DOI: https://doi.org/10.36910/6775-2524-0560-2021-43-32
УДК 004.05(075.8)
[1]**Марценюк Василь Петрович**, д.т.н., професор,
https://orcid.org/0000-0001-5622-1038
[2]**Сверстюк Андрій Степанович**, д.т.н., професор,
https://orcid.org/0000-0001-8644-0776
[3]**Андрущак Ігор Євгенович**, д.т.н., професор,
https://orcid.org/0000-0002-8751-4420
[3]**Риковська Лілія Олексіївна,** асистент,
https://orcid.org/0000-0001-9282-1639
[3]**Кошелюк Віктор Андрійович,** к.т.н., доцент,
https://orcid.org/0000-0002-4136-5087
[1]Університет Бєльсько-Бяли, Польща
[2]Тернопільський національнийний медичний університет імені І.Я. Горбачевського, Україна
[3]Луцький національний технічний університет

ОСОБЛИВОСТІ КІБЕРБЕЗПЕКИ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЧАС ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Марценюк В.П., Сверстюк А.С., Андрущак І.Є., Риковська Л.О., Кошелюк В.А. Особливості кібербезпеки сучасних інформаційних технологій в час цифрової трансформації. У статті розглянуті загальносистемні погляди на питання забезпечення кібербезпеки в час цифрової трансформації, виділені ключові фактори, що визначають проблеми захисту інформаційних систем. Наводиться відповідна трансформація систем управління інформаційною безпекою. Розглядаються нові загрози цифровому виробництва, їх особливості та канали впливу.
Ключові слова: кібербезпека, цифрова трансформація, кіберзагроза, дистанційне обслуговування, цифрове виробництво, кіберзахист.

Марценюк В.П., Сверстюк А.С., Андрущак И.Е., Риковска Л.А., Кошелюк В.А. Особенности кибербезопасности современных информационных технологий во время цифровой трансформации. В статье рассмотрены общесистемные взгляды на вопросы обеспечения кибербезопасности во время цифровой трансформации, выделенные ключевые факторы, определяющие проблемы защиты информационных систем. Приводится соответствующая трансформация систем управления информационной безопасностью. Рассматриваются новые угрозы цифровом производства, их особенности и каналы воздействия.
Ключевые слова: кибербезопасность, цифровая трансформация, киберугрозы, дистанционное обслуживание, цифровое производство, киберзащита.

Martsenyuk V.P., Sverstyuk A.S., Andrushchak I.Ye., Rykovska L.O., Koshelyuk V.A. Features of cybersecurity of modern information technologies during the digital transformation. The article considers system-wide views on cybersecurity during the digital transformation, highlights the key factors that determine the problems of information systems protection. The corresponding transformation of information security management systems is given. New threats to digital production, their features and channels of influence are considered.
Key words: cybersecurity, digital transformation, cyber threat, remote maintenance, digital production, cyber protection.

Formulation of the problem. The changes in the modern world caused by the rapid growth from information technology and universal digitalization could not but affect production systems. The invention and widespread use of programmable controllers, robots and digital control systems integrated with corporate networks of enterprises led to a change in approaches to production management, the rapid development of several new technological departments. This so-called "new industrial revolution" could not but find reflection in the tasks of ensuring the safety of industrial systems.

The evolution of technologies and management tools towards the widespread use of computerized components has led to the emergence and rapid growth of the number of new attacks on industrial systems. A modern attacker uses targeted attacks on digital production facilities, specialized arsenals of means of influence; not only technical methods, but, for example, social engineering.

In this paper, the authors consider the main changes in industrial systems with the emergence of the concept of "digital production", the transformation of production processes and approaches to ensuring their safety when moving to the digital economy. Changes in the object of protection, or production system, lead to new, targeted attacks, expansion of channels of influence. A new class of threats, called, in accordance with the requirements of the time, "cyber threats" is being put in correspondence with a new class of security systems: cybersecurity systems of digital production.

Analysis of research. Modern production is undergoing significant changes due to the widespread introduction of information technologies and systems. Almost all industrial elements are equipped with electronic sensors and controllers, and thanks to them, information flows are also added to the process of organizing the flows of matter and energy during production. The book "The Fourth Industrial Revolution", which declared these changes in 2019 [1], describes in detail the process of changing the production economy caused by the rapid pace of technological development, the breadth of application of information and telecommunication technologies and the consistency of the use of digital devices. The term "Industry 4.0", widely used to denote new production realities, sounded for the first time in 2016 at the Hanover Fair when referring to the process of radical transformation of global value chains [1,2]. The technology of "smart" production, equipment, household appliances became the main part of this process. Today, the flexible interaction of various physical systems through digital technologies is changing the appearance not only of industry, but also of the economy as a whole.

The modern period is called the "second machine age" [3], emphasizing the difference between the traditional approaches to using hardware and software that have been steadily developing throughout the twentieth century, and new trends, solutions of global computing and artificial intelligence. Despite the fact that software and hardware control appeared in production for a relatively long time, its use in recent years has significant differences. The scale of penetration of digital technologies is significantly increasing, both in various industries and areas of activity, and in individual production processes.

A synthesis of technologies is taking place, from decoding the genome to nanotechnology and renewable energy systems. The rate of change is rapidly increasing - unlike previous industrial revolutions, industrial revolution 4.0 is developing not linearly, but exponentially [1].

The main value of the "Industry 4.0" society is not products, but information and the potential of information impact, due to the widespread use of automation and data exchange, computerized production systems, the Internet of things and cloud services. According to forecasts, the potential of the Industrial Internet of Things (IIOT, Industrial Internet of Things) [4], which unites networks of physical objects, platforms, systems and applications with embedded technologies for exchanging data with each other, the external environment and people, is estimated by analysts at more than thirty trillions of dollars and will continue to grow [5].

All these technologies are directly related to the digital transformation of production and new, cyber-physical systems. They affect both the systems of controllers and interacting industrial devices themselves, and related areas. The leading directions of development, in addition to the actual cybernetization of production, analysts [6] consider:

- Changes in ACS interfaces associated with the development of graphical interfaces, the use of touch-screen technologies and augmented / virtual reality technologies. Despite the fact that the rapid development of this area is taking place in the segment of consumer devices, its advance into the area is also not far off.

- Technologies for processing data generated by devices in the course of operation and interaction. According to analytical reports, 40% of such data has never been saved, and the remaining 60% is stored for a short time, locally and is hardly analyzed and processed. Integrated control of digital manufacturing requires the collection and processing of all this information in data centers and computing systems.

Data analytics and artificial intelligence technologies are at the top of the list. They are necessary to get real benefits from the collected and processed production data, operational and long-term monitoring and planning of the production process. The technological breakthrough should result in production systems that are resistant to external changes and self-adapting.

The object of protection, previously understood as a set of classified data, acquires a more complex representation - as a cyberspace, including not only data, but also systems for their transmission, processing and storage; control systems; means of protection; as well as their dynamically changing relationships, which constitute a certain value. Segments of cyberspace include supercomputers, corporate and home networks, mobile systems, cloud services, and even social networks and consumer devices. Let us define cyberspace as a global sphere in the information space, which is an interconnected set of infrastructures and information technologies, including the Internet, telecommunication networks, computer systems, embedded processors and controllers. The transformation of industrial informatization can be represent, and now we can talk not about two (old and new, cyberphysical), but about three stages of changing the industrial environment. The first includes traditional information systems and information and telecommunication systems. The emergence of the second stage is caused by the cybernation of the production process and the widespread introduction of industrial controllers. The third is a look into the future, already voiced by a number of specialists. It involves the digital integration of not only physical systems, but also organizational ones: the cybernetization of the business processes of enterprises.

Today there is an active development of cyber-physical systems and a transition to the stage of integration with business processes - digital production and the digital economy. Formal concepts of cyber-physical objects and systems. A cyberphysical object (CFO) is a conceptual paradigm for representing production and technological schemes in the form of a conglomerate of means for converting various types of matter and energy and an information and telecommunication environment that provides both information exchange between components and the stable functioning of the entire system under external influences using auto - matized management.

Presentation of the main material and the justification of the results. Manufacturing systems have undergone significant changes as a result of computerization. Two generalized stages of production can be distinguished, characteristic of both traditional and modern, computerized systems of Industry 4.0.

The first stage is the creation of a digital twin of an industrial product or product - for production systems, this can be a computer model or a 3D image of a product in design systems. In this case, production systems are relatively localized and we can talk about them as traditional design systems to which we can apply generally accepted information security measures: creating a trusted environment, controlling external access, and so on. The second stage is modern additive manufacturing, in the management of which computer technology is also widely used - as shown above, it is integrated with the external environment much more than is accepted in traditional solutions. In this case, it becomes almost impossible to completely control or exclude external influences on the production system, and an urgent problem arises to ensure the stability of the production process in conditions of a variable set of different external influences. In the future, the article focuses specifically on the safety of additive manufacturing and production process control, as a new area in the field of ensuring the safety of industrial systems.

The features of security incidents in recent years have become an increasing increase in serious incidents associated with. According to the distribution of statistics of cyberattacks in the fall of 2016, industry accounted for more than 20% of all recorded incidents, together with the state and the military industry, confidently exceeding 50% of all attacks. The share of areas such as social media, file hosting, news sites, mobile telecommunications companies together accounted for less than 13% of all incidents. In many ways, the growth of attacks on production systems is associated with changes in their structure, digitalization and the emergence of new security challenges. Today's intruder, acting through telecommunication channels or having access to information resources of the corporate network of an enterprise, has the ability to influence production as a whole The second important point is the ability for an intruder to influence through digital control components (networks and controllers) the material output of the production system, the result of the production process.

According to SecurityLab, for 2019, it can be noted that cybercriminals gain access to the personal data of users of the LastPass service, and, thus, to a variety of credentials, including production systems. Viruses in images on legitimate websites were used as penetration channels for the same data in various incidents; a vulnerability found in Samsung smartphones; and even electrical interference in DRAM. The main channels of influence that an intruder can use are influence on devices; impact on the control subsystem; impact on protocols and network equipment; impact on the human-machine interface. Within the framework of digital production, impacts through all of the above channels can be implemented as informational. According to the statistics of security breaches, there is currently an abrupt increase in the number of incidents related to their cybersecurity, and is due to the trend of integrating technological process control systems and corporate information networks.

In almost 50% of cases, impacts on automated control systems for technological processes already occur from the corporate network, and in almost 20% of cases - from the Internet. According to statistics, the general nature of attacks on cyber-physical systems is changing. Targeted attacks that can be carried out transitively are becoming characteristic of digital production. For their frequent preparation and implementation, specialists are involved in the relevant industrial sectors and the equipment involved. Attackers use several methods and "vectors" of attacks at once, an integrated approach to the implementation of the impact. Attacks include a wide range of not only technical methods, but also methods based on social engineering and psychology. Also new is the purpose of the attack itself - it is not theft of information, but the impact directly on the ongoing technological process. Today, this threat is often assessed more seriously than data theft [6,7]. Separately, it is necessary to note the emergence of additional critical modules due to informatization and the lag of the regulatory framework. The widespread use of cloud systems and systems with a fuzzy perimeter is associated with the development of the following threats:

1) Threats aimed at using the computing power of the cloud to solve the tasks of an attacker (for example, brute force passwords and hashes) or to mask the source of influence on other objects.

2) Threats directed to platforms, infrastructures and software of cloud users from other cloud users or from the Internet.

The emergence of smart home systems, or more generally the emergence of the concept of the Internet of Things, has led to the possibility of violating the security of personal space in the form of:

1) The use of household devices to penetrate personal computers and mobile phones.

2) Threat to the life and health of users (disruption of the operation of household devices can lead to fires, poisoning, etc.).

3) Substitution of media content as a means of waging information wars.

SCADA security threats are determined by the fact that the number of industrial networks connected to the Internet is growing - this is due, among other things, to the introduction of smart grids and smart meters, but many of them still use isolation as the main measure of protection, which means the number and complexity of attacks on ICS is increasing. The systematization of new threats is given in Table 1.

Table 1.

Technology	**Vulnerable elements**	**Consequences of threat realization**	**Protection features**
Virtualization	Hypervisor	Capturing control	Protection of the "last resort" - it is impossible to detect a successful attack
Cloud technologies	Access control mechanisms	Destruction of the structure of the cloud	The need to differentiate personal resources
Mobile systems	Authentication and encryption mechanisms (not used or partially used)	Interception of data management and use for attacks on related devices	Lack of energy resources
"Smart House"	Insecure connection to the Internet, software integrity	Collecting critical information, incapacitation, takeover of control	Impossibility of interactive interaction with user

The main difficulties in assessing and solving the problem of information security of modern industrial cyber-physical systems, and, as a consequence, digital production, are:

- lack of due attention to the problem;
- changes in the characteristics of the impact;
- lagging of the regulatory framework.

Indeed, less than 2% of attacked enterprises report incidents, and experts overestimate the degree of security of their systems: lack of Internet connection, firewall capabilities, security of emergency protection systems and their protection from external influences.

The combination of new attack targets such as interception and disruption of technological processes, new penetration mechanisms and new targets of attacks leads to the need for new approaches to ensuring the security of industrial systems in the era of digital production.

The information globalization of industry and energy in the post-industrial era goes through several stages, characterized by varying degrees of transfer of the functions of a human operator to a computer system. In the early stages, this was expressed in the degree of automation of the production sphere, which consists, first of all, in the automation of workflow, the processes of collecting and processing information and preparing it in an appropriate format for the user who makes decisions or retaining full control over the process for the person.

Further integration with computer systems led to the gradual transfer of the right to form decisions from a human operator to an automated system, which was primarily caused by the need to speed up the execution of the corresponding actions or commands as much as possible. This stage is characterized by the intensive development of methods and means of artificial intelligence, as a tactic of substantiation and optimization of the decision-making process, which led to the creation of expert systems, fuzzy inference, predictive systems.

Along with the transformation of traditional production, there is a transformation of information security. With the advent of cyber-physical systems and Internet things, flagships of digital production, the

concept of cyber security was added to the concept of information security based on the security of information and telecommunication systems. Assessments and methods are being developed to support this new direction. Also, when integrating with business processes, the traditional concept of information security can be expanded to one more level. It is still difficult to say what it will be today.

The nature of digital production determines the main difficulty arising in the creation of a threat model for this class of systems. A large number of users, components, and production integration make it impossible to use traditional attack models, which can be seen from the example of work in the field of threat modeling of modern industrial systems. It becomes difficult, if not impossible, to predict and describe all the variety of possible impacts - and their number increases with the development and integration of technologies.

Cybersecurity is a set of principles and tools for ensuring the security of information processes, approaches to security management and other technologies that are used to actively counter the implementation of cyber threats. The tasks of ensuring cybersecurity can be systematized as an analysis of the mechanisms of violation of the protection of cyberspace, modeling of destructive influences; cyber security management, determination of the stability zone of the protected object, analysis of cyber risks, development of standards and norms for cyberspace security; synthesis of cyberspace protection means and control of the current state and functioning of cyberspace components. Accordingly, the modern security paradigm includes:

1. Revision of access control models, taking into account openness, flexibility and distribution. Models should be based on temporal logic.

2. Adoption of virtualization technology as a powerful means of protection, which allows you to move from the concept of a "protected system" (from a fixed set of threats) to the concept of "a system with predictable behavior."

3. Implementation of the principle of separation of the information processing environment and protection means.

4. Construction of theoretical foundations of dynamic protection management (adapting to current threats) as an object of automatic regulation with the concept of a stability zone, aftereffect (inertia) of dynamic characteristics

5. Acceptance of the openness of systems (connection with the Internet) as an integral property and construction of protection with this in mind:

6. Development of the basis for assessing the elasticity (customizability of the system) and scalability. Development of new principles for detecting attacks, viruses, rootkits, worms.

7. Taking into account the possibility of using super-computers to create new attack scenarios, scanning systems, intervention in production management, cryptanalysis. Considering that we have entered the era of cyber warfare, the supercomputer is an opportunity to create new weapons.

8. Analysis of the existing trends in the development of security means allows us to conclude about a change in protection paradigms based on protection technologies, which can be conditionally defined as static, active, adaptive and dynamic. The idea of such a classification of protection technologies is borrowed from control theory. Despite the difference in the goals pursued in the theory of control and the theory of information security, one can see the similarity of the approaches used to achieve these goals and aimed at keeping the system within a certain set of states. At the same time, control theory has a longer history of development and, due to this, a richer terminological base. The set of criteria on the basis of which the classifications of management methods are built, usually include the following parameters:

- the presence of feedback - in the general case, controllers with feedback can use many (more than one) measured values and form several control actions on the controlled object;

- the presence of an adaptive control loop is built on top of the control loop, the purpose of which is to adjust the internal parameters of the regulator so that an optimum is achieved, characterized by a certain set of criteria - quality indicators;

- the presence in the feedback loop of functions for predicting the state of the system - on the basis of indicators characterizing the system and its environment, a set of conditional scenarios is built that predict the development of the system. The forecast is fed to the input of the regulators and affects the formation of the current control action.

On the basis of the listed criteria, it is possible to unambiguously classify the existing protection technologies - each of the classes is characterized by the presence of a certain set of the listed circuits. In a static protection technology, the control function does not change over time, and the operating mode is described by the functions of the dependence of the output state of the protected object on constant values of control actions and other destabilizing factors, feedback, adaptive control and prediction of the system state are absent. Active protection technology complements the static one by introducing feedback - the results of experimental testing of the protected object are used to change the configurable parameters of the security

systems. Adaptive protection technology, accordingly, requires an adaptive control loop - the parameters of security systems are periodically changed in such a way that the protection efficiency indicators (calculated based on the characteristics of the protected object during monitoring) tend to the maximum. The set goal of management within the framework of dynamic protection technology is dynamic compensation of undesirable changes in the state of the system "on the fly" by interacting with both the protected object and its infrastructure. The fundamental distinguishing feature of dynamic protection is that the protected system is treated by the protection system as a nonlinear dynamic object with continuous time, and the protection system itself becomes discrete-continuous.

Therefore, the full set of dynamic protection methods that underlie the cyber security paradigm include methods of studying and influencing the environment of the object under study, aimed at predicting the state of the system depending on the dynamics of changes in internal and external (in relation to the protected system) factors. This is how we come to the concept of "predictable behavior system" - to ensure cybersecurity, it is not enough to describe the state of the system's security. It is necessary to be able to predict the behavior of the system in a given (but uncontrolled and untrusted) environment, and in the future - to predict the dynamics of changes in external influences on the protected system.

This means that dynamic protection should be aimed at studying not only the protected system and mechanisms for the implementation of threats, but also the environment of the protected object, and promising means of violating security. The authors propose an integrated approach to ensuring cybersecurity, the main task of which is to preserve the operability of the digital production system in the context of various targeted impacts. This concept corresponds to the main direction of development of protection systems today - this is the implementation of a proactive protection strategy: the presentiment of the threat and adapting the system to future exposure.

The safety block must ensure control of the main parameters of the production process and assess the safety of the current state of the system based on data from all major levels: controllers, SCADA - networks and devices, communication network. The general set of stages of functioning of the safety unit corresponds to the position of active dynamic protection [9] in order to meet the new requirements for the need to predict impacts. These are the stages of monitoring, assessment, decision-making and development of a control action from the security subsystem (if necessary).

Monitoring is implemented by a set of methods and components that collect and preprocess data on the processes occurring in the digital production system, using big data processing technologies, methods for normalizing and aggregating information, integrating information from various sources.

The assessment is carried out through the hierarchy of indicators of sustainability of digital production. The basic is the self-similarity indicator, which reflects the current state of the system. Depending on the specifics of the data and the process, self-similarity can be determined based on the analysis of correlations, Hurst exponent, Fano factor, fractal estimates [10]. An additional important component is the prediction block included in the evaluation module. Forecasting is necessary for analyzing the behavior of the system in the nearest time interval, assessing the applicability of certain compensating influences, since each of them requires a certain time of implementation. Forecasting in digital manufacturing systems is based on big data analysis technologies and methods for evaluating the behavior of dynamic systems.

The stability of the system as a whole is determined by its ability for homeostasis, that is, the ability to develop and implement compensating influences. The decision-making module can be based on one or several, applied simultaneously, approaches. This is the choice of a scenario from the ready-made knowledge base, the development of a compensating effect based on the rules laid down or obtained as a result of machine learning, or another decision-making mechanism. The basis for the construction of this module should be the theory of situational management, based on the assessment of the current situation and the formation of a course of action. The tool for implementing the selected scenarios and reactions is already present in modern technologies. These are software-defined and managed solutions such as software-defined networks.

Built according to the described principles, the security unit will be able to adequately assess the situation, generate forecasts for its development, make and implement a decision on compensating or anticipatory impact with all the variety of threats to digital production.

Conclusion and prospects for further research

The authors considered modern trends in the development of production systems, the features of digital production and the digital economy, from the point of view of technological changes and changes in the field of security. The main technologies that formed the basis of industrial changes and their impact on production and information security technologies are presented.

The digital transformation of production, the emergence of cyber-physical objects and systems, the formation of a cyber environment is an inevitable consequence of the widespread use of programmable controllers and computerization of control processes. At the same time, there has been an increase and change in the specifics of attacks on production systems. The main ones are APT (advanced persistent threat) attacks, targeted, implemented by groups of attackers using various technologies from specialized software solutions to social engineering, implementing several attack vectors. Often, these attacks are not aimed at obtaining data from production systems, but at controlling the production process itself, controlling physical objects. New attacks are diverse and rather ingenious; for large heterogeneous digital production systems, all of their diversity becomes difficult to describe with generally accepted models. Attackers use a wide range of channels of influence, ranging from direct influence on equipment and ending with penetration through corporate networks and the general communication environment.

In these conditions, the development of cybersecurity as a part of information security is becoming an important direction. Cybersecurity combines approaches, methods and means of protecting cyber-physical systems of digital production. The authors propose an integrated approach to protection based on the development of a secure security management module. The main components of the module are: a monitoring unit based on big data technologies; a block of threat-invariant system self-similarity assessment and forecasting; a decision making unit and a homeostasis control unit. Successful implementation of security solutions is ensured by the use of configurable components and networks in process control.

References

1. Shvab K. Chetvertaya promishlennaya revolutsia / K. Shvab - «Aksmo», 2016 - (Top Business Awards)
2. Briniiolfsson A., MacAffi A. «Vtoraya era mashin: rabota, progress i protsvetanie v epochy blestyashih technologii» / A. Briniiolfsson, A. MacAffi, W. W. Norton & Company, 2014.
3. Evans P. C., Annunziata M. Industrial Internet: Pushing the Boundaries of Minds and Machines // Peter C. Evans, Marco Annunziata November 26, 2012 http://files.gereports.com/wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf
4. Annenkov M. Osnovi kiberustoichivosti na finansovom rinke Bezopasnost delovoi informatsii. Cyberustoichivost. No 17 2017.
5. Akinin A. Cyberustoichivost: velenie vremeni !Bezopasnost delovoi informatsii. Cyberustoichivost. No 17 2017.
6. Vasilev U.S., Zegzhda D.P., Poltavtseva M.A. Problemi bezopasnosti tsifrovogo proizvodstva i ego ustoichivost k cyberugrozam. Problemi informatsionnoi besopasnosti. Computer systems. 2017. No 4. P. 47-63.
7. Zegzhda P.D., Poltavtseva M.A., Lavrova D.S. Systematizatsia cyberphizicheskih system i ozenka ih bezopasnosti Problemi informatsionnoi besopasnosti. Computer systems. 2017. No 2. P. 127-138.
8. Zegzhda D.P. Sustainability as a criterion for information security in cyber-physical systems // Automatic Control and Computer Sciences. 2016. T. 50. No 8. P. 813-819.
9. Drobotyn E.B. Teoreticheskie osnovi postroenia systemi zachity ot computernih atak dlya avtomatizirovannich system upravlenia. SPb: Naukoemkie technologii, 2017. – 120 p.
10. D. P. Zegzhda E. Yu. Pavlenko Cyber-Physical System Homeostatic Security Management // Automatic Control and Computer Sciences ISSN 0146-4116. Vol. 51, No. 8, 2017