Использование программного обеспечения Kaspersky Industrial CyberSecurity для критической защиты информации промышленных предприятий

А.В. Познякевич, менеджер по развитию бизнеса,
Лаборатория Касперского, г. Москва,
Е.Н. Горбанева, методист, Центр педагогического Мастерства, г. Москва,
Н.А. Кирилина, аспирант направления подготовки «Экономическая социология и демография»
НИУ ВШЭ, г. Москва

В наши дни очень остро стоит вопрос информационной защиты автоматизированных систем управления технологическими процессами в Российской Федерации. Число кибератак на промышленные системы увеличивается с каждым годом, что критически влияет на экологическую, социальную и макроэкономическую составляющей государства.

Кибербезопасность, информационные технологии, операционные технологии, ИТ-безопасность.

Usage of the software Kaspersky Industrial CyberSecurity for critical information protection of industrial enterprises

A.V. Poznyakevich, business developer manager, Kaspersky Lab, Moscow,
E.N. Gorbaneva, the metodolologist in the Center of Pedagogical Skills of Moscow,
N.A. Kirilina, graduate student specializing in «Economic sociology and demography», National Research University Higher School of Economics, Moscow

Today the question of information protection of automated process control systems in the Russian Federation is particularly acute. The number of cyber attacks to industrial systems increase every year that critically influences on ecological, social and macroeconomic component the state.

Cybersecurity, information technology, operating technology, IT-security.

Nowadays hacker attacks lead to serious problems not only for owners of computers, but also for industrial control systems, different information systems supporting city life and other critical information infrastructures. Number of reported incidents on industrial objects has been dramatically growing from 11 incidents in 2010 to 290 incidents per year these days (based on ICS CERT US report). Business and technological interruption has ranked as the number one risk concern globally. Traditional security measures are not enough for protection of industrial environments against cyber threats. The aim of the research is to identify and analyze software solutions with new holistic approach to cybersecurity of industrial enterprises. The stages of the work include analysis of research works and analytical reports in the field industrial cybersecurity; investigation of standard and legal documents regulating industrial cybersecurity in the Russian Federation; industrial cybersecurity software market research; software selection; determination requirements of industrial software; comparison of the software.

Introduction

Background. Current technology transformation (IoT, IIoT, Industry 4.0 etc.) and business pressure to make decisions faster and better than competitors creates new big opportunity – «industrial digitalization». Essential part of it – industrial cyber security – to avoid those cyber-physical systems will be out of the control. Last research of Kaspersky Lab, published on July 2016, showed that about 220.000 of ICS elements are available from the Internet globally. Even one incident can cause significant losses, reputation of the company and even human or ecological victims.

Problem statement. Thereby the problem that studied in this work is growing number of cyber threats and new approaches to protect industrial systems.

Professional significance. Modern challenges require now to build new approach to provide comprehensive operational technology protection as it should be addressed to the level of company, protected elements and stakeholder’s communication. Therefore, industrial cyber security is transforming into industrial cyber risk management and it is essential to use more complicated and holistic software to mitigate risks.
The subject of the study is the functionality of the software «Kaspersky Industrial CyberSecurity» developed by Kaspersky Lab.

**Delimitations of the study.** The aim of this investigation is to identify and analyze software solutions with new holistic approach to cybersecurity of industrial enterprises. In accordance with the aim the following objectives were set:

1. to study the research works and analytical reports in the field industrial cybersecurity;
2. to analyze the standard and legal documents regulating industrial cybersecurity in the Russian Federation;
3. to identify cyber security software on Russian market and make their comparative analysis;

In particular, the research will include the following methods:

- scientific generalization method;
- method of comparison;
- method of systematic analysis.

**Literature review**

Industrial cybersecurity scientific and regulating documentation in the Russian Federation began to develop quite recently. The question of industrial cybersecurity emerged only after the number of cyber-attacks on industrial plants in Iran, the USA and Europe. That is why almost all Russian cybersecurity researches based on European and American experience. Another argument is that all occurring cyber incidents in the USA are subjected to criminalistics inspection and should be reported in government. Similar cooperation of industrial enterprises with government and information security experts will be possible in Russia only in few years in accordance with the Federal law «About Safety of Critical Information Infrastructure of the Russian Federation» № 187-FZ. The State Duma and the Federation Council assented the document on July 26, 2017 and it took legal effect on January 01, 2018. The law establishes the general principles of legal regulation of the relationship in the field critical information infrastructure safety in the Russian Federation. In conformity with the law, all critical infrastructure objects have to be referred to one of the category of importance. After categorizing, they need to follow requirements for safety of significant critical information infrastructure objects and the requirement for creation of security systems of this objects and ensuring their operability. Also critical information infrastructure objects should immediately inform the Federal executive authority of occurred computer incidents.

Today Russian and foreign theorists and practitioners in the field of information security quite often open up the question of industrial control systems security in their research works and analytical reports of the malicious software. In the report «To Kill a Centrifuge» by Ralph Langner (2013) the author analyses the first reported cyber-physical attack on industrial plant named «Stuxnet». The document combines results from reverse engineering the code of the attack with information about attacked plant and background information on the attacked uranium technological process. Ralph Langner shows that it was a targeted attack created by motivated and qualified hackers. They knew every detail of technological process and even models of programmable logic controllers that operate centrifuges. The author describes how difficult it would be to use Stuxnet as a blueprint for cyber-physical attacks against critical infrastructure of the United States and their allies. The overall aim of this report is to show problems in the area of cybersecurity and to explain how industrial enterprises and governments can protect their infrastructures against sophisticated cyber-physical attacks like Stuxnet.

Another paper that has made a significant contribution to understanding the problem of industrial cybersecurity is «SCADA Safety in Numbers» by Gleb Gritsai, Alexander Timorin, Yury Goltsev, Roman Ilin, Sergey Gordeychik and Anton Karpin (2012). The group of experts compare discovered vulnerabilities in industrial hardware for the period from 2005 to October 1, 2012. The paper shows that about a half of industrial supervisory control and data acquisition systems are available from the Internet are vulnerable and can be hacked by poorly trained malware users. In general, it means that such systems should be protected by problem-oriented software designed with understanding of industrial characteristic aspects.

In recent years a considerable amount of work has been written to identify risks and safeguard industrial control systems and networks from malicious and targeted attacks. The survey «Securing Industrial Control Systems-2017» written by Bengt Gregory-Brown gathers and analyzes different data from hundreds of IT and industrial control systems (ICS) security practitioners from a huge amount of industries. The paper shows that industrial managers understand cyber risks and increases budgets of their companies on security of systems that control and monitor industrial and infrastructure processes. Nowadays specialists consider the top threat vector to their ICS to be adding devices to the network that
cannot protect themselves. Industrial automation vendors also recognize these risks and publish their own reports about industrial cybersecurity, for example the paper «Cybersecurity for Industrial Automation & Control Environments» by Industry Director of Schneider Electric Ivan Fernandez (2013). The author argues that more open and collaborative industrial networks can make industrial control systems more vulnerable to hackers’ attacks. Ivan Fernandez explains how to minimize the risks of cyber-attacks and prevent potentially significant monetary loss. The expert also dramatizes the importance of using security solutions that can protect critical information infrastructures of industrial enterprises.

Methods

The common idea of all used methods is to analyze thematic research works and analytical reports, find out the best practices of industrial cybersecurity and then using this background compare the industrial cybersecurity software presented on Russian market.

Method of scientific generalization was used to study the current state of the problem of critical information infrastructures security, gather and analyze basic research works and analytical reports in this area.

Systematic analysis and comparison methods were used to identify key features of software for industrial cybersecurity, to compare them and find out the most complex software designed with understanding of industrial characteristic aspects. The absence of methods below consists in lack of publicly available data about software. In this case, it is possible to compare indicators to averages or assume such data away.

The review of decisions on ensuring cyber security of automated control systems

Modern digital transformation of technologies (The Internet of things, the Industry 4.0, etc.) and requirements of business departments of the companies to make decisions quicker and more effectively, than competitors, creates new opportunities — “the digital industry”. Her important part is an industrial cyber security. Approach to ensuring cyber security of automated control systems cardinaly differs from approach to protection of IT infrastructures. In a technological segment emergence even of one incident can cause falling of reputation of the company, considerable financial losses and even the human or ecological victims. So, one of the last purposeful attacks is the attack to power supply networks in December, 2015 in Ukraine which has caused blackout in 5 regions for 6 hours [1, page 12].

Emergence of large-scale cyberincidents of IB in the industry and objects of critical infrastructure has revealed need for detailed study of vectors of the attacks and models of the violators inherent in directly industrial systems. There was a need for development of complex strategy of providing IB for the industrial control system systems. Modern problems in the field of providing IB industrial control system lead to creation of new approach to providing a comprehensive protection of Operational technologies which has to be directed to all levels of the company, protecting elements and communications between them. Thus, the industrial cyber security is transformed to industrial department of cyber-risks.

The industrial companies impose more serious requirements to decisions on protection of industrial control system, they have to be adapted to work in a technological segment and consider features which haven't been realized in traditional means of anti-virus protection. Approach to providing IB industrial control system requirements and recommendations have to be the cornerstone of both the Russian, and international normative documents on IB [2, with. 6].

Perhaps, for this reason today in the market of decisions on IB industrial control system in the Russian Federation a small amount of competitive decisions is observed.

Thus, in the analysis of the Russian market of decisions on ensuring cyber security of industrial control system the following criteria have been defined:

1. the decision has to provide cyber security of the industrial control system components – the SCADA, RSU elements, industrial networks and PLK;
2. the decision has to provide comprehensive cyber defense without impact on technological process;
3. the decision has to trace in real time safety events at the level of certain teams of technological process;
4. the decision has to be developed taking into account operational compatibility to give ample opportunities to integration with third-party SIEM, MES systems, etc.

For the purpose of detection of the decisions corresponding to the criteria described above within this work the materials from open sources published by the authoritative Russian companies experts in the
field of IB namely by Kaspersky Lab, Infosistema Jett, DialogNauka, Softline, Positive Technologies and drugm have been analysed.

As a result of the analysis of sources, for further detailed consideration and comparison solutions of DATAPK, InfoWatch ASAP, Kaspersky Industrial CyberSecurity and Positive Technologies Industrial Security Incident Manager of development of the companies the Ural Center of Security systems, InfoWatch, Kaspersky Lab and Positive Technologies respectively have been chosen. Lower in work will be considered in more detail these decisions are described.

1) DATAPK

The decision of the company the Ural Center of Security systems has been officially submitted in 2015. The vendor developed a product as the system of monitoring and detection of invasions in technological network. The main functionality and purpose of the decision are presented in the Figure 1.

![Figure 1 – Functionality of DATAPK](https://www.slideshare.net/zlonov/datapk)

DATAPK provides control and the analysis of a condition of security of industrial control system of production objects and combines to a vseba the following functionality:

- functionality of map development of technological network, identification in her unauthorized changes;
- control of a configuration of the industrial control system components;
- management of safety events;
- detection of the computer attacks in the industrial control system technological network, identification of network anomalies;
- detecting of vulnerabilities in the industrial control system components.

The considered product has undergone approbation at a number of customers of the UTsSB company from fuel and energy complex, metallurgy and other industries of Russia. In separate projects the decision is introduced in trial operation.

In addition It should be noted that in 2017 DATAPK has undergone certification of FSTEC of Russia. The certificate of conformity issued by the regulator certifies that the software of DATAPK is the software of control (analysis) of security of information which isn't containing the data which are the state secret and also conforms to requirements of specifications at implementation of instructions on operation. The certificate is issued for the term of three years [31].

2) InfoWatch ASAP

The product has been developed by the InfoWatch company, officially released in 2016 and represents a hardware and software system (further – the PACK ICE) for safety of industrial control system as it is presented in the Figure 2.

The functionality of the decision allows to find and prevent the attacks directed to information infrastructure of systems of automated control systems [3].

It is possible to allocate the following key opportunities of the decision:

- detection of invasions into industrial network and protection against insert in data transmission channels;
• a possibility of firewalling at the level of industrial protocols;
• ensuring control of correctness of technological process;
• control of integrity of transmitted data;
• monitoring of vulnerabilities of industrial control system;
• support of proprietary protocols of industrial systems of automation.

3) Positive Technologies Industrial Security Incident Manager (далее – PT ISIM).

The decision of the Positive Technologies company has been officially submitted to the public in the field of IB in 2016. PT ISIM is an implementation of approach of the Positive Technologies company to protection of industrial control system. It should be noted that for different industries specialists of the company create various interfaces, and at each introduction PT ISIM adapts to a real operational environment – to protocols, architecture, rules of correlation and the equipment, typical for her. According to the head of this direction of the Positive Technologies company, at similar approach the efficiency of detection of the attacks increases many times. Physical service conditions in the industry happen extremely aggressive therefore industrial execution of PT ISIM is selected under a real operational environment taking into account specifics of specific industry. However it should be noted that this approach can be considered and on the other hand. The decision of PT ISIM isn't «box» and demands completion under almost each client, and even up to completion under this or that installation of the customer. These completions, for example in the conditions of the compressed delivery time, can be not fully tested and in a consequence to lead to failure in work on an object. Besides, the customer should be engaged constantly in «custom» projects on each new installation [4]. The developer company states that the product of PT ISIM helps to fight both with internal, and against external threats of information security. From them it is possible to allocate such threats as:

• unauthorized connection
• attempts of selection of the password
• illegal managing directors of team
• substitution of an insertion of the industrial equipment,
• potentially dangerous actions of personnel
• equipment configuration errors.

The principle of work of PT ISIM consists in collecting and the analysis of the copy of traffic of technological network, standard introduction of the decision is presented in the Figure 3. The mechanism of intellectual processing of events used by PT ISIM allows to connect separate events of safety in chains of actions of the malefactor and to reveal the attacks distributed in time (even on the long periods), notifying on an incident of employees on places or in the situational center. In this decision the functionality of monitoring and control of technological network is worked perfectly out, however protection of final knots is presented very modestly.
Figure 3 – Standard introduction of the decision of PT ISIM

Distinctive feature of this system is the built-in mechanism of correlation of events which can connect all preventions in a certain chain of events. Thanks to this function it is possible to restore a full picture of the taken place safety event. Also it should be noted that well worked user's interface. Today the company has finished a number of pilot projects with application of this decision.

4) Kaspersky Industrial CyberSecurity (далее – KICS)

The decision of KICS has been officially submitted by the JSC Kaspersky Lab company in 2015. It should be noted that development of the decision was conducted since 2012, i.e. the decision has entered the market rather worked and tested. An integrated approach to providing IB industrial control system which realizes as protection of final knots of technological network (jobs, SCADA servers, HMI panels), and monitoring of integrity and identification of the attacks in technological network is the cornerstone of a product.

The solution of Kaspersky Industrial CyberSecurity includes the functional components and services of the company presented in the Figure 4. The functional component includes 3 main components:

- Kaspersky Industrial CyberSecurity for Nodes – protection of final knots of technological network, servers and workstations;
- Kaspersky Industrial CyberSecurity for Networks – protection of technological network, detection of anomalies and control of integrity of network;
- Kaspersky Security Center – the centralized management of protection of knots, reception and transfer to the external systems of events of information security.
Figure 4 Functional components and services of the decision of KICS

From remarkable functions it is expedient to allocate the following:
- The centralized management (control is exercised from the uniform Kaspersky Security Center console)
- Protection against malicious software (signature, heuristic analysis)
- Passive analysis of dens of OS
- Control of integrity of network (applications launch control, control of integrity of industrial process and PLK projects, control of devices)
- Protection against encoders
- Prevention of invasions (protection against the network attacks, exploits and firewall)
- Integration with other systems
- Certification of industrial control system by vendors and state regulators [4, 5]

In section 2.2 of Chapter 2 detailed comparison of the above-stated decisions on their functional and nonfunctional signs will be carried out, the most reliable and complex decision on ensuring cyber security of industrial control system is revealed and also the possibilities of use and commercial operation of the chosen decision are considered.

Results
After applying three different methods may be obtained that the most complex and reliable software solution is «Kaspersky Industrial CyberSecurity» developed by Kaspersky Lab. Specialized component based software solution was launched globally in 2016. It distinguish from its competitors by holistic protection of the whole environment of industrial systems – end network nodes, industrial network and programmable logic controllers. The software provides comprehensive cyber protection in a passive way without any technology process influence and includes anomaly detection engine that can monitor real time events on the level of particular technology process command. Another essential figure is that it is based on multi-year research of KL and insight from more than 270 thousand customers of the company.

Conclusion
A survey of the main thematic research works and analytical reports proved that nowadays industrial companies and government work extensively to protect industrial environment from malicious programs and hackers attacks, but the problem of industrial cybersecurity exists and much still remains to be done in this area. The study is focused on identification key features of software for industrial cybersecurity, comparison pf this solutions and finding out the most complex software with new holistic approach, designed with understanding of industrial characteristic aspects. The detailed analysis revealed
that the software solution «Kaspersky Industrial CyberSecurity» developed by Kaspersky Lab is more relevant to protect industrial enterprises then its competitors. The software may be recommended to increase the level of protection and quality of industrial cyber landscape.

References