INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT

UDC 681.3
https://doi.org/10.23947/2687-1653-2022-22-1-57-66

Original article

Challenge of the performance management of trust control systems with deep learning

Aleksandr A. Zelensky ✉, **Tagir K. Abdullin**, **Marina M. Zhdanova**, **Vyacheslav V. Voronin**, **Andrey A. Gribkov**
Moscow State Technological University "STANKIN" (Moscow, Russian Federation)
✉ Zelenskyaa@gmail.com

Introduction. The significance of machine learning under the conditions of digital transformation of industry, and methods of implementing deep learning to provide the performance of trust management systems are considered. The necessity of using convolutional artificial neural networks for deep machine learning is determined. Various technologies and architectures for the implementation of artificial neural networks are briefly considered; a comparative analysis of their performance is carried out. The work objective is to study the need to develop new approaches to the architecture of computing machines for solving problems of deep machine learning in the trust management system implementation.

Materials and Methods. In the context of digital transformation, the use of artificial intelligence reaches a new level. The technical implementation of artificial neural systems with deep machine learning is based on the use of one of three basic technologies: high performance computing (HPC) with parallel data processing, neuromorphic computing (NC), and quantum computing (QC).

Results. Implementation models for deep machine learning, basic technologies and architecture of computing machines, as well as requirements for trust assurance in control systems using deep machine learning are analyzed. The problem of shortage of computation power for solving such problems is identified. None of the currently existing technologies can solve the full range of learning and impedance problems. The current level of technology does not provide information security and reliability of neural networks. The practical implementation of trust management systems with deep machine learning based on existing technologies for a significant part of the tasks does not provide a sufficient level of performance.

Discussion and Conclusions. The study made it possible to identify the challenge of the computation power shortage for solving problems of deep machine learning. Through the analysis of the requirements for trust management systems, the external challenges of their implementation on the basis of existing technologies, and the need to develop new approaches to the computer architecture are determined.

Keywords: deep machine learning, processor, trust system, information security, computer, artificial intelligence.

For citation: A. A. Zelensky, T. K. Abdullin, M. M. Zhdanova, V. V. Voronin, A. A. Gribkov. Challenge of the performance management of trust control systems with deep learning. Advanced Engineering Research, 2022, vol. 22, no. 1, pp. 57–66. (In Russ). https://doi.org/10.23947/2687-1653-2022-22-1-57-66

Funding information: the research is done on the Russian Science Foundation grant no. 21-79-10392, https://rscf.ru/project/21-79-10392/

Introduction. Over the past 9 years, the fourth industrial revolution has been taking place on an increasingly large scale in the world, including in Russia. One of its key components is digital transformation affecting all aspects of economic life — from a large-scale industrial production to the service sector, science, education, and households. Under these conditions, the use of the machine in tasks with which a person does not cope or copes worse than the machine, significantly expands. If earlier it was about the mechanization of manual labor and production automation, now a human being can be replaced by a machine in solving the problems of data processing, analysis, forecasting and management of various systems: equipment, engineering processes, industrial enterprises, retail chains, etc.

The practical basis for replacing a human being with a machine in certain areas of intellectual activity is the use of artificial intelligence. The creation of a "strong" artificial intelligence is a task of the future, associated with the need to create and develop new technologies, as well as solving significant ethical problems. Currently, machine learning systems of varying complexity are available for application, representing a step towards creating a "strong" artificial intelligence.

The global market for machine learning systems is expanding rapidly. In 2020, its volume amounted to $11.33 bln, in 2021, it grew to $15.50 bln, and by 2028, it will reach $152.24 bln, showing an average annual growth of 38.6 %[1].

The scope of machine learning systems is very large and includes marketing and trade, banking, industrial production, medicine, etc. Machine learning systems are most in demand in the following industries:

— robotics for the intellectualization of industrial and service robots, including collaborative ones;
— automated control systems for processes and enterprises;
— production process control systems;
— supply chain and customer relationship management systems;
— executive production systems;
— production analytics systems for process equipment;
— business intelligence systems, etc.

Complex process systems, e.g., implemented in the designs of machine tools with real-time numerical control, currently cannot be equipped with control systems suitable for machine learning. This requires computing power capable of performing significant computations in tens of microseconds. Such a problem cannot be solved with the help of modern technical means. Therefore, in most cases, the process of machine learning of the control system is carried out on computers separated from it without time limits, and then the learning results are transferred to the control system in the form of recommendations, instructions on operating modes, tool changes, verification intervals, etc.

Machine learning methods conditionally correspond to the types of inferences that underlie them: induction, deduction, and traduction. The case-based supervised learning method, when large amounts of data prelabeled by a human operator are loaded into the machine, corresponds to induction. The unsupervised learning method, when the machine itself must find patterns in the data, identify patterns, arrange and structure the data, corresponds to induction and traduction. The expert method based on the use of specified patterns and patterns for data processing correspond to deduction and traduction. Traduction is implemented mainly through the use of transfer learning, based on the application to a given task of knowledge gained in solving another task.

Machine learning uses various technologies and mathematical models. The model of artificial neural networks (ANN), built by analogy with biological neural networks, i.e., networks of nerve cells of a living organism, has the greatest potential for development. ANN is a system of interconnected and interacting artificial neurons implemented in the form of processors, processor elements in the form of accelerators or coprocessors under the control of a central

[1] Machine Learning Market, 2021-2028. Hardware & Software IT Services Market Research Report. 2021. P. 160. URL: https://www.fortunebusinessinsights.com/infographics/machine-learning-market-102226 (accessed: 06.11.2021)

processor. ANN neurons are located in levels (layers). The first level corresponds to receiving, processing input data, and passing them to the next level. Intermediate levels are hidden, their task is to process incoming data and transfer it to the last (output) level. A neural network may have several hidden levels interspersed with levels where logical, mathematical, and other transformations are performed. From level to level, the data is processed, at each subsequent level, the relationships of the previous one, are identified. Such a multi-level ANN has great potential and can be used to implement deep machine learning [1–3].

Deep machine learning is an ANN design method using multilayer filters to extract and model features from a set of input data[2]. Such learning can be supervised or unsupervised. It is also possible to use deep machine learning for expert systems.

The technical implementation of artificial neural systems with deep machine learning is based on the application of one of three basic technologies: high-performance computing with parallel data processing, neuromorphic and quantum computing[3].

Materials and Methods

High-performance computing. High-performance computing with parallel data processing is implemented through hybrid computing systems, i.e., systems with a heterogeneous hardware computing structure, including a central processing unit (CPU) and an additional computing module in the form of an accelerator or coprocessor. Depending on the processors used for parallel data processing, hybrid computers have one of four architectures:

1. Graphic processing unit (GPU) based architecture. The most common solutions are graphics accelerators that expand the computing capabilities of the central processing unit of a computer system. The latest advances in this field are NVIDIA Tesla V100 graphics accelerators, providing 120 TFLOPS performance for deep machine learning tasks, i.e., 1.2×1014 floating-point operations per second[4].This is 500-1000 times higher than the performance of an ordinary personal computer (PC). It should also be taken into account that the specified performance is provided when solving problems that require significant computing power and significant time costs, but not when working in real time. Currently, GPU-based architecture is the most accessible one. In particular, to implement a system with limited computing power, it is enough to have a video card with a NVidia graphics processor on a PC that implements the CUDA parallel computing hardware and software architecture. Along with CUDA, GPGPU technologies that use the graphics processor of a video card for computer graphics to perform mathematical calculations include AMD FireStream technology (for ATI graphics processors). The global GPU market is currently around $26 bln and is growing at a rate of up to 34% per year[5].

2. Architecture based on field-programmable gate arrays (FPGA) — semiconductor devices that can be reprogrammed and change the topology of connections in use. The rated performance of these devices is relatively low — about 20 TFLOPS, however, the efficiency of using computing power is the highest among all the considered architectures. It is 6-7 times higher than that of graphics accelerators. The high efficiency of FPGA is due to the flexibility and speed of adjustment to the computational tasks being solved. According to Grand View Research, in 2020, the global FPGA market amounted to $ 9.85 bln, the expected market growth rate for the period up to 2027 is 9.7% per year[6].

[2] Glek P. Deep Learning: short tutorial. neurohive.io. URL: https:// neurohive.io /ru/osnovy-data-science/glubokoe-obuchenie-deep-learning-kratkij-tutorial/ (accessed: 06.11.2021) (In Russ.)
[3] Kak sokratit' izderzhki pri ispol'zovanii II. HitachiVantaraCorporation. URL: https://hitachi.cnews.ru/articles/2021-06-14_kak_sokratit_izderzhki_pri_ispolzovanii (accessed: 07.11.2021) (In Russ)
[4] Kak sokratit' izderzhki pri ispol'zovanii II. Op. cit.
[5] Global Graphics Processing Unit (GPU) Market Insights and Forecast to 2027. QYResearch. 2021. P. 116. URL: https://reports.valuates.com/market-reports/QYRE-Auto-25V3358/global-graphics-processing-unit-gpu (accessed: 10.11.2021)
[6] Field Programmable Gate Array Market, 2020 — 2027. Grand View Research, 2020. P. 130. URL: https://www.grandviewresearch.com/industry-analysis/fpga-market (accessed: 11.11.2021)

3. Architecture based on the advanced special integrated circuit (ASIC). Due to the narrow specialization of the computational problems to be solved, they can be much simpler, cheaper, and more compact. ASIC performance can reach 1000 TFLOPS, but the efficiency of using computing power, e.g., the number of recognized images, is about 2 times lower than in graphics accelerators. The growth rate of the ASIC market is significantly lower than that of the GPU market. In 2020, according to Global Industry Analysts, the global ASIC market amounted to $17.3 billion, the expected average annual market growth until 2027 is 7.7%[7].

4. Architecture based on single-chip accelerators (SoC). “System on a chip” SoC is a fully functional electronic device that has a motherboard, processor, and other components required for operation, placed on a single integrated circuit. SoC are common in mobile computers (smartphones), single board computers, and other embedded systems. At the same time, SoC have a significant potential use as part of hybrid computers. In addition, solutions are possible in the form of a single-chip SoC assembly with FPGA elements (Xilinx[8] Versal architecture for adaptive computing). The SoC market is currently very large, and it was worth $79.7 bln in 2020. For the period up to 2027, the market is projected to grow by 4.4% per year, by 2027, the market volume will reach $107.4 bln $[9].

Figures 1 and 2 show data on the actual and projected growth of the global market for chips for deep machine learning, prepared by Omdia[10] consulting company.

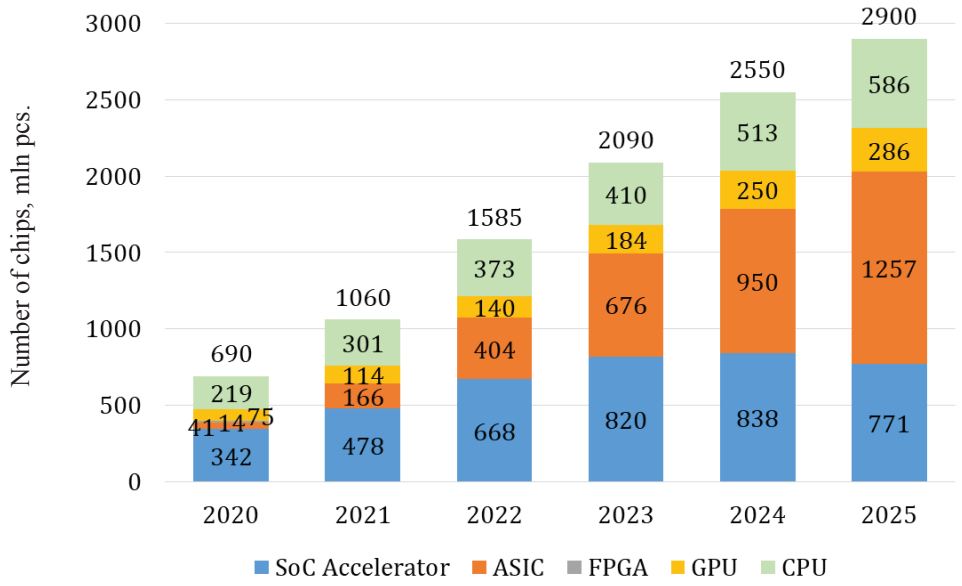

Fig. 1. Growth dynamics of number of chips for deep learning year-wise

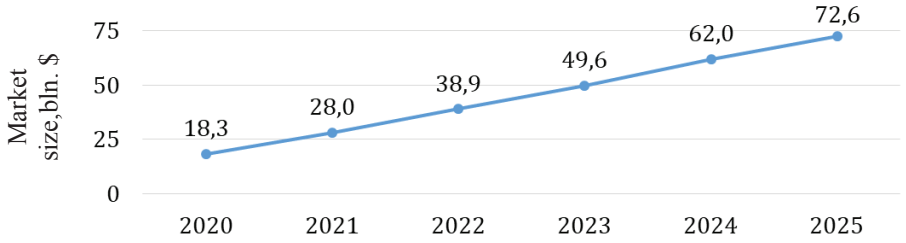

Fig. 2. Dynamics of the market for deep learning chips year-wise[11]

[7] ASIC - Global Market Trajectory & Analytics April 2021. Global Industry Analysts, Inc.; 2021. P. 185. URL: https://www.researchandmarkets.com/reports/5140939/asic-global-market-trajectory-and-analytics (accessed: 11.11.2021)
[8] Michael Feldman. Xilinx Unveils Its Most Ambitious Accelerator Platform. 2018. URL: https://www.top500.org/news/xilinx-unveils-its-most-ambitious-accelerator-platform/ (accessed: 10.11.2021)
[9] System-On-A-Chip (SoC) - Global Market Trajectory & Analytics. Report, April 2021. Global Industry Analysts, Inc.; 2021. URL: https://www.researchandmarkets.com/reports/2832316/system-on-a-chip-soc-global-market-trajectory (accessed: 11.11.2021)
[10] Joshi A. Deep Learning Chipsets Report – 2020. Omdia Marke, 2020. URL: https://omdia.tech.informa.com/products/deep-learning-chipsets-report---2020 (accessed: 11.11.2021)
[11] Joshi A. Deep Learning Chipsets Report – 2020. Op cit. (accessed: 12.11.2021)

The analysis shows that against the background of the general growth of the market, ASIC have the greatest prospects, GPU and SoC will also retain significant positions. For a fairly long term, GPU accelerators do not have an adequate replacement for solving complex problems, including in the learning process, and SoC are indispensable for mobile implementations of deep machine learning systems, as well as for parallel computing to offload the central processor. Rejection of FPGA in deep machine learning systems seems optional, although the share of such processors is likely to be relatively small.

One of the most promising directions in the development of hybrid computers is the use of tensor and other specialized coprocessors, such as machine vision processors. Such coprocessors can be based on the most common and high-performance ASIC, as well as FPGA or GPU. The difference between coprocessors and accelerators is in the degree of integration with the central processor. The central processor translates control instructions to the accelerator through a special memory area. The coprocessor monitors the flow of machine code instructions from RAM to the CPU and intercepts instructions appropriate to its functional purpose, such as tensor transform tasks, pattern recognition, etc. To solve large-scale problems that require long-term distributed computing, it is advisable to use an accelerator; for frequent and repeated execution of simple computing tasks, use a coprocessor, in which the central processor is not loaded and does not slow down data processing.

The operational properties of computers depend significantly on the architecture used. For solving deep machine learning problems, where up to 80% of computing power is spent, machines based on graphics accelerators are best suited. They have high performance in solving complex tasks that require a significant investment of time, have high flexibility and maximum calculation accuracy, but low relative performance. Specifically, for NVidia processors, it is 1.3–1.8 GOPS/W. ASIC-based computers have the highest absolute and relative performance. For neuIBM processors, e.g., the relative performance is 254 GOPS/W [4]. However, such machines have low flexibility and limited accuracy, so, it is advisable to use them when solving typical, e.g., matrix or tensor transformations, repetitive or multi-threaded tasks in real time.

FPGA-based computers have high parameters of flexibility, accuracy, absolute and relative performance. For Tegra TX1 processors, e.g., the relative performance is 70 GOPS/W. However, such machines have a relatively high cost, so it is advisable to use them for scientific purposes, when only a few computers of a given configuration are required, as well as for developing the architecture of mass-produced ASIC and SoC processors.

Despite the improvement in the architecture of computers, the potential for growth in capacities for high-performance computing will soon be exhausted. The number of transistors on a chip over the past 5 years has increased by about 12 times [5], and the amount of calculation in the process of machine learning has increased by 150 thousand times[12].

Neuromorphic computing. A possible way to address the lack of computing power for artificial neural systems with deep machine learning is to use neuromorphic computing and related chips. A neuromorphic chip is a processor based on the principles of the human brain. Such a chip simulates the work of neurons and their processes — axons and dendrites, which are responsible for the data transmission and perception. Connections between neurons are formed by synapses — special contacts through which electrical signals are transmitted.

Some of the best-known developments in this area include IBM TrueNorth neuromorphic processors and Intel Loihi processors. They use an asynchronous cluster architecture and a convolutional neural network model — a unidirectional multilayer network with alternating convolutional and subsampling layers. TrueNorth processor is based on 28 nm technologies, Loihi — on 14 nm [6].

[12]Thompson NC, Greenewald K, Lee K, et al. The Computational Limits of Deep Learning. arXiv preprint arXiv:2007.05558. 2020 (accessed: 12.11.2021)

TrueNorth NS16e-4 multiprocessor system, containing 100 mln neurons and designed to work with networks for deep machine learning, was introduced by IBM in 2018 [7]. Each chip contains 1 mln digital neurons and 256 mln synapses enclosed in 4096 synapse nuclei; power consumption of each chip is 70 mW.

Loihi processor, introduced in 2017, contains 131,000 artificial neurons and 131 mln synapses. In 2019–2020, Intel introduced two products based on Loihi — PohoikiBeach and PohoikiSprings. PohoikiBeach computing system, which includes 64 Loihi processors, has a total of 8.32 mln neurons and 8.32 bln synapses. PohoikiSprings Computing System Includes 768 Loihi processors, 100 mln neurons, and 100 bln synapses[13].

In Russia, work on the creation of neuromorphic processors has been going on for several years. In 2020, Motive Neuromorphic Technologies created the Altai neurochip [8]. The processor technology standard is 28 nm, power consumption is about 0.5 W, the crystal area is 64 mm^2 (for comparison: TrueNorth - 430 mm^2, Loihi - 60 mm^2). It has 131 thousand neurons, between them, there are 67 mln connections.

To assess the quality of neuromorphic processors, the following is used:

1. Absolute performance indicator. This is the number of billions of synoptic operations performed per second (GSOPS).

2. Energy efficiency indicator. This is the number of picojoules of energy expended in performing one synaptic operation (pJ/SOP).

TrueNorth processor has a performance of 58 GSOPS and an energy efficiency of 26 pJ/SOP[14]. Similar power efficiency (23.7 pJ/SOP [9]) is provided by Loihi processor.

The only competitor of neuromorphic processors in the implementation of neural networks with deep machine learning in the midterm (8–12 years) is hybrid computers with ASIC coprocessors. Such processors have a lower but comparable performance of synaptic operations and higher energy efficiency. In particular, ASIC processor described in [10] provides a synaptic performance of 8.7 GSOPS and an energy efficiency of 15.2 pJ/SOP.

The global market for neuromorphic chips is relatively new and therefore small. In 2020, its volume amounted to only $22.5 mln. At the same time, the growth rate of the market is very high. By 2026, the market will grow to $333.6 mln, which corresponds to an average annual growth of 47.4%[15].

Sometimes neuromorphic chips are understood as all types of processors that externally reproduce the work of neurons, regardless of the internal structure of the technical device, which may not correspond to the nature of the interaction of neurons. Such processors used to build artificial neural networks are properly called neural. Along with neuromorphic chips, neural processors also include processors (chips) with tensor and other specialized coprocessors for machine vision, speech recognition, etc. The world market for neural processors currently stands at $2.3 bln, and, by 2027, it will grow to $10.4 bln, thus, the average growth will be 24.2% per year[16].

Quantum computing. In the long term, the development of quantum computing can become a means of eliminating the shortage of computing power. Quantum computing solves problems through manipulating quantum objects: atoms, molecules, photons, electrons, and specially created macrostructures. Manipulations of quantum objects provide using:

— quantum superposition, which manifests itself in the ability of quantum systems to simultaneously be in all possible states;

[13] Intel Scales Neuromorphic Research System to 100 Million Neurons. Intel, 2020. URL: https://newsroom.intel.com/news/intel-scales-neuromorphic-research-system-100-million-neurons/?utm_source=ixbtcom#gs.7oc6iw (accessed: 12.11.2021)
[14] Neurochip “Altai”. motivnt.ru. URL: https://motivnt.ru/neurochip-altai/ (accessed: 10.11.2021) (In Russ.).
[15] Neuromorphic Chip Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026). Mordor Intelligence, 2020. URL: https://www.mordorintelligence.com/industry-reports/neuromorphic-chip-market (accessed: 11.11.2021)
[16] Neuromorphic Chips - Global Market Trajectory & Analytics. Global Industry Analysts, Inc. 2021. 118 p. URL: https://www.researchandmarkets.com/reports/4805280/neuromorphic-chips-global-market-trajectory-and (accessed: 10.11.2021)

— quantum entanglement, which manifests itself in a strong relationship between the parameters of specially prepared quantum systems.

Devices for quantum computing are usually divided into two large classes [11]: general purpose quantum computers and quantum simulators. The former, like central processing units, can solve any algorithmic problem, and quantum simulators are analog computers for solving highly specialized problems.

Technologies for creating universal quantum computers are currently at the stage of formation. The created computers demonstrate "quantum superiority" in solving certain problems, but so far, they cannot be used to form artificial neural networks with deep machine learning. Companies that are most active in creating a quantum computer include:

1. Google. In 2018, a 72-qubit Bristlecone quantum processor was built, in 2019, a more accurate 53-qubit Sycamore quantum processor was built.
2. Intel. A 49-qubit TangleLake superconducting quantum chip was built in 2018.
3. IBM. In 2017, a 50-qubit quantum processor was created and tested, in 2019 — the world's first commercial 20-qubit quantum computer IBM Q SystemOne, etc.

The only adiabatic quantum computer on the market is D-WaveSystems, available in 16 to 2000 qubits, arranged in clusters of 8 qubits each.

The field of quantum simulators is also rapidly developing. One of the most complex simulators of this type is a 2017 joint development of the University of Maryland and the National Institute of Standards and Technology (USA). This 53-qubit simulator uses cold ytterbium ions as qubits. A similarly capable 51-qubit quantum simulator based on rubidium atoms was developed by a group of scientists at Harvard University and Massachusetts Institute of Technology.

A number of projects developing quantum computing technologies are also being implemented in Russia. In particular, for several years now, the development of a superconducting processor has been carried out by scientists from a consortium, which includes National University of Science and Technology (MISIS), Osipyan Institute of Solid State Physics of the Russian Academy of Sciences (ISSP RAS), Institute of Solid State Physics, Bauman Moscow State Technical University (MBSTU), Dukhov Automatics Research Institute (VNIIA), and other organizations. To date, the consortium has debugged the technology for manufacturing superconducting two-qubit circuits, experimentally characterized and demonstrated two-qubit logic gates that perform quantum entanglement, which is required for the operation of quantum processors. The reliability of logical operations is in the range of 85–95%.

In 2020, $675 mln was invested in quantum computing in the world, which is more than 3 times the investment amount in 2019 ($211 mln). In 2021, the volume of investments in quantum computing exceeds $800 mln [12].

Trust management systems. One of the basic requirements for management systems, including production ones, is to provide them with the required level of trust. According to GOST R 54583-2011 "Information technology. Security techniques. A framework for IT security assurance. Part 3. Analysis of assurance methods", the purpose of providing credibility is to create confidence in the reliable functioning of the product under given conditions. To provide this, the information system must have the following operational properties [13]:

— functional reliability, i.e., the ability to perform its function with a given reliability, which in turn is normalized by the number of failures, the error and repeatability of the calculation results;

— information security, i.e., the ability to provide a given level of confidentiality, availability and integrity of information: stored, transmitted, received, and processed during the operation of the system.

The subject of this research is control systems that relate to information. Therefore, the above requirements for performance properties are also valid for them. However, management systems have their own specifics in the definition of trust. A trust control system must have:

— the ability to control, e.g., a robot, a machine tool, an enterprise, etc., according to a given number of parameters with a specified reliability, which is regulated by the number of failures, error, and repeatability, and with a given performance, which in turn is regulated by the time of data processing and execution of control commands;

— the ability to control the elements, structure and processes of the system at the hardware and software levels to provide information security.

If the control system has the function of deep machine learning, then the fulfillment of the first of these requirements imposes severe restrictions on the means of technical implementation used. This should be the optimal computer for the formation of a convolutional neural network with high parameters of performance, accuracy, and calculation reliability.

If we do not consider the option of using quantum processors, the full-featured implementations of which are not yet available, then neither hybrid computers based on all the considered architectures, nor computers based on neuromorphic processors fully comply with the first requirement. Computers based on ASIC and neuromorphic processors do not provide high accuracy and reliability, and hybrid computers with GPU or SoC accelerators are not optimal for real-time operation, including impedance.

A certain compromise is provided when using FPGA-based hybrid computers, however, such machines have a high cost in mass production, significantly lower performance than ASIC machines, and significantly less complex computing capabilities than GPU machines. Another compromise option is the simultaneous use of a CPU with a graphics accelerator to solve complex tasks in the process of machine learning and tensor or other highly specialized ASIC-based coprocessors for real-time data processing.

The second requirement, although technical in content, in practice acts as an economic one. The implementation of a control system for process equipment with deep machine learning is possible only through a convolutional neural network, the control of which from the outside is not possible. Information security can be only provided that the main part of the computer will be created by domestic manufacturers who have been certified in the field of information security.

At present, the main part of control systems in Russia is built on the basis of foreign microelectronic components. The share of such components exceeds 85% [14]. Providing information security in the case of using imported components in computers does not have an unambiguous solution and depends on the structure of the created artificial neural network and the order of its use. In particular, when using hybrid computers, information security can be significantly improved through localizing data transfer between the central processor and the accelerator or coprocessor.

Research Results. The analysis of deep machine learning models, basic technologies, and architecture of computers, as well as the requirements for providing confidence in control systems using deep machine learning, allows us to draw the following conclusions:

1. There is an objective problem of lack of computing power for solving problems of deep machine learning. None of the currently existing technologies can solve the full range of training and impedance problems.

2. Since deep machine learning is implemented on the basis of a model of convolutional neural networks, their external control to provide information security and reliability of work is not possible. The only option is developer control, which also has limited capabilities. This determines the need for the production of processors required for ANN in Russia.

3. The practical implementation of trust control systems with deep machine learning based on existing technologies for a significant part of the tasks in real time cannot be provided, for the other part of the tasks, such an implementation is associated with a significant drop in performance.

4. The performance gain of trust control systems can be based on improving the architecture of hybrid computers, including the simultaneous use of processors of different architectures that are optimal for solving the corresponding problems of analysis and control.

Discussion and Conclusions. This paper analyzes and discusses the relevance and implementation of machine learning in the context of digital transformation of industry. The scientific problem covered in the work is in the insufficient development of the technical level of modern computers to provide high performance of algorithms based on deep machine learning. Attention is drawn to the problem of information security, which is one of the prerequisites for the development of domestic processors for ANN. Based on the analysis of the requirements for trust control systems, the objective difficulties of their implementation based on existing technologies and the need to develop new approaches to the architecture of computers are determined.

References

1. Zelensky A, Semenishchev E, Alepko A, et al. Using neuro-accelerators on FPGAs in collaborative robotics tasks. SPIE Optical Instrument Science, Technology, and Applications II. 2021;11876:1187600. https://doi.org/10.1117/12.2600582

2. Zelenskii AA, Pismenskova MM, Voronin VV. Control of Collaborative Robot Systems and Flexible Production Cells on the Basis of Deep Learning. Russian Engineering Research. 2019;39:1065–1068. http://dx.doi.org/10.3103/S1068798X19120256

3. Voronin VV, Sizyakin RA, Zhdanova M, et al. Automated visual inspection of fabric image using deep learning approach for defect detection. Automated Visual Inspection and Machine Vision IV. 2021;11787:117870 http://dx.doi.org/10.1117/12.2592872

4. Phi-Hung Pham, Jelaca D, Farabet C, et al. NeuFlow: Dataflow Vision Processing System-on-a-Chip. In: Proc. IEEE 55th International Midwest Symposium on Circuits and Systems (MWSCAS). 2012. P. 1044–1047. http://dx.doi.org/10.1109/MWSCAS.2012.6292202

5. Shuremov EL. Whether it is worth being fond of big data? Accounting. Analysis. Auditing. 2020;7:17–29. https://doi.org/10.26794/2408-9303-2020-7-2-17-29

6. Jing Pei, Lei Deng, Sen Song, et al. Towards artificial general intelligence with hybrid Tianjic chip architecture. Nature. 2019;572:106–111. http://dx.doi.org/10.1038/s41586-019-1424-8

7. Modha D. TrueNorth: from zero to 64 million neurons. Open Systems. DBMS. 2019;3:8.

8. Akopyan A, Sawada J, Cassidy A, et al. TrueNorth: design and tool flow of a 65 mw 1 million neuron programmable neurosynaptic chip. IEEE transactions on computer-aided design of integrated circuits and systems. 2015;34:1537–1557. http://dx.doi.org/10.1109/TCAD.2015.2474396

9. Mike Davies, Narayan Srinivasa, Tsung-Han Lin, et al. Loihi: A neuromorphic manycore processor with on-chip learning. IEEE Micro. 2018;38:82–99. http://dx.doi.org/10.1109/MM.2018.112130359

10. Kim J, Koo J, Kim T, et al. Efficient synapse memory structure for reconfigurable digital neuromorphic hardware. Frontiers in neuroscience. 2018;12:829. http://dx.doi.org/10.3389/fnins.2018.00829

11. Fedorov A. Kvantovye vychisleniya: ot nauki k prilozheniyam. Open Systems. DBMS. 2019;3:14. (In Russ.)

12. Bobier J-F, Langione M, Tao E, et al. What Happens When 'If' Turns to 'When' in Quantum Computing? BCG Digital Transformation. 2021. 20 p.

13. Sabanov AG. Doverennye sistemy kak sredstvo protivodeistviya kiberugrozam. Zaŝita informacii. Inside. 2015;63:17–21.

14. Kalyaev IA, Melnik EV. Trusted control systems. Mechatronics, Automation, Control. 2021;22:227–236. https://doi.org/10.17587/mau.22.227-236 (In Russ.)

Received 27.12.2021
Revised 22.01.2022
Accepted 26.01.2022

About the Authors:

Zelensky, Alexander A., Director of the Institute of Digital Intelligent Systems, Moscow State University of Technology "STANKIN" (3a, Vadkovsky Lane, Moscow, 127005, RF), Cand.Sci. (Eng.), associate professor, ResearcherID, ScopusID, ORCID, Zelenskyaa@gmail.com

Abdullin, Tagir H., lecturer of the Industrial Electronics and Intelligent Digital Systems Department, Moscow State University of Technology "STANKIN" (3a, Vadkovsky Lane, Moscow, 127005, RF), senior engineer, ScopusID, ORCID, everestultimate@yandex.ru

Zhdanova, Marina M., Junior Research Scholar, Moscow State University of Technology "STANKIN" (3a, Vadkovsky Lane, Moscow, 127005, RF), ResearcherID, ScopusID, ORCID, mpismenskova@mail.ru

Voronin, Viacheslav V., Associate Director of the Center for Cognitive Technologies and Machine Vision, Moscow State University of Technology "STANKIN" (3a, Vadkovsky Lane, Moscow, 127005, RF), Cand.Sci. (Eng.), associate professor, ResearcherID, ScopusID, ORCID, voronin_sl@mail.ru

Gribkov, Andrey A., Director of the Analytical Center, Moscow State University of Technology "STANKIN" (3a, Vadkovsky Lane, Moscow, 127005, RF), Dr.Sci. (Eng.), professor, ResearcherID, ScopusID, ORCID, andarmo@yandex.ru

Claimed contributorship

A. A. Zelensky: basic concept formulation; research objectives and tasks setting; text preparation; formulation of conclusions. T. H. Abdullin and M. M. Zhdanova: conducting research; analysis of existing approaches. V. V. Voronin and A. A. Gribkov: analysis of the research results; the text revision; correction of the conclusions.

All authors have read and approved the final manuscript.