symmetry

MDPI

Article

Key Concepts of Systemological Approach to CPS Adaptive Information Security Monitoring

Maria Poltavtseva [1,*], Alexander Shelupanov [2], Dmitriy Bragin [2], Dmitry Zegzhda [1] and Elena Alexandrova [1]

[1] Institute of Cybersecurity and Information Protection, Peter the Great St. Petersburg Polytechnic University, 195251 Saint Petersburg, Russia; dmitry@ibks.spbstu.ru (D.Z.); helen@ibks.spbstu.ru (E.A.)
[2] Department of Comprehensive Information Security of Electronic Computer Systems, Tomsk State University of Control Systems and Radioelectronics, 634050 Tomsk, Russia; saa@tusur.ru (A.S.); bds@csp.tusur.ru (D.B.)
* Correspondence: poltavtseva@ibks.spbstu.ru; Tel.: +7-965-057-4399

Abstract: Modern cyber-physical systems (CPS) use digital control of physical processes. This allows attackers to conduct various cyberattacks on these systems. According to the current trends, an information security monitoring system (ISMS) becomes part of a security management system of CPS. It provides information to make a decision and generate a response. A large number of new methods are aimed at CPS security, including security assessment, intrusion detection, and ensuring sustainability. However, as a cyber-physical system operates over time, its structure and requirements may change. The datasets available for the protection object (CPS) and the security requirements have become dynamic. This dynamic effect causes asymmetry between the monitoring data collection and processing subsystem and the presented security tasks. The problem herein is the choice of the most appropriate set of methods in order to solve the security problems of a particular CPS configuration from a particular bank of the available methods. To solve this problem, the authors present a method for the management of an adaptive information security monitoring system. The method consists of solving a multicriteria discrete optimization problem under Pareto-optimality conditions when the available data, methods or external requirements change. The experimental study was performed on an example of smart home intrusion detection. In the study, the introduction of a constraint (a change in requirements) led to the revision of the monitoring scheme and a different recommendation of the monitoring method. As a result, the information security monitoring system gains the property of adaptability to changes in tasks and the available data. An important result from the study is the fact that the monitoring scheme obtained using the proposed management method has a proven optimality under the given conditions. Therefore, the asymmetry between the information security monitoring data collection and processing subsystem and the set of security requirements in cyber-physical systems can be overcome.

Keywords: adaptive control; information security monitoring; cyber-physical systems; system analysis

Citation: Poltavtseva, M.; Shelupanov, A.; Bragin, D.; Zegzhda, D.; Alexandrova, E. Key Concepts of Systemological Approach to CPS Adaptive Information Security Monitoring. *Symmetry* **2021**, *13*, 2425. https://doi.org/10.3390/sym13122425

Academic Editor: Jeng-Shyang Pan

Received: 20 October 2021
Accepted: 23 November 2021
Published: 15 December 2021

1. Introduction

The development of digital technologies has led to the emergence of a new system class, known as cyber-physical systems (CPS). These systems combine digital and physical process controls. Moreover, the implementation of digital technologies has led to an increase in the number of cyberattacks on various spheres: From medical science to industry related systems, etc. [1] Today, there are a large number of security breaches associated with CPS. Researchers are developing new approaches for the security of cyber-physical systems [2,3], including authentication methods, encryption, etc. However, the current work shows that the task of overcoming protection systems remains possible [2–5].

A wide variety of CPS, their heterogeneity both structurally and technologically, and the features of operation complicate the task of creating effective protection systems. Due

to the continuous changes in the legal framework, the expansion of security objectives in relation to CPS also require continuous changes in systems that ensure their security.

During the process of ensuring the stable functioning of cyber-physical systems, decision-making is based on the information entered into the information security management system from the monitoring system. Therefore, the monitoring system is a key module in ensuring the information security management of cyber systems. A large number of research works have been devoted to modern information security monitoring systems (ISMS), from architectural solutions [6–11] to individual methods for solving security problems [12–15]. However, all of these works pay little attention to the task of ensuring the adaptability of ISMS to the structural and functional evolution of the protected object and the changing environmental conditions.

At present, CPS security methods are actively improved. Researchers are adapting solutions for computer networks and developing specialized approaches. Therefore, in the face of multiple challenges, the choice of the most appropriate method is quite difficult. More importantly, cybernetic systems do not remain unchanged. Their structural elements and the connections between them change, as well as their settings, configurations, and security requirements. In this case, it is necessary not to create a new protection system every time, but to adapt to the existing one. In addition, the methods of solving security problems change due to the changes in data and requirements. Solving this problem for large-scale cyber-physical systems is impossible without applying the analysis and synthesis approaches of complex systems. To manage the security of the CPS effectively, it is necessary to create new adaptive information security monitoring systems (AISMS). AISMS are able to ensure the awareness of the information security management system in the context of the evolution of the object of protection and changes in the external environment. The purpose of this work is to form a systemological approach for this kind of AISMS development based on a systematic approach and system analysis methodology.

2. Approach to Adaptive Information Security

2.1. The Problem of Modern CPS Security Monitoring

Changes in technological process control systems, an increase in the degree of digitalization, in threats and attacks on digital systems, as well as an increase in the severity of the consequences of these attacks [16,17] have led to a change in the approach to information security monitoring. Until recently, the ISMS performed the conformity assessment task [18], which solves the problem of security information and event management (SIEM). Today, this functionality is significantly expanding, which is evident in the example of the creation of a large number of security control centers based on monitoring systems [19], as well as changes in the legal system [20]. The modern ISMS is a continuous process of monitoring and analyzing the results of registration of security events [20]. The purpose of this process is to identify violations of information security, as well as thunderstorms and vulnerabilities in the computer systems of the protected object.

In order to solve the problem of ensuring the security of the CPS, the ISMS system must collect and analyze data on various aspects of the protected object, starting from the functioning of individual objects, to the assessment of the CPS in a complex, and finally the analysis of the external environment (Figure 1).

At the same time, the variety of security tasks leads to the requirement of a large number of monitoring methods. Modern methods for solving ISMS security problems have different efficiencies in relation to the different objects and/or conditions. In addition, these methods require prompt correction of their set in the event of external and internal changes and, often, the joint use of several methods to solve one security problem. A cyber-physical system, as an object of protection, is a complex dynamic system that does not lend itself well to analytical description and modeling [21]. The general theory of systems and the systems approach describe the system features as hierarchy, integration, and connectivity [22]. Under these conditions, the information security monitoring subsystem faces two priority tasks. The first is to ensure the collection and preparation of data from the protected object

in all the above aspects. The second is to provide and support methods for analyzing this data in order to solve security problems at all levels of object presentation: From individual components to industrial CPS as a whole, taking into account the context of the external environment, the convergence, and interconnections of the components.

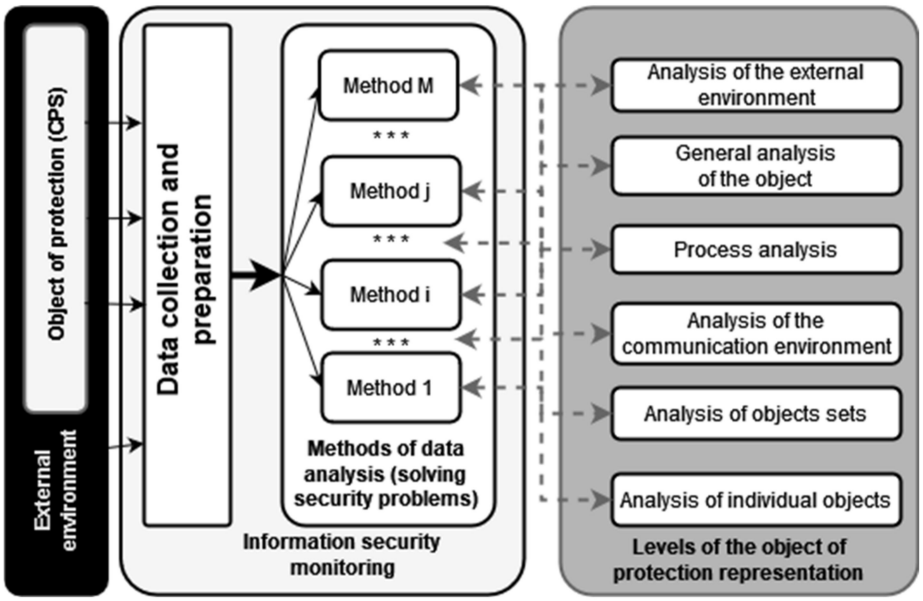

Figure 1. CPS data analysis in the system of information security monitoring (*** display the quantity of methods).

2.2. Principles of the Systemological Approach to Adaptive Information Security Monitoring

The choice of an effective set of methods, the timely preparation of data for their application, and the adjustment of the set of methods and data in the case of changes in the object and/or the external environment, require a systemological approach to the adaptive monitoring of information security. It is based on the system analysis methodology and the construction of mutual mappings between the security problems and their solution methods and the available datasets from the object of protection.

The approach to consider the object of the research in the system analysis [22] and the research levels of the object in the general systems theory [23], which is applied to solve the problem of intelligent adaptive monitoring, allows one to formulate the general principles of the adaptive monitoring of information security of CPS, such as:

1. The principle of integrity.
2. The principle of evolutionary adaptability.
3. The principle of hierarchical connectivity.

The principle of integrity is a comprehensive consideration of the research object (object of protection) in relation to all of the security tasks. This is an assessment of both the internal and external environment of functioning. Any system, including the object of protection, is considered both as a set of components/systems of a smaller size, and as part of a system of a higher order. This principle establishes the ability of the monitoring system to take into account all types of security tasks, including security assessment, analysis of the operating environment, and change of protection goals. To implement this principle, the object of protection is represented as a dynamic set of all the observed parameters of its operation, both external and internal due to data-driving technologies. The set of measured parameters is determined by the set of security problems to be solved.

The convergence principle implies a change in the information security monitoring system along with the evolutionary development of the protected object and its functioning environment. It requires not only maintaining the implementation of current security tasks, taking into account the interrelationships, but also changing this list during the

evolution of the protected system and environment, as well as the automated or automatic rebuilding of the monitoring process when the working conditions change. Then, the set of measured parameters of the monitoring object in the current operating mode is determined by external factors and is dynamic in the process of functioning.

The evolution of the set of measured parameters requires adaptation of the protected object model, as well as the structures and formats of the data collected during monitoring. To ensure the automatic processing of information in this case, it is necessary to highlight the main data models, which are both used in security monitoring and internally by processing and storage tools.

The principle of hierarchical connectivity highlights the hierarchical organization of systems and components when considering the object of protection from the point of system analysis view. It declares the consideration of an object in the form of a set of hierarchically related representations, corresponding to varying degrees of detail of both the components of the object of monitoring and levels of monitoring from the point of view of the theory and methods of ensuring information security [19,24].

The principles of the systematic approach ensure that the ISMS is adaptive to the changing tasks and structural dynamics of the protection object. Figure 2 contains the proposed scheme of an adaptive ISMS, highlighting the implementation of the principles of the systematic approach.

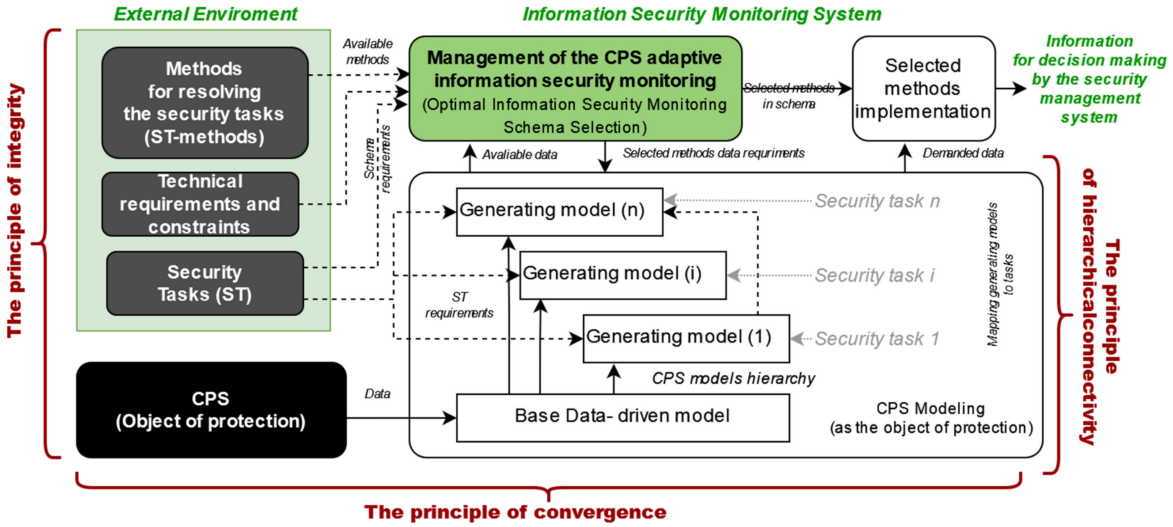

Figure 2. CPS adaptive ISMS scheme, highlighting the principles of the systematic approach.

Each method of solving each security problem requires a specific set of input data. A basic data-driven model of the security object generates these sets. Each set is called a generating model (according to the theory of complex systems [22,23]). The technology of data-driven CPS model development is a separate task and is beyond the scope of this article. The authors of [25–28] consider it in detail. Next, we will focus on the key technology for implementing the systematic approach in our solution. This is the ISMS management methodology.

The adaptation of monitoring approaches to the changing conditions consists of changing the methods of data processing. It takes place when the old methods no longer meet the requirements (e.g., attack detection rates) or the available datasets have changed and the old methods are no longer applicable since there is no data for them. To ensure optimal performance and meet the given constraints in monitoring adaptation, we used an optimal choice theory approach. The problem, of discrete multicriteria optimization of the monitoring scheme (as a set and order of data processing methods) under the given constraints and the Pareto-optimal set of possible outcomes, is set. The solution for this problem and an experimental example are given below.

3. Management of the CPS Adaptive Information Security Monitoring

To implement the principles of integrity and convergence, it is necessary to mutually map the security problems (goals), solution methods, and datasets.

Based on this map, a formal definition of the monitoring scheme is: $S = \left\langle \left(I^{Cur}, M^{Cur}, D^{Cur}\right), F_{IM}, F_{MD} \right\rangle$ where $I^{Cur} \subseteq I = \{i_1, \ldots, i_I\}$ is the set of security goals, uniquely determined and used within the framework of a given scheme; $M^{Cur} \subseteq M = \{m_1, \ldots m_M\}$ is the set of all the available methods used to solve these problems at the moment (but only in this scheme or monitoring system mode); $D^{Cur} \subseteq D = \{d_1, \ldots d_D\}$ is the set of used data groups from the protected object, respectively.

$F_{ID} : I \to D$—security tasks mapping to multiple security object datasets. Reverse mapping $F_{ID}^{-1} : D \to I$ shows which problem is solved using specific data.

$F_{IM} : I \to M$—security tasks mapping to a variety of solving methods. Reverse mapping $F_{IM}^{-1} : M \to I$ shows which problem the given method solves.

$F_{MD} : M \to D$—security tasks solving methods mapping to a set of the protected object datasets. Reverse mapping $F_{DM}^{-1} : D \to M$ shows which method uses the given data.

The main stages of the adaptation process in the information security monitoring system are:

1. Assessment of the state, including the assessment of the all the security goals fulfillment and objectives, as well as the assessment of the sufficiency conditions and minimality of data and methods for solving the problem.
2. Adjustment and fixation of security tasks.
3. Determination of the available methods. In their absence, a transition to a higher-level adjustment of security objectives or system parameters, including technical capabilities for data collection and resource-based boundary conditions.
4. Development of a new monitoring scheme, including the assessment of the time methods characteristics and data preparation, the assessment of the entire set of boundary conditions, and the solution of the problem of finding the optimal monitoring scheme.
5. Adjustment of the data collection and preprocessing scheme in accordance with the new information security monitoring scheme.

Then, the adaptability of information security monitoring from the point of a systematic approach and within the framework of the proposed systemological principles is achieved by timely adjusting the monitoring scheme through building a new map in the context of the changed data sets, methods or tasks.

Managing the adaptive monitoring process includes the construction of a mutual map between a variety of security problems, a variety of methods for their solution, and a variety of sets of observable data of an object, followed by a selection of applied methods subsets and measured data based on a fixed set of tasks.

For each monitoring scheme, we will assign a set of parameters or characteristics Par, where parameter $pr_q \in Par$ is defined by tuple $pr_q = \langle Name, Value \rangle$. In addition, for each of these parameters, there is an objective function $Fpr_q^0\left(i_j, m_k, D_k^{Cur}\right)$, defined in class $\mathbb{R}$ real numbers for all the security problems accepted in a certain scheme $i_j \in I^{Cur}$, for the method of solving each individual problem $m_k \in M^{Cur}$, and the datasets for that solution $D_k^{Cur} \subseteq D^{Cur}$.

The set of parameters Par is defined as:

$$Par = \left\{ \begin{array}{c} pr_q \middle| \forall \left(i_j \in I^{Cur}, m_k \in M^{Cur}, D_k^{Cur} \subseteq D^{Cur}\right) \\ \exists Fpr_q^0\left(i_j, m_k, D_k^{Cur}\right) \in \mathbb{R} \end{array} \right\} \quad (1)$$

A corresponding objective function is available for each parameter of the scheme. In this case, the parameter value will be the value of this objective function of this parameter or $pr_q = \left\langle Name, Value = Fpr_q^0 \right\rangle$.

The objective functions of the different parameters are multidirectional. For example, when defining the parameter "the processing time for detecting some attack", the value

of the time function should be minimized to accelerate the work. At the same time, the parameter "the accuracy of detecting the some attack" should be maximized to reduce the number of errors of the first and second work.

To reduce the objective functions of the parameters to a general form and form a generalized objective function of the monitoring scheme, along with maximizing its value when solving the problem of finding the optimal scheme, we introduce the following transformation rules for the initial objective functions of the parameters:

- For the initial objective functions of parameters of the form $Fpr_q^0 \to max$, take the resulting objective function of this parameter as $Fpr_q = Fpr_q^0$.
- For the initial objective functions of parameters of the form $Fpr_q^0 \to min$, take the resulting objective function of this parameter as $Fpr_q = 1/Fpr_q^0$.

Let us give an example of the original objective function parameter transformation, which is the decision time for a scheme $s_l \in S$ and security objectives i_j. The time of this operation, in the general case, consists of the preparation time of the slowest piece of data for making a decision $\max\limits_t \left(t_t^{d_{j,k,t}^{Imp} \in F_{MD}(m_{j,k})} \right)$, where t is a dataset number, $m_{j,k}$ is the k method for solving the j security problem, $d_{j,k,t}^{Imp}$ is the processed data fragment t by method k for task j, and the running time of the analysis method is $t_j^{m_{j,k} \subseteq F_{IM}(i_j)}$, where i_j is a security problem. Then, the time function that minimizes the total decision-making time, transformed in accordance with the rules above is as follows:

$$pr_i^{decision\ time}.Value = 1/\min_k \left(t_j^{m_{j,k} \subseteq F_{IM}(i_j)} + \max_t \left(t_t^{d_{j,k,t}^{Imp} \in F_{MD}(m_{j,k})} \right) \right) \quad (2)$$

In fact, the transformed function (2) reflects the "speed" of decision-making in solving the security problem and is subject to maximization.

On the basis of the maximized objective functions of the parameters of the scheme, we define the general objective function of information security monitoring scheme s_i as a multiparameter function of the form:

$$F_{s_i}^{\Sigma} = F\left(\sum \left(Fpr_q | q \in [1, |Par|]\right)\right) \to max \quad (3)$$

which is a function of the overall objective functions of parameters. Determination of a specific objective function (3) is a specific task of AISMS management. It regulates the final criteria for choosing the optimal data scheme and may be dependent on the protected object.

Based on the set of possible mappings between the security problems, methods, and data, a number of monitoring schemes can be formed that implement the solution of a given set of security problems and, potentially, even satisfy the boundary condition R.

In addition to this set, it is proposed to formulate and solve a discrete multicriteria optimization problem based on the above-defined target function of the monitoring scheme and to search for an optimal scheme for collecting, processing, and analyzing data for adaptive monitoring of industrial CPS. Taking into account the convergence principle based on the mutual mapping of F_{IM}, F_{MD}, due to the reduction of the set R, it is defined as $\left\{ \left\langle \left[(i, m, d) : i \in I^{Cur}, m \in M, d \in D \right] \right\rangle \right\}$ where based on functions F_{IM}, F_{MD} each security problem is associated with some non-empty set of methods for its solution, and each method corresponds to a non-empty set of initial data consumed by it. Then, the set of security problems, taking into account the related methods and data, can be represented as U, which is a set of variants of triplets for monitoring schemes:

$$U = \left\{ \left(i_j, \left\{ \left(m_{j,k}, D_{j,k}^{Imp} \right) \middle| \begin{array}{c} m_{j,k} \subseteq F_{IM}(i_j) \\ D_{j,k}^{Imp} \subseteq F_{MD}\left(m_{j,k}\right) \end{array} \right\} \right) \middle| i_j \in I^{Cur} \right\} \quad (4)$$

where each problem from a fixed I^{Cur} is assigned a set of possible solution methods and the data required for them $\left(m_{j,k}, D_{j,k}^{Imp}\right)$, which corresponds with the mapping rules $m_{j,k} \subseteq F_{IM}(i_j)$ and $D_{j,k}^{Imp} \subseteq F_{MD}\left(m_{j,k}\right)$.

Furthermore, the set of solutions R satisfying the conditions of sufficiency and non-redundancy is reduced based on the boundary values determined by the characteristics of the goals and objectives of security.

Since every solution of the set R is initial for some monitoring scheme from the set $S \subseteq S_0$ based on (4), the monitoring scheme parameters for which the objective functions are set can also be applied. For each significant parameter of the scheme $par_h \in Par$, the boundary condition b_h is determined as the minimum boundary of the objective function value Fpr_q. The identification of the parameter and the corresponding boundary is carried out by name. The boundary value is then described as a tuple $b_h = \langle Name,\ Value \rangle$, where the value as well as Fpr_q are defined on the set of real numbers and the aggregate set of boundary values can be given as:

$$B = \{b_h | b_h = \langle Name,\ Value \rangle,\ Value \in \mathbb{R}, h \in [1, H]\} \tag{5}$$

The fulfillment of the boundary conditions, in accordance with the constraint (5), over the scheme parameters determines the following rule:

$$\forall b_h \in B \exists pr_q \in Par\left[\left(pr_q.\ Name = b_h.Name\right) \wedge \left(Fpr_q > b_h.Value\right)\right] \tag{6}$$

If above a certain scheme $s_l \in R$, the condition specified by the corresponding rule (6) is met, indicating that this scheme satisfies all of the boundary conditions. Then, the s_l scheme satisfies all of the requirements for the security goals and objectives, as well as the technological capabilities of the protected object. In addition, it can be included in many potentially applicable monitoring schemes S^{Imp}. For the formation of a set $S^{Imp} \subseteq S$, the following steps are needed:

1. For each initial information security monitoring scheme $s_l \in R$, significant parameters of the scheme are determined and a vector of parameter values $\vec{Par}_l$ is formed.
2. The creation of the sorted scheme $s_l \in R$ projections of the form $\left\langle s_l, par_{q,l} \right\rangle$ ascending the parameter value, which is $\forall\left(pr_{q,l} \in \vec{Par}_l, pr_{q,l+1} \in \vec{Par}_{l+1}\right)\left[pr_{q,l}.Value > pr_{q,l+1}.Value\right]$ where $q \in \left[1, \left|\vec{Par}_l\right|\right]$ ш$l \in [1, |R|]$.
3. Filtering projections according to the boundary condition for each significant parameter for which the corresponding boundary is set (5). In this case, schemes with parameters not exceeding the boundary value are excluded from the set S, which is $S^{Imp} = S \backslash \{s_l\}$, where $\{s_l\}$ is a set of schemes that do not satisfy the boundary conditions. For each excluded element s_l of set $\{s_l\}$, there is a way out of at least one boundary value:

$$\forall s_l \exists b_h \in B\left[pr_{q,l}.Name = b_h.Name \wedge pr_{q,l}.Value \leq b_h.Value\right] \tag{7}$$

   where (7) defines the filtering rule.
4. Formation of the resulting set S^{Imp} after eliminating from R all of the schemes that violate at least one boundary.

The resulting set of schemes S^{Imp} defines a variety of monitoring schemes that satisfy all of the requirements. If eventually $S^{Imp} = \varnothing$, therefore, a monitoring scheme that satisfies all of the boundary conditions does not exist within the given technological boundaries (although there are schemes that satisfy the conditions of sufficiency and non-redundancy). If $\left|S^{Imp}\right| > 1$, the next task is to determine the optimal scheme from this set, corresponding to the protected object.

The choice of the final optimal information security monitoring scheme is based on solving the optimization problem along with maximizing the objective function of the monitoring scheme $F_{s_i}^{\Sigma}$ by maximizing its constituent components. Due to the complexity of the problem solving and the inconsistency of the monitoring scheme parameters, the t Pareto optimal solutions set S^{Opt} with its subsequent narrowing is the only variant of the scheme.

To form a set S^{Opt} over the potentially applicable schemes ISMS S^{Imp} the dominance relation is given: Scheme s_x dominates s_y ($s_x \succ s_y$), if for all Fpr_q values $Fpr_q^{s_x} \geq Fpr_q^{s_y}$. Scheme s_x dominates $\succ$ scheme s_y if and only all the values of the scheme parameters s_x are greater than or equal to the corresponding values of the scheme s_y parameters.

$$\left(\begin{array}{c} \forall par_q \in Par\left[par_q^{s_x}.Value \geq par_q^{s_y}.Value\right] \\ \wedge \exists par_q \in Par\left[par_i^{s_x}.Value > par_i^{s_y}.Value\right] \end{array} \right) \Longleftrightarrow s_x \succ s_y \tag{8}$$

Monitoring schemes s_x, s_y ($s_x = s_y$) are considered equivalent if for all Fpr_q values $Fpr_q^{s_x} = Fpr_q^{s_y}$. To determine the optimal monitoring scheme from a variety of potentially applicable monitoring schemes S^{Imp} , satisfying the boundary conditions excludes all of the schemes for which there is a dominant or equivalent scheme in the following set:

$$\forall s_l \in S^{Imp}, s_g \in S^{Imp} \left[\left(s_g \succ s_l\right) \vee \left(s_g = s_l\right) \Rightarrow S^{Imp} := S^{Imp} \backslash \{s_l\} \right] \tag{9}$$

A set of optimal schemes S^{Opt} is formed based on the rule (2.16):

$$S^{Opt} = \left\{ s_l \middle| \left(s_l \in S^{Imp}\right) \wedge \left(\nexists \left(s_g \in S^{Imp}\right) | \left(s_g \succ s_l\right) \vee \left(s_g = s_l\right) \right) \right\} \tag{10}$$

Evidently, this set cannot be empty, since the exclusion of the schemes occurs sequentially, and $S^{Opt} = \varnothing$ is possible only by excluding the last single scheme. However, the exclusion of this scheme is possible only if there is a dominant one over it, which, given its singleness is impossible. If $\left|S^{Opt}\right| = 1$, we can say that $S^{Opt} = \{s_l\}$, where scheme s_l is the only optimal solution and optimal scheme for monitoring information security, which is $s^{Cur} = s_l = \left\langle \left(I^{Cur}, M^{Cur}, D^{Cur}\right), F_{IM}, F_{MD} \right\rangle$. Otherwise, when $\left|S^{Opt}\right| > 1$, the multitude S^{Opt} (10) is the Pareto optimal and needs to be reduced to a single solution.

In modern mathematics and the optimization theory, a set of methods has been developed to reduce the Pareto optimal sets in the field of discrete optimization [29]. Today, the main approaches to solving this problem are:

1. Method of criteria (parameters) prioritization.
2. Method for calculating the generalized criterion.
3. Derived methods.

A preference relation allows one to take into account the characteristics of a particular cyber-physical system and correct the preference attitude throughout the life cycle of a protected object. The introduction of a generalized criterion presupposes a strict formalization of the above-defined objective function of the monitoring scheme $F_{s_i}^{\Sigma}$ with the establishment of a relationship between heterogeneous parameters of the monitoring scheme. However, today the parameters of the monitoring scheme are very heterogeneous, including both temporal and qualitative resource characteristics, in which the formation of a method for generating a generalized criterion seems to be too heterogeneous and a poorly formalized task.

For industrial cyber-physical systems, we propose the prioritization of the monitoring scheme parameters, since this approach will allow the following:

1. Reflect the peculiarities of a particular industrial CPS from the point of view of decision-makers and combine the automatic and automated selection of the optimal monitoring scheme.

2. Reflect the shift in priorities in the choice of the monitoring scheme when the stability margin changes the CPS for a particular set of limited resources taken into account in the scheme parameters.
3. Conduct a correspondence between the generation of the information security monitoring scheme and the risk-based threat model CPS, automatically prioritizing the directions of increased risk, which is, for threats with maximum residual risk values, maximize the margin of detection accuracy while remaining in the boundary values for the rest of the characteristics.

In the general case, it is proposed to prioritize the characteristics of detecting destructive impacts by ranking them in accordance with the residual risk assessments. Then, over the set of parameters of the monitoring scheme $pr_q \in Par$ a priority relation $\succ$ must form a ranked list of parameters $pr_1 \succ pr_2 \succ \ldots \succ pr_{|Par|}$. Due to the risk-oriented approach to the information security of the CPS [30–33], the following procedure is proposed for the formation of this list:

1. Comparison of the set of residual risks Ri with the parameters of the monitoring scheme through mappings to security objectives $Ri \to I^{Cur}$, $I^{Cur} \to Par$ and construction of the transitive mapping $Ri \to Par$, forming a pair of risks and related parameters of the ISMS scheme of the form $\{r_i, Par_{r_i}\}$, where $r_i \in Ri$ a $Par_{r_i} \subseteq Par$.
2. Ranking a set of pairs $\{r_i, Par_{r_i}\}$ based on the cost of the risks.
3. Ranking of each subset Par_{r_i} according to the degree of influence on the corresponding risk of each individual parameter.

Selecting the final scheme $s^{Cur} = \langle (I^{Cur}, M^{Cur}, D^{Cur}), F_{IM}, F_{MD} \rangle$ based on a ranked list of prioritized schema parameters $pr_1 \succ pr_2 \succ \ldots \succ pr_{|Par|}$ is produced by taking previously constructed parametric projections of the schemes $\left\langle s_l, par_{q,l} \right\rangle$ for $s_l \in S^{Opt}$, ranking according to order $pr_1 \succ pr_2 \succ \ldots \succ pr_{|Par|}$ and consistent reduction S^{Opt} until $\left|S^{Opt}\right| > 1$. The latter scheme will be selected as the optimal solution to the problem of constructing an information security monitoring scheme based on the convergence of security problems, methods for their solution, and datasets of the protected object.

4. Experimental Studies

To test the adaptive monitoring management method experimentally, the security task of detecting anomalies in network traffic signaling the presence of cyber-attacks based on the [34–40] papers, was considered. Data-driven technologies for CPS were used to collect data and model the object of protection [41–43].

Figure 3 shows a schematic of the experimental stand. The CPS is represented by the dataset from the water treatment system [40]. The data contained a normal operation and attacks. The security management system was not simulated. The monitoring system is represented by the management subsystem (gray in Figure 3). The management subsystem contains a method bank and a management module. The control module is implemented according to the methodology based on the multicriteria optimization problem previously mentioned.

The bank of methods is represented by 18 algorithms for solving a given security task. It contains two types of machine learning-based and one of the multifractal algorithms in six different implementations each, including multi-threaded implementations. The algorithms have different characteristics in terms of time, accuracy, and computational requirements. The variability in characteristics is sufficient to test the control method, as shown in the example below. Newer algorithms, such as [41–44], were not included, since their implementation and testing on a given dataset for the comparability of results would be time consuming [45–47]. By the time this data was ready, there would still be new algorithms. The bank of methods can be extended by any new method, including [2,48–52]. At the same time, the comparative characteristics of the methods are important for management methodology testing, since the task of choosing the best method from the existing ones is not set. Here, we solve the task of a method selecting by the given criteria.

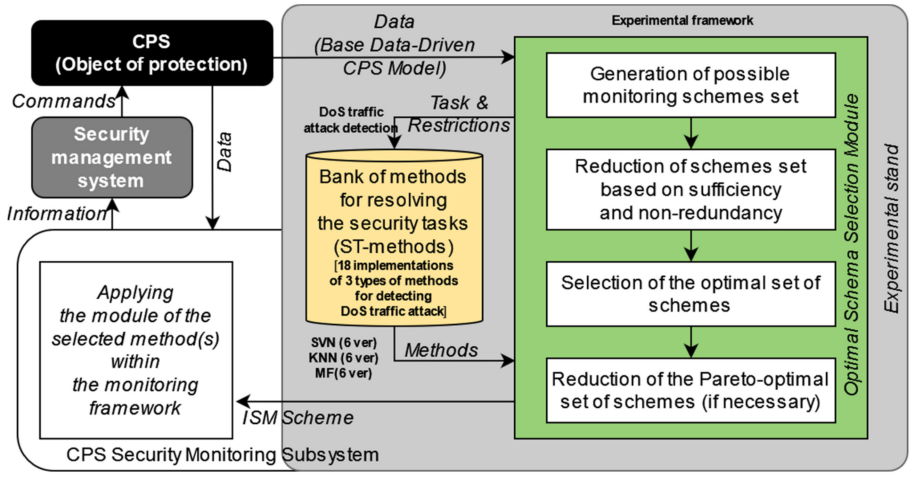

Figure 3. Schematic of the experimental stand.

In the experimental example, we considered the task of monitoring control to solve the problem of the detection of DoS attack on the CPS traffic. The number of published methods for detecting specific attacks was not sufficiently diverse [45,47] for each attack to test the control module. We will repeat this experience when there are more of them, expanding the method bank in industrial implementation.

The bank of methods for solving the problem was formed on the basis of methods well described in the sources, the characteristics of which are available for evaluation, in particular, on the basis of references [36–39]. The solution bank included methods based on two well-known industry classifiers of network traffic: The classifier k-nearest neighbor (KNN 1–6) and the support vector machine (SVM 1–6) in various modifications (six modifications of each classifier), as well as the multifractal (MF) analysis method in various implementations. For the latter, the characteristics of five different implementations were included, taking into account data parallelization, starting from one computational node.

The problem of finding the optimal scheme was considered under certain constraints. First, the use of only one solution method (both technological and financial constraint). Secondly, the required quality of detection, expressed in the indicator $Accuracy = 0.85$. Third, the time to detect an attack is no more than 1 s, excluding data preparation time.

Since the time spent on detecting an attack is minimized, according to the method used, the function expressing this indicator during the formation of the objective function of this parameter was replaced by the inverse (*Velocity* was introduced) and a limitation was set: $F_{vel}^{a_1^{DoS}} = {}^1/_{F_{\text{attack detection time}}^{a_1^{DoS}}} > B_{vel}.Value$. All of the methods located in the knowledge base accept a fixed input dataset in the form of a time series, the preparation time of which is the same for all of them: $\forall\left(m_i \in M_{a_1^{DoS}}\right) \rightarrow t_{preprocessing} = const$. This eliminates the influence of the preprocessing stage on the final efficiency. As a result, the limitation of the anomaly detection time was set as: $F_{vel}^{a_1^{DoS}} = {}^1/_{F_{\text{attack detection time}}^{a_1^{DoS}}} > 1$

Then, the boundary conditions are: $B_{vel} = \{\langle Velocity,\ 1\rangle\}, B_{Accur} = \{\ \langle Accuracy,\ 0.85\rangle\}$. Limitations on the number of methods $Method_{NUM} = 1$ are also used consider various situations. An additional limitation on the number of nodes was introduced $Parralell = 0$. The conditions on the number of methods and computational nodes were applied in filtering (reduction of sets of monitoring schemes), first during the initial generation of schemes and second during the last assessment of applicability, as an additional condition.

The initial set of schemes S after the primary filtering of the set R, taking into account the conditions of sufficiency, non-redundancy, and restrictions on the number of methods, took the form presented in Table 1.

Table 1. Set of monitoring schemes and their characteristics.

Scheme	Scheme Parameters		
	Parralell	*Velocity*	*Accuracy*
KNN-1	0	0.0001	0.915
KNN-2	0	0.0002	0.9
KNN-3	0	0.0002	0.874
KNN-4	0	0.0001	0.823
KNN-5	0	0.0002	0.775
KNN-6	0	0.0003	0.86
SVM-1	0	0.938	0.907
SVM-2	0	1.183	0.89
SVM-3	0	1.480	0.863
SVM-4	0	2.427	0.807
SVM-5	0	2.469	0.757
SVM-6	0	5.181	0.837
MF-1 sequential	0	0.779	0.97
MF-1 parallel	1	3.211	0.97
MF-2 parallel	1	3.305	0.97
MF-3 parallel	1	3.439	0.97
MF-4 parallel	1	3.787	0.97
MF-5 parallel	1	4.224	0.97

Furthermore, mandatory restrictions B_vel and B_Accur were applied for these schemes for constructing a set of valid schemes. In this case, a boundary estimate of time (Figure 4) and accuracy (Figure 5) was carried out.

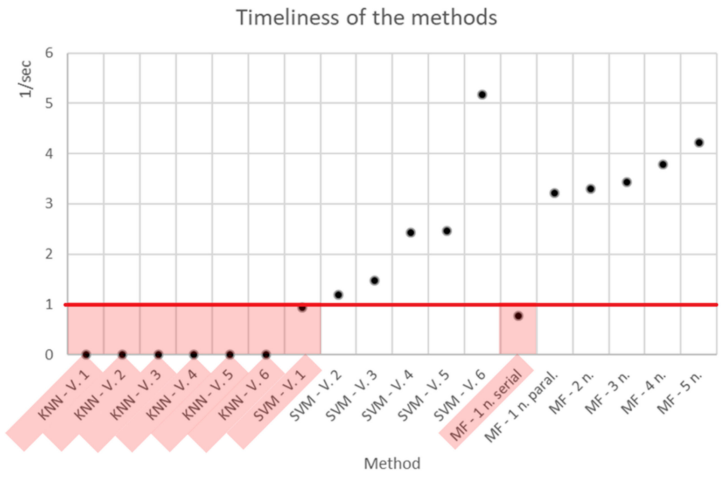

Figure 4. Estimation of the boundary condition by the time of the methods operation.

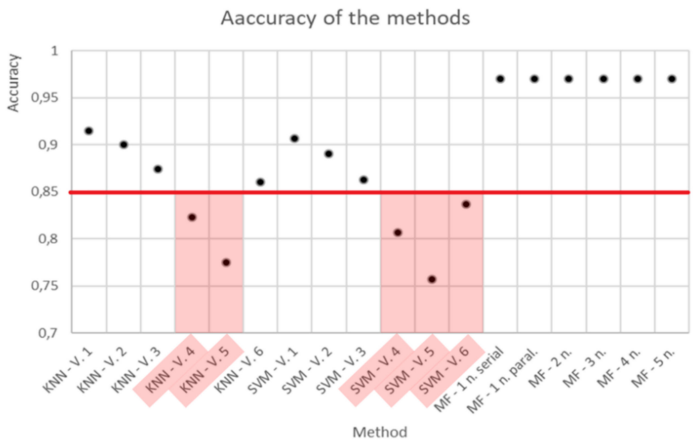

Figure 5. Evaluation of the boundary *Accuracy* condition.

Next, we will consider the basic version of solving the problem of finding the optimal scheme without taking into account the possibility of parallel computing or its absence $Parralell$. Then, the reduction of the original set of schemes according to the indicated restrictions (B_{vel} and B_{Accur}) leads to a set of potential security monitoring schemes S^{Imp}, including the schemes SVM 2, 3 and MF parallel 1–5.

The set S^{Opt} is defined based on the application to $\boldsymbol{S^{Imp}}$ by assessing the dominance relationship between the schemes $(s_i, s_j) \in \boldsymbol{S^{Imp}}$. In this example, the scheme "MF-5 parallel" dominates the rest in terms of time and accuracy, which leads to a single solution s^{Cur} = "MF -5 parallel".

The next example with the additional condition $Parralell = No$ occurs when the reduction of the set of the initial monitoring schemes takes place. Then, the reduction by the indicated constraints leads to a set of potential security monitoring schemes $\boldsymbol{S^{Imp}}$, including the schemes from Table 2.

Table 2. The set of monitoring schemes $\boldsymbol{S^{Imp}}$ and their characteristics (option 2).

Scheme	Scheme Parameters		
	Parralell	***Velocity***	***Accuracy***
SVM-2	1	1.183	0.89
SVM-3	1	1.480	0.863

In this case, the assessment of dominance will not allow the exclusion of one of the schemes, since "SVM-2" prevails ***Accuracy*** and "SVM-3" prevails ***Velocity***. Consequently, $\boldsymbol{S^{Imp}}$ is a Pareto-optimal set, which is proposed to be prioritized according to the accuracy of observations and $\boldsymbol{s^{Cur}}$ = SVM-2.

5. Discussion

Three characteristics of information security monitoring (in general) are considered: Completeness, reliability, and timeliness. The completeness of information security monitoring indicates the provision of all the security problems with methods and data for their solution. Reliability indicates the ability to reflect the real processes of the protected object or the provision of methods for solving security problems with non-obsolete data reflecting the state of the CPS. Timeliness refers to the ability to analyze information security monitoring data in compliance with the specified boundary conditions.

Let us formally prove the compliance of the obtained solution with the requirements of completeness, reliability, and efficiency of monitoring. At first, let us show that the above-mentioned approach to finding a rational mapping between the sets A, M, D expressed in the final information-processing scheme $s^{Cur} = \langle (A^{Cur}, M^{Cur}, D^{Cur}), F_{AM}, F_{MD} \rangle$ allows one to meet the requirements for completeness, reliability, and timeliness of information security monitoring, if there is no distortion of data of the protected object during transmission to the monitoring system.

To ensure the completeness of adaptive monitoring, the following conditions ought to be met:

1. All of the sets of safety problems have methods for their solution, if these methods exist.
2. All of the applied methods of solving security problems have data from the protected object.

Both of the conditions are based on the construction of mappings F_{AM}, F_{MD}. The completeness of these mappings is based on the fulfillment of the conditions of sufficiency and minimality of the data collected and the methods used. Then, the completeness of adaptive monitoring under an intelligent control is ensured if the sufficiency condition is not violated during the search for a rational scheme, as described above.

Let us prove that any resulting scheme s^{Cur} meets these conditions. According to the definition of the original set of schemes $S = \langle (A^{Cur}, M^{Cur}, D^{Cur}), F_{AM}, F_{MD} \rangle$, corresponding to the set of sufficient and minimal mappings, the conditions of sufficiency and

minimality are satisfied for any scheme $s_l \in S$. Then, in the process of searching for the final scheme in order for these conditions to not be met for s^{Cur}, it is necessary to replenish the set S by the scheme s+, over which F_{AM}, F_{MD} are not executed. However, only a reduction of the set S occurs, and this scheme is impossible. Consequently, s^{Cur} meets the condition of sufficiency and the completeness of adaptive monitoring is ensured.

Ensuring the reliability of active monitoring, without taking into account the timeliness of data which is defined in its other characteristic, is ensured by the following conditions:

1. The representation (model) of the protected object in the monitoring system is complete and reliable.
2. Data of the protected object were not distorted during the transfer to the monitoring system.
3. All of the methods for solving security problems are provided with the exact data and in the format required for their work.

The completeness and reliability of the representation of the protected object (condition (1)) is based on the use of the systemological approach of the protected object models hierarchy. Each security problem corresponds to a data-based generating model and a solution method. This ensures that there is no task that is not monitored. The condition of not distorting the data during transmission to the monitoring system is key and is stipulated in the condition of completeness, reliability, and timeliness of the proposed approach. Its implementation reduces the task of protecting monitoring data, which is beyond the scope of this article (condition (2)). The provision of methods for solving security problems not only with datasets, but with sets of data demanded by them in the appropriate format (condition (3)) is due to the correctness of the F_{MD} display, defined in the active monitoring model and included in the monitoring scheme s^{Cur}.

Ensuring the timeliness of the active monitoring of information security consists of solving security problems in less time than is required for the full or partial implementation of destructive impacts (depending on the type of impact and the task). This property depends on the monitoring methods (modern methods improve the characteristic). Timeliness assurance is based on the fulfillment of the boundary conditions, in terms of the time of generating the result using methods of solving safety problems. Violation of timeliness in relation to a security task a_i consists of exceeding the time interval for developing a solution or in terms of maximizing the parametric functions of the scheme, non-observance of the boundary condition:

$$Fpr_i = pr_i^{decision\ time}.Value \leq\ b_i^{decision\ time}.Value \tag{11}$$

Fpr_i is the speed of a reaction developing to the i-impact, and $b_i^{attak\ time}$ is the time during which the corresponding response must be developed by the monitoring system. However, the rate of action development is limited by condition (4), according to which all of the schemes that do not satisfy (4) are excluded from the set of possible schemes S and for $pr_i^{decision\ time}$.The $value$, if $pr_i^{decision\ time}$, is a characteristic of the resulting scheme s^{Cur} and should also be executed:

$$\left(pr_q \in Par\right) \wedge \left(pr_q.Name = b_h.Name =' decision\ time'\right) \rightarrow \left(Fpr_q >\ b_h.Value\right) \tag{12}$$

Therefore, a contradiction was obtained and it was proved that violation of (11) is impossible for the final scheme.

Consequently, when a complex systemological approach is applied, the properties of completeness, timeliness, and reliability of monitoring are achieved in the absence of data distortion.

6. Conclusions

The construction of an adaptive information security monitoring of the CPS in modern conditions is a difficult task due to the variety of security problems and the dynamic characteristics of the protected object (CPS). The use of the system approach methodology and sys-

tem theory allows for the formulation of the monitoring principles: Integrity, convergence, and hierarchical connectivity, which generalize the systemological approach to AISMS.

Within the framework of the approach, in accordance with the principle of integrity, the object of protection (the cyber-physical system) is considered from various sides, from individual components to the object as a whole, as well as the characteristics of the external environment. When the adaptive characteristics of monitoring are managed, in order to ensure the compliance of the monitoring system with the protected object and to implement the principles of integrity and convergence, the construction of a mutual mapping process between the security tasks, methods of their solution, and available data is used. Based on this process, an optimal monitoring scheme may be determined, including sets of tasks, methods, data, and mapping between them, that correspond to the boundary conditions, including time and other restrictions (if this scheme can be specified under the current conditions).

The optimality of generating a monitoring scheme in the proposed methodology is based on solving the problem of multicriteria optimization in the choice of data processing methods. The overall efficiency of monitoring depends on the efficiency of individual methods. The proposed methodology allows one to choose the most effective method or a combination of methods from a predetermined set, which can be supplemented with more advanced methods. Based on the generation of the monitoring scheme, when the input requirements or initial datasets, methods, and tasks for the adaptive management of information security monitoring of the CPS are changed, the proposed method makes it possible to determine the optimal monitoring scheme and ensure compliance with the boundary conditions, including the requirement of promptness.

Author Contributions: Conceptualization, M.P. and D.Z.; methodology, M.P.; software, D.B.; validation, A.S., D.B. and D.Z.; formal analysis, A.S.; investigation, M.P.; resources M.P.; data curation, E.A.; writing—original draft preparation, M.P.; writing—review and editing, M.P.; visualization, E.A.; supervision, A.S.; project administration, D.Z.; funding acquisition, D.Z. All authors have read and agreed to the published version of the manuscript.

Funding: The research is funded by the Ministry of Science and Higher Education of the Russian Federation as part of the World-Class Research Center program: Advanced Digital Technologies (contract No. 075-15-2020-934; dated 17 November 2020).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Analiz Gromkih Incidentov v Sfere Informacionnoj Bezopasnosti v 2019 Godu [Elektronnyj Resurs]. 2020. Available online: https://www.tadviser.ru/a/498885 (accessed on 25 November 2021).
2. Dehghani, M.; Niknam, T.; Ghiasi, M.; Siano, P.; Haes Alhelou, H.; Al-Hinai, A. Fourier Singular Values-Based False Data Injection Attack Detection in AC Smart-Grids. *Appl. Sci.* **2021**, *11*, 5706. [CrossRef]
3. Wang, C.; Wang, D.; Xu, G.; He, D. Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0. *Sci. China Inf. Sci.* **2022**, *65*, 112301. [CrossRef]
4. Jiang, Q.; Zhang, N.; Ni, J.; Ma, J.; Ma, X.; Choo, K.-K.R. Unified Biometric Privacy Preserving Three-Factor Authentication and Key Agreement for Cloud-Assisted Autonomous Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 9390–9401. [CrossRef]
5. Li, Z.; Wang, D.; Morais, E. Quantum-Safe Round-Optimal Password Authentication for Mobile Devices. *IEEE Trans. Dependable Secur. Comput. Early Access* **2020**, 1–14. [CrossRef]
6. Stevens, M. Security Information and Event Management (SIEM). In Proceedings of the NEbraska CERT Conference, Omaha, NE, USA, 9–11 August 2005; Available online: http://www.certconf.org/presentations/2005/files/WC4.pdf. (accessed on 25 November 2021).
7. Kotenko, I.V. Primenenie tekhnologii upravleniya informaciej i sobytiyami bezopasnosti dlya zashchity informacii v kriticheski vazhnyh infrastrukturah. *Trudy SPIIRAN Vyp* **2012**, *1*, 2–7.
8. Lavrova, D.S. Podhod k razrabotke SIEM-sistemy dlya Interneta veshchej. *Probl. Inf. Bezopasnosti. Komp'yuternye Sist.* **2016**, *2*, 51–59.

9. Lavrova, D.S.; Zaitseva, E.A.; Zegzhda, D.P. Approach to Presenting Network Infrastructure of Cyberphysical Systems to Minimize the Cyberattack Neutralization Time. *Autom. Control Comp. Sci.* **2019**, *53*, 387–392. [CrossRef]
10. Klyanchin, A.I.; Markov, A.S.; Fadin, A.A.; Ilyuhin, M.V. SIEM–tekhnologiya kak osnova postroeniya zashchishchennyh system. Informatizaciya i informacionnaya bezopasnost' pravoohranitel'nyh organov. In Proceedings of the XXII Vserossijskaya Nauchnaya Konferenciya, Moskva, Russia, 29–30 May 2013; pp. 270–273. Available online: https://www.elibrary.ru/item.asp?id=24711035 (accessed on 25 November 2021).
11. Nashivochnikov, N.V.; Lukashin, A.A.; Bol'shakov, A.A. Primenenie analiticheskih sredstv v sisteme operacionnogo monitoringa i analiza bezopasnosti kiberfizicheskih sistem dlya predpriyatij toplivno-energeticheskogo kompleksa, Matematicheskie metody v tekhnike i tekhnologiyah. *MMTT-32* **2019**, *2*, 1–5.
12. Siddiqui, S.; Khan, M.S.; Ferens, K.; Kinsner, W. Fractal based cognitive neural network to detect obfuscated and indistinguishable internet threats. In Proceedings of the 2017 IEEE 16th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC), Oxford, UK, 26–28 July 2017; pp. 297–308. [CrossRef]
13. Knapp, E.D.; Langill, J.T. Chapter 12-Security Monitoring of Industrial Control Systems. In *Industrial Network Security*, 2nd ed.; Eric, D., Knapp, J.T., Eds.; Syngress: New York, NY, USA, 2015; pp. 351–386. [CrossRef]
14. Jiang, Y.; Yin, S.; Kaynak, O. Data-Driven Monitoring and Safety Control of Industrial Cyber-Physical Systems: Basics and Beyond. *IEEE Access* **2018**, *6*, 47374–47384. [CrossRef]
15. Cao, L. Data Science: A Comprehensive Overview. *ACM Comput. Surv.* **2017**, *50*, 1–42. [CrossRef]
16. Solar JSOC Security Report. Itogi 2019 Goda [Elektronnyj Resurs]. 2020. Available online: https://rt-solar.ru/upload/iblock/faf/Solar-JSOC-Security-Report-2019.pdf. (accessed on 25 November 2021).
17. Kiberataki na Sistemy ASU TP v Energetike v Evrope. Pervyj Kvartal 2020 Goda [Elektronnyj Resurs]. 2020. Available online: https://ics-cert.kaspersky.ru/reports/2020/09/03/cyberthreats-for-ics-in-energy-in-europe-q1-2020/. (accessed on 25 November 2021).
18. GOST R 50922-2006 Zashchita Informacii. Osnovnye Terminy i Opredeleniya Utverzhden i Vveden v Dejstvie Prikazom Federal'nogo Agentstva po Tekhnicheskomu Regulirovaniyu i Metrologii ot 27 dekabrya 2006 g. N 373-st. Available online: https://docs.cntd.ru/document/1200058320 (accessed on 25 November 2021).
19. Lukackij, A. Izmerenie effektivnosti SOC. Chast' 2. *Inf. Bezop.* **2020**, *3*. Available online: https://www.itsec.ru/articles/izmerenie-effectivnosti-soc-part-2. (accessed on 25 November 2021).
20. Proekt Standarta Zashchita Informacii. Monitoring Informacionnoj Bezopasnosti. *Obshchie Polozheniya» [Elektronnyj resurs]–2020.* Available online: https://fstec.ru/component/attachments/download/243. (accessed on 25 November 2021).
21. Ge, Z. Review on data-driven modeling and monitoring for plant-wide industrial processes. *Chemom. Intell. Lab. Syst.* **2017**, *171*, 16–25. [CrossRef]
22. Klir, G.J. *Architecture of Systems Problem Solving*; Plenum Publishing Corporation: New York, NY, USA, 1985; p. 354.
23. Wang, H.; Li, S. General Systems Theory and Systems Engineering. In *Introduction to Social Systems Engineering*; Springer: Singapore, 2018; pp. 31–83. [CrossRef]
24. Pereira, T.; Barreto, L.; Amaral, A. Network and information security challenges within Industry 4.0 paradigm. *Procedia Manuf.* **2017**, *13*, 1253–1260. [CrossRef]
25. Chhetri, S.R. *Abdullah, M. Data-Driven Modeling of Cyber-Physical Systems Using Side-Channel Analysis*; Springer Nature: Cham, Switzerland, 2020; p. 234. [CrossRef]
26. Zhao, Z.; Huang, Y.; Zhen, Z.; Li, Y. Data-Driven False Data-Injection Attack Design and Detection in Cyber-Physical Systems. *IEEE Trans. Cybern. Early Access* **2020**, 1–9. Available online: https://ieeexplore.ieee.org/abstract/document/9003529 (accessed on 25 November 2021).
27. Poltavtseva, M.A.; Zegzhda, D.P. Building an Adaptive System for Collecting and Preparing Data for Security Monitoring. *Autom. Control Comp. Sci.* **2020**, *54*, 968–976. [CrossRef]
28. Poltavtseva, M.A. Heterogeneous data aggregation and normalization in information security monitoring and intrusion detection systems of large-scale industrial CPS. *Proc. Inst. Syst. Program. RAS* **2020**, *32*, 131–142. [CrossRef]
29. Podinovskij, V.V.; Nogin, V.D. *Pareto–Optimal'nye Resheniya Mnogokriterialnyh Zadach*; Fizmatlit: Moscow, Russia, 2007; p. 256.
30. Nogin, V.D. Problema suzheniya mnozhestva Pareto: Podhody k resheniyu. *Iskusstv. Intell. i Prinyatie Reshenij* **2008**, *1*, 98–112.
31. Anisimov, V.G.; Zegzhda, P.D.; Suprun, A.F.; Anisimov, E.G.; Bazhin, D.A. Risk–orientirovannyj podhod k organizacii kontrolya v podsistemah obespecheniya bezopasnosti informacionnyh system. *Probl. Inf. Bezopasnosti. Komp'yuternye Sist.* **2016**, *3*, 61–67.
32. Krundyshev, V.M.; Kalinin, M.O. Metodika analiza riskov informacionnoj bezopasnosti dlya intellektual'nyh kibersred. In *Fundamental'nye Problemy Upravleniya Proizvodstvennymi Processami v Usloviyah Perekhoda k Industrii 4.0. Tezisy Dokladov Nauchnogo Seminara v Ramkah Mezhdunarodnoj Nauchno-Tekhnicheskoj Konferencii "\Avtomatizaciya\"*; Ministerstvo Nauki i Vysshego Obrazovaniya Rossijskoj Federacii Federal'noe Gosudarstvennoe: Moscow, Russia, 2020; pp. 139–141.
33. Zegzhda, P.D.; Lavrova, D.S.; Shtyrkina, A.A. Mul'tifraktal'nyj analiz trafika magistral'nyh setej internet dlya obnaruzheniya atak otkaza v obsluzhivanii, Problemy informacionnoj bezopasnosti. *Komp'yuternye Sist.* **2018**, *2*, 48–58.
34. Sheluhin, O.; Atayero, A.; Garmashev, A. Detection of Teletraffic Anomalies Using Multifractal Analysis. *Int. J. Adv. Comput. Technol.* **2011**, *3*, 174–182.
35. Coletta, A. Security Monitoring for Industrial Control Systems. In *Security of Industrial Control Systems and Cyber Physical Systems*; Springer: Cham, Switzerland, 2015; Volume 9588, pp. 48–62.

36. Lavrova, D.S.; Zegzhda, D.P.; Zajceva, E.A. Modelirovanie setevoj infrastruktury slozhnyh ob"ektov dlya resheniya zadachi protivodejstviya kiberatakam. *Vopr. Kiberbezopasnosti* **2019**, *2*, 13–20. [CrossRef]
37. Goh, J.; Adepu, S.; Junejo, K.N.; Mathur, A. A Dataset to Support Research in the Design of Secure Water Treatment Systems. In *Critical Information Infrastructures Security*; Havarneanu, G., Setola, R., Nassopoulos, H., Wolthusen, S., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2017; Volume 10242.
38. Dehghani, M.; Ghiasi, M.; Niknam, T.; Kavousi-Fard, A.; Tajik, E.; Padmanaban, S.; Aliev, H. Cyber Attack Detection Based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack. *IEEE Access* **2021**, *9*, 16488–16507. [CrossRef]
39. Singh, V.K.; Govindarasu, M.A. Cyber-Physical Anomaly Detection for Wide-Area Protection Using Machine Learning. *IEEE Trans. Smart Grid* **2021**, *12*, 3514–3526. [CrossRef]
40. Paredes, C.M.; Martínez-Castro, D.; Ibarra-Junquera, V.; González-Potes, A. Detection and Isolation of DoS and Integrity Cyber Attacks in Cyber-Physical Systems with a Neural Network-Based Architecture. *Electronics* **2021**, *10*, 2238. [CrossRef]
41. Kutz, J.N. *Data-Driven Modeling & Scientific Computation: Methods for Complex Systems & Big Data*; OUP: Oxford, UK, 2013; p. 608.
42. Kondrat'eva, N.V.; Valeev, S.S. Modelirovanie zhiznennogo cikla slozhnogo tekhnicheskogo ob"ekta na osnove koncepcii bol'shih dannyh. In Proceedings of the 3rd Russian Conference. Mathematical Modeling and Information Technologies, Yekaterinburg, Russia, 16 November 2016; pp. 216–223.
43. Bol'shakov, A.S. Obnaruzhenie anomalij v komp'yuternyh setyah s ispol'zovaniem metodov mashinnogo obucheniya. *REDS Telekommun. Ustrojstva i Sist.* **2020**, *1*, 27–43.
44. Mozaffari, F.S.; Karimipour, H.; Parizi, R.M. Learning Based Anomaly Detection in Critical Cyber-Physical Systems. In *Security of Cyber-Physical Systems*; Karimipour, H., Srikantha, P., Farag, H., Wei-Kocsis, J., Eds.; Springer: Cham, Switzerland, 2020. [CrossRef]
45. Nithya, J.K.; Shyamala, K. A Systematic Review on Various Attack Detection Methods for Wireless Sensor Networks. In *International Conference on Innovative Computing and Communications. Advances in Intelligent Systems and Computing*; Khanna, A., Gupta, D., Bhattacharyya, S., Hassanien, A.E., Anand, S., Jaiswal, A., Eds.; Springer: Singapore, 2022; Volume 1394. [CrossRef]
46. Haque, N.I.; Shahriar, M.H.; Dastgir, M.G.; Debnath, A.; Parvez, I.; Sarwat, A.; Rahman, M.A. A Survey of Machine Learning-based Cyber-physical Attack Generation, Detection, and Mitigation in Smart-Grid. In Proceedings of the 2020 52nd North American Power Symposium (NAPS), Tempe, AZ, USA, 11–13 April 2021; pp. 1–6. [CrossRef]
47. Zhang, J.; Pan, L.; Han, Q.-L.; Chen, C.; Wen, S.; Xiang, Y. Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey. *IEEE/CAA J. Autom. Sin.* **2021**, 1–15. [CrossRef]
48. Zhang, D.; Wang, Q.-G.; Feng, G.; Shi, Y.; Vasilakos, A.V. A survey on attack detection, estimation and control of industrial cyber–physical systems. *ISA Trans.* **2021**, *16*, 1–16. [CrossRef]
49. Akowuah, F.; Kong, F. Real-Time Adaptive Sensor Attack Detection in Autonomous Cyber-Physical Systems. In Proceedings of the 2021 IEEE 27th Real-Time and Embedded Technology and Applications Symposium (RTAS), Nashville, TN, USA, 7 July 2021; pp. 237–250. [CrossRef]
50. Ghiasi, M.; Dehghani, M.; Niknam, T.; Kavousi-Fard, A.; Siano, P.; Alhelou, H.H. Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform. *IEEE Access* **2021**, *9*, 29429–29440. [CrossRef]
51. Kordestani, M.; Saif, M. Observer-Based Attack Detection and Mitigation for Cyberphysical Systems: A Review. *IEEE Syst. Man Cybern. Mag.* **2021**, *7*, 35–60. [CrossRef]
52. Dehghani, M.; Niknam, T.; Ghiasi, M.; Bayati, N.; Savaghebi, M. Cyber-Attack Detection in DC Microgrids Based on Deep Machine Learning and Wavelet Singular Values Approach. *Electronics* **2021**, *10*, 1914. [CrossRef]