\alpha}{T_{\text{Д}}} & 0 & 0 \\ \frac{1}{T_{\text{В1}}} & -\left(\frac{1}{T_{\text{Д}}} + \frac{1}{T_{\text{В1}}}\right) & 0 & 0 & \frac{1-\beta}{T_{\text{Д}}} & \frac{\beta}{T_{\text{Д}}} \\ \frac{1}{T_{\text{П}}} & 0 & -\frac{1}{T_{\text{П}}} & 0 & 0 & 0 \\ \frac{1}{T_{\text{В2}}} & 0 & 0 & -\frac{1}{T_{\text{В2}}} & 0 & 0 \\ \frac{1}{T_{\text{В2}}} & 0 & 0 & 0 & -\frac{1}{T_{\text{В2}}} & 0 \\ 0 & \frac{1}{T_{\text{П}}} & 0 & 0 & 0 & -\frac{1}{T_{\text{П}}} \end{bmatrix}. \quad (8)$$

$$\mathbf{P} = \begin{bmatrix} 1-\left(\frac{1}{T_{\text{Д}}}+\frac{1}{T_{\text{СР}}}\right)\cdot\Delta t & \frac{1}{T_{\text{СР}}}\cdot\Delta t & \frac{1-\alpha}{T_{\text{Д}}}\cdot\Delta t & \frac{\alpha}{T_{\text{Д}}}\cdot\Delta t & 0 & 0 \\ \frac{1}{T_{\text{В1}}}\cdot\Delta t & 1-\left(\frac{1}{T_{\text{Д}}}+\frac{1}{T_{\text{В1}}}\right)\cdot\Delta t & 0 & 0 & \frac{1-\beta}{T_{\text{Д}}}\cdot\Delta t & \frac{\beta}{T_{\text{Д}}}\cdot\Delta t \\ \frac{1}{T_{\text{П}}}\cdot\Delta t & 0 & 1-\frac{1}{T_{\text{П}}}\cdot\Delta t & 0 & 0 & 0 \\ \frac{1}{T_{\text{В2}}}\cdot\Delta t & 0 & 0 & 1-\frac{1}{T_{\text{В2}}}\cdot\Delta t & 0 & 0 \\ \frac{1}{T_{\text{В2}}}\cdot\Delta t & 0 & 0 & 0 & 1-\frac{1}{T_{\text{В2}}}\cdot\Delta t & 0 \\ 0 & \frac{1}{T_{\text{П}}}\cdot\Delta t & 0 & 0 & 0 & 1-\frac{1}{T_{\text{П}}}\cdot\Delta t \end{bmatrix}. \quad (9)$$

Схема построенной в среде Stateflow имитационной модели надежности и диагностирования приведена на рис. 3 («Δt» обозначили как dt, так как $dt = \Delta t$ при $\Delta t \to 0$, а величины α, β обозначены как «a» и «b» соответственно).

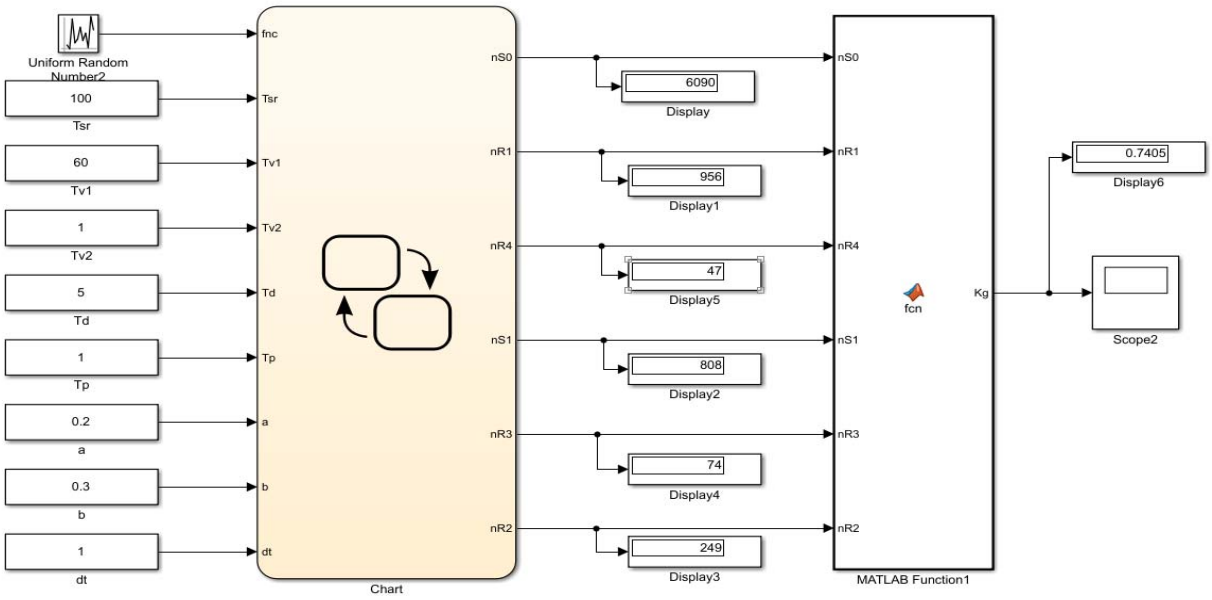


Рис. 2. Схема имитационной модели надежности и диагностирования

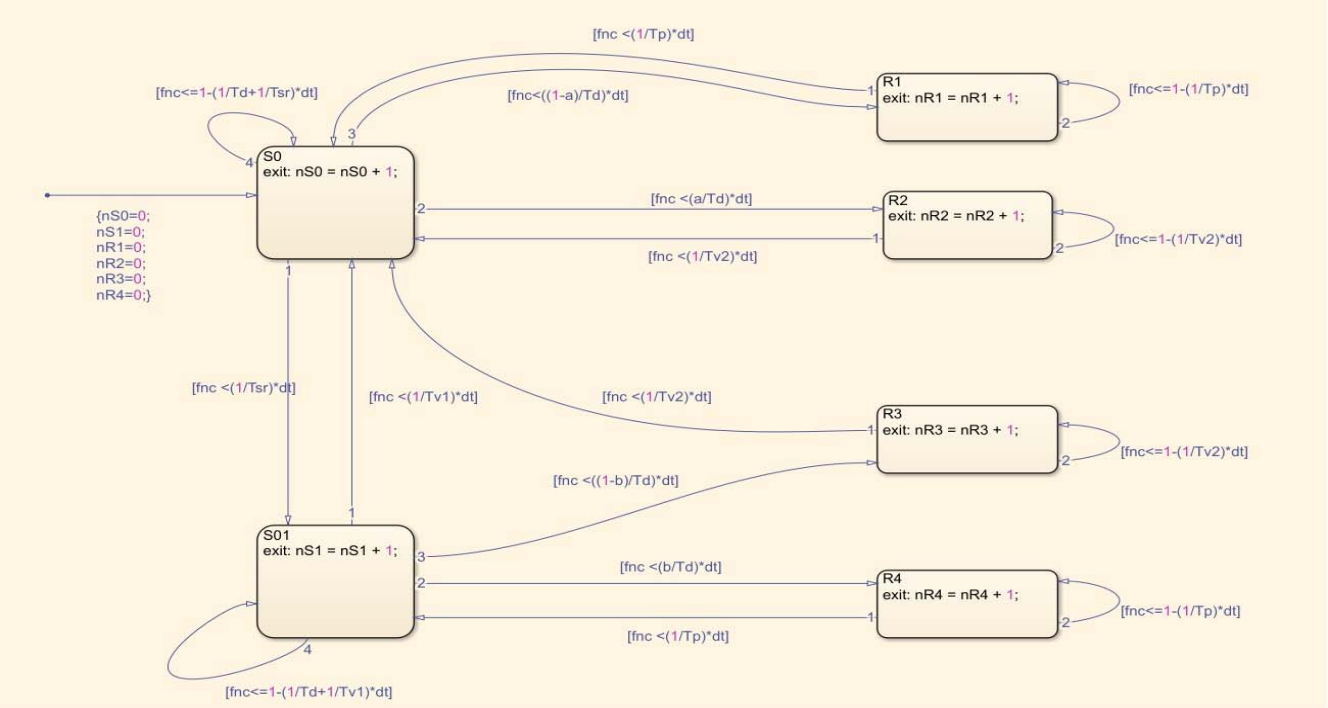


Рис. 3. Содержание блока «Chart»

Для проверки на адекватность сначала влияние контроля и диагностирования не рассматривалось ($T_{Д} \to \infty$). При этом коэффициент готовности должен был вычисляться по известной аналитической зависимости (7):

$$K_{Г} = \frac{T_{СР}}{T_{СР} + T_{В1}} = \frac{100 \text{ ч}}{100 \text{ ч} + 60 \text{ ч}} \approx 0{,}625.$$

На рисунке 4 представлены результаты имитационного моделирования.

Исходными данными для имитационного моделирования являлись следующие значения: $T_{СР} = 100$ ч, $T_{В1} = 60$ ч, $T_{В2} = 1$ ч, $T_{Д} = 1\,000\,000$ ч (т. е. период диагностирования очень большой: $T_{Д} \to \infty$); $T_{П} = 1$ ч, $\alpha = \beta = 0$. На рисунке 4 представлены результаты расчета коэффициента готовности с помощью имитационного моделирования.

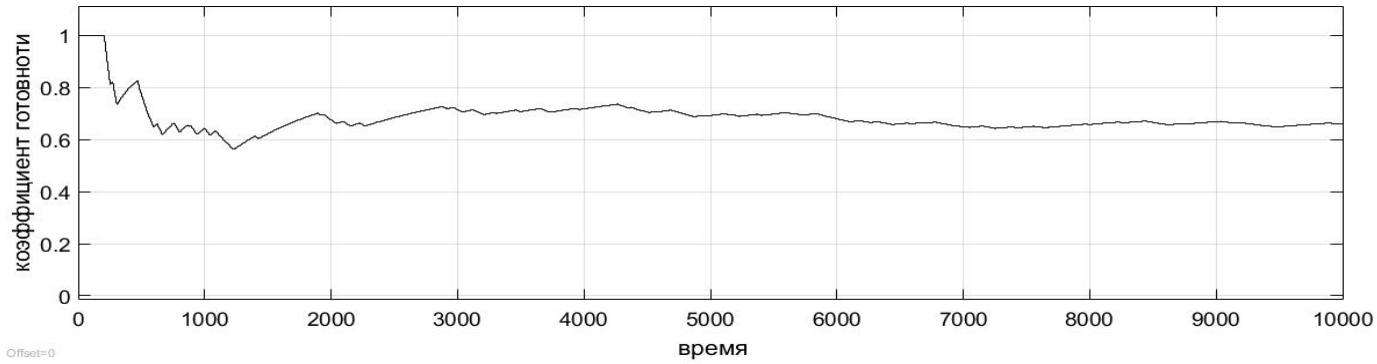


Рис. 4. Зависимость коэффициента готовности от времени без учета влияния контроля (диагностирования)

Далее при имитационном моделировании учитывались только достоверные результаты контроля и диагностирования (т. е. $\alpha = \beta = 0$), при этом $T_д = 5$ ч. На рисунке 5 представлены результаты имитационного моделирования.

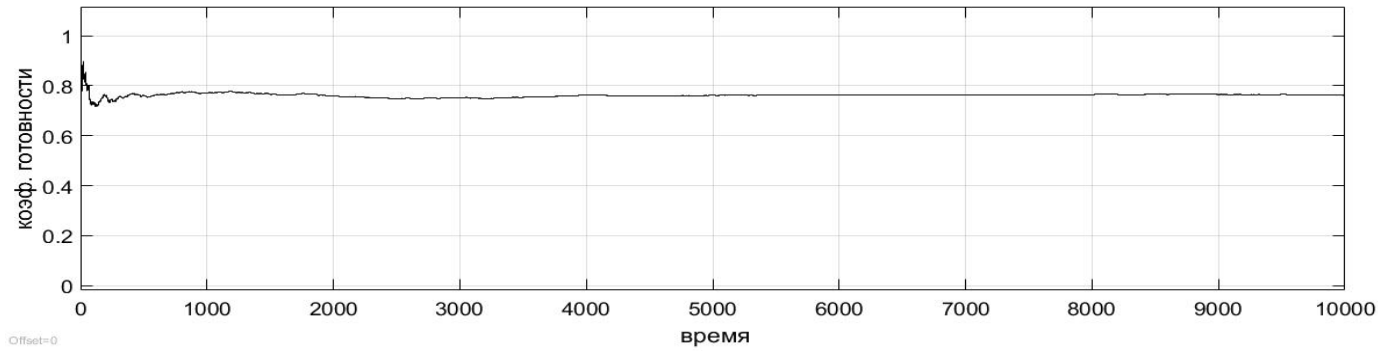


Рис. 5. Зависимость коэффициента готовности от времени с учетом контроля, но без учета ошибочных решений

Значение коэффициента готовности, вычисленное по аналитической модели (3), равно 0,797.

Затем учитывались ошибки 1-го и 2-го рода. Исходными данными для имитационного моделирования являлись следующие значения: $T_{СР} = 100$ ч, $T_{В1} = 60$ ч, $T_{В2} = 1$ ч, $T_Д = 5$ ч; $T_П = 1$ ч, $\alpha = 0{,}2$, $\beta = 0{,}3$.

На рисунке 6 представлены результаты имитационного моделирования.

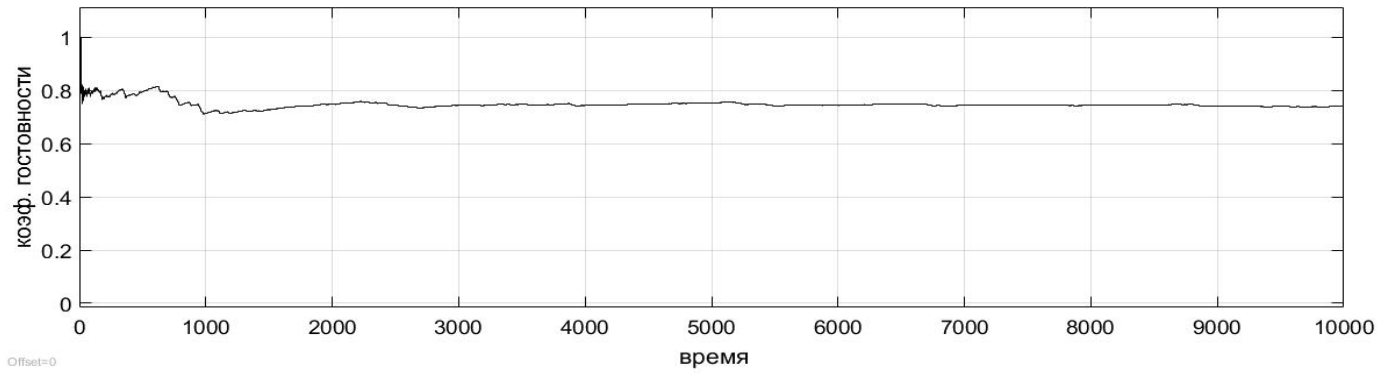


Рис. 6. Зависимость коэффициента готовности от времени с учетом показателей контроля

Значение коэффициента готовности, вычисленное по аналитической модели (3), равно 0,783.

Таким образом, с помощью разработанной имитационной модели были получены результаты, практически совпадающие с результатами вычислений по аналитической модели. Незначительные расхождения объясняются тем, что имитационная модель выдает конкретную реализацию работы комплекса, а аналитическая модель – обобщенную усредненную оценку. Повторив несколько раз эксперимент с имитационной моделью при одних и тех же исходных данных и обработав полученные результаты, можно получить полное совпадение результатов имитационной и аналитической моделей. При этом имитационная модель имеет ряд преимуществ по сравнению с аналитической моделью, а именно:

1. Аналитическое представление подходит лишь для простых объектов. Для сложных технических объектов при составлении графа состояний необходимо учитывать различные режимы эксплуатации, больше состояний объекта, следовательно, значительно вырастет уровень слож-

ности аналитического решения систем уравнений. К сожалению, аналитические решения можно найти не для всех задач.

2. Данная имитационная модель в отличие от аналитической представляет не конечную систему уравнений, а развернутую схему с детально описанной структурой и поведением объекта.

3. Разработанную имитационную модель можно постепенно усложнять, дорабатывать, модифицировать. В качестве входных параметров, например $T_{СР}$, $T_{Д}$, использовать не константы, а изменяющиеся величины. Например, объект может иметь различную $T_{СР}$ в зависимости от режима эксплуатации (для хранения – одно значение $T_{СР}$, для применения – другое). В справочных данных указывается, что средняя наработка на отказ в режиме хранения составляет примерно $\left(10^2...10^3\right)\cdot T_{СР}$.

На рис. 7 представлен график изменения $T_{СР}$ в зависимости от смены режимов эксплуатации (чередуются режимы хранения и применения по назначению) согласно технологическому графику.

На рис. 8 представлен вид имитационной модели надежности и диагностирования с учетом смены режимов эксплуатации.

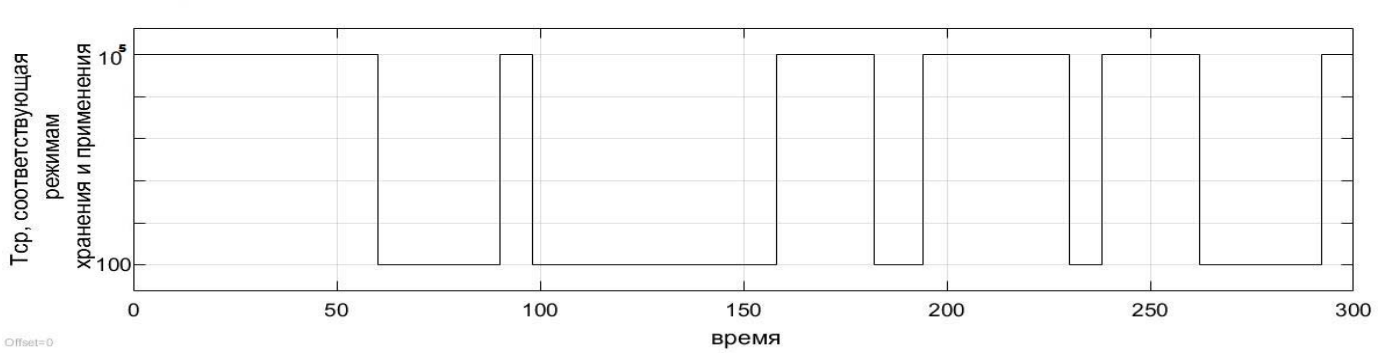


Рис. 7. График изменения $T_{СР}$ в зависимости от режима эксплуатации

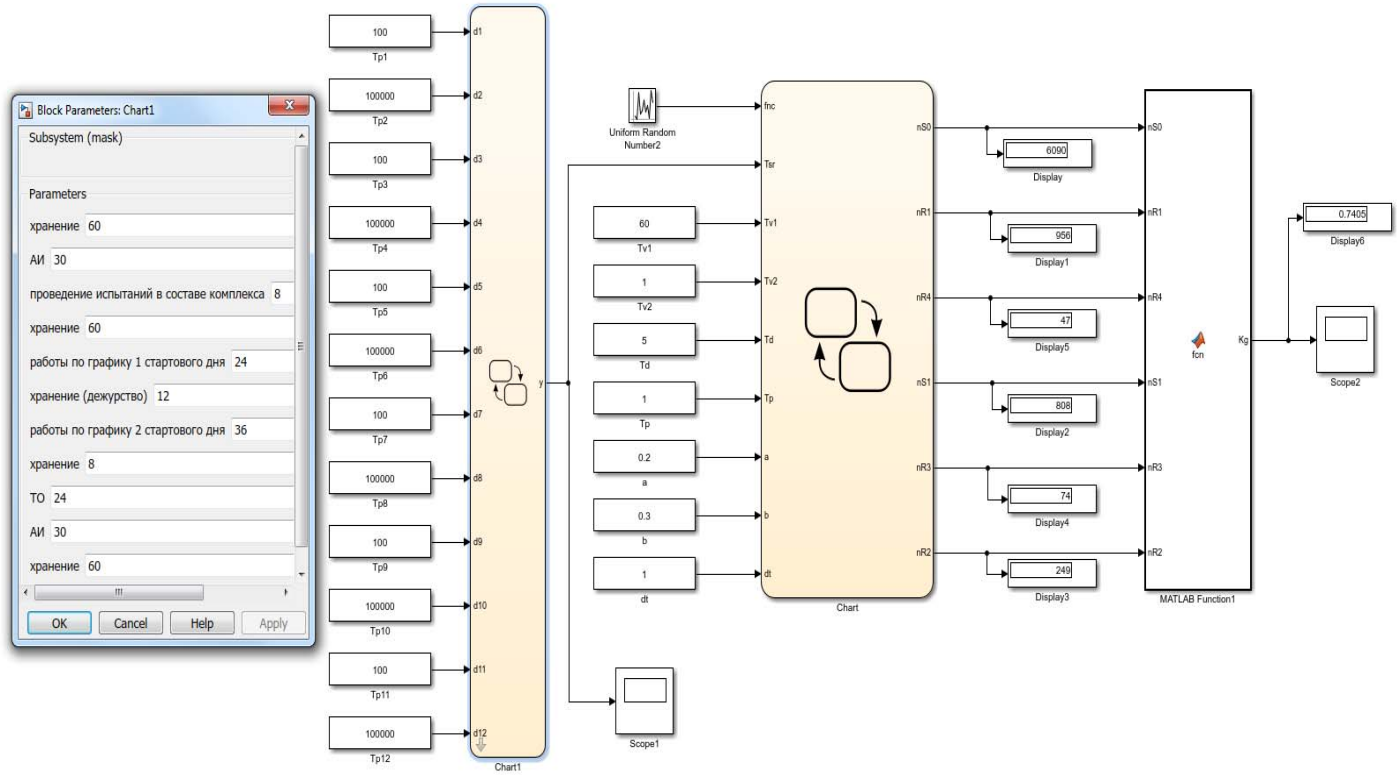


Рис. 8. Схема имитационной модели надежности и диагностирования с учетом режимов эксплуатации

На рис. 9 представлены результаты расчета коэффициента готовности с помощью имитационного моделирования.

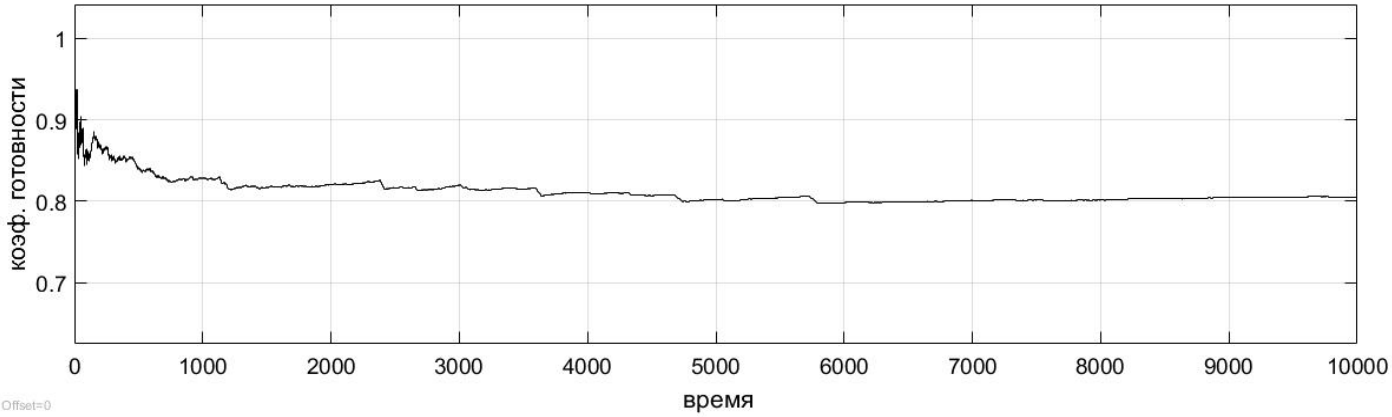


Рис. 9. Зависимость коэффициента готовности от времени, полученная с учетом различных режимов эксплуатации, отличающихся значениями $T_{СР}$

Заключение

Разработанная имитационная модель представляет дальнейшее развитие направлений, связанных с учетом показателей контроля и диагностирования сложных технических комплексов при оценивании показателей надежности. С помощью предложенной имитационной модели может быть обеспечен различный, в том числе высокий, уровень детализации моделируемых процессов, можно учитывать различные режимы эксплуатации сложных технических комплексов. Дальнейшее развитие имитационной модели связано с решением задач обеспечения требуемого значения коэффициента готовности путем управления входными параметрами, например регулированием периодичности контроля (диагностирования). Для этого может быть применен контроллер с нечеткой логикой или нестационарные модели надежности [15–16]. В зависимости от реального значения коэффициента готовности на выходе имитационной модели и предъявляемого требования к коэффициенту готовности можно получить значение изменения коэффициента готовности и использовать его для коррекции периодичности контроля (диагностирования) с помощью, например, правил нечеткого логического вывода.

Литература

1. Научно-методический подход к оцениванию готовности сложных технических комплексов с учетом метрологического обеспечения / Я.Н. Гусеница, И.В. Дорожко, И.А. Кочанов и др. // Труды МАИ. – 2018. – № 90. – С. 20.

2. Комплексная модель надежности и диагностирования сложных технических систем / И.В. Дорожко, И.А. Кочанов, Н.А. Осипов и др. // Труды Военно-космической академии им. А.Ф. Можайского. – 2016. – № 652. – С. 137–146.

3. ГОСТ В 20.911-89. Техническая диагностика. Термины и определения. – Введ. 1991-01-01. – М. : Издательство стандартов, 1990. – 12 с.

4. Технические средства диагностирования : справочник / [В.В. Клюев и др.] ; под общ. ред В.В. Клюева. – М. : Машиностроение, 1989. – 671с.

5. ГОСТ 27.002-15.Надежность в технике. Основные понятия. Термины и определения. – Введ. 2017-03-01. – М. : Стандартинформ, 2016. – 24 с.

6. Половко А.М., Гуров С.В. Основы теории надежности. – СПб. : БХВ-Петербург, 2006. – 704 с.

7. Расчет показателей надежности радиоэлектронных средств / С.М. Боровиков, И.Н. Цырельчук, Ф.Д. Троян. – Минск : БГУИР, 2010. – 68 с.

8. Острейковский В.А. Теория надежности. – М. : Высшая школа, 2003. – 463 с.

9. Дьяконов В.П. Simulink5/6/7 : самоучитель. – М. : ДМК-Пресс, 2008.− 784 с.

10. IEC 61165 (2006-05). Application of Markov techniques, BSI, 2008, 40 p.

11. IEC 61070 (1991-11). Compliance test procedures for steady-state availability, IEC, 52 p.

12. Mechatronic Systems Techniques and Applications. Taylor & Francis Group, 2000. XVI, Volume 5, 362 p.

13. Shubinsky Igor B., Zamyshlyaev Alexey M. Topological semimarkov method for calculation of stationary parameters of reliability and functional safety of technical systems – Reliability: Theory & Applications, San-Diego, USA, № 2, 2012.

14. Stateflow® and Stateflow® Coder™ User's Guide 2017 by The MathWorks, Inc. 3290 p.

15. Bubnov V.P., Khomonenko A.D., Tyrva A.V. Software Reliability Model with Coxian Distribution of Length of Intervals Between Errors Detection and Fixing Moments. In proceedings of 35th Annual IEEE Computer Software and Applications Conference Workshops (COMPSACW 2011), Munich, 18–22 July 2011. – P. 310–314.

16. Дорожко И.В. Оценка надежности структурно-сложных технических комплексов с помощью моделей байесовских сетей доверия в среде GeNIe / И.В. Дорожко, А.Г. Тарасов, А.М. Барановский // Интеллектуальные технологии на транспорте (Intellectual Technologies on Transport). – 2015. – № 3 – С. 36–45.

A Study of the Coefficient of Readiness of Complex Technical Systems Using the Simulation Models Developed in the Stateflow Environment of MatLab Package

I.V. Dorozhko, A.L. Kopeyka
Military Space academy named after A.F. Mozhaisky
Saint-Petersburg, Russia
Doroghko-Igor@yandex.ru

Abstract. **The work is devoted to research of dependence of reliability indicators and control (diagnosing) of complex technical complexes. The article presents the simulation model of estimation of the complex indicator of reliability (readiness coefficient) taking into account the indicators of control and diagnostics of complex technical complexes, developed with the help of modeling environment Stateflow product Matlab. The adequacy of the developed simulation model is confirmed by analytical calculations. The developed simulation model allows to calculate the readiness coefficient taking into account the modes, i.e. for non-stationary processes, in which parameters can change over time. Also, unlike analytical, the simulation model can be expanded to take into account all possible types of technical states, avoiding cumbersome formulas.**

Keywords: **reliability, control, diagnostics, readiness coefficient, reliability, errors, Markov process, simulation model.**

REFERENCES

1. Gusenitsa Ya.N., Dorozhko I.V., Kochanov I.A., Petukhov A.B. Scientific-methodical approach to an estimation of readiness of complex technical systems, taking into account metrological maintenance [*Nauchno-metodicheskij podkhod k otsenivaniyu gotovnosti slozhnykh tekhnicheskikh kompleksov s uchetom metrologi-cheskogo obespecheniya*], Trudy MAI *[Trudy MAI]*, 2018, no.90, 20 P.

2. Dorozhko I.V., Osipov N.A., Kochanov I.A., Butyrin A.V. Integrated model of reliability and diagnostics of complex technical systems [*Kompleksnaya model nadezhnosti i diagnostirovaniya slozhnykh tekhnicheskikh sistem*], *Trudy Voenno-kosmicheskoy akademii imeni A.F. Mozhayskogo [Proceedings of the Military Space academy named after A.F.Mozhaisky]*, 2016, no.652, pp. 137–146.

3. *Tekhnicheskaya diagnostika. terminy i opredeleniya: GOST V 20.911-89* [Technical diagnostics. Terms and definitions: GOST V 20.911-89], Moskow, Publishing standards, 1990, 12 p.

4. Klyuev V.V., Parkhomenko P.P., Abramchuk V.E. i dr. Technical Diagnostic Tools: Reference [*Tekhnicheskie sredstva diagnostirovaniya: spravochnik*] *Mashinostroenie [Engineering]*, 1989, 671 p.

5. *Nadezhnost v tekhnike. Terminy i opredeleniya: GOST R 27.002-2015* [Reliability in technics. Terms and definitions: GOST 27.002-2015], Moskow, Publishing standards, 2016, 24 p.

6. Polovko A.M., Gurov S.V. *Osnovy teorii nadezhnosti* [Fundamentals of theory of reliability], SPb, BVKh-Peterburg, 2006, 704 p.

7. Borovikov S.M., Tsyrelchuk I.N., Troyan F.D. Calculation of indicators of reliability of radio-electronic means [Raschet pokazatelej nadezhnosti radioelektronnykh sredstv], Minsk, 2010, 68 p.

8. Ostrejkovskij V.A. Reliability theory [*Teoriya nadezhnosti*], Moskow,2003, 463 p.

9. Dyakonov V.P.Simulink5/6/7: Tutorial – Moskow, 2008, 784 p.

10. IEC 61165 (2006-05). Application of Markov techniques, BSI, 2008, 40 p.

11. IEC 61070 (1991-11). Compliance test procedures for steady-state availability, IEC, 52 p.

12. Mechatronic Systems Techniques and Applications. Taylor & Francis Group, 2000. XVI, Volume 5, 362 p.

13. Shubinsky Igor B., Zamyshlyaev Alexey M. Topological semimarkov method for calculation of stationary parameters of reliability and functional safety of technical systems – Reliability: Theory & Applications, San-Diego, USA, №2, 2012.

14. Stateflow® and Stateflow® Coder™ User's Guide 2017 by The MathWorks, Inc. 3290 p.

15. Bubnov V.P., Khomonenko A.D., Tyrva A.V. Software Reliability Model with Coxian Distribution of Length of Intervals Between Errors Detection and Fixing Moments. In proceedings of 35th Annual IEEE Computer Software and Applications Conference Workshops (COMPSACW 2011), Munich, 18-22 July 2011. – P. 310–314.

16. Dorozhko I.V.,Tarasov A.G., Baranovsky A.M. Estimation to reliability of structural complex technical systems by using Bayesian networks belief models in the environment of GeNIe [*Otsenka nadezhnosti strukturno-slozhnykh tekhnicheskikh kompleksov s pomoschyu modelej bajesovskikh setej doveriya v srede* GeNIe], *Trudy Voenno-kosmicheskoy akademii imeni A.F. Mozhayskogo [Intellectual Technologies on Transport]*, 2015, no.3, pp. 36–45.

Модель оценивания вычислительной сложности интеллектуального распознавания объектов на изображениях на борту беспилотных летательных аппаратов

Е.Л. Яковлев
Военно-космическая академия имени А.Ф.Можайского
Санкт-Петербург, Россия
evgen-1932@yandex.ru

Аннотация. **Предложена модель системы автоматического распознавания объектов, основанная на использовании базы знаний. База знаний состоит из набора заранее подготовленных модулей. Каждый модуль характеризуется определённым классом объектов, условиями применения, вычислительной сложностью. Критерием выбора модуля является пространственное пиксельное разрешение. На основе предложенной модели проведен сравнительный расчет вычислительной сложности алгоритмов распознавания изображений.**

Ключевые слова: **система автоматического распознавания объектов на изображениях, вычислительная сложность, беспилотный летательный аппарат.**

Введение

Отличительной особенностью развития авиационной техники конца XX – начала XXI века является быстрое развитие и широкое использование различных беспилотных летательных аппаратов (БЛА). Причинами такого успеха является возможность применения БЛА в условиях, когда использование пилотируемых летательных аппаратов невозможно либо экономически нецелесообразно. БЛА активно применяются вооруженными силами многих государств для решения таких задач, как обнаружение, идентификация и поражение наземных стационарных и подвижных объектов, морских и воздушных целей; подавление средств противовоздушной обороны; радиоэлектронная борьба для вывода из строя средств связи и управления противника; вспомогательные задачи по обеспечению войск: ретрансляция радиосигналов, доставка грузов, метеорологическое обеспечение и др.

Сфера применения БЛА постоянно расширяется в различных сферах: мониторинг подстилающей поверхности, атмосферы, объектов инфраструктуры и других объектов; ретрансляция радиосигналов; доставка и сброс грузов службы ликвидации чрезвычайных ситуаций; сельское хозяйство, геологоразведка и др.

Перспективным представляется использование БЛА с целью обследования объектов железнодорожной инфраструктуры для обеспечения безопасности. Для широкого использования подобных комплексов необходимо, чтобы БЛА обладали высокой степенью автономности и оперативности – могли в автоматическом режиме распознавать опасные объекты с помощью бортовой информационной системы (БИС) и передавать об этом информацию на ближайший поезд, станцию, так как постоянное поддержание информационного канала с пунктом управления не всегда возможно. Этому могут препятствовать как естественные преграды – горная местность, так и целенаправленное радиоэлектронное воздействие на информационные каналы управления, телеметрии, передачи данных и приёма сигналов глобальных навигационных систем БЛА. Кроме этого, анализ на земле данных, получаемых с оптико-электронных датчиков, требует создания инфраструктуры по обработке этих данных – операторов или автоматических систем. Реализация автоматического распознавания объектов на изображениях от оптико-электронных датчиков в БИС позволит создавать БЛА, способные решать задачу по мониторингу объектов ж.-д. транспорта в автоматическом режиме.

При построении интеллектуальных БИС БЛА, способных решать задачи обнаружения и распознавания объектов по данным систем технического зрения, необходимо учитывать преимущества и недостатки применения различных датчиков, создавать системы, обрабатывающие потоки информации от нескольких датчиков в режиме реального времени. В [1] приводится обзор датчиков различной физической природы: оптические, ИК, акустические, радиолокационные, лазерные и др.

В настоящее время существует ряд систем автоматического распознавания объектов на изображениях, получаемых с датчиков различной физической природы, в основном они применяются в гражданских сферах деятельности общества:

– системы распознавания регистрационных номеров автомобилей в потоке;

– системы опознавания людей по изображению лица;

– системы распознавания по отпечаткам пальцев и сетчатке глаз и др.

За последние годы в данном направлении появилось несколько подходов по автоматическому распознаванию объектов на изображениях: в [2] предлагается идея на основе вейвлет-методов, в [3] рассматривается алгоритм Виолы–Джонса с модификациями, в [4] использовались совместно технологии BOW (bag of words), SVM и SIFT. Однако анализ вычислительной сложности этих моделей

приводит к необходимости разработки новой модели автоматического распознавания объектов в БИС БЛА.

Для решения задачи автоматического распознавания заданных объектов и их параметров предлагаем модель процесса распознавания объектов с учетом аппаратных и временных ограничений, которая позволяет оценить аппаратные и временные ресурсы, необходимые для решения задачи автономного распознавания объектов, определения их параметров в процессе функционирования в режиме реального времени.

Постановка задачи

Решению проблемы распознавания изображений посвящено большое число работ, однако до сих пор она не решена полностью. Это связано с большой информационной емкостью и априорной неопределенностью, присущей изображениям, а также с большой изменчивостью изображений за счет изменение ракурса или освещения, что приводит к изменению значений одновременно во всех элементах изображения. В общем случае задачу распознавания объектов на изображениях можно представить как классификацию по нескольким заранее определенным категориям или классам.

Одним из центральных компонентов методов распознавания принято считать используемое представление изображений [5]. Одним из наиболее перспективных является представление, основанное на знаниях, это не только выходное представление системы распознавания изображений, но и используемое в самом процессе распознавания [6].

Для описания модели функционирования системы автоматического распознавания объектов предлагается использование базы знаний, состоящей из заранее подготовленных модулей для обработки входного потока изображений. Каждый такой модуль характеризуется классом распознаваемых объектов, вычислительной сложностью, объемом занимаемой памяти и критериями применимости. В качестве основного критерия рассматривается диапазон пространственного пиксельного разрешения на местности.

Необходимо разработать модель, способную определить зависимость ресурсоемкости автоматического распознавания от используемых методов и алгоритмов, характеристик оптико-электронных датчиков и требований по качеству распознания.

Модель автономного распознавания объектов на изображениях

Математическая модель распознавания, представленная ниже, связывает значение потребляемых ресурсов (количество операций и памяти) с используемой конфигурацией модулей распознавания, потоком входных изображений при ограничениях по точности распознавания:

$$\begin{cases} R = R(\mathrm{IM}, \mathrm{C}, \mathrm{T}, \mathrm{F}); \\ \mathrm{F} : \mathrm{IM} \to \mathrm{Y}; P \ge P^{д}, P_1 \le P_1^{Д}, P_2 \le P_2^{Д}; \\ R =< R_Q, R_M >; R_Q \le R_Q^{Д}, R_M \le R_м^{Д}, \end{cases}$$

где T – множество моментов времени *t*;

IM – поток изображений с оптико-электронного модуля;

F – множество отдельных модулей распознавания, образующих базу знаний;

C – используемая конфигурация модулей распознавания;

R – ресурсоемкость;

P – вероятность успешного распознавания;

P_1, P_2 – вероятность ошибок первого и второго рода;

R_Q – ресурсоемкость по числу операций процессора;

R_M – ресурсоемкость по объему памяти;

$R_Q^Д$ и $K_Q^Д$ – допустимые производительность процессора и емкость памяти бортовой вычислительной системы.

В общем случае процесс автономного распознавания можно описать следующим образом (рис. 1).

1. Бортовой оптико-электронный модуль (ОЭМ) формирует изображение, которое затем проходит специальную предварительную подготовку, представляющую собой применение операций усреднения и выравнивания гистограмм, различного типа фильтров для исключения помех, возникающих в результате аппаратной дискретизации и квантования, а также подавления внешних шумов. Для упрощения будем считать, что предварительная обработка осуществляется на этапе формирования изображения в самом ОЭМ. Кроме этого, считаем, что ОЭМ при съемке ориентирован строго перпендикулярно к поверхности земли.

2. Полученное изображение передается в БИС. По характеристикам матрицы, фокусному расстоянию и высоте съемки вычисляется пространственное пиксельное разрешение изображения на местности:

$$R_t = \frac{dH_t}{f}, \qquad (1)$$

где d – размер пикселя, f – фокусное расстояние, H_t – высота съемки.

3. Согласно рассчитанному значению R_t, подсистема принятия решений в базе знаний в соответствии с программой полета выбирает модули распознавания, реализующие в скользящем окне на изображении IM_t отображение $\mathrm{F_г} : \mathrm{X_г} \to \mathrm{Y_г}$. В процессе распознавания для достижения максимальной вероятности распознавания объектов (близко расположенных друг к другу – группы объектов) можно использовать различную степень перекрытия $K_{ск}$ скользящим окном обрабатываемого изображения.

4. При распознавании объектов из заранее определенных классов $\mathrm{Y}_r = \{Y_1, ...Y_r\}$ формируется запись в базу данных в формате $\boldsymbol{Y_k}$ = <*Y, U, V, t, P,* P_1, P_2>.

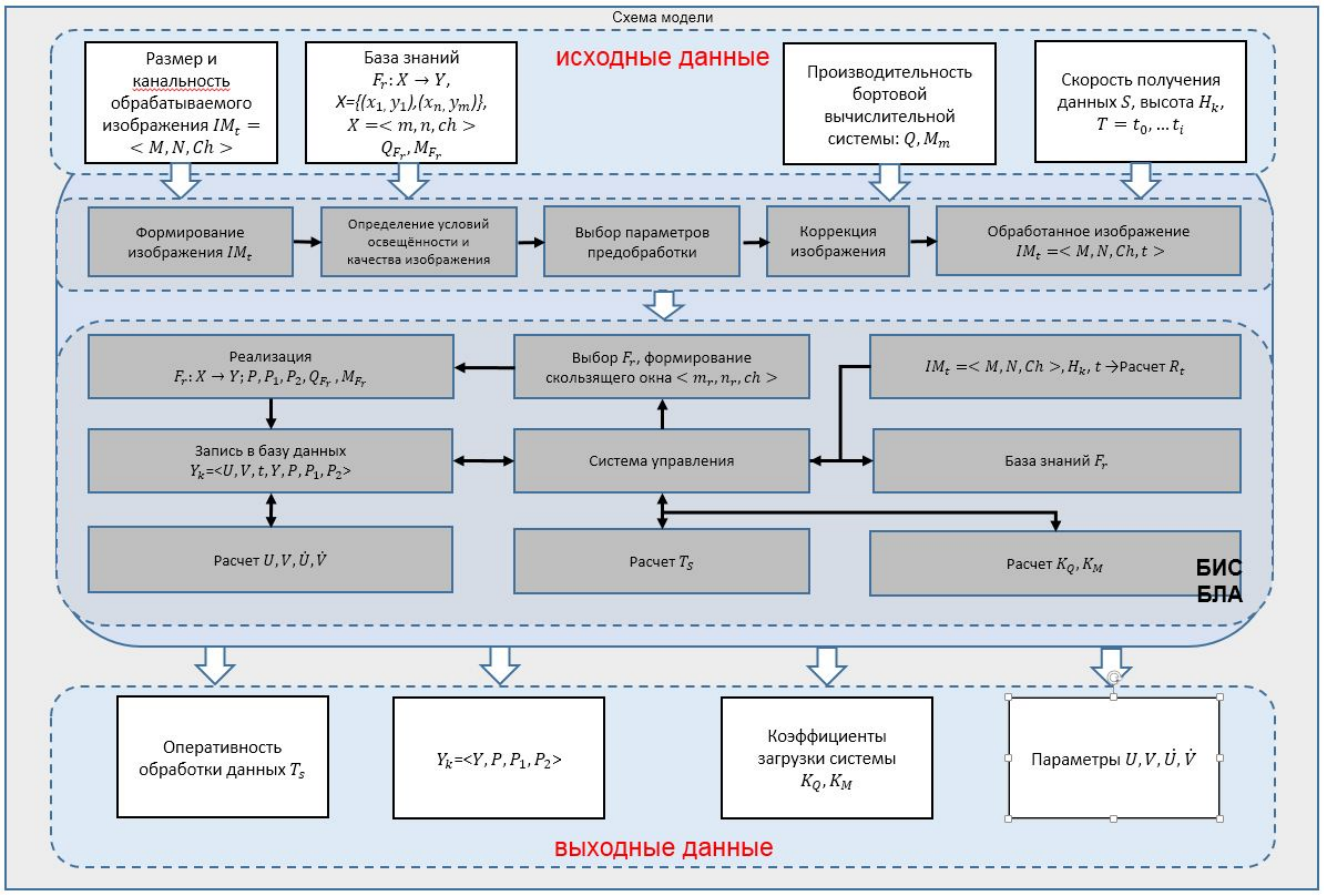


Рис. 1. Процесс автономного распознавания объектов на изображениях в БИС БЛА

Здесь Y – класс объекта; U, V – его координаты; t – момент времени (время съемки); P, P_1, P_2 – вероятность распознавания, ошибки первого и второго рода.

5. Процесс является непрерывным, при обработке последующих изображений в базу данных заносятся новые записи, для подвижных объектов вычисляется средняя скорость и направление движения $\dot{V}, \dot{U}$.

Входными данными для модели распознавания являются:

1. $IM_t =< M, N, Ch >$ – характеристика изображения, формируемого оптико-электронным датчиком,
   – M – высота цифрового изображения;
   – N – ширина цифрового изображения;
   – Ch – количество каналов в изображении.
2. Q и Q_m – производительность процессора и емкость памяти бортовой вычислительной системы.
3. $\mathrm{F_r} : \mathrm{X_r} \to \mathrm{Y}_r$, где $\mathrm{X}_r =< m, n, ch >$ входной вектор для каждого F_r; $r \in [1:n]$ – количество отдельных модулей классификации,
   – m – высота цифрового изображения;
   – n – ширина цифрового изображения;
   – ch – количество каналов в изображении.
4. $\mathrm{Y}_r = \{Y_1, \dots Y_r\}$ – классы распознаваемых объектов для каждого F_r.
5. Q_F – количество операций при реализации одного графа вычислений F_r.
6. M_{F_r} – емкость памяти для F_r.
7. T – множество моментов времени t.
8. H_k – высота съемки.

В результате функционирования модели должны быть получены следующие данные:

1. T_s – оперативность обработки данных.
2. K_Q – коэффициент загрузки процессора (процессоров) БИС.
3. K_M – коэффициент использования памяти БИС.
4. $\mathrm{Y}_k =< Y, U, V, t, P, P_1, P_2 >$ – запись в базу данных информации об объекте.

Расчет показателей БИС

Для оценки показателей ресурсоемкости системы предлагается следующий алгоритм:

1. Вычисляется количество операций, необходимых для обработки одного изображения одним модулем F_r:

$$Q_{IM}^{r} = \frac{MN}{m_r n_r} Q_{\mathbf{F}_r}. \quad (2)$$

2. Путем суммирования рассчитывается общее число операций при обработке одного изображения:

$$Q_{IM} = \sum_{r=1}^{n} Q_{\mathbf{F}_r}, \quad (3)$$

где n – число модулей, участвующих в обработке изображения.

3. Тогда общее время обработки одного изображения:

$$T_s = (\sum_{r=1}^{n} \frac{MN}{m_r n_r} Q_{\mathbf{F}_r}) / Q. \quad (4)$$

4. Для выполнения условия обработки данных в режиме реального времени рассчитаем коэффициенты загрузки системы:

$$K_q = (S \sum_{r=1}^{n} \frac{MN}{m_r n_r} Q_{\mathbf{F}_r}) / Q, \quad (5)$$

где S – скорость получения данных (изображений в секунду). Для режима реального времени необходимо соблюдение условия $1 \geq K_q$.

5. Для выполнения условия по общему объему используемой памяти

$$K_m = \frac{\sum_{r=1}^{n} M_{\mathbf{F}_r}}{M_m}, \quad (6)$$

где $K_m \leq 1$ – условие реализуемости бортовой вычислительной системы (БВС).

Результаты экспериментов

В ходе эксперимента рассмотрены следующие три распространенных метода распознавания изображений:

– метод, основанный на применении инвариантов моментов Hu [7–9];

– метод Виолы-Джонса [10–12];

– метод на основе сверточной нейронной сети [13–15].

Для оценки ресурсоемкости данных методов применялся набор данных Planestnet [16], состоящий из цветных изображений (32 тыс.), полученных нарезкой спутниковых снимков и разбитый на два класса: изображения, содержащие самолеты, и изображения без самолетов.

Расчет оценки ресурсоемкости данных методов проводился следующим образом: сначала рассчитывалась трудоемкость отдельного модуля с учетом памяти и количества операций, необходимых для реализации одного графа вычислений в скользящем окне, причем для расчета количества операций на один пиксель для инвариантов моментов применялась методика [17]. Затем происходит анализ спутникового изображения с помощью данных модулей в скользящем окне с различными значениями коэффициента перекрытия 1; 1,5; 2. Кроме трудоемкости, алгоритмы оценивались по следующим параметрам:

P – точность распознавания;

P_1 – число объектов, обнаруженных модулем, но отсутствующих на изображении;

P_2 – число объектов, пропущенных модулем.

Сводные данные моделирования приведены в таблице 1.

ТАБЛИЦА 1. Оценка алгоритмов распознавания

Методы	***Q*, млн. опер.**	**M, мб**	***K*ск = 1**			***K*ск = 1,5**			***K*ск = 2**		
			P	***P*1**	***P*2**	***P***	***P*1**	***P*2**	***P***	***P*1**	***P*2**
Инварианты моментов	0,35	0,44	0,618	0,473	0,381	0,690	0,427	0,309	0,709	0,363	0,290
Виола-Джонс	0,2	0,63	0,718	0,281	0,281	0,736	0,236	0,263	0,763	0,218	0,236
Сверточные нейронные сети	0,67	0,87	0,909	0,081	0,090	0,945	0,081	0,054	0,965	0,063	0,045

Результаты проведенных экспериментов показывают, что лучшую точность распознавания продемонстрировали сверточные нейронные сети. Однако для вычислений они являются самыми трудоемкими. Алгоритмы на основе инвариантов моментов и Виолы–Джонса работают быстрее, но качество распознавания существенно хуже, особенно в случае инвариантов моментов. Увеличение коэффициента перекрытия скользящего окна незначительно увеличивает точность распознавания.

Дальнейшим перспективным направлением исследований планируется исследование архитектуры сверточных нейронных сетей с целью снижения трудоемкости вычислений и используемого объема памяти.

Заключение

Предложенная модель автоматического распознавания объектов на изображениях в БИС БЛА описывает основные зависимости вычислительной сложности и условия реализации алгоритмов распознавания в режиме реального времени. Она может применяться для обоснования состава и определения основных параметров перспективных БИС БЛА. Эта модель позволяет проводить анализ существующих и перспективных алгоритмов распознавания объектов на изображениях с целью обоснования их применения для построения интеллектуальных БИС.

Применение предложенной модели в перспективных БИС позволит создавать новые БЛА, способные решать различные задачи в автономном режиме без использования информационных каналов.

ЛИТЕРАТУРА

1. Желтов С.Ю. Перспективы интеллектуализации систем управления ЛА за счёт применения технологий машинного зрения / С.Ю. Желтов, Ю.В. Визильтер // Труды МФТИ. – 2009. – Т. 1, № 4. – С. 164–181.

2. Медведев М.В. Система управления беспилотным летательным аппаратом на основе вейвлет-методов обнаружения и распознавания объектов на изображениях / М.В. Медведев, А.П. Кирпичников // Вестник Казанского технологического университета. – 2014. – Т. 17, № 19. – С. 359–363.

3. Амосов О.С. Модифицированный алгоритм локализации номерных знаков транспортных средств на основе метода Виолы–Джонса / О.С. Амосов, Ю.С. Иванов // Информатика и системы управления. – 2014. – № 1 (39). – С. 127–140.

4. Перспективные методы обработки потоков видовых данных для повышения результативности применения БЛА / Н.Ю. Кожанов, А.П. Танченко, Ю.В. Москаленко // сборник докладов научно-практической конференции «Перспективы развития и применения комплексов с беспилотными летательными аппаратами», г. Коломна. – 2016. – С. 165–171.

5. Васильев В. Н. Современная видеоинформатика: проблемы и перспективы / В.Н. Васильев, И.П. Гуров, А.С. Потапов // Оптический журнал. – 2012, № 11. – С. 5–15.

6. Головко В.А. Нейроинтеллект: теория и применение. Кн. 2. – Брест : БПИ, 1999. – 228 с.

7. Hu M. Visual Pattern Recognition by Moment Invariants / M. Hu // IRE Trans. Inf. Theory. – 1962. – Vol. 8. – P. 179–187.

8. Старобинец Д.Ю. Автоматический выбор параметров сжатия изображений с потерями на основе инвариантных моментов при дистанционном зондировании Земли / Д.Ю. Старобинец, А.Д. Хомоненко, Н.А. Гаврилова // Современные проблемы дистанционного зондирования Земли из космоса. – 2017. – Т. 14. № 5. – С. 26–36.

9. Жигалко Е.Ф. Особенность асимптотических свойств интегральных инвариантов / Е.Ф. Жигалко // Интеллектуальные технологии на транспорте. – 2015. – № 4. – С. 55–58.

10. Viola P., Jones M. J. Robust Real-time face detection / P. Viola, M. Jones // International Journal of Computer Vision, – 2004. – Vol. 57. no. 2. – P. 137–154.

11. Viola P., Jones M., Snow D., Detecting Pedestrians Using Patterns of Motion and Appearance / P. Viola, M. Jones, D. Snow // International Journal of Computer Vision, Vol. 63, no. 2, 2005, p. 153–161.

12. Brousseau B., Rose J. An energy-efficient, fast FPGA hardware architecture for OpenCV-compatible object detection / FPT, 2012.

13. LeCun Y. et al. Gradient-Based Learning Applied to Document Recognition / Y. LeCun et al. // Proc. IEEE.1998. Vol. 86. no. 11. – P. 2278–2324.

14. lmageNet Classification with Deep Convolutional Neural Networks / A. Krizhevsky, I. Sutskever, G. Hinton // Avances in Neural Information Processing Systems. 25 Curran Associates, lnc., 2012. – P. 1097–1105.

15. Szegedy C. et al. Rethinking the lnception Architecture for Computer Vision / C. Szegedy et al. // arXiv, – 2015. http://arxiv.org/abs/ 1512 .00567.

16. Https://www.kaggle.com/rhammell/planesnet (дата обращения 17.05.2018).

17. Медведик А.Д. Оценка вычислительной сложности моментных инвариантов, используемых в задачах распознавания / А.Д. Медведик, В.А. Верченко, П.Е. Бабак // Радиоэлектронные и компьютерные системы. – 2015. – № 4 (74). – С 124–130.

Model of Estimation of Computational Complexity of Intelligent Recognition of Objects on Images on Board the UAV

E.L. Yakovlev
A.F. Mozhaisky Military Aerospace Academy
St. Petersburg, Russia
evgen-1932@yandex.ru

Abstract. **The model of automatic object recognition system, based on the use of the knowledge base is offered. The knowledge base consists of a set of pre-prepared modules. Each module is characterized by a certain class of objects, conditions of application, computational complexity. The criterion for selecting a module is the spatial pixel resolution. On the basis of the offered model the comparative calculation of computational complexity of algorithms of image recognition is made.**

Keywords: **system of automatic recognition of objects on images, computational complexity, unmanned aerial vehicle.**

REFERENCES

1. Zheltov S.Yu. Prospects of intelligent control systems of Aircraft through the use of machine vision technologies [Perspektivy intellektualizatsii sistem upravleniya LA za schet primeneniya tekhnologiy mashinnogo zreniya] MIPT Works [Trudy MFTI], 2009. vol. 1, no. 4, pp. 164–181.

2. Medvedev M.V. Control system of the unmanned aerial vehicle on the basis of wavelet methods of detection and recognition of objects on images [Sistema upravleniya bespilotnym letatel'nym apparatom na osnove veyvlet-metodov obnaruzheniya i raspoznavaniya ob"ektov na izobrazheniyakh] Herald of the Kazan University of Technology [Vestnik Kazanskogo tekhnologicheskogo universiteta], 2014, vol. 17, no.19, pp. 359–363.

3. Amosov O.S., Ivanov Yu.S. A modified algorithm for the localization of vehicle license plates based on the Viola-Jones method [Modifitsirovannyy algoritm lokalizatsii nomernykh znakov transportnykh sredstv na osnove metoda Violy-Dzhonsa.] Informatics and Management Systems [Informatika i sistemy upravleniya], 2014, no. 1(39), pp. 127–140.

4. Kozhanov N.Yu, Tanchenko A.P., Moskalenko Yu.V, Martimov R.Yu, Petrochenko A.V. Perspective methods of processing data streams to increase the efficiency of the use of UAV. [Perspektivnye metody obrabotki potokov vidovykh dannykh dlya povysheniya rezul'tativnosti primeneniya BLA]. The collection of reports of scientific and Practical Conference "Perspectives of Development and application of complexes with unmanned aerial vehicles" [Sbornik dokladov nauchno-prakticheskoy konferentsii «Perspektivy razvitiya i primeneniya kompleksov s bespilotnymi letatel'nymi apparatami»], Kolomna, 2016, pp. 165–171.

5. Vasil'yev V.N., Gurov I.P., Potapov A.S. Modern computer Science: Problems and Prospects [Sovremennaya videoinformatika: problemy i perspektivy]// Optical Magazine [opticheskiy zhurnal], 2012, no. 11, pp. 5–15.

6. Golovko V.A. Neyrointellekt: Nejrointellekt: Theory and applications. Book 2. Organization, resiliency and application of neural networks [Teoriya i primeneniya. Kniga 2. Samoorganizatsiya, otkazoustoychivost' i primenenie neyronnykh setey]. Belarus, Brest: BPI, 1999, 228 p.

7. Hu M, Visual Pattern Recognition by Moment Invariants, IRE Trans. Inf. Theory, 1962, vol. 8, pp. 179–187.

8. Starobinets D.Yu., Khomonenko A.D., Gavrilova N.A. Automatic selection of lost image compression options based on invariant moments in remote sensing of the Earth [Avtomaticheskiy vybor parametrov szhatiya izobrazheniy s poteryami na osnove invariantnykh momentov pri distantsionnom zondirovanii Zemli] Modern problems of remote sensing of the Earth from space [Sovremennye problemy distantsionnogo zondirovaniya Zemli iz kosmosa], 2017. vol. 14. no. 5. pp. 26–36.

9. Zhigalko E.Th., Feature of asymptotic properties of integral invariants [Osobennost' asimptoticheskikh svoystv integral'nykh invariantov] / Intellectual Technologies on Transport, 2015. no. 4, pp. 55–58.

10. Viola P., Jones M. J. Robust real_time face detection. International Journal of Computer Vision, 2004, vol. 57, no. 2, pp. 137–154.

11. P. Viola, M. Jones, and D. Snow, Detecting Pedestrians Using Patterns of Motion and Appearance, International Journal of Computer Vision, vol. 63, no. 2, 2005, pp. 153–161.

12. Brousseau B., Rose J. An energy-efficient, fast FPGA hardware architecture for OpenCV-compatible object detection. FPT, 2012.

13. LeCun Y. et al. Gradient-Based Learning Applied to Document. Proc. IEEE.1998, vol. 86. no. 11, pp. 2278–2324.

14. Krizhevsky A ., Sutskever I., Hinton G. lmageNet Classification with Deep Convolutional Neural Networks, Avances in Neural Information Processing Systems 25 / Curran Associates, lnc., 2012, pp. 1097–1105.

15. Szegedy C. et al. Rethinking the lnception Architecture for Computer Vision, arXiv, 2015, http://arxiv.org/abs/ 1512 .00567.

16. Https://www.kaggle.com/rhammell/planesnet.

17. Medvedik A. D., Verchenko V. A., Babak P. E. Evaluation of computational complexity of momentary invariants used in recognition tasks [Otsenka vychislitel'noy slozhnosti momentnykh invariantov, ispol'zuemykh v zadachakh raspoznavaniya]// Radio-Electronic and computer systems [Radioelektronnye i komp'yuternye sistemy], 2015, no. 4(74), pp. 124–130.

Выявление инсайдерских угроз в транспортных организациях

М.А. Поляничко
ФГБОУ ВО ПГУПС
Санкт-Петербург, Россия
polyanichko@pgups.ru

Аннотация. **Рассматривается проблема выявления инсайдерских угроз в транспортных организациях. Предлагается подход к выявлению инсайдерских угроз, который базируется на анализе различных показателей риска предрасположенности к инсайдерскому поведению. Характеризуется проблема выявления инсайдеров. Рассматриваются различные показатели риска: психологические, личностные, скрининговые, поведенческие, коммуникативные, контекстные и технические.**

Показатели риска условно разделяются на три группы: динамические, периодически актуализируемые и стационарные. Для определения значений периодически актуализируемых показателей предлагается использовать метод анализа иерархий. Динамические показатели (технические) могут быть автоматизированно собраны на основе данных вычислительной сети организации и ее информационных систем. Периодически актуализируемые показатели (личностные, поведенческие, контекстные) определяются методом анализа иерархий, скрининговые показатели определяются специализированными средствами. Стационарные показатели риска (психологические и коммуникативные) определяются анкетированием.

Ключевые слова: **внутренние угрозы информационной безопасности, инсайдер, выявление инсайдеров.**

Введение

Под инсайдерами в данной статье подразумеваются работники (действующие и бывшие), подрядчики и деловые партнеры, которые имеют доступ к данным организации, методам обеспечения безопасности и информационным системам, используемым в организации. Угрозы, исходящие от инсайдеров, включают мошенничество, кражу конфиденциальной информации или интеллектуальной собственности, саботаж работы информационных систем и другие угрозы.

Растущая зависимость транспортных организаций от своей информационной инфраструктуры, технологий и информационных активов свидетельствует о том, что проблема инсайдеров будет приобретать всё большую актуальность [1–4].

Выявление инсайдеров

На данный момент не существует полного, эффективного и системного метода, разработанного для решения проблем выявления внутренних угроз информационной безопасности, исходящих от инсайдеров. Решение проблемы противодействия инсайдерам требует создания комплекса мер, направленных на выявление признаков склонности к инсайдерской деятельности [5, 6]. Противодействие инсайдерским угрозам требует применения не только программных и технических средств обеспечения информационной безопасности, но и внедрения внутренних процедур и регламентов [7].

В данной статье предлагается комплекс показателей, значения которых позволяют выявить потенциальных инсайдеров. Далее рассматриваются психологические, личностные, скрининговые, поведенческие, коммуникативные, контекстные и технические показатели риска.

Психологические показатели риска

Индивидуальные черты характера отдельных людей довольно стабильны и не изменяются в течение жизни. Обнаружение статистически значимой связи между различными профилями личности может служить основой для разработки и внедрения протоколов безопасности, учитывающих специфические психологические характеристики работников [8].

Существует несколько подходов к анализу личности человека. Предлагаемая для использования характеристика личности включает в себя пять общих и относительно независимых черт (диспозиций) характера: экстраверсию, доброжелательность (способность прийти к согласию), сознательность (добросовестность), невротизм (противоположность – эмоциональная стабильность) и открытость опыту (интеллект).

ТАБЛИЦА 1. Психологические показатели риска

Показатель	**Описание показателя**
1	**2**
Экстраверсия Возможные значения Положительные: коммуникабельность, энергичность Негативные: склонность к уединению, замкнутость	Выражается в энергичности, положительных эмоциях, уверенности в себе, разговорчивости, коммуникабельности и склонности искать вдохновение в обществе других людей. Высокая экстраверсия часто воспринимается как попытки к поиску внимания и склонности к доминированию. Низкая экстраверсия характеризует замкнутую, отражающую личность, которую можно воспринимать как отчужденную или поглощенную собой
Способность прийти к согласию Возможные значения Положительные: дружелюбие, сострадание Негативные: вызывающее поведение, отрешенность	Выражается в умении сострадать и склонности к сотрудничеству. Это также мера доверчивости и способности помогать людям, общей уравновешенности. Склонность соглашаться часто рассматривается как наивность или покорность. Неспособность прийти к согласию характерна для неудовлетворенных личностей, склонных к соперничеству. Такие люди, как правило, не внушают доверия

Окончание табл. 1

1	2
Сознательность Возможные значения Положительные: эффективность, организованность Негативные: беспечность, неосторожность	Выражается в склонности к самоорганизованности, проявлении дисциплины, прилежности, стремлении к достижениям, предпочтении запланированных, а не спонтанных поступков. Высокая сознательность часто воспринимается как упрямство и одержимость. Низкая добросовестность связана с гибкостью и спонтанностью, но может также проявиться в неряшливости и ненадежности
Невротизм Возможные значения Положительные: чувствительность, нервозность Негативные: спокойствие, уверенность в себе	Выражается в склонности легко испытывать неприятные эмоции, такие как гнев, беспокойство и чувство уязвимости. Невротизм также отражает степень эмоциональной устойчивости, умение контролировать импульсы и иногда упоминается как «эмоциональная стабильность». Высокая потребность в стабильности характерна для спокойной личности, но такие люди могут быть восприняты как невнимательные и равнодушные. Низкая потребность в стабильности характерна для возбудимых и динамичных личностей, их обычно воспринимают как нестабильных или небезопасных
Открытость опыту Возможные значения Положительные: изобретательность; любопытство Негативные: последовательность, осторожность	Выражается в способности понимать искусство, эмоции, приключения, необычные идеи, любопытстве и разносторонности интересов. Открытость отражает степень интеллектуального уровня, креативности и тяги к новому. Открытость также описывается как степень, в которой человек является творческим и предпочитает различные виды деятельности строгой рутине. Высокий уровень открытости может восприниматься как непредсказуемость или недостаток концентрации, потенциальной склонности к рискованному поведению. Кроме того, люди с высокой открытостью могут тянуться к самореализации и напряженным переживаниям. И наоборот, личности с низкой открытостью получают удовлетворение от постоянства и могут характеризоваться как замкнутые

Личностные показатели риска

Причины инсайдерских инцидентов часто можно обнаружить в личных проблемах в жизни нарушителей, что подтверждается эмпирическими исследованиями. Стоит заметить, что работники могут и скорее всего будут скрывать личную информацию, даже если раскрытие такой информации предусмотрено существующими процедурами организации. Тем не менее наличие проблем может быть замечено другими сотрудниками или может проявляться в виде специфической активности в социальных сетях.

К личностным показателям риска можно отнести депрессию, наличие зависимостей (алкоголь, наркотики, азартные игры), расставание или развод, смерть близкого человека, недовольство условиями труда, наличие хронических заболеваний у самого работника или у его близких.

Поведенческие показатели риска

Поведение работника может заранее указывать на наличие инсайдерской угрозы. Чем большему количеству поведенческих рисков подвержен человек, тем больше вероятность нарушения им режима информационной безопасности.

К основным проявлениям поведенческого риска можно отнести нежелание соблюдать установленные правила и процедуры, преднамеренное вредительство, неоднократное нарушение трудового распорядка, резкие высказывания, импульсивность и агрессию.

Контекстные показатели риска

В то время как предыдущие показатели риска основываются на субъективных оценках со стороны коллег и других источников, оценка контекстных показателей риска подразумевает использование объективной информации, связанной с фактами из биографии потенциального инсайдера. Многие организации используют базовые проверки при проведении процедуры найма на работу и собирают данные, которые могут быть использованы для обнаружения вредоносного поведения. Для этого предлагаются показатели, которые наиболее часто используются в проверках при приеме на работу и которые можно подтвердить.

Контекстные показатели проявляются в участии в деятельности отдельных лиц или групп, выступающих против основных убеждений организации, наличии судимости, участии в деятельности, которая может вызвать конфликт интересов, ведении собственного бизнеса, наличии кредитов и иных финансовых обязательств.

Скрининговые показатели риска

Под скрининговыми показателями риска понимаются данные, полученные в результате проведения процедуры скрининга. Скрининг – процедура верификации данных, представленных кандидатом на трудоустройство в своем резюме и заявлении, выполняемая работодателем (или сторонней организацией). Данная процедура может позволить выявить слабые стороны характера подчиненного и наклонности к нелегальной деятельности, которые могут нанести ущерб организации и ее репутации или служить ограничением для эффективного выполнения им своих обязанностей.

Скрининг часто выполняется для того, чтобы определить, можно ли доверять работнику доступ к финансовым ресурсам и конфиденциальной информации. Также скрининг часто требуется для кандидатов на должности, требующие высокого уровня доверия, такие как работа в сфере образования, в судах, медицинских учреждениях, аэропортах или правительстве. Данная проверка может выполняться частной компанией и быть дорогостоящей. В результате скрининга проверяются данные по прежним местам работы, кредитной истории и записях о судимостях.

Эти проверки часто используются работодателями в качестве средства оценки прошлых ошибок, его характера и пригодности кандидата на работу, а также для выявления потенциальных рисков найма по соображениям безопасности. Проверки также используются для тщательного изучения потенциальных государственных служащих, с тем чтобы получить разрешение на доступ к тайне. Однако эти проверки иногда могут использоваться в незаконных целях, таких как незаконная дискриминация, кража личных данных и нарушение неприкосновенности частной жизни.

Часто проводятся проверки для подтверждения информации, указанной в заявлении о приеме на работу или резюме/биографических данных.

Исследование показало, что половина всех контрольных проверок, проведенных в отношении потенциальных работников, выявляют различия между тем, что предоставил кандидат на работу, и тем, что сообщил источник. Проверки также могут проводиться с целью дальнейшего дифференцирования потенциальных работников и выбора того, который, по мнению работодателя, лучше всего подходит для этой должности. Работодатели обязаны следить за тем, чтобы условия труда были безопасными для всех работников, и предотвращать другие проблемы на рабочем месте.

Скрининговые показатели: наличие алкогольной зависимости, наличие наркотической зависимости, наличие зависимости от азартных игр, наличие хронических заболеваний, наличие хронических заболеваний у близких, кражи по предыдущим местам работы, наличие кредитов и иных финансовых обязательств, искажение данных о себе (документы, записи в трудовой книжке, анкетные данные) при поступлении на работу, наличие связей в криминальном мире, передача конфиденциальной информации посторонним лицам, совершение противоправных действий, в том числе оставшихся нераскрытыми.

Технические показатели риска

Предлагается использование пяти групп показателей, получаемых из систем журналирования, которые могут быть использованы для обнаружения подозрительных действий. К ним относятся данные об аутентификации, изменении данных, сетевой активности, получении доступа к ресурсам, системные ошибки и другие события. Программные средства защиты информации, такие как SIEM- и IDS/IPS-системы могут быть использованы для предоставления администраторам достаточной информации для обнаружения подозрительной активности. Изменения в конфигурационных файлах, получение доступа к журналам авторизации могут быть проанализированы для наблюдения за активностью сотрудников. Информация из журналов событий может быть использована для создания профиля поведения нормального пользователя. В случае если обнаружено необычное поведение, отличное от профиля нормального поведения, может быть сделано предположение об инсайдерской деятельности [9–13].

ТАБЛИЦА 2. Технические показатели риска

Группа показателей	**Показатель**
1	**2**
Печать документов	Увеличение количества выводимых на печать документов
	Выполнение печати в нерабочее время
	Удаленная печать
	Печать документов, запрещенных для копирования
	Печать больших документов

Окончание табл. 2

1	2
Поисковые запросы	Увеличение количества запросов
	Осуществление поиска в нерабочее время
	Запросы из черного списка
	Прямой доступ к базе данных
	Запросы на странные темы
	Высокое количество уникальных запросов
Осуществление доступа	Высокое использование одного IP-адреса для доступа
	Доступ в нерабочее время
	Доступ к запрещенным ресурсам
	Попытки получения администраторского доступа
Скачивание информации	Увеличение количества скачиваемой информации
	Скачивание информации в нерабочее время
	Скачивание с удаленных серверов
	Скачивание документов, запрещенных для копирования
	Скачивание больших файлов
Использование браузера	Частое обращение к одному и тому же ресурсу
	Использование браузера в нерабочее время
	Просмотр запрещенных ресурсов
	Просмотр большого количества документов

Определение значений показателей риска

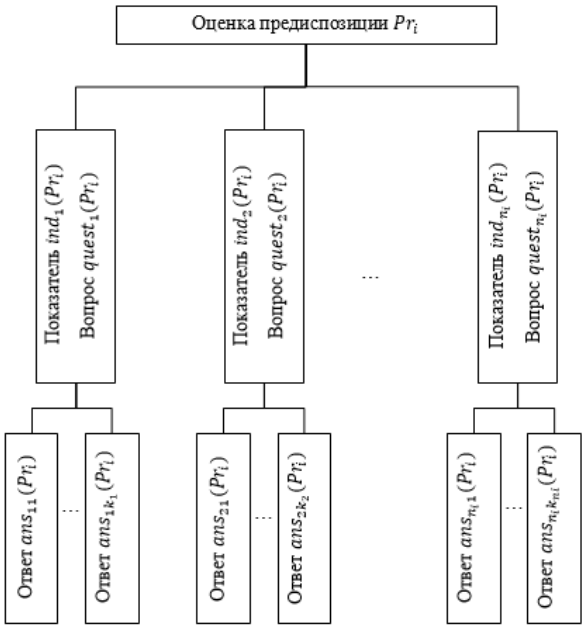
Приведенные выше показатели предлагается условно разделить на три группы: динамические, периодически актуализируемые и стационарные. Для определения значений периодически актуализируемых показателей предлагается использовать метод анализа иерархий (МАИ). Метод анализа иерархий успешно применяется для осуществления количественной оценки показателей ущерба от реализации угроз информационной безопасности [14].

Данный метод состоит из этапа определения частных показателей, влияющих на формирование оценки предрасположенности к инсайдерской деятельности (предиспозиции), и нечеткой оценки на основе количественной оценки частных показателей.

Эксперты формируют множество показателей, влияющих на предиспозицию Pr_i. Для оценки каждого показателя формируется соответствующий опросный лист $quest_j(Pr_i)$ с множеством ответов $ans_{jk}(Pr_i)$.

$$\{ind_1(Pr_i), \dots, ind_{n_i}(Pr_i)\}, \quad (1)$$

где Pr_i – предиспозиция; $ind_j(Pr_i), j = 1, \dots, n_i$ – показатели предиспозиции (см. рисунок).



Дерево декомпозиции для *i*-й предиспозиции

Оценка предиспозиции вычисляется на основе следующего алгоритма [2]:
Шаг 1. Формирование группы экспертов.
Шаг 2. Оценка приоритетов важности для вопросов.
Шаг 3. Формирование нечетких приоритетов важности для вопросов.
Шаг 4. Определение нечетких значений баллов.
Шаг 5. Оценка приоритетов важности для ответов внутри вопросов.
Шаг 6. Формирование нечетких приоритетов важности для ответов внутри вопросов.
Шаг 7. Определение абсолютных значений баллов.
Шаг 8. Определение значений баллов, влияющих положительно или отрицательно на оценку предиспозиции
Шаг 9. Получение от эксперта вариантов ответов .
Шаг 10. Нормирование общего количества баллов.

К динамическим показателям относятся технические показатели (собираются DLP или SIEM), которые могут быть автоматизированно собраны на основе данных вычислительной сети организации и ее информационных систем.

К периодически актуализируемым относятся личностные показатели (МАИ), поведенческие показатели (МАИ), скрининговые показатели (определяются специализированными средствами), контекстные показатели (МАИ).

К стационарным показателям риска относятся психологические и коммуникативные показатели, зависящие от личности человека (определяются анкетированием).

Заключение

На основе сказанного выше можно сделать вывод, что несмотря на растущую потребность в методе, способном помогать выявлять инсайдерские угрозы, на данный момент отсутствует универсальный подход, способный комплексно решать проблему обнаружения внутренних угроз и противодействия им. Предложенные показатели могут быть использованы для построения автоматизированной системы выявления инсайдеров в организации, позволяющей повысить эффективность работы администратора безопасности и уменьшить время, требуемое для выявления наличия инсайдерской угрозы.

Литература

1. Анализ угроз информационной безопасности 2016–2017 // [сайт] URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Analysis_information_security_threats_2016_2017.

2. Поляничко М.А., Пунанова К.В. Основные проблемы практического применения человеко-ориентированного подхода к обеспечению информационной безопасности // Фундаментальные и прикладные разработки в области технических и физико-математических наук : сборник научных статей по итогам работы третьего международного круглого стола. – М. : Общество с ограниченной ответственностью «КОНВЕРТ», 2018. – С. 57–60.

3. Поляничко М.А. Основные меры противодействия инсайдерским угрозам информационной безопасности // Фундаментальные и прикладные разработки в области технических и физико-математических наук : сборник научных статей по итогам работы четвертого международного круглого стола. – М. : Общество с ограниченной ответственностью «КОНВЕРТ», 2018. – С. 43–46.

4. Zeadally S. Detecting insider threats solutions and trends // Information Security Journal. 2012. № 4 (21), pp. 183–192.

5. Fagade T., Spyridopoulos T., Albishry N., Tryfonas T. (2017) System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis. In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science, vol 10292. Springer.

6. Forrest S., Hofmeyr, S., and Somayaji, A. (2008). The evolution of system-call monitoring. Proceedings of Annual Computer Security Applications Conference, pp. 418–430.

7. Kumar S. (1995). Classification and detection of computer intrusions. (Unpublished doctoral dissertation). Purdue University, West Lafayette, IN.

8. Первин Л., Джон О. Психология личности. Теория и исследования. – М. : Аспект Пресс, 2000. – 607 с.

9. Keeney M., Kowalski E., Cappelli D., Moore A., Shimeall T. and S. Rogers. (2005, May). Insider threat study: Computer system sabotage in critical infrastructure sectors. CMU/SEI and U.S. Secret Service.

10. Kruegel C., Mutz D., VaIeur F., and Vigna G. (2003). On the detection of anomalous system call arguments. 8th European Symposium on Research in Computer Security (ESORICS 2003), Gjovik, Norway.

11. Liu A., Martin C., Hetherington T. and Matzner S. (2005). A comparison of system call feature representations for insider threat detection. Proceedings of 2005 IEEE Workshop of Information Assurance and Security, pp. 340–347.

12. Nguyen N., Reiher P., and Kuenning G. (2003). Detecting insider threats by monitoring system call activity. Proceedings of Information AssuranceWorkshop, IEEE Systems, Man and Cybernetics Society, pp. 45–52.

13. Wang X., Jhi Y., Zhu S. and Liu P. (2009). Detecting software theft via system call based birthmarks. Proceedings of Annual Computer Security Applications Conference, pp. 149–158.

14. Аникин И.В. Метод анализа иерархий в задачах оценки и анализа рисков информационной безопасности // Вестник Казанского государственного технического университета им. А.Н. Туполева. – 2006. – № 3. – С. 11–18.

Insider Threats Identification in Transport Organizations

M.A. Polyanichko
Emperor Alexander I
St. Petersburg state transport university
Saint-Petersburg, Russia
polyanichko@pgups.ru

Abstract. **The article deals with the problem of identifying insider threats in transport organizations. The approach to the identification of insider threats, which based on the analysis of various indicators of risk predisposition to insider behavior, is proposed. The problem of identification of insiders characterized. Various risk indicators considered: psychological, personal, screening, behavioral, communicative, contextual and technical. Risk indicators divided into three groups: dynamic, periodically updated and stationary. To determine the values of periodically updated indicators it proposed to use the hierarchy analysis method. Dynamic indicators (technical) can automated collected on the basis on the data of the organization's computer network and its information systems. Periodically updated (personal, behavioral, contextual) indicators are determined by the method of analysis hierarchies, screening indicators are determined by specialized means. The steady-state risk indicators (psychological and communicative) determined by the questionnaire.**

Keywords: **internal threats to information security, insider, detection of insiders.**

REFERENCES

1. Analiz ugroz informacionnoj bezopasnosti 2016–2017 // [sajt] URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Analysis_infor-mation_security_threats_2016_2017.
2. Polyanichko M.A., Punanova K.V. Osnovnye problemy prakticheskogo primeneniya cheloveko-orientirovannogo podhoda k obespecheniyu informacion-noj bezopasnosti // «Fundamental'nye i prikladnye razrabotki v oblasti tekhnicheskih i fiziko-matematicheskih nauk» Sbornik nauchnyh statej po ito-gam raboty tret'ego mezhdunarodnogo kruglogo stola. – M. : Obshchestvo s ogranichennoj otvetstvennost'yu «KONVERT». – 2018. – C. 57–60.
3. Polyanichko M.A. Osnovnye mery protivodejstviya insajderskim ugrozam informacionnoj bezopasnosti // «Fundamental'nye i prikladnye razrabotki v oblasti tekhnicheskih i fiziko-matematicheskih nauk» Sbornik nauchnyh statej po itogam raboty chetvertogo mezhduna-rodnogo kruglogo stola. – M. : Obshchestvo s ogranichennoj otvetstvennost'yu «KONVERT». – 2018. C. 43–46.
4. Zeadally S. Detecting insider threats solutions and trends // Information Security Journal. – 2012. – № 4 (21). pp. 183–192.
5. Fagade T., Spyridopoulos T., Albishry N., Tryfonas T. (2017) System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis. In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science, vol 10292. Springer.
6. Forrest S., Hofmeyr S., and Somayaji A. (2008). The evolution of system-call monitoring. Proceedings of An-nual Computer Security Applications Conference, pp. 418–430.
7. Kumar S. (1995). Classification and detection of computer intrusions. (Unpublished doctoral dissertation). Pur-due University, West Lafayette, IN.
8. Pervin L., Dzhon O. Psihologiya lichnosti: Teoriya i issledovaniya. – M. : Aspekt Press, 2000. – 607 s.
9. Keeney M., Kowalski E., Cappelli D., Moore, A., Shimeall, T. and S. Rogers. (2005, May). Insider threat study: Computer system sabotage in critical infrastructure sectors. CMU/SEI and U.S. Secret Service.
10. Kruegel C., Mutz, D., VaIeur, F., and Vigna G. (2003). On the detection of anomalous system call arguments. 8th European Symposium on Research in Computer Security (ESORICS 2003), Gjovik, Norway.
11. Liu A., Martin C., Hetherington T., and Matzner S. (2005). A comparison of system call feature representations for insider threat detection. Proceedings of 2005 IEEE Work-shop of Information Assurance and Security, pp. 340 – 347.
12. Nguyen N., Reiher P. and Kuenning G. (2003). Detecting insider threats by monitoring system call activity. Proceedings of Information AssuranceWorkshop, IEEE Systems, Man and Cybernetics Society, pp. 45–52.
13. Wang X., Jhi Y., Zhu S. and Liu, P. (2009). Detect-ing software theft via system call based birthmarks. Proceedings of Annual Computer Security Applications Conference, pp. 149–158.
14. Anikin I.V. Metod analiza ierarhij v zadachah ocenki i analiza riskov informacionnoj bezopasnosti // Vestnik Kazanskogo gosudarstvennogo tekhnicheskogo universiteta im. A.N. Tupoleva. – 2006, № 3. – S. 11–18.

Once again about Blockchain Technology

V.N. Kustov, T.L. Stankevich
Emperor Alexander I Petersburg State Transport University
St.-Petersburg, Russia
kvnvika@mail.ru, Stankevich-t@gaz-is.ru

Abstract. **Recently, the blockchain technology was not written or spoken only by the lazy one. Blockchain – what is it: future technology or self-deception in the light of its small study and applicability? To argue, answering this question, it is possible long and persistently. The same article are considered implementation its technological features, which often remain «behind the scenes» or represent a kind of superficial, short and nonrevealing essence description.**

Keywords**: blockchain, block, transaction, Merkl's tree, mining, hash, miner, node.**

Lately about blockchain, technology did not write and did not tell only the lazy. The views expressed by information security and information technology experts in articles and oral presentations can be defined as diametrically opposed and considered at two levels of criteria:

1. Prospects for implementation;
2. Consequences of implementation.

The second criterion directly follows from the first, and both of them allow experts to be divided into skeptics and enthusiasts. At the first level, «Prospects» opinions are divided into those that express a sincere belief in the blockchain and its existence within a variety of systems and services, and those that deny it, referring to the possibility of alternative approaches to solving certain problems. The second criterion divides the experts into those who express great enthusiasm about the upcoming «revolution», comparable with the creation of the Internet, and those who connect the blockchain with the death of existing information and payment systems. Schematic representation of the described criteria is shown in figure 1.

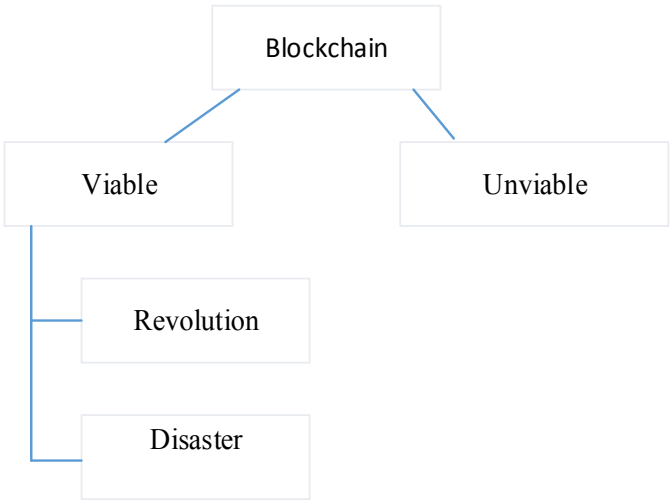


Fig. 1. Classification of expert opinions on blockchain technology

This article discusses the technological features of the blockchain technology implementation, which often remain «behind the scenes» or represent its surface, short and undisguised nature. So, what is the blockchain?

Blockchain is a technology of reliable distributed storage of reliable records [6]. At the same time, we want to emphasize that the main advantage of blockchain technology in comparison with distributed databases is the inability to violate the integrity of stored records (blocks). Thus, blockchain technology provides two of the three main properties of information security: data integrity and availability.

How does the blockchain work?

On the one hand, the blockchain is nothing new: linked lists in distributed databases have always been used, and the connection of list items in such databases is provided by links from one node to the next and (or) the previous one; new nodes are added to the end of the list. It also happens in solutions implemented based on blockchain: each block is a collection of certain elements and is a node of the list. The newly created blocks are always added strictly to the end of the chain, as shown in figure 2.

On the other hand, blockchain has a set of new properties that are not related to the lists and meet the following principles:

1. Spatial distribution.
2. Availability and openness of information.
3. Internal security.
4. Each blockchain user has access to the data stored in the system. Each node (user's computer) keeps and maintains a complete copy of the system blocks, which is provided by special synchronization mechanisms. This organization allows excluding the possibility of hacking the system, built based on blockchain, because in case of malicious modification of data on one node of the system, the rest of the system will immediately detect this fact. The network excludes centralized management, and each participant can join or leave the network at any time.
5. Any user, while maintaining the principles of openness and availability of records (transactions) in blocks, as well as the principle of anonymity easily verifies Block elements in the system.
6. The internal security of the blockchain is implemented using cryptographic mechanisms.

Fig. 2. The chain of blocks – Blockchain

HASH FUNCTION

The integrity and availability of data stored and processed by systems implemented based on blockchain ensures the use of a cryptographic mechanism that operates based on a hash function.

The hash function has only one argument – an arbitrary set of data: strings, documents, messages, data arrays, registers, etc. [1] The result of the hash function calculation over the input data is a bit string of fixed length – hash. Hash calculated using a special algorithm, which is a mathematical representation of a hash function.

The main properties of hash functions are as follows:

1. The hash function argument can be any size.
2. The calculated value of the hash function (hash) must always be a fixed size.
3. The h(m) hash function is easy and simple to compute for any m message.
4. The hash function must be sensitive to various, even the smallest, changes in the content of the m input dataset.
5. The hash function must be irreversible, that is, it must have a unidirectional property.
6. The probability of an event that the hash values of two different arguments (regardless of their size) coincide should be very small.
7. As it was mentioned earlier, the format and size of the input data for the hash function calculation are not limited, and a hash – bit string of fixed length should represent the hash result of the calculation. Standard hash sizes in bits can be as follows: 224, 256, 384 and 512. It is easy and simple to calculate a hash function by a certain algorithm, but it is almost impossible to recover the initial data (argument) from the hash, i.e. in other words, the hash function is unidirectional, the sensitivity of the hash function to the slightest changes in the argument is high. Examples of initial data slightly different from each other, and the results of applying hash functions to them are given in table 1 (calculations are made for the hash algorithm SHA-2(256) [2] using the utility Alternate HASH-Generator 1.450 [3]).

TABLE 1. The property of the hash function sensitivity to changes in the input data

Source data	HASH
The hash for this line will be as follows	907ec14038421a67c15a43452404e0d0b9a6e3950822f42ff391845a4dd5703e
The hash for this line will be as follows:	475935ef4c722c6978e5d84942cb90c14def34e03b0e4c7fdfea959c9af78a32
The HASH for this line will be as follows:	3eb5f620077b3cc68316d50f9c87f1e07c3e1df173c71afcd3b5d6e06d9d4154
The HasH FOR this line will be as follows:	cdc9a7bb2069343282d5e6eab10cbbd456b00d41c20d287ac0170f275fbfd1ad

BLOCKCHAIN NETWORK

By registering in a system built based on blockchain technology, the user is able to interact with other network nodes (create new transactions, which will be included in the blocks of the chain, view the elements of existing blocks). At the same time, the blockchain network is international in nature and is not subject to the laws of any state.

All users of the blockchain network (see fig. 3) can be divided into 3 categories:

1. Normal user.
2. Intruders.
3. Miners – the creators (generators) blocks and the transaction collectors in blocks.

The functions of a standard user include:

1. Create new records and send them to miners for entering into blocks.
2. Obtaining new data and checking their reliability.
3. Save verified data and share it with other users.

Attackers can create fake records and perform the same functions as regular users.

The main function of the miners is to create blocks. The process of creating a new block is very time-consuming and complex, requiring significant material, time and computing resources. In addition, some implementations of blockchain have very strict requirements for block generation and the maximum number of blocks that can be created is fixed. In addition to this task, miners provide the collection and verification of new records for their subsequent inclusion in the blocks, as well as their distribution on the blockchain network.

A new record is not considered reliable until it is entered in any block. As a rule, users send new records on the blockchain-network, so that eventually they reach the miner, and he in turn will include them in the block. Only after checking the new record for correctness, it will be included in the block and it will be impossible to cancel it.

BLOCK STRUCTURE

The data block consists of two parts: the header and the body (fig. 4).

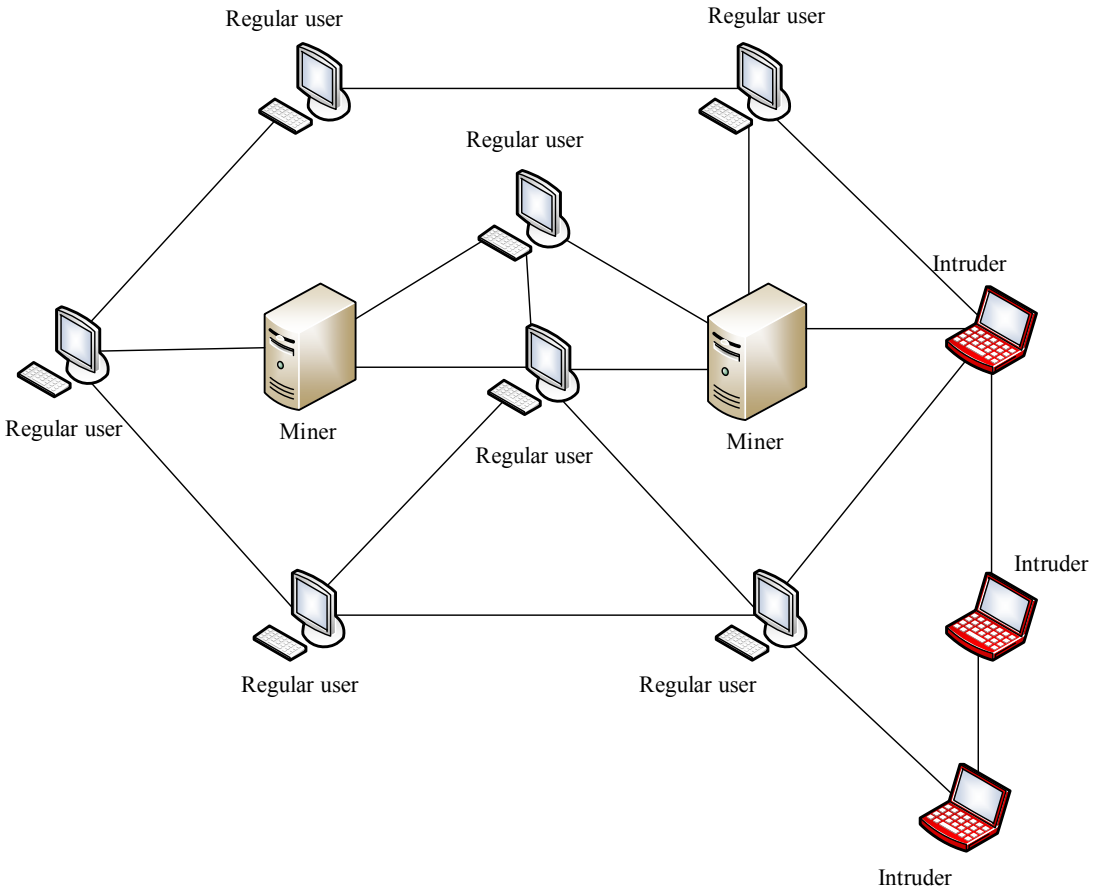


Fig. 3. Users of the blockchain network

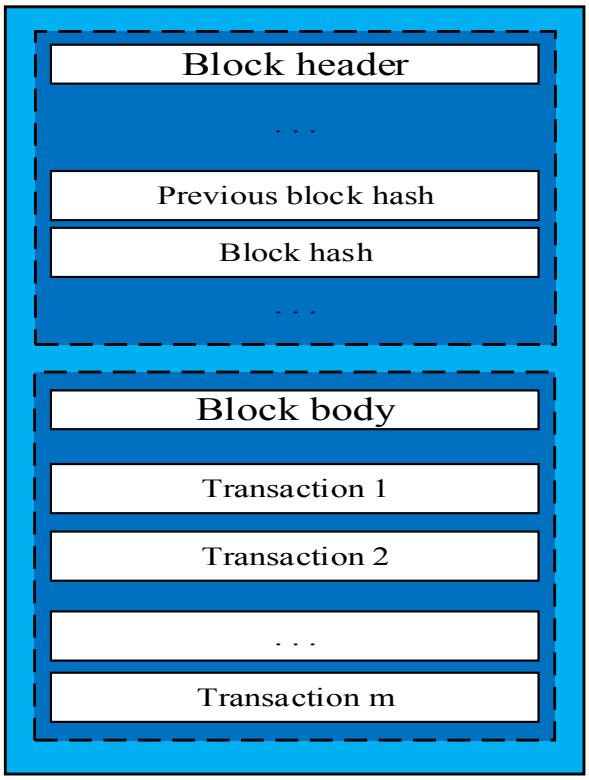


Fig. 4. The data block structure of the blockchain network

The block body is a collection of individual records (transactions), and the block header contains the main «secret» of blockchain technology: the header of each subsequent block contains the hash of the previous block and its own hash (fig. 5), which in turn guarantees the integrity of the blockchain data.

A minor change in the content of any block will result in a complete change in its hash, which in turn will require a change in the hashes of all subsequent blocks. Insert a new dummy block into the chain becomes impossible.

The hash block must meet important security rules that increase the level of network security. For example, in bitcoin, the hashes of blocks created by miners start with ten zeros, which sets the degree of new blocks creating complexity.

However, for any data set there is always a strictly one hash and to fulfill the hash requirement starting with ten zeros, it is necessary to generate and drop a huge number of unsuitable blocks until a block is found, the hash of which will meet this requirement, that is, will start with ten zeros, for example, will have this form: «00000000000000d1d2e97987d0e86679ae6d7d4e45cb231969757cb7cb7ec0ef273d6ee».

Thus, any user can easily verify whether the sequence of blocks is correct, whether the block is missing, whether a new block is added, and whether the block hash corresponds to the data stored in it.

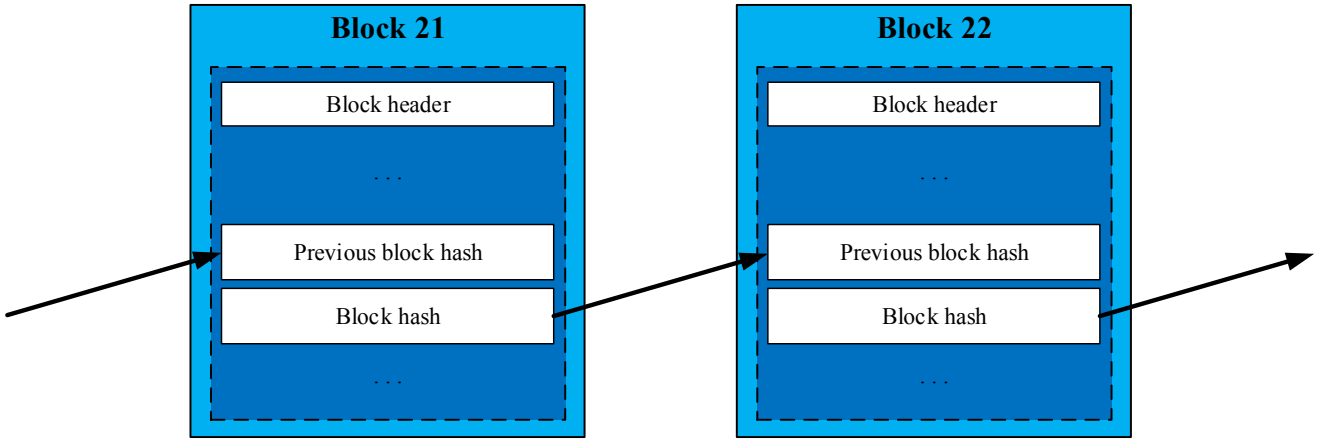


Fig. 5. The connectivity blocks in the blockchain

Once such a block is found, you must ensure that it has not been found before and is no longer included in the blockchain. If such a block has already been included in the blockchain, it is discarded and the search process is resumed until a unique block not yet included in the blockchain is found. Such laborious work reminds, figuratively speaking, search of pearl grain in a huge heap of manure.

Now about «mining» or «production» of blocks.

MINING OF BLOCKS

The miner is the same user of the blockchain network as everyone else. However, in addition to checking and disseminating data, he is still engaged in the creation of new blocks.

Receiving new transactions from the other network members, the miner gathers them together, generates the future block header and calculates the block hash. Let us consider an example for Bitcoin network: let us say after the first calculation made by the miner, the following hash value was obtained: «5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9». However, according to the rules, the hash should start with ten zeros. To change the hash, you must change the original data. To do this, a special field called «Nonce»is provided in the header of the block. At the first calculation, it is equal to 0, at the second iteration of calculations the miner changes value of a field on 1. Now the hash has changed and became equal to «6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b». We see that the conditions imposed on the hash values of bitcoin network blocks are not met again; therefore, the miner must increase the value of the «Nonce» field to 2 and once again recalculate the hash. To find a suitable hash value, miner have to perform billions and trillions of recalculations on their computing power. In addition, when a suitable hash is found, the miner saves the block to the blockchain network and sends it to other participants. Now all the transactions in the block are confirmed and protected by the hash value of the block, which is very difficult to fake. Recall that the hash of the block is encoded and the hash of the previous block, which is now simply impossible to do.

The secret hashing key is in the fact that this process has progress. It does not matter when the hash search started, how many records the block contains, how much time has been spent, how much hash has already been iterated – the probability of finding the required value at any iteration is always the same. This, in turn, means that it is impossible to make a preliminary calculation, it is impossible to «accumulate» new blocks and create a «warehouse» of blocks. Each miner has only one opportunity to get a suitable block – it is copulate, copulate and copulate.

For each block created in Bitcoin, as well as in other systems that provide cryptocurrencies, the miner receives a fee: who first found the required hash value, he created the block and earned. The link http://blockchain.info/ru/blocks it is possible to observe in real time how the born or extracted blocks, the hard work of miners for this, we have described the blockchain.

TRANSACTIONS

The information in the blockchain network is transmitted via transactions. Transactions are signed with the user's Electronic Signature (ES). To do this, each user has 2 keys: key of electronic signature and the verification key of the electronic signature. The ES key is stored by the owner and is not available to other users. The ES verification key is distributed over the blockchain network along with transactions. The next user sends the transaction to the next user (fig. 6) along with the signed hash of the previous transaction and the key of the ES verification. The receiver can easily check each ES using the sender's ES verification key to confirm the correctness of the whole chain.

In order to protect the network from malicious attacks, users must openly publish transactions [4], and agree on the order in which they are to be conducted. The recipient needs proof that for each transaction in the chain, most users agree to consider it first.

Now it becomes clear that it is almost impossible to forge transactions or insert a dummy block into the blockchain network.

Blockchain users always consider the longest version of the chain to be the true one and continuously increase it. If 2 nodes of the network publish different versions of the next block at the same time, then one of the nodes of the network will get one version of the chain before, and some – another. In this

case, each of them will start working on its own version of the chain, keeping the other in case it will be continued earlier. The duality will disappear as soon as a new block is received that will continue any of the branches, and those nodes that worked on the competing version will switch to the chain with the new block that has become longer.

New transactions do not have to reach all nodes: if many nodes of the blockchain network know about them, they will soon fall into one of the blocks. Block distribution rules are also not strict about lost blocks: once a node that misses one of the blocks gets the next one, it will ask for the missing information to fill in the obvious pass.

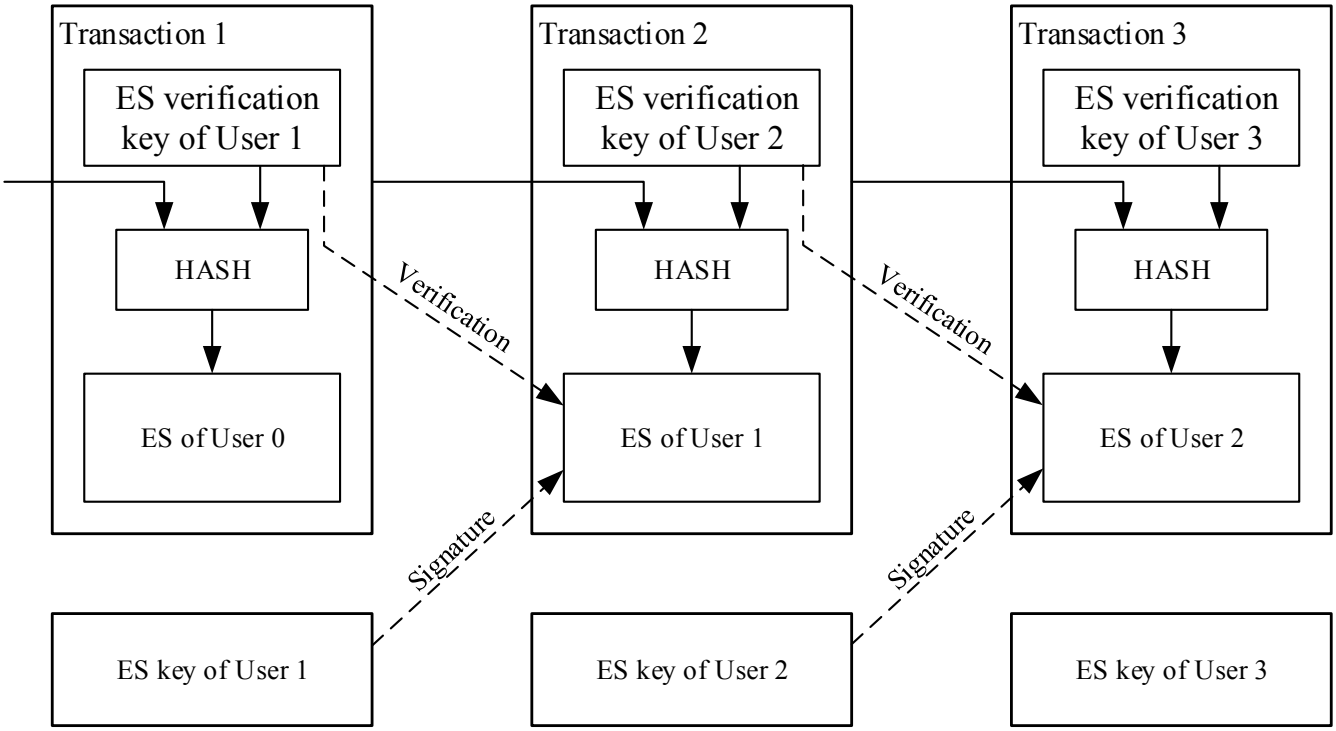


Fig. 6. Link of transaction block blockchain data

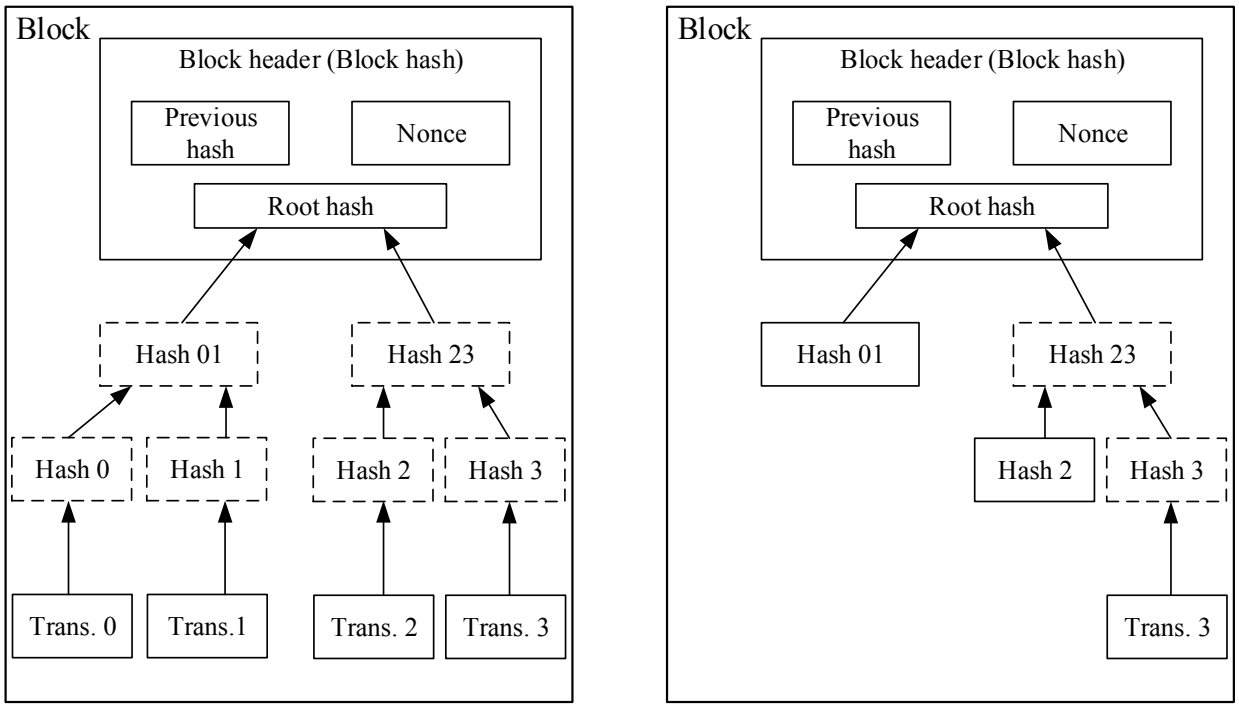
Memory saving

Writing to the block of the last transaction in the chain allows nodes to delete all previous transactions in order to clear disk memory. All transactions in the block are stored in the form of a Merkle hash tree [5] and only its root is included in the block hash, which in turn ensures its immutability and integrity. The size of filled blocks can be reduced by removing unnecessary branches of this tree, it is not necessary to store intermediate hashes (fig. 7).

A few words about the amount of memory required to store blockchain network data. The header of an empty block takes about 80 bytes of memory. Based on the calculation of the block generation rate, we get an increase in the blockchain size of 4.2 MB per year on average once every ten minutes. For an average computer with 2 GB of RAM and taking into account Moore's law, which predicts the growth of memory of 1.2 GB per year, data storage, as the authors [4] believed, will not be a problem, even if all block headers are in memory. The authors of blockchain technology, apparently, were not much mistaken in their assessments. The total size of memory occupied by blockchain blocks and transactions at 03:00 hours on December 26, 2017 was 148,291 MB (source: https://blockchain.info/charts/blocks-size).

In addition, transaction verification is possible without running a fully functional node. The user only needs to store the block headers of the longest chain he has received from other nodes and request a hash subtree for the necessary transaction. He cannot verify the correctness of the transaction itself, but after receiving a link to the block in which it is located, the user can easily make sure that this block and all subsequent accepted and confirmed by the network (fig. 8).

This method of verification can be used as long as the network is under the control of honest participants, that is, until the attackers do not take over most of the resources (more than 51%, the so called «attack 51%» [6]). Normal nodes can check transactions themselves, but if an attacker manages to generate the longest chain of blocks, he can compromise the simplified scheme with his fabricated transactions. One of the strategies to counter this can be sending alarms from normal nodes that receive a «false» block. This alarm will force the client program to load the block completely to independently confirm the incorrect data.



The hash tree of transactions — The Hash-tree after removal of the transactions 0, 1, 2

Fig. 7. The Merkle Tree

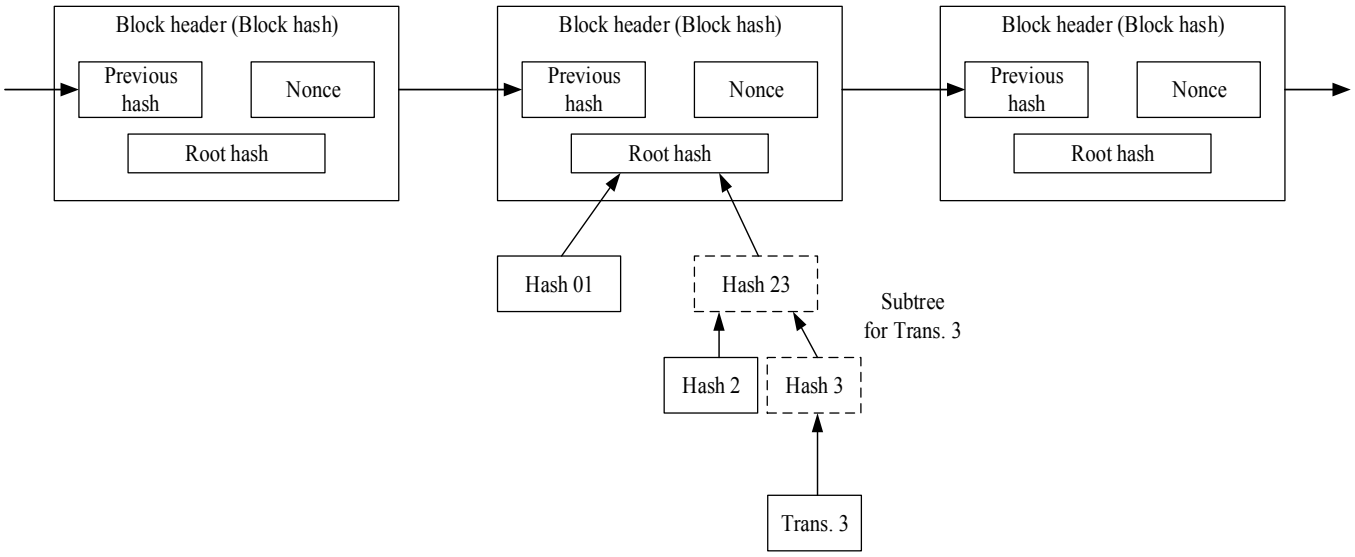


Fig. 8. Blockchain network block chain

SOME CALCULATIONS

Consider a scenario in which an attacker attempts to generate a sequence of blocks that are longer than those generated by normal users (honest network members). Even if he succeeds in this, it will not lead to success. Nodes will never accept an invalid transaction or block containing it. An attacker can only attempt to modify one or more of his transactions, but this can also be easily detected.

The race between users and the attacker can be thought of as a binomial random walk. A successful event, when a «good» chain is extended by one block, leads to an increase in the separation by one, and unsuccessful, when the next block is created by an attacker, — to reduce the separation.

The probability that an attacker succeeds, as well as the probability that the attacker will be able to catch up with honest participants, is calculated as follows [7]:

q_z – the probability that the attacker will make up, the gap in the z blocks.

$$q_z = 1, \text{ if } p \le q, \quad q_z = (q/p)^z, \text{ if } p > q,$$

where p – the probability of a block in an honest chain;

q – the probability of a block being created by an attacker;

q_z – the probability that the attacker will make up, the gap in the z blocks.

If p > q, the probability of q_z decreases exponentially as the number of blocks z that the attacker lags behind increases. Since the attacker is in a deliberately worse situation, then without a large successful breakthrough at the very beginning of the process of creating a blockchain, his chances of success are negligible.

If we take into account that the expectation of the rate of generation of honest blocks is a known value, the number of blocks created by an attacker can be considered subject to an exponential distribution with mathematical expectation $\lambda = z\frac{q}{p}$.

To calculate the value of P – probability that the attacker will be ahead of the respectable participants, multiply the random value – the number of blocks created by the offender, the probability that he will be able to level the remaining difference and eventually get:

$$P = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!}(q/p)^{z-k} \text{ if } k \le z \text{ and}$$

$$P = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \text{ if } k > z.$$

By rearranging the summands and changing the symbol ∞ to z, that is, getting rid of infinity, we get the following expression:

$$P = \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!}(1-(q/p)^{(z-k)}).$$

Table 2 and 3 the results of calculations of P value depending on z values for $q = 0{,}1$ are presented (table 2) and $q = 0{,}3$ (table 3), and in figures 9 and 10 – the diagrams corresponding to them.

TABLE 2. The results of P calculations at $q = 0{,}1$

$q = 0{,}1$	
z	P
0	1,0000000
1	0,2045873
2	0,0509779
3	0,0131722
4	0,0034552
5	0,0009137
6	0,0002428
7	0,0000647
8	0,0000173
9	0,0000046
10	0.0000012

TABLE 3. The results of P calculations at $q = 0{,}3$

$q = 0{,}3$	
z	P
0	1,0000000
5	0,1773523
10	0,0416605
15	0,0101008
20	0,0024804
25	0,0006132
30	0,0001522
35	0,0000379
40	0,0000095
45	0,0000024
50	0,0000006

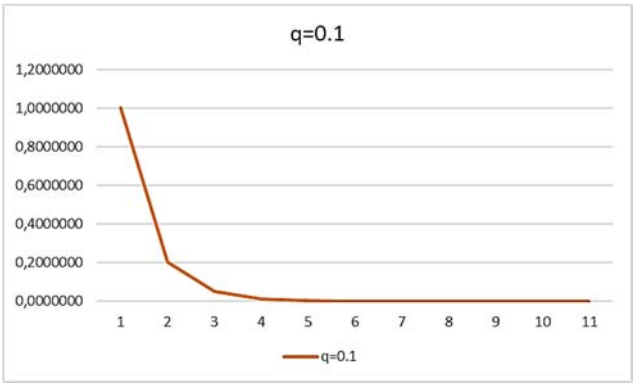


Fig. 9. Graphic representation of P calculations at $q = 0{,}1$

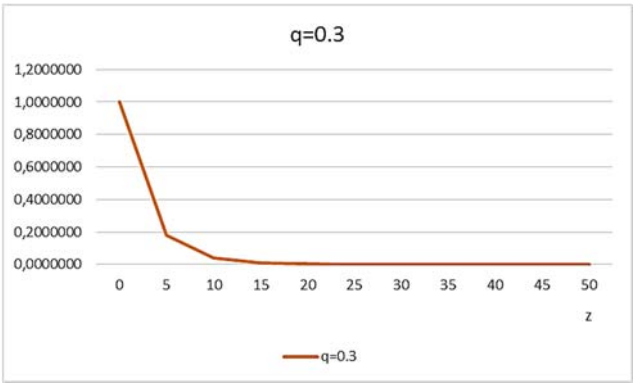


Fig. 10. Graphic representation of P calculations at $q = 0{,}3$.
calculations at $q = 0{,}1$

Conclusion

Therefore, we have read the blockchain device in detail. The attractive side of the blockchain network is the simplicity of its structure. Each node of the network works completely independently, sometimes exchanging information with other nodes. At the same time, there is no need for strict identification, since the messages are transmitted not by any given route, but only in accordance with the principle of «lowest cost». Nodes can leave the blockchain network and reconnect to it, always loading the longest chain of blocks in order to confirm the missed transaction history. Each node independently agrees to load the correct block into the chain, and use its processing power to extend the loaded chain, or failure if the loaded block contains incorrect data without extending the chain. Any other rules of the protocol could be implemented through such a simple voting mechanism. All attempts of the malefactors who do not possess the prevailing part of resources of the blockchain network to replace the checked records become practically impossible from the computational point of view. Blockchain technology is reliable, simple and open. Its advantages are obvious.

References

1. Vijay Ganesh (University of Waterloo). Cryptographic Hash Functions 2013. https://ece.uwaterloo.ca/~vganesh/TEACHING/W2013/ECE458/Lecture-11.pdf.

2. Стандарт безопасного хэша (SHS). FIPS PUB 180-3. Лаборатория информационных технологий института стандартов и технологий, Gaithersburg, MD 20899-8900, Октябрь 2008. http://mzdm.narod.ru/FIPS-180-3-Rus.pdf.

3. Alternate HASH-Generator 1.450, https://xetcom.com/programs/system/components/275-alternate-hash-generator.

4. Satoshi Nakamoto: Bitcoin. A Peer-to-Peer Electronic Cash System, satoshin@gmx.com, 2008. https://bitcoin.org/bitcoin.pdf.

5. R. C. Merkle, «Protocols for public key cryptosystem», in Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

6. George Shnurenko. Bitcoin 51% Attack: How It Works, How Much Bitcoin 51 Attack Costs. https://cryptocomes.com/bitcoin-51-attack-how-it-works-how-much-bitcoin-51-attack-costs.

7. Feller V. Introduction to probability theory and its applications. In 2 volumes. Vol. 1:Intr. with English. – M. : publishing Mir, 1984, – 528 p.

8. 3D Explorer, http://blockchain3d.info/

9. Michael Crosby (Google), Nachiappan (Yahoo), Pradhan Pattanayak (Yahoo), Sanjeev Verma (Samsung Research America), Vignesh Kalyanaraman (Fairchild Semiconductor). Sutardja Center for Entrepreneurship & Technology Technical Report, Date: October 16, 2015. https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

10. Tania H. How the Blockchain Works. https://rubygarage.org/blog/how-blockchain-works.

Еще раз о технологии Blockchain

В.Н. Кустов, Т.Л. Станкевич
Петербургский Государственный университет путей сообщения Императора Александра I
kvnvika@mail.ru, Stankevich-t@gaz-is.ru

Аннотация. **В последнее время о технологии blockchain не писал и не говорил только ленивый. Blockchain – что это: технология будущего или самообман в свете ее малой изученности и применимости на сегодняшний день? Рассуждать, отвечая на этот вопрос, можно долго и упорно. В статье рассмотрены технологические особенности ее реализации, которые часто остаются «за кадром» либо освещаются с помощью некоторого поверхностного, короткого и не раскрывающего сущность описания.**

Ключевые слова: **блокчейн, блок, транзакция, дерево Меркла, майнинг, хэш, майнер, узел.**

Литературы

1. Vijay Ganesh (University of Waterloo). Cryptographic Hash Functions 2013. https://ece.uwaterloo.ca/~vganesh/TEACHING/W2013/ECE458/Lecture-11.pdf.

2. Стандарт безопасного хэша (SHS). FIPS PUB 180-3. Лаборатория информационных технологий института стандартов и технологий, Gaithersburg, MD 20899-8900, Октябрь 2008. http://mzdm.narod.ru/FIPS-180-3-Rus.pdf.

3. Alternate HASH-Generator 1.450 [Электронный ресурс]. – Режим доступа: https://xetcom.com/programs/system/components/275-alternate-hash-generator/.

4. Satoshi Nakamoto: Bitcoin.APeer-to-Peer Electronic Cash System [Электронный ресурс]. – Режим доступа: https://bitcoin.org/bitcoin.pdf.

5. Merkle R. C. Protocols for public key cryptosystems, In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society. April 1980. – P. 122–133.

6. George Shnurenko. Bitcoin 51% Attack: How It Works, How Much Bitcoin 51 Attack Costs. https://cryptocomes.com/bitcoin-51-attack-how-it-works-how-much-bitcoin-51-attack-costs.

7. Феллер В. Введение в теорию вероятностей и ее приложения. В 2 т. Т. 1; пер.с англ. – М. : Мир. – 1984. – 528 с.

8. 3D Explorer [Электронный ресурс]. – Режим доступа: http://blockchain3d.info/.

9. Michael Crosby (Google), Nachiappan (Yahoo), Pradhan Pattanayak (Yahoo), Sanjeev Verma (Samsung Research America), Vignesh Kalyanaraman (Fairchild Semiconductor). Sutardja Center for Entrepreneurship & Technology Technical Report, Date: October 16, 2015. https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

10. Tania H. How the Blockchain Works. https://rubygarage.org/blog/how-blockchain-works.

Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения

М.О. Калинин
Санкт-Петербургский политехнический университет Петра Великого
Санкт-Петербург, Россия
max@ibks.spbstu.ru

С.И. Штеренберг
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Санкт-Петербург, Россия
shterenberg.stanislaw@yandex.ru

Аннотация. **Рассматривается метод применения машинного обучения для обеспечения информационной безопасности (ИБ) предприятия. Для анализа информационной безопасности проводится рассмотрение нескольких способов работы с данными, которые в совокупности позволяют разработать модель поведения пользователей и объектов в информационной системе (ИС). Машинное обучение используется для более точного определения девиантного поведения пользователя и объектов в ИС. Описанные способы позволяют создать надежную распределенную систему обнаружения вторжений.**

Ключевые слова: **машинное обучение, Python, информационная безопасность, аудит, мониторинг, обнаружение вторжений.**

Введение

В настоящее время машинное обучение занимает огромное место в жизни человека в связи с наличием большого спектра его применений. Например, оно используется в анализе дорожных пробок или медицинской диагностике. Можно привести большое количество таких примеров, но в данной статье будет рассматриваться использование машинного обучения для более точного определения поведения пользователя и объектов информатизации в информационной системе (ИС).

Проведение исследования

Машинное обучение (machine learning) чаще всего подразделяют на два типа:

– контролируемое – поиск зависимости между первоначальной постановкой задачи и её конечным результатом;

– неконтролируемое – в данном случае конечный результат заранее не известен и необходимо найти различные зависимости между объектами, т. е. целью является упорядочить данные или описать их структуру.

В первом случае определяются такие популярные алгоритмы, как классификация, ранжирование, регрессия, обнаружение аномалий (используется, например, для выявления фактов мошенничества в банковских системах или нарушения правил поведения в корпоративной сети). В случае второго типа – кластеризация, поиск ассоциаций, фильтрация выбросов и так далее. Так же определяют машинное обучение, которое применяется в робототехнике. В этом случае для каждого текущего действия выбирается наилучшее последующее. Кроме того, этот метод обладает обратной связью для уведомления об успешности выбранного действия [1].

Выбор алгоритма машинного обучения зависит от большого числа факторов, таких как длительность обучения, линейность, точность, число параметров и многое другое. Если необходимо получить системы с коротким временем обучения, используется алгоритм регрессии, а если необходимо получить высокую точность – лес решений или нейронная сеть [2, 3].

Существует множество подходов к машинному обучению, но они имеют нечеткие границы, так как каждый из подходов подразумевает использование различных алгоритмов и часто пересекается с другими. Среди существующих подходов самыми популярными являются: байесовская теория классификации, классификация на основе сходства, поиск закономерностей, нейронные сети и другие [3]. На рис. 1 и 2 приведены два примера использования машинного обучения.

Рис. 1. Пример использования машинного обучения

На рис. 1 показано, как работает алгоритм машинного обучения на примере использования электронной почты. При поступлении какого-либо сообщения данный алгоритм определяет, является это сообщение спамом или не является. На основе поступления сообщений с типовой

структурой система обучается распознавать спам и блокировать его.

В данном случае обучение системы происходит следующим образом. На начальной стадии система анализирует, как пользователь проводит фильтрацию сообщений на спам – не спам. Она понимает этот алгоритм действий пользователя, обучается этому алгоритму и далее автоматически проводит фильтрацию входящих сообщений, облегчая работу пользователя [1, 2, 3].

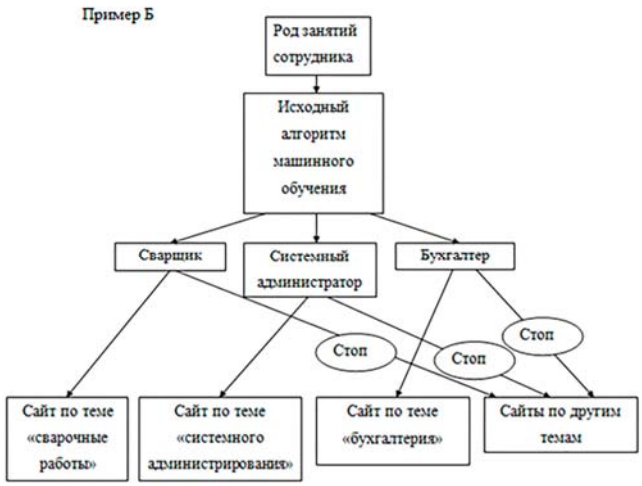


Рис. 2. Пример использования машинного обучения

Второй пример является более сложным аналогом работы алгоритма машинного обучения. В этом случае алгоритм определяет, к каким сайтам имеет доступ сотрудник в связи с его родом занятий. То есть, например, сварщик имеет доступ только к сайтам по тематике его работы, но не имеет доступа к сайтам с тематикой, не относящейся к его роду деятельности.

В данном случае обучение системы проходит таким образом. В начале работы система анализирует запросы работников, то есть, например, бухгалтер пользуется сайтами, относящимися к его роду деятельности, в это время система обрабатывает запросы этого пользователя, запоминает их и на основе этих запросов строит характеристическую модель пользователя, что позволяет ей сортировать запросы работника. На основе этой модели система разграничивает доступ к тем или иным сайтам. В итоге работник будет получать доступ только к сайтам с его тематикой.

Описание предлагаемого метода

Представленные выше примеры использования машинного обучения являются общеизвестными. В данной статье машинное обучение будет рассмотрено как необходимый инструмент любой системы IT-безопасности, основывающийся на нескольких способах работы с информацией [4].

Рассмотрим первый способ: сбор и анализ информации о пользователе.

В настоящее время основным средством хранения и распространения информации является сеть Интернет. «Всемирная паутина» всё чаще используется для решения огромного количества различных задач. Таким образом, Интернет является необходимым механизмом, позволяющим организовывать работу различных предприятий.

Но, говоря о работе с данной сетью, нельзя забывать о безопасности корпоративной информации. Безопасность данных является одной из основных задач как малых, так и крупных организаций. При этом речь идет не только о возможных утечках информации и противодействии этому, отражении различных атак на ресурсы компании, но и об оптимизации функционирования системы в целом.

Одним из инструментов для обеспечения безопасности корпоративной информации предприятия является сбор и анализ ключевой информации о пользователях. Но тут возникают две ключевые проблемы:

– большие объемы данных: в связи с бурным ростом сети Интернет и большим количеством контента невозможно вручную собирать данные;

– частое обновление контента: один человек или специальная группа сотрудников не в силах обслуживать огромные потоки динамично изменяющейся информации самостоятельно.

Для решения этих проблем предполагается использование синтаксического анализа (парсинга), позволяющего собирать данные о пользователях для их дальнейшей обработки. Парсинг сайтов является оптимальным и эффективным решением для автоматизации сбора и анализа информации [5]. В отличие от человека программа-парсер может:

– быстро просматривать огромное количество веб-страниц;

– отделить машинный код от контента, воспринимаемого человеком;

– выделить необходимую информацию и отбросить лишнюю;

– предоставить конечные данные в необходимом виде.

Далее с полученными структурированными данными (база данных или электронная таблица) можно проводить различные манипуляции, необходимые предприятиям.

Преимущества использования парсинга сайтов:

– автоматический режим работы, практически без участия оператора;

– безотказность работы программы, отсутствие ошибок;

– экономия времени и средств;

– обработка большого количества информации;

– способность обрабатывать динамичную, то есть постоянно меняющуюся информацию.

Виды парсинга сайтов:

– заполнение веб-сайтов текстовой или мультимедийной информацией;

– сбор данных о товарах и их стоимости для интернет-магазинов;

– сбор данных о пользователях;

– работа с социальными сетями;

– другое.

На рис. 3 представлен простейший алгоритм работы программы-парсера для сбора информации из какого-либо информационного источника, например веб-страницы.

Программа-парсер может быть реализована на большом количестве языков программирования. Например, C++, Delphi, Python, PHP и других.

Подводя итог, можно с уверенностью сказать, что синтаксический анализ (парсинг) сайтов является удобным инструментом для сбора информации о пользователях, который позволит предприятиям контролировать влияние действий сотрудников на состояние информационной безопасности [6].

Рис. 3. Алгоритм работы программы-парсера

Второй способ: мониторинг ресурсов облачной инфраструктуры. Способ позволяет производить мониторинг ресурсов и аналитику данных мониторинга. Он будет направлен на облачную инфраструктуру предприятий, так как она подходит для малого, среднего и крупного бизнеса.

Такая инфраструктура обычно строится на стандартном наборе компонентов: сервис идентификации, сервер хранения данных, серверы с вычислительными ресурсами. Сервис идентификации – главный элемент системы, отвечающий за все сервисы, использующиеся в работе облака. Сервисы в свою очередь предоставляют тот или иной функционал системе.

Например: сервис вычислительных ресурсов предоставляет системе ресурсы для запуска виртуальных машин (инстансов); сетевой сервис отвечает за предоставление сетевых ресурсов, таких как выделение пула IP-адресов, маршрутизацию и построение оверлейных туннелей; сервис управления отвечает за работу других сервисов; сервис идентификации и авторизации позволяет производить аутентификацию для всех сервисов, служб и пользователей; сервис хранения предоставляет пространство для хранения данных.

Все сервисы взаимодействуют между собой при помощи сервиса сообщений для обеспечения стабильной и синхронной работы, он передает запросы на выделение ресурсов, данные о состоянии и т. д. Все сообщения передаются при помощи зашифрованных https-запросов, поэтому без специального клиента невозможно получить данные [7, 8].

В роли клиента выступает сервис сбора телеметрии. С его помощью можно собирать разные полезные данные. Каждый инстанс может получать некое количество ресурсов, таких как количество процессорного времени, количество оперативной памяти и дискового пространства. Каждый из этих ресурсов можно рассматривать как источник данных о состоянии данного инстанса или даже целого сервера предоставления вычислительных ресурсов. Также есть возможность сбора трафика для его дальнейшего анализа. На границе виртуальной сети предприятия устанавливается DPI (deep packet inspection), позволяющий просматривать пакет целиком в обоих направлениях и получать полезные данные.

На рис. 4 представлена схема взаимодействия сервисов облачной инфраструктуры. Третий способ: анализ поведения пользователей в информационной системе.

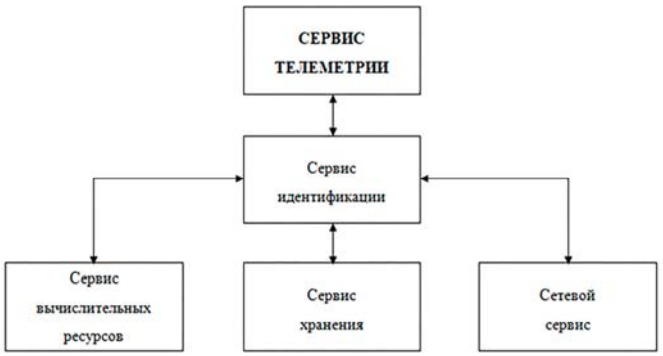


Рис. 4. Схема взаимодействия сервисов облачной инфраструктуры

Данный способ подразумевает проведение анализа поведения пользователей в информационной системе.

Непрерывное развитие и внедрение информационных технологий, появление больших объёмов данных и их ценности приводит к необходимости защиты информации. Основной угрозой безопасности являются вторжения в вычислительные системы. Под ними понимается какая-либо деятельность пользователей или объектов, нарушающая целостность, доступность и конфиденциальность данных [7, 8].

Для предотвращения подобных вторжений целесообразно проводить анализ поведения пользователей и объектов в системе. В таблице представлен пример журнала событий для определения поведения пользователей на основе операционной системы Windows [9].

События журналов аудита для определения поведения пользователей

Категория	Описание
Системное событие	Перезагрузка операционной системы
Системное событие	Завершение работы операционной системы (shutdown)
Системное событие	Загрузка пакета аутентификации
Системное событие	Запуск процесса аутентификации (используется WinLogon.exe)
Системное событие	Сбой при регистрации одного или нескольких событий аудита
Системное событие	Очистка журнала аудита
Системное событие	Загрузка пакета оповещения об изменениях в списке пользователей
Вход/выход пользователя из системы	Пользователь успешно вошел в систему
Вход/выход пользователя из системы	Вход пользователя в систему запрещен – имя или пароль некорректны
Вход/выход пользователя из системы	Вход пользователя в домен в данное время запрещен
Изменения в списке пользователей	Произведены изменения в учетной записи пользователей глобальной группы, не связанные с изменением членства пользователей в этой группе
Изменения в списке пользователей	Произведены изменения в учетной записи пользователя, не связанные с изменением типа учетной записи, пароля пользователя и членства в группах
Аудит доступа к объектам	Открытие папок
Аудит доступа к объектам	Создание/удаление/изменение файлов

Построение модели определения поведения пользователей и объектов в системе позволит:

– идентифицировать пользователей и объекты в системе;

– определить род деятельности пользователей;

– предотвратить возможные нарушения безопасности в системе;

– исследовать влияние объектов информатизации на инфраструктуру предприятия.

Статистический анализ метода

Для анализа информационной безопасности в данной статье были рассмотрены несколько способов работы с данными, такие как сбор и систематизация данных пользователей открытых источников и ресурсов и мониторинг распределения ресурсов облачной инфраструктуры предприятия, которые в совокупности позволяют разработать модель поведения пользователей и объектов в системе для повышения уровня информационной безопасности [10].

Для исследования представим группы способов, предложенных в работе [4].

1. *Способ «Альфа»*. Характерной особенностью данного способа является пренебрежение параметрами самой методики обнаружения вторжений и разделения его на активные и неактивные стадии, когда 1-я категория может нести в себе определённую информацию о вторжениях, а 2-я категория предлагает к действию полиморфные алгоритмы и запутывает противника. Обобщенная структура компьютерной системы на основе способа может быть представлена с помощью выражения:

$$N = S(t) + I(t), \qquad (1)$$

где N – общее количество объектов в системе (общий диапазон до 1600 объектов во всех тестах); $S(t)$ – количество объектов без действий; $I(t)$ – количество объектов с действием (t – примерное время выполнения, до 200 с). У данного способа отсутствует учет топологических характеристик.

Графики зависимостей изменения количества узлов от времени функционирования распределенной информационной сети (РИС) в условиях распространения двумя ранее представленными способами приведены на рис. 5.

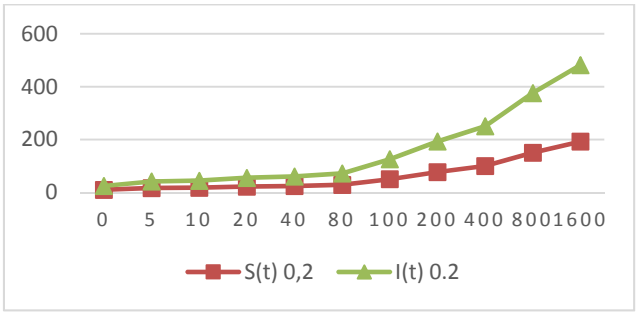


Рис. 5. Зависимости изменения количества узлов от времени функционирования РИС при β = 0,2

2. *Способ «Бета»*. Исследования показали, что способ «Бета» характеризуется наличием трех типов объектов управления: вторжение 1-й категории (I) и 2-й категории (S), 3-й категории с наличием вторжений (R). Обобщенная структура компьютерной системы на основе данного способа может быть представлена с помощью выражения:

$$N = S(t) + I(t) + R(t), \qquad (2)$$

где $R(t)$ – количество объектов с действием корреляционного анализа. С учетом топологических особенностей компьютерной сети (функции связности $f(c_i)$).

Графики зависимости изменения количества зараженных узлов от времени функционирования компьютерной системы в условиях распространения вторжения представлены на рис. 6. Топологические допущения условий моделирования аналогичны рис. 5.

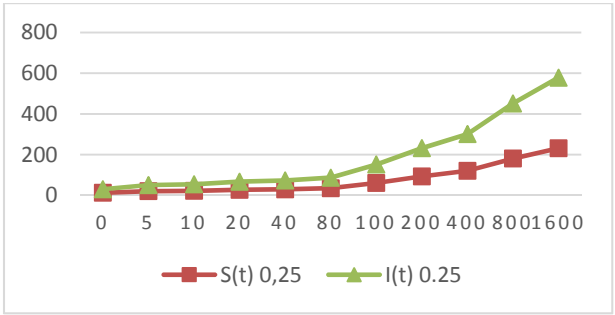


Рис. 6. Зависимости изменения количества узлов от времени функционирования РИС при β = 0,25, k = 0,02

3. *Способ «Гамма»*. Способ характеризуется наличием четырех типов объектов по двухэтапному сбору данных в предложенной методики: 1-й категории (I) и 2-й категории (S), 3-й категории с наличием вторжений (R) и найденные

объекты, а именно неудачные действия распределенной системы обнаружения вторжений (РСОВ) 4-й категории при необнаруженной угрозе (D). Этот способ, описывающий поведение системы в условиях воздействия злоумышленного ПО, содержит два этапа: 1) применение реверса; 2) добавление фактора лечения при повторном реверсе. Обобщенная структура РИС на основе способа «Гамма» может быть представлена с помощью выражения:

$$N = S(t) + I(t) + R(t) + D(t), \qquad (3)$$

где $D(t)$ – количество объектов, в которых обнаружено вторжение, запущенное с помощью РСОВ.

Анализ графиков рис. 7 и 8 показал, что в соответствии со способом «Гамма» происходит замедление процесса обнаружения вторжений в 1,65 раз и уменьшение максимального количества обнаруженных деструктивных действий в 1,1 раз. Это приводит к замедлению процесса выявления вторжений до 1,01 раз.

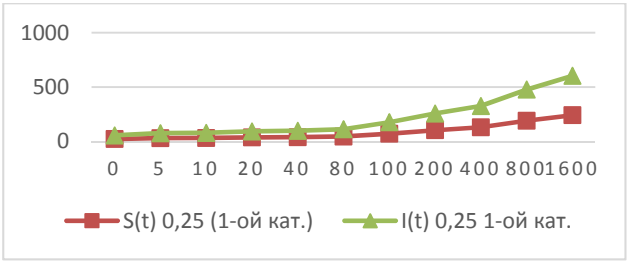


Рис. 7. Зависимости изменения количества узлов от времени функционирования РИС (первый этап сбора данных) при β = 0,25, k = 0,02

Проведенный анализ способа «Гамма» показал [3], что разбиение модели распространения компьютерных угроз на два этапа по методике сбора данных дает возможность независимого анализа процесса обнаружения вторжений.

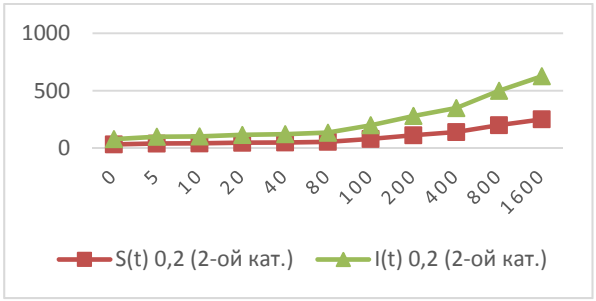


Рис. 8. Графики зависимости изменения количества узлов от времени функционирования РИС (второй этап сбора данных), при β = 0,25, k = 0,02

На рис. 9 дана оценка вероятности обнаружения вторжений в ходе различных атак на защищенную РИС, при этом для наглядности приведены сравнительные данные по различным категориям обнаружения вторжений [2].

В общем результате анализа графика на рис. 9 получается, что по совершенным операциям распространение ошибок в предлагаемой РСОВ значительно возрастает при обработке по категориям Б и В, однако их уровень не так критичен. Единственным объяснением этим расчетам является то, что при возрастании количества ошибок операция по обнаружению вторжений повышает риски для РИС. В любом из проведенных тестов вероятности по успеху различного рода атак практически никогда не доходили до 100 %, в то время как вероятности по необнаружению многих действий нарушителя были всегда выше 50 %.

В настоящее время основные данные для статистики компьютерных атак (более 4 000 000 в 2012 году по статистике, собранной антивирусными средствами лаборатории Касперского) дают базы данных компьютерных атак, размещенные в сети Интернет и поддерживаемые крупными организациями-разработчиками систем обнаружения компьютерных атак, общего программного обеспечения и исследовательскими центрами [1, 2].

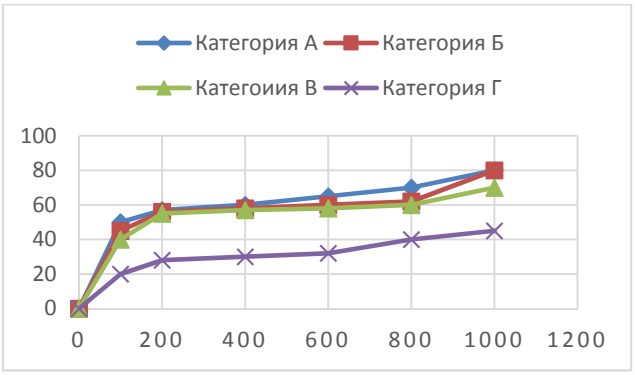


Рис. 9. Оценка вероятности обнаружения вторжений РСОВ в ходе различных атак (синего цвета – для категории А, красного – для категории Б, серого – для категории В, желтого – для категории Г)

Под противодействием компьютерным атакам на РИС понимаются взаимосвязанные процессы предупреждения о фактах угроз подготовки к реализации компьютерных атак [11], обнаружения признаков атак, анализа параметров атак и активного противодействия источникам атаки [12], а также комплексная защита РИС от подобных воздействий.

Заключение

Технологии машинного обучения могут быть использованы для создания динамических моделей поведения пользователей, наиболее полно раскрывающих специфику обязанностей сотрудников и позволяющих динамически распределять их нагрузку. С помощью данных технологий, в зависимости от временных рамок, можно увеличивать или уменьшать загрузку ресурсов облачной инфраструктуры предприятия, а также варьировать информационные ресурсы для выполнения должностных обязанностей сотрудников в зависимости от специфики их деятельности. Машинное обучение является необходимым инструментом для обеспечения информационной безопасности предприятия, основывающимся на рассмотренных в данной статье способах работы с информацией.

Литература

1. Штеренберг С.И. Анализ использования эквивалентных инструкций при скрытом встраивании информа-

ции в исполняемые файлы / С.И. Штеренберг, А.В. Красов, И.А. Ушаков // Журнал теоретических и прикладных информационных технологий. – 2015. – Т. 80. – № 1. – С. 28–34.

2. Штеренберг С.И. Методика применения самомодификации файлов для скрытой передачи данных в экспертной системе / С.И. Штеренберг, Р.И. Кафланов, А.С. Дружин, С.С. Марченко // Наукоемкие технологии в космических исследованиях Земли. – 2016. – Т. 8. – № 1. – С. 71–75.

3. Штеренберг С.И. Методика применения в адаптивной системе локальных вычислительных сетей стеговложения в исполнимые файлы на основе самомодифицирующегося кода / С.И. Штеренберг // Системы управления и информационные технологии. – 2016. – Т. 63. – № 1. – С. 51–54.

4. Красов А.В. Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код / А.В. Красов, А.С. Верещагин, А.Ю. Цветков // Телекоммуникации. – 2013. – № S7. – С. 27–29.

5. Красов А.В. Методы скрытого вложения информации в исполняемые файлы / А.В. Красов, А.С. Верещагин, В.С. Абатуров // Известия Санкт-Петербургского государственного электротехнического университета ЛЭТИ. – 2012. – № 8. – С. 51–55.

6. Виткова Л.А. Исследование распределённой компьютерной системы адаптивного действия / Л.А. Виткова // Наукоемкие технологии в космических исследованиях Земли. – 2015. – Т. 7. – № 5. – С. 44–48.

7. Коржик В.И. Метод обнаружения стегосистем на основе анализа статистики криптограмм, формируемых при помощи шифрования вкладываемых сообщений / В.И. Коржик, М.В. Токарева // Актуальные проблемы инфотелекоммуникаций в науке и образовании : сб. научных статей V международной научно-технической и научно-методической конференции. – 2016. – С. 431–436.

8. Буйневич М.В. Метод алгоритмизации машинного кода телекоммуникационных устройств / М.В. Буйневич, К.Е. Израилов // Телекоммуникации. – 2012. – № 12. – С. 2–6.

9. Кузнецов И.А. Способ управления информационно-вычислительной сетью на основе краткосрочного прогнозирования распространения компьютерного вируса / И.А. Кузнецов, В.А. Липатников, Д.В. Сахаров // Актуальные проблемы инфотелекоммуникаций в науке и образовании : сб. научных статей V международной научно-технической и научно-методической конференции. – 2016. – С. 441–446.

10. Штеренберг С.И. Методы построения цифровой стеганографии в исполнимых файлах на основе и принципах построения самомодифицирующегося кода / С.И. Штеренберг // Известия высших учебных заведений. Технология легкой промышленности. – 2016. – Т. 31. – № 1. – С. 28–36.

11. Зегжда П.Д. Основные направления развития средств обеспечения информационной безопасности / П.Д. Зегжда // Проблемы информационной безопасности. Компьютерные системы. – 1999. – № 1. – С. 27.

12. Зегжда П.Д. Использование искусственной нейронной сети для определения автоматически управляемых аккаунтов в социальных сетях / П.Д. Зегжда, Е.В. Малышев, Е.Ю. Павленко // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 4. – С. 9–15.

The Analysis of Information Security of the Enterprise on the Basis of Monitoring of Information Resources with use of Machine Learning

M.O. Kalinin
The Peter the Great St. Petersburg Polytechnic University
Saint-Petersburg, Russia
max@ibks.spbstu.ru

S.I. Shterenberg
The Bonch-Bruevich Saint-Petersburg State University
of Telecommunications, Saint-Petersburg, Russia
shterenberg.stanislaw@yandex.ru

Abstract. **This article discusses the method of using machine learning to ensure information security of an enterprise. To analyze the information without the risk of conducting analysis in real time. Machine learning is used to more accurately determine the deviant behavior of the user and the objects in the information system. The described methods make it possible to create a reliable distributed intrusion detection system.**

Keywords: **machine learning, Python, information security, auditing, monitoring, intrusion detection.**

REFERENCES

1. Shterenberg S.I. Analysis of using equivalent instructions at the hidden embedding of information into the executable files [Analiz ispolzovania ekvivalentnih instrukcii pri skritom vstraivanii v ispolniaemie faili] / S.I. Shterenberg, A.V. Krasov, I.A. Ushakov // Journal of Theoretical and Applied Information Technology. [Zhurnal teoreticheskikh I prikladnikh informationnikh tekhnologiy] 2015. – T. 80. – № 1. – C. 28–34. (In Rus.)

2. Shterenberg S.I. Self-modification method of application files for secure communication in the expert system. [Metodika primenenia samomodifikatsii failov dlia skritoy peredachi dannih v ekspertnoy sisteme] / S.I. Shterenberg, R.I. Kaflanov, A.S. Druzhin, S.S. Marchenko // High technology in space-based Earth research. [Naukoyemkir tekhnologii v kosmichiskikh issledivaniyakh Zemli] 2016. – T. 8. – № 1. – S. 71–75. (In Rus.)

3. Shterenberg S.I. Method of use in the adaptive system of local area networks hidden embedding in executables based on self-modifying code. [Metodika primenenia v adaptivnoy sisteme lokalnikh vichislitilnikh setey stegovloginia v ispolnimye fayly na osnove somomodifitsiruyushchegosya koda] / S.I Shterenberg // Control Systems and Information Technology. [Sistemy upravlenia I informatsionnie tekhnologii] 2016. – T. 63. – № 1. – S. 51–54. (In Rus.)

4. Krasov A.V. Software Authentication using embedding digital watermarks into executable code [Autentifikatiya programmnogo obespecheniya pri pomoshchi vlogenia tsifrivikh vodianikh znakov v ispolniaemiy kod] / A.V. Krasov, A.S. Vereshchagin, A.Y. Tsvetkov // Telecommunications. [Telekommunikatsii] 2013. – № S7. – S. 27–29. (In Rus.)

5. Krasov A.V. Methods of hidden information in the attachment executable files [Metodi skritogo vlogenia informatiy v ispolniaemie fayly] / A.V. Krasov, A.S. Vereshchagin, V.S. Abaturov // Proceedings of the St. Petersburg State Electrotechnical University LETI. [Izvestia SPb gosudarstvennogo elektrotekhnicheskogo universiteta LETI] 2012. – № 8. – S. 51–55. (In Rus.)

6. Vitkova L.A. Study of adaptive distributed computing system actions [Issledovaniye raspredelennoy kompiuternoy sistemy adaptivnogo deystviya] / L.A. Vitkova // High Tech Earth in space research. [Naukoyemkir tekhnologii v kosmichiskikh issledivaniyakh Zemli] 2015. – T. 7. – № 5. – S. 44–48. (In Rus.)

7. Korzhik V.I. Stegosystems detection method based on the analysis of cryptograms statistics generated by encrypting invested posts [Metod obnarugenia stegosistem na osnove analiza statistki kriptogrammi, formiruemih pri pomoshi shifrivania vkladivaemih soobshcheniy] / V.I. Korzhik, M.V. Tokarev // In: Recent infotelecommunications problems in science and education collection of scientific articles V International scientific and methodological conference. [V sbornike: Aktualnie problemy infotelekommunikatsiy v nauke I obrazovanii sbornik nauchnikh statey V mezhdunarodnoy nauchno-tekhnicheskoy I nauchno metodicheskoy konferentsii] 2016. – pp 431–436. (In Rus.)

8. Buinevich M.V. Algorithmizing Method Machine Code telecommunication devices [Metod algoritmizacii mashinnogo koda telekommunikacionnikh ustroistv] / M.V. Buinevich, K.E. Israel // Telecommunications. [Telekommunikatsii] 2012. – № 12. – S. 2–6. (In Rus.)

9. Kuznetsov I.A. The process control computer and information network based on short-term forecasting the spread of a computer virus [Sposob upravlenia informationno vichislitelnoy setiy na osnove kratkosrochnogo prognozirovania rasprostranenia kompiuternogo virusa] / I.A. Kuznetsov, V.A. Lipatnikov // In: Recent infotelecommunications problems in science and education collection of scientific articles V International scientific and methodological conference. [V

sbornike: Aktualnie problemy infotelekommunikatsiy v nauke I obrazovanii sbornik nauchnikh statey V mezhdunarodnoy nauchno-tekhnicheskoy I nauchno metodicheskoy konferentsii] 2016. – pp. 441–446. (In Rus.)

10. Shterenberg S.I. Methods for constructing digital steganography in executable files based on the principles of constructing a self-modifying code [Metody postroeniya tsifrovoi staganografiy v ispolnimih faylakh na osnove i prontsipakh postroeniya somomodifitsiruyushchegosya koda] / S.I. Shterenberg // News of higher educational institutions. Light industry technology. [Izvestia vysshikh uchebnikh zavedeniy. Tekhnologiya legkoy promyshlennosti] 2016. – V. 31. – No. 1. – S. 28–36. (In Rus.)

11. Zegzhda P.D. The main directions of development of information security tools [Osnovnie nepravlenia razvitia sredstv obespechenia informacionniy bezopasnosti]/ P.D. Zegzhda // Problems of information security. Computer systems. [Problemy informatsionnoy bezopasnosti. Kompiuternii sistemy] 1999. – № 1. – S. 27. (In Rus.)

12. Zegzhda P.D. Using an artificial neural network to determine automatically managed accounts in social networks [Ispolzovania iskusstvennoy neironnoy seti dlia opredelenia avtomaticheski upravliaemikh akkauntov v socialnikh setiakh] / P.D. Zegzhda, E.V. Malyshev, E.Yu. Pavlenko // Problems of information security. Computer systems. [Problemy informatsionnoy bezopasnosti. Kompiuternii sistemy] 2016. – No. 4. – P. 9–15. (In Rus.)