Intrusion detection system on the basis of data mining algorithms in the industrial network

M A Gurin[1], A M Vulfin[1], V I Vasilyev[1] and A V Nikonov[1]

[1]Ufa State Aviation Technical University, K. Marks st., 12, Ufa, Russia, 450008

e-mail: vulfin.alexey@gmail.com, nikonovandrey1994@gmail.com

Abstract. The purpose of the work is to increase the security of the industrial network of an automated process control system based on intelligent network traffic analysis algorithms. The analysis of the problem of detecting and recording actions of violators on the implementation of a network attack on an automated process control system in the industrial network of an enterprise has been performed. A structural and functional model of the monitoring system of the industrial network of industrial control systems is proposed. An algorithm is developed for the intellectual analysis of network traffic of industrial protocols and a software package that implements the proposed algorithms as part of a monitoring system to evaluate the effectiveness of the proposed solution on field data.

1. Introduction

Security of the critical infrastructure of automated process control system (APCS) [1] under the conditions of the automation level of modern production in the Russian Federation and around the world is becoming an increasingly priority task. The imperfection of the protection and vulnerability of modern SCADA-systems (Supervisory Control and Data Acquisition systems) is due to a number of features of the organization of such systems [2]. Special viruses and target attacks, sponsored by terrorist groups or governments of competing countries, increasingly began to target at the industrial production facilities [3, 4, 5]. The Internet of things gradually comes to the enterprises networks, expanding the already extensive list of industrial protocols and forming the concept of an industrial Internet of things (IIoT) [4, 5]. The means to ensure the information security of process control systems at this stage of their development are not able to withstand such threats [6, 7].

Today, there is a transition to automated digital production, controlled by intelligent systems in real time, in constant interaction with the external environment, going beyond the boundaries of one enterprise, with the prospect of combining into a global industrial network of things and services. This approach is developed in the concept of “Industry 4.0” and describes the current trend in the development of automation and data exchange, which includes cyber-physical systems, the Internet of things and cloud computing [8, 9, 10]. There are many advantages of using wireless sensor networks (WSN, Wireless sensor network) as an environment for wireless interaction of digital objects within the industrial Internet of things network in various automated systems [11].

Network security is becoming one of the main directions in the development of information security through the use of a set of technical means [3]. Since any computer process control system

can be attacked, which usually results in serious technical, reputation and economic losses, it is necessary to timely detect both known and previously unknown attacks in industrial networks. Attacks of malicious persons are constantly improving, becoming combined and spread almost instantly. Intrusion detection systems (IDS) implement monitoring functions and detect attacks that have bypassed the firewall. IDS informs the administrator, who, in turn, takes a further decision on the response to the attack [12].

Thus, it can be concluded that the network attacks detection systems based on the use of artificial intelligence methods as a key element of ensuring cybersecurity of the critical infrastructure [13, 14, 15] of the APCS in the concept of the development of the digital economy are of relevance and need to be improved.

The research goal is to increase the effectiveness of network attack detection system by using a neural network analysis module as part of the IDS. To achieve this goal, it is necessary to solve the following tasks:

- Analysis of the problem of detecting network attacks in industrial networks APCS.
- Development of the structure of the system for monitoring the industrial network of APCS;
- Development of algorithms for intellectual analysis of network traffic of industrial networks;

Development of a software package that implements the proposed algorithms as part of a monitoring system, and an assessment of the effectiveness of the proposed solution on full-scale data.

2. Analysis of the problem of detecting network attacks in industrial networks

The process of automation of industrial production continues to evolve: the number of “intelligent” terminal devices is increasing, the number of microcontroller-based computing systems involved in the process control and process control is growing. Under these conditions, the role of data collected at all levels of the process control system significantly increases. Requirements imposed by consumers of this information are increasingly being tightened in terms of the volume, speed and reliability of data acquisition, as well as information security of the entire system [5]. In turn, increasing degree of automation of the enterprise functioning promoted the mutual integration of information (IT) and so-called operational (OT) technologies [7].

An industrial network is a data transmission environment that must meet a variety of diverse, often contradictory requirements; a set of standard data exchange protocols that allow to link equipment together (often from different manufacturers), and also to ensure interaction between the lower and upper levels of the enterprise management system.

In IIoT, the main types of “things” that need to be connected to the network are various types of sensors and actuators. These devices, on the one hand, have an interface with a communication network, and on the other hand, an interface that provides physical interaction with the process to be monitored (Ethernet, Wi-Fi, cellular networks, Sigfox, LoRa, ZigBee, etc.).

Not so long ago, the hierarchy of the APCS had a clear boundary between the levels. The trends of recent years have made this structure much more complex and diffuse. The automated process control system is more and more integrated with the automated control system, and through it inevitably enters the sphere of Internet technologies. Unification of the corporate and industrial network of an enterprise inevitably poses a serious problem of information security of the industrial network of industrial control systems.

The traditional process control system is a real-time system. To ensure error-free process control, continuous process operation monitoring is necessary [16]. If IT security methods are applied in the process control system, in the event of possible data comprometation, the security system may limit access to this data. This, in turn, can lead to loss of control over the TP and man-made or environmental catastrophe (in critical infrastructure, petrochemical industry and other industries). Therefore, in relation to industrial control systems, the inverse distribution of the significance of safety aspects is widely used [16, 17]:

- availability;
- integrity;
- confidentiality.

The following main threats to the security of an industrial network can be identified [16, 17]:

- Traditional virus software (malware);
- Targeted attacks;
- Unintentional staff errors;
- Suppliers of equipment and software, partners, contractors;
- extortion programs;
- Internal and external sabotage;
- Errors of specialized industrial control systems;
- Failure of hardware.

Summary information of the information security systems of automated process control systems shown in Table 1.

Table 1. Information security support systems in APCS.

Product name	**Kaspersky Industrial CyberSecurity** [17,18]	**Security Matters SilentDefense** [20,21]	**Positive Technologies Industrial Security Incident Manager (PT ISIM)** [19]	**Honeywell Risk Manager**
Meeting the requirements of regulators (FSTEC №31)	+	-	+	-
Security audit	+	-	+	+
Creating rules for the operation of technological processes	+	+	+	-
Intgration with Human-Machine Interface (HMI)	+	-	-	-
System distribution	KICS for Nodes, KICS for Networks, Security Center	Sensors + Command Center	Full distribution	A single control center that collects information from external monitoring and security systems
Recommendations for elimination	-	-	+	+
Intervention in technological process	Uses a copy of network traffic (SPAN / TAP), but contains an intrusion prevention system	Uses copy of network traffic (SPAN-ports)	Uses copy of network traffic (unidirectional gateway)	Data collection without intervention, integration with intrusion prevention system is possible
Software developer certification for APCS	Siemens (WinCC, WinCC OA), Emerson	-	-	Honeywell Experion

An example of the use of wireless sensor networks is the use of wireless sensor networks in electrical substations [22]. The compactness and autonomy of the sensor nodes make it possible to install them in hard-to-reach places without solving the tasks of organizing wired communication

channels for transmitting telemetric information such as: power flows in the power system, control of active and reactive power, frequency and voltage in certain areas to the control room. Due to the transition from wired to wireless network technologies to collect telemetry data, network security is determined not only by hardware and software solutions for industrial controllers and sensor nodes, but also by the chosen principles of their information interaction during the synthesis of network topology, determination of routing parameters and data transmission.

A wireless sensor network [11] consists of many autonomous sensor nodes distributed in areas of the industrial system that are of interest for the collection of operational data and the joint transmission of collected data over wireless channels to a central node that is a node or base station (BS).

Most information security threats in wireless networks are similar to threats and attacks on wired networks, except that wireless networks are harder to protect due to the use of an open medium as a data transmission channel and the broadcast nature of wireless connections. Network protection is complicated due to limited resources: the energy of an autonomous power source and computing resources. Such limiting characteristics make traditional security measures, for example, the use of complex encryption algorithms, multifactor authentication, firewalls, etc. [23] – not always sufficient. A significant factor is the time delay requirements for data transmission in the transport environment and closed protocols for the operation of the software and hardware of the APCS, which do not always allow the implementation of protection technologies using IPSec, SSL, VPN.

The current trend in the development of the transport environment of industrial networks is the use of self-organizing wireless networks with equal rights of nodes, a dynamically changing topology, the possibility of reconfiguration, self-healing, dynamic routing, etc.

The classification of attacks on wireless sensor networks in the direction of impact is given in [24, 25, 26].

Active attacks are various modifications of data during communication by unauthorized persons. Of most interest are routing attacks implemented at the network level. The most common attacks are presented in [11].

Wireless Intrusion Detection System – WIDS [27, 28, 29] is a software and hardware solution that includes software agents that perform the function of collecting, processing and analyzing network traffic packets. Agents interact with the server, transmit intercepted packets to it. The server processes the received data to detect attack signatures and detect abnormal behavior of network nodes, and also responds to events.

3. Network attack detection methods

There are two groups of methods: learning with a teacher (supervised) showed in Table 2, and uncontrolled learning (without a teacher) showed in Table 3 [30, 35, 36]. The essential difference between them is the fact that learning with a teacher uses a fixed sequence of assessment parameters and some data on the meaning of assessment parameters. In learning without a teacher, the set of assessment parameters changes and the process of further training is continuous. Table 4 describes supervised learning methods for intrusion detections.

Table 2. Network attack detection: supervised learning [30].

Method	Description
Rule modeling	Intrusion detection system during training determines a set of rules for normal network behavior. During the operation process, an IDS applies this set of rules and, if it does not match, generates an intrusion detection signal.
Descriptive statistics	The system determines the “distance” between the actual vectors of indicators and vectors collected during the training stage. If the distance between the vectors exceeds a certain threshold, the behavior is considered abnormal.
Neural networks	The neural network is trained on data describing the normal functioning of the system.

Table 3. Network attack detection: learning without a teacher [30].

Method	Description
Simulation of multiple states	Network behavior is described by a set of states and transitions between them. States are described by feature vectors.
Descriptive statistics	The system determines the “distance” between the actual vectors of indicators and vectors collected during the training stage. If the distance between the vectors exceeds a certain threshold, the behavior is considered abnormal.

Table 4. Abuse detection: supervised learning [30].

Method	Description
States modelling	An intrusion is represented as a set of states and transitions between them. States are described by feature vectors. Such systems use Petri nets tools or ordinary chains of events.
Expert systems	Intrusions are represented as a set of rules.
Rules modelling	Simplified expert systems.
Parsing	The intrusion detection system performs parsing to detect a specific combination of characters.

4. Development of the structure of the system for monitoring the industrial network of APCS

Figure 1 shows network structure of an enterprise with tools for collecting and analyzing network traffic of a network intrusion detection system (IDS).

The structure of the network attack detection system based on data mining is shown in the Figure 2. At the first stage, network traffic is captured. In Figure 1, the numbers indicate the following components: 1 is a router as a means of collecting incoming / outgoing network traffic, 2 is a router as a means of collecting traffic within the enterprise network. The collection of necessary data is performed using the package sniffer.

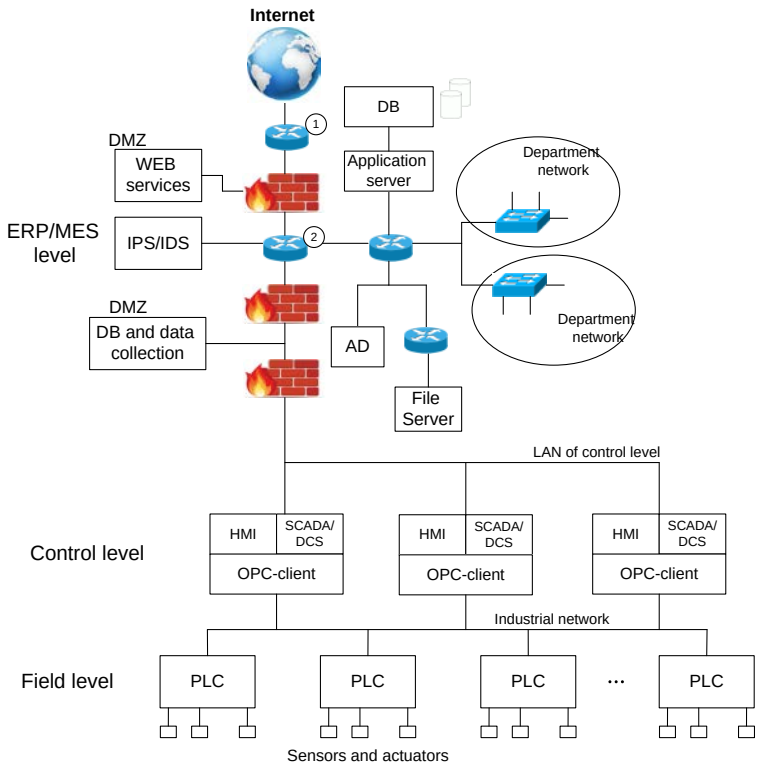

Figure 1. The structure of the enterprise network in which information is collected.

The second stage identifies the most significant parameters that characterize network activity.

At the third stage, detection and classification of attacks is carried out. The results of this recognition are transmitted to related systems for reporting and visualization, depending on the capabilities and specifics of adjacent systems. In addition, information about the attack on the APCS is added to a special archive designed to investigate cybersecurity incidents by authorized specialists and managers.

5. Development of algorithms for intellectual analysis of network traffic of industrial networks

An effective network attack detection system based on artificial intelligence methods can be built only with a high-quality dataset of training and test samples that simulates various intrusions.

KDDCUP99 – intrusion detection dataset based on the data set DARPA 98, is one of the only publicly available labeled data set [31]. Dataset NSL-KDD proposed to improve KDD dataset. This dataset has the following advantages over the KDD dataset:

- it does not include redundant entries in the training set, therefore classifiers will not be retrained due to the frequency of such entries;
- there are no duplicate entries in the proposed test suites;
- number of records in the training and test sets is optimal, which makes it possible to conduct experiments on the full set.

Each entry has 41 attributes describing the various functions of the connection, and the label assigned to each of them: attack or normal connection.

Dataset UNSW-NB15 [32] contains data of normal traffic in modern networks and network traffic of synthesized networks.

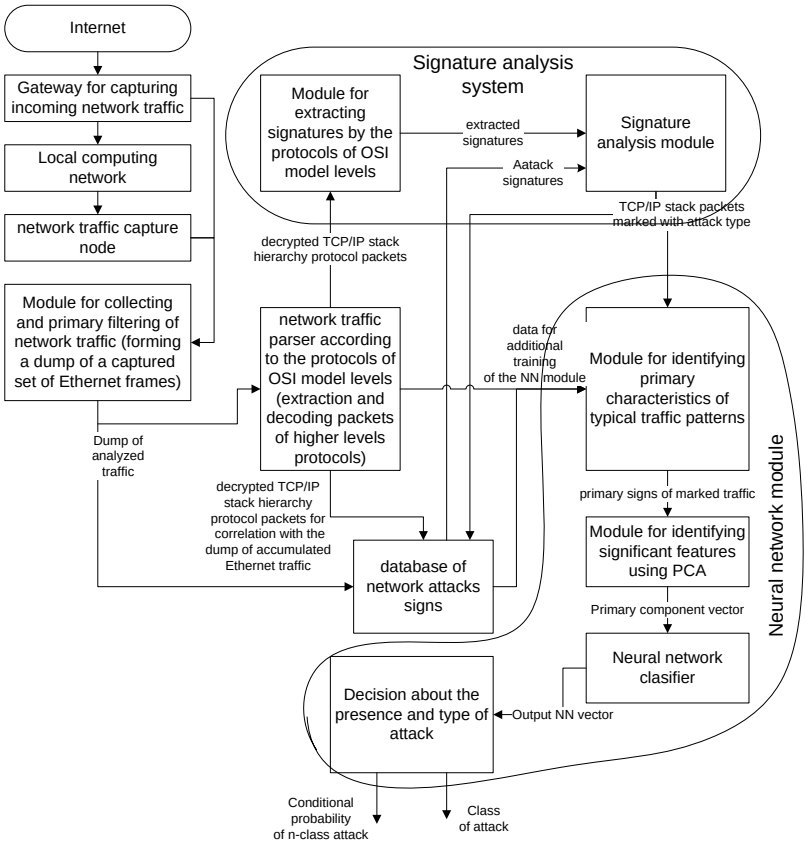

Figure 2. Structural scheme of the network attack detection system.

Each entry in this set contains attributes that describe the various functions of the connection, and the label assigned to each of them: attack or normal connection [32].

The comparative table (Table 5) of the NSL-KDD and UNSW-NB15 methods is shown below:

Table 5. Comparative table of the NSL-KDD and UNSW-NB15 methods.

№	Parameters	NSL-KDD	UNSW-NB15
1	Number of networks	2	33
2	Number of different IP addresses	11	45
3	Traffic simulation	Yes	Yes
4	Duration of data collection	5 weeks	16 days 15 hours
5	Format of data collected	3 types (tcpdump, BSM and dump-files)	PCAP-files
6	Attack classes	4	9
7	Feature Extraction Tools	Bro-IDS	Argus, Bro-IDS and etc.
8	Number of attributes in the record	42	49

Table 6. Network attack methods comparison.

Attack Type	Description	Implementation Features	Method of combating
Buffer overflows	Search for vulnerabilities that can violate the memory boundaries, execute an arbitrary binary code on behalf of an authorized user	1. Preparation of code to be executed in the context of a privileged program. 2. Changing the sequence of program execution with transfer of control to the prepared code.	• Adjustment of the source code of the program. • The use of non-executable buffers. • The use of checks overstep the border. • Conduct integrity checks.
Specialized programs	Viruses, Trojan horse, sniffer, rootkit	The hidden nature of the functioning in the system, data collection, avalanche dissemination	• Anti-virus tools and regular updating of their signatures; • Encryption; • Antisniffera; • Firewalls; • Anti-rootkits [4].
Network intelligence	Collect network information using publicly available data and attack planning applications.	Network intelligence is conducted in the form of DNS queries, ping sweep, and port scanning	• Disable ICMP echo and echo reply on peripheral routers. • The use of intrusion detection systems (IDS).
IP- spoofing	The attacker impersonating an authorized user of the system	Insert false information or malicious commands into the normal data stream	• Access control • The use of cryptographic authentication.
Injections	SQL injection, crossite scripting (XSS attack), XPath injection.	Changing the query parameters to the database, embedding arbitrary code in the web page.	• Rules for building SQL queries; • Encoding data and control characters; • Regular update.
Denial of Service (DoS)	Creating conditions under which legitimate users cannot access the system.	Keeping all connections in busy state. During DoS attacks, normal Internet protocols (TCP and ICMP) can be used.	• Anti-spoofing functions. • Anti-DoS features. • The use of network attack detection systems.
Phishing-attacks	Cheating or social development of enterprise employees to steal their identity and transfer them for criminal use.	Using spam-mailing via e-mail or instant messengers, the use of computer-bots, methods of social engineering.	• The use of proven resources; • Antivirus tools and signature database updates; • Education and training of staff.

Dataset UNSW-NB15 is selected for use in the system:

- number of classes of attacks is more than 2 times;
- test stand contained 33 subnets (NSL-KDD – 2 subnets);

- when collecting traffic on the network, 45 IP addresses participated in the exchange of information against 11 in NSL-KDD;
- traffic was collected by several means (in NSL-KDD - Bro-IDS);
- UNSW-NB15 set contains more attributes for the record (49 vs. 42 in NSL-KDD).

At the moment, in relation to industrial networks the following types of network attacks can be distinguished (Table 6).

Of all types of attacks implemented in the industrial network, network attack detection systems are able to most effectively cope with network intelligence, DoS attacks, as well as various types of injections and buffer overflow attacks. IDS is a practically universal tool capable of detecting most types of attacks implemented on an industrial network.

Main steps of the network traffic analysis algorithm in the industrial network are presented in the Table 7.

Table 7. Characteristics and tools for analysis.

Analysis stage	Characteristics and tools used
Extract traffic	To solve the problem of capturing traffic, it is proposed to use switches with port mirroring and connecting devices with the sniffer and packet analyzer installed.
Feature selection	When analyzing the main parameters of network traffic, one has to deal with an interconnected system of input parameters (factors). Not all of the factors studied are essentially interconnected, but separate groups of input parameters. A transition is needed to a set of independent parameters containing the necessary information about the variation or dispersion of the initial set of factors of the process under study [15]. It is proposed to use: • Principal Component Analysis, PCA; • Neural network autoencoder; • Neural network autoencoder on the basis of convolutional neural network.
Classification	In relation to the problem of classification of network traffic and network discovery it is proposed to use: • Artificial neural networks (multilayer perceptrons); • Decision Tree Ensemble; • Classifier k nearest neighbors (KNN).

6. Development of a software package that implements the proposed algorithms as part of a monitoring system

Table 8 presents the parameters of two common data sets used to build and test network attack detection systems. The choice is made in favor of the UNSW-NB15 data set.

Table 8. Dataset statistics.

Analysis stage		NSL-KDD	UNSW-NB15
Duration of data collection		16 hours	15 hours
Amount of threads		987,627	976,882
Number of bytes of packet sender		4,860,168,866	5,940,523,728
Number of bytes of packet recipient		44,743,560,943	44,303,195,509
Number of sender packets		41,168,425	41,129,810
Number of recipient packets		53,402,915	52,585,462
Protocol	TCP	720,665	720,665
	UDP	301,528	688,616
	ICMP	150	374
	Other	150	374
Label	Normal	1,064,987	1,153,774
	Attack	22,215	299,068
Unique adresses	Sender	40	41
	Recipient	44	45

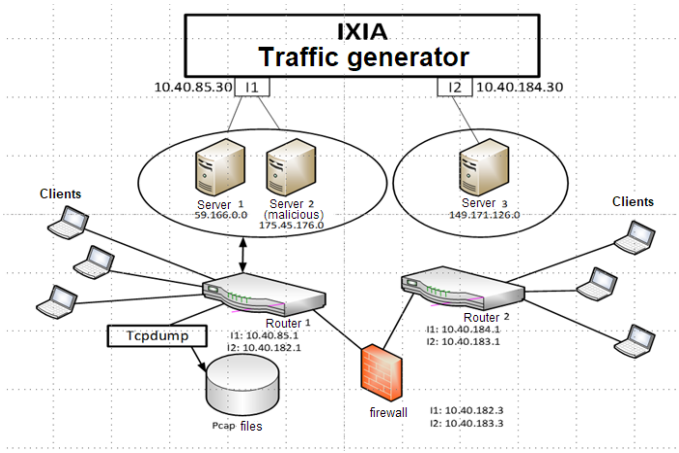

Figure 3. The structure of the experimental stand.

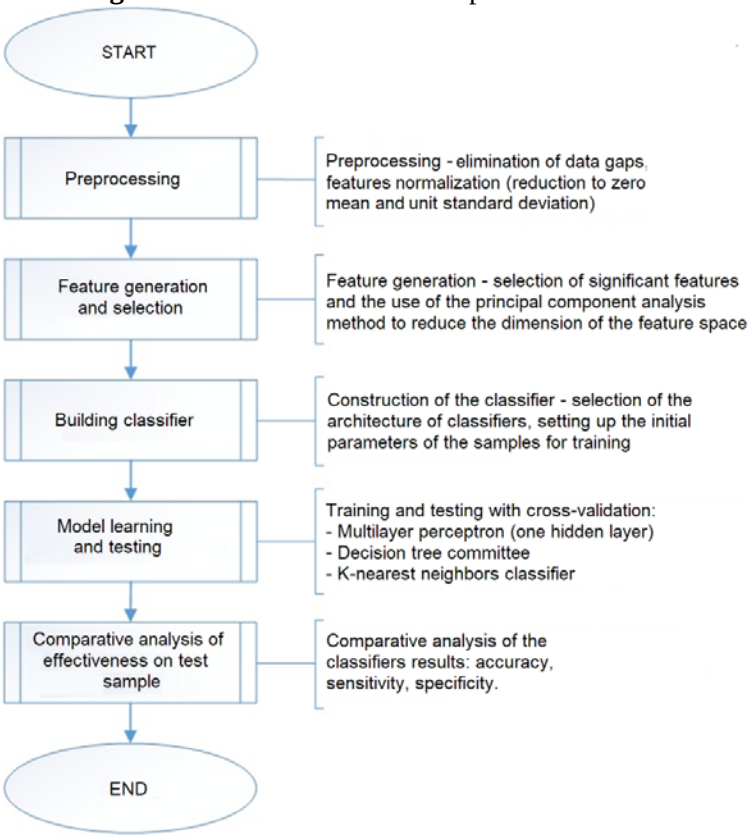

Figure 4. Flow chart of network traffic analysis.

When pre-processing the parameters of the selected data set UNSW-NB15, the attack classes containing less than 5000 examples are excluded from the training set (Table 9).

Table 9. The attack classes.

id	Class name	Number of records
1	DoS	16353
2	Exploits	44525
3	Fuzzers	24246
4	Generic	58871
5	Normal	93000
6	Reconnaissance	13987

Categorical variables are coded into numeric ones. The entire data set is divided into a training and test sample in the ratio of 75% to 25%.

In order to compare the effectiveness of the use the classifier for a specific task, it is necessary to compare the learning results of these classifiers on real data sets. To quantify the classifiers, the following coefficients are applied [34]:

1) False Positive Rate – FPR;
2) True Positive Rate – TPR;
3) Sensitivity;
4) Specificity;
5) Proportion of correctly recognized examples – Correct Rate.

The sensitivity of the algorithm is equal to the proportion of false positive classifications FPR (a, X).

$$Sen = FPR(a, X)$$

A sensitive diagnostic test is called overdiagnosis – the maximum prevention of missing malicious code.

Table 10. Classifier Parameters.

Classifier	Basic Parameters
Decision Trees Committee (RFT)	The maximum number of nodes in the decision tree is assumed to be 250.
Multilayer perceptron (MLP)	The number of neurons in the hidden layer was selected during training to achieve the minimum error on the test sample, the activation function of the hidden layer neurons is the hyperbolic tangent; The number of 5000 epochs of learning, the learning algorithm is conjugate gradients.
Decision Trees Committee (RFT) + main component method for feature selection	Before the classification, features are selected by the method of principal components. The maximum number of nodes of the decision tree is assumed to be 100. The results of the work of the "decision trees" method using feature selection by the principal component method on the test sample are presented in Table 12. The maximum number of nodes in the decision tree is assumed to be 250. The results of the "decision trees" method are presented in table 11.
Classifier based on k-nearest neighbors	Parameter k was hit to achieve optimal error on the test sample. $k \in [5; 100]$
Multilayer perceptron + Autoencoder	Before making a classification, features are selected using a two-layer neural network autoencoder

Table 11. Inaccuracy matrix for decision trees.

	C_1	C_2	C_3	C_4	C_5	C_6
C_1	**23317** **100%**	0 0%	0 0%	0 0%	0 0%	0 0%
C_2	0 0%	**2677** **76.55%**	172 1.52%	5 0.08%	28 0.68%	1 0.01%
C_3	0 0%	711 20.33%	**10156** **90.31%**	689 11.43%	3410 82.25%	239 1.65%
C_4	0 0%	15 0.43%	252 2.24%	**5256** **87.21%**	68 1.64%	23 0.16%
C_5	0 0%	94 2.69%	649 5.77%	73 1.21%	**632** **15.24%**	24 0.17%
C_6	0 0%	0 0%	17 0.15%	4 0.07%	8 0.19%	**14226** **98.02%**
Total	**23317** 100%	**3497** 100%	**11246** 100%	**6027** 100%	**4146** 100%	**14513** 100%

The specificity of the algorithm is calculated as follows:

$$Spe = 1 - TPR(a, X)$$

A specific diagnostic test only diagnoses for certain traffic related to network attacks.

In the course of the research, a series of experiments were carried out, the essence of which consists in determining the presence of an attack and attributing it to a specific class (Table 10).

Table 12. Indicators of detection efficiency of the “decision trees” method depending on the number of components on the test sample.

Number of components	2	4	6	8	10	12	14	16
Average proportion of correctly recognized examples (correct rate)	0.695	0.725	0.755	0.764	0.771	0.776	0.805	0.811
Scatter	0.001	0.001	0.001	0.001	0.002	0	0.001	0

Dependence of the Correct Rate indicator on the number of main components is presented in Figure 5.

A comparison of all methods is presented in table 13. The results given in the table are indicated with an accuracy of 0.01%.

As can be seen from the summary table, in the course of the experiments, the best indicators of correctly recognized images were shown by the algorithms “decision trees” (89.67%) and the multilayer perceptron (89.06%). Sensitivity indicators for FitKNN, MLP and autocoder methods do not exceed 20%.

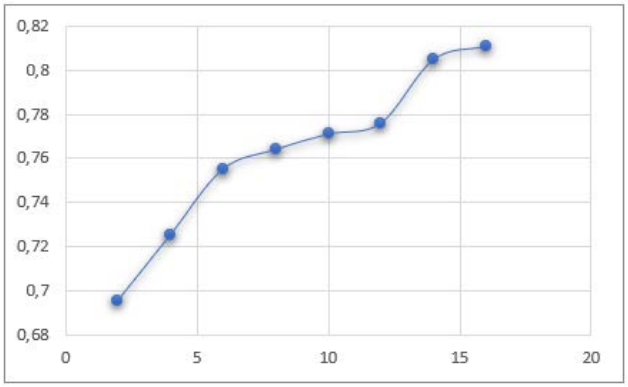

Figure 5. Dependence of the Correct Rate indicator on the number of main components.

Table 13. Comparative experimental results.

Name of the indicator	FitKNN	RFT	MLP	Autocoder	RFT+PCA
Sensitivity	0.1746	0.9877	0.1356	0.0842	0.9168
Specificity	0.9776	0.9897	0.9888	0.9917	0.9335
Correct rate,%	86.24%	89.67%	89.06%	88.58%	81.10%

When using the “decision trees” method together with the principal component method for decreasing the dimension, the indicators decrease (sensitivity - by 8%, specificity - by 6.6%, the proportion of correctly recognized examples - by 8.5%), and require more time and computational resources.

7. Conclusion

During the research the following tasks were solved:

1) The main security threats and the types of intruders in the industrial network of the enterprise are considered. A comparative analysis of software systems to ensure the safety of automated

process control systems was conducted: Kaspersky Industrial CyberSecurity, Silent Defense, PT Industrial Security Incidents Manager, Honeywell Risk Manager.

2) A structural scheme of a network attack detection system based on data mining techniques has been developed.
3) Analyzed the data sets of network traffic, suitable for modeling the traffic of the industrial network of enterprises: KDD99 CUP, NSL-KDD, UNSW-NB15 for the task of detecting network attacks. The UNSW-NB15 set is selected for use in the system, since the number of attack classes is twice as large; test stand contained 33 subnets (NSL-KDD – 2 subnets); in collecting traffic on the network, 45 IP addresses participated in the exchange of information against 11 in NSL-KDD; traffic collection was carried out by several means (in NSL-KDD – Bro-IDS); the UNSW-NB15 set contains more attributes in the record (49 vs. 42 in NSL-KDD).
4) A software package has been developed that implements a comparative analysis of network attack detection algorithms. The most effective is the "decision trees" method with sensitivity indicators Sen = 1, specificity Spe = 0.9877, and the mean correct rate MCR = 89.67%.

8. References

[1] Knapp E D, Langill J T 2014 Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems *Syngress*
[2] Ralston P A, Graham J H and Hieb J L 2007 Cyber security risk assessment for SCADA and DCS networks *ISA transactions* **46(4)** 583-594
[3] Montgomery G *SCADA: Threat landscape* URL: https://energy.gov/sites/prod/files/cioprod/documents/Cracking_Down_SCADA_Security_-_Garrett_Montgomery.pdf
[4] Langner R *To kill a centrifuge – a technical analysis of what Stuxnet's creators tried to achieve* URL: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf
[5] Alert IR-ALERT-H-16-056-01 Cyber-Attack Against Ukrainian Critical Infrastructure URL: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
[6] Ginter A 2016 *SCADA Security. What's broken and how to fix it* (Abterra Technologies) p 165
[7] Steenstrup K IT and Operational Technology Alignment Innovation Key Initiative Overview URL: https://www.gartner.com/doc/2691517/it-operational-technology-alignment-innovation #a-98481934
[8] Greengard S 2015 *The internet of things* (MIT Press) p 232
[9] Zaramenskih E, Artemev I 2017 *Internet of Things. Research and scope* (Infra-M Publisher) p 188
[10] Roth A 2016 *Einführung und Umsetzung von Industrie 4.0. Grundlagen, Vorgehensmodell und Use Cases aus der Praxis* (Springer Gabler Verlag, Wiesbaden) p 272
[11] Almomani I, Al-Kasasbeh B and Al-Akhras M 2016 WSN-DS: a dataset for intrusion detection systems in wireless sensor networks *Journal of Sensors* **2016**
[12] Karnouskos S 2012 A SOA-based architecture for empowering future collaborative cloud-based industrial automation *38th Annual Conference on IEEE Industrial Electronics Society* 5766-5772
[13] Yan Y, Qian Y, Sharif H, and Tipper D 2012 A survey on smart grid communication infrastructures: Motivations, requirements and challenges *IEEE communications surveys & tutorials* **15(1)** 5-20
[14] Maglaras L A 2018 Cyber security of critical infrastructures *ICT Express* **4(1)** 42-45
[15] Sun C C, Hahn A and Liu C C 2018 Cyber security of a power grid: State-of-the-art *International Journal of Electrical Power & Energy Systems* **99** 45-56
[16] Meltzer D, Lund J *Industrial Cyber Security for dummies* URL: http://www.vectorinfotech.com/assets/files/Industrial-Cyber-Security-for-dummies.pdf
[17] Kaspersky Industrial CyberSecurity URL: https://ics.kaspersky.ru/
[18] Kaspersky Industrial Cybersecurity URL: https://softprom.com/sites/default/files/materials/KICS_rus_0816.pdf

[19] Positive Technologies Industrial Security Incident Manager URL: https://www.ptsecurity.com /ru-ru/products/isim/
[20] Security Matters SilentDefense URL: https://www.secmatters.com/product
[21] SilentDefense datasheet URL: https://www.secmatters.com/hubfs/Security_Matters-March 2017/PDF/SilentDefense-Datasheet.pdf
[22] Yick J, Mukherjee B and Ghosal D 2008 Wireless sensor network survey *Computer networks* **12(52)** 2292-2330
[23] Pathan A S K, Lee H W and Hong C S 2006 Security in wireless sensor networks: issues and challenges *8th International Conference Advanced Communication Technology (ICACT)* **2** 1043- 1048
[24] Chelli K 2015 Security issues in wireless sensor networks: Attacks and countermeasures *Proceedings of the World Congress on Engineering* (London, UK) 1-3
[25] Loo J, Mauri J L and Ortiz J H 2016 *Mobile ad hoc networks: current status and future trends* (CRC Press) p 538
[26] Sinha P 2017 Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey *IEEE International Conference on Signal Processing and Communication (ICSPC)* (Coimbatore, Tamil Nadu, India) 288-293
[27] Can O, Sahingoz O K 2015 A survey of intrusion detection systems in wireless sensor networks *6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO)* (Istanbul, Turkey) 1-6
[28] Al-Dabbagh A W, Li Y and Chen T 2018 An intrusion detection system for cyber attacks in wireless networked control systems *IEEE Transactions on Circuits and Systems II: Express Briefs* **8(65)** 1049-1053
[29] Almomani and Al-Kasasbeh B 2015 Performance analysis of LEACH protocol under Denial of Service attacks *Proceedings of the 6th IEEE International Conference on Information and Communication Systems (ICICS)* (Amman, Jordan) 292-297
[30] Kornienko A A, Slyusarenko I M *Intrusion Detection Systems and Methods: Current State and Areas for Improvement* URL: http://citforum.ru/security/internet/ids_overview/
[31] Kashyap S, Agrawal P, Pandey V S and Keshri S P 2013 Soft Computing Based Classification Technique Using KDD 99 Data Set for Intrusion Detection System *Int. J. Advanced Research in Electrical, Electronics and Instrumentation Engineering* **2(2)** 1398-1405
[32] Moustafa N, Slay J 2015 UNSW-NB15: a comprehensive data set for network intrusion detection system (UNSW-NB15 network data set) *Military Communications and Information Systems Conference (MilCIS)* (Canberra, Australia)
[33] Perrin C *The CIA Triad* URL: https://www.techrepublic.com/blog/it- security/the-cia-triad/
[34] Easton V J, McColl J H *Hypothesis testing* URL: http://www.stats.gla.ac.uk/steps/ glossary/hypothesis_testing.html
[35] Branitskiy A A, Kotenko I V 2016 Analysis and classification of network attack detection methods *Proc. SPIIRAN* **2(45)** 207-44
[36] Katasev A S, Kataseva D V and Kirpichnikov A P 2015 Neural network diagnostics of abnormal network activity *Bulletin of Kazan Technological University* **18(6)** 163-167

Acknowledgments
This work was supported by the Russian Foundation for Basic Research, research №17-48-020095.