Comparison of Information Security Systems for Asymptotic Information Security Management Critical Information Infrastructures

Sergey Erokhin[1], Andrey Petukhov[2], Pavel Pilyugin[3]
Moscow Technical University of Communications and Informatics, Moscow, Russia
[1]esd@mtuci.ru
[2]anpetukhov@yandex.ru
[3]paul.pilyugin@gmail.ru

Abstract—**The article reviews the options for critical information infrastructures (CII) protection management and discusses approaches to developing security policies that don’t lean on assessing residual risks and identifying a fixed list of threats. We examine and substantiate the possibility of building information security management systems based on monitoring of security events. A formal description of security events as well as relevant protection methods is proposed. The paper introduces an order relation for information security systems comparison and asymptotic CII security control implementation paper.**

I. Introduction

Critical information infrastructures (CII) in different fields of activity and in different countries can be assigned to completely different objects, but, despite this, all these objects have a number of common features that determine the specifics of CII from the point of view of security.

Usually, security characterizes the effectiveness of efforts to counter the aggressiveness of the environment. This expresses the sufficiency of the protection's response to possible negative impacts. In this case, security metrication is based on the Clements model (model with complete overlap) [1]. In this model, the high-level entities of the "General criteria"[2] include the "risk" parameter as an integral remainder of incomplete security.

Security assessments usually use the probability of a threat and the probability of its implementation (usually without specifying the attack scenario or other details). These are usually expert characteristics (with the exception of those related to cryptographic security) and they allow us to consider security as the inverse of the residual risk.

The approach based on the asymptotic management of information security [3] for critical information infrastructures (CII) involves the rejection of the assessment of acceptable (residual) risk to assess the effectiveness of protection. In this regard, there is a natural question about the ratio (at least qualitative) of security levels when using different protective measures.

The ISO 27005 information security risk assessment procedure considers two approaches to risk assessment: qualitative and quantitative. "As a rule, qualitative analysis is first used to identify high-priority risks, and then quantitative analysis is used for identified risks, which is more time-consuming and gives more accurate results" [4].

For CII, the asymptotic approach to information security management uses a consistent improvement in the quality of the security system. Let us consider the possibility of using qualitative (ordinal) scales to determine the improvement (direction of development) of the properties of security systems. This requires introducing an order relation for space consisting of security systems.

The security event monitor is used as a universal model of the security mechanism in the asymptotic management of information security [5]. In this case, the protection system is considered as a set of protection mechanisms. The protection mechanism performs two main functions: detection and counteraction. Detection is necessary for the effectiveness of the mechanism, since undetected events cannot be countered. This allows us to consider the set of security events available for observation (from the entire space of such events) as the main characteristic of the security mechanism [5].

II. Properties Of Security Incidents And Events In The Model Under Consideration

A security event according to ISO 18044-2007 is a detectable (through a set of functions) state of the monitored system that can lead to an incident or simply indicate the possibility of an incident occurring. In both cases, technically, this is the correlation of events with an incident: “different conditional probabilities of the observed event: the incident occurred η=P(event/incident is), and when it did not happen, μ=P(event/incident no)” [6]. Further, we denote $A=\{a_i\}$ the set of security events detected by the corresponding security mechanisms of the concrete protection system. For further discussion, it should be borne in mind that it does not matter whether there is an accurate estimate of these probabilities, it is only important, as noted above, that they are not equal, otherwise the event will not be informative.

At the same time, it is important that security events are independent or "almost" independent, i.e. weakly correlated with each other. There is no need to observe two security events if they always occur together. Thus, security events from the group of events indicating a specific incident will be considered independent or "almost" independent. If we add only independent events, we can assume that all events from A will be independent.

In addition, events from A will be combined, since it is possible to observe several independent features simultaneously or during the observation period.

We mean that an event can indicate multiple incidents. Therefore, the significance (importance) of such an event for the indication is less; the more incidents are indicated by it. This is because the fact that such an event is observed does not make it possible to accurately indicate a specific incident. Such an event can usually be used to confirm a hazard and increase confidence when observing other security events. It is possible that several such "ambiguous" events point to one specific incident (the sets of incidents they indicate have a single element as an intersection). However, on further consideration, we will assume (assumption P-1) that there are no such "ambiguous" security events.

By incident I_k, we mean an event associated with a disruption of some critical process in the system, which leads to the termination of CII operations (full or partial). For such incidents, it is assumed:

First, that the incident itself is also monitored by monitoring tools (which is not always possible, but acceptable for computer and telecommunication networks).

Secondly, the incident in this case is considered as a critical violation of the functioning of CII (or violation of the critical process of CII [7]). This makes it possible to clarify the General definition of an ISO 18044-2007 incident as " an undesirable or unexpected is event(s) that are associated with a significant probability of compromising business operations and creating an is threat [8]".

Third, incidents are considered as independent or "almost" independent events (i.e. weakly correlated). Therefore, when they occur together, they may correspond structurally to different components of the system. In this case, we can assume that they have a common cause, which should be considered an incident.

Fourth, it is assumed that the composition of incidents is fixed (assumption P-2). Indeed, for the considered problem of information security management, it is assumed that all critical processes (possible incidents) were identified earlier in accordance with the inventory of CII [7]. Changing the composition of incidents is possible based on getting more information, and the new security system will correspond to the new composition of incidents. Then again, you can improve the protection properties based on monitoring in the process of asymptotic control.

The latter circumstance emphasizes the piecewise continuous nature of the asymptotic control process. The current functioning of the adaptive component during the "continuous" period of asymptotic control accumulates a certain "critical mass" of information of the predictive component. This can lead to a qualitative jump and change in the composition of incidents. In addition, the composition of incidents can be changed from the outside, for example, through the channels of interaction with SIEM or CERT.

III. Comparison Of Information Security Systems Based On Observed Security Events

The comparison of security systems is based on the model of a security system with complete overlap. However, in the proposed approach, this model is transformed from the structure "threat-protection mechanism - protection object" to the structure "threat – security event - protection mechanism – security incident - protection object".

That is, instead of a triple (t_i, m_j, o_k), a triple (a_i, m_j, I_k) is considered. Where $\{t_i\}$ are threats; $\{m_j\}$ -mechanisms; $\{o_k\}$ - objects; $\{a_i\}$ -events; $\{I_k\}$ - incidents (Fig.1).

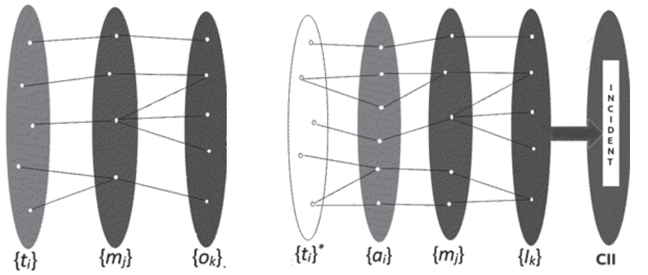

Fig. 1. Transformation of the model with complete overlap

For network protection mechanisms (Firewall, IDS, IPS, SIEM, etc.), security events are indicated during monitoring. The definition of events is based on the comparison of signatures and the identification of anomalies [9].

The signature of a security event (pattern, pattern, complex of attributes, etc.) is designed to detect the fact that an event or group of events has occurred. The signature can be determined by the sources of information about the event (for example, sensors of primary measurements) and the structure of complex aggregates obtained from them (aggregation scheme).

In the first case, a set (vector) of n parameters of sequential system states $s_i = (p_1, ... p_n)$ can be considered as a representation of a security event (or a set of such events) described by the signature of some incident Im. Here $(p_1, ... p_n)$, these are the sets of parameters of the system states observed at different times of the observation interval, which corresponds to the above definitions of a security event and an incident.

Thus, we can further consider the correspondence of the observed system parameters to the signature as the identification (observation) of the corresponding security events. That is, if $S = \{s_i\}$ is the set of all possible signatures, then we denote the mapping of the set of signatures to the set of security events as $\theta (s_i) \subseteq A$, where $\theta: S \rightarrow A$. This mapping may not be one-to-one, in this case θ^{-1} can be considered as a method of aggregating security events $\{\theta^{-1} (a_1, ... a_r)\} = \{s_i\}$, and $\{s_i \mid \theta (s_i) \subseteq A\} \subseteq S$ as a new set of independent security events described by signatures.

In the second case, the monitor can detect some deviations from the expected "behavior" of the system. At the same time, network traffic anomalies can be quite safe [10]. Therefore, the identification of anomalies as security events requires additional filtering and processing of the received data [11] using various methods [12]. Such anomalies, identified as security events, are tracked by the monitor based on the corresponding signatures (for example, exceeded password attempts or concurrent opening of a large number of TCP connections, etc.).

Let's explain the concept of a security event signature. This concept is used much more widely than a similar concept when creating antivirus programs (a piece of program code that is characteristic of malware). The signature of a security event (template, pattern, set of features, etc.) is intended for detecting the fact that the corresponding event occurred. The signature may include a specification of event information sources (for example, primary measurement sensors). A security event can also represent a more complex structure formed from this information. For this purpose, aggregation methods are used that correspond to complex events (aggregation schemes) correlated with a security incident. At the same time, it is absolutely not necessary to fix matches by templates, patterns, etc., it may be quite the opposite. For example, detecting the security event "the flag field in the packet header does not match the RFC" assumes that the signature uses the value of the flag field as the primary dimension, the aggregation scheme includes logical functions for comparing this field with all the options provided by the RFC, and combining these functions with disjunction negation. Thus, to detect an event, it is necessary that no matches occur

Therefore, we can view signature-based event detection monitoring as a model of protection mechanisms. We will assume that all security mechanisms are described by a set of observable security events. Then the set of protection mechanisms corresponds to the set of incident signatures: $M = \{s_i \mid \theta(si) \subseteq A\}$.

Using these statements, we will show the possibility of comparing protection systems using monitoring based on signature-based event detection.

The basis for a comparative assessment of the effectiveness of various security systems can be the set of security event signatures used by them $S_k \subseteq S$ (operational and architectural parameters are not considered here).

In order to compare security systems, we can compare the sets of their security events, thereby establishing a partial order relation. Based on this, it is necessary to consider the possibility of introducing a partial order relation $\succcurlyeq^S$ for comparing information security systems (ISS) based on the partial order relation $\succcurlyeq_S$ for comparison on a set of security system signatures.

IV. Partial order relation on sets of security event signatures

Let the set of incidents contain only one incident (assumption P-3) and let, as described above, the information security systems ISS_1 and ISS_2 be completely characterized by their sets of signatures: S_1 and S_2.

Then when comparing sets of signatures, the following cases are possible:

1. $S_1 \supseteq S_2$ or $S_1 \subseteq S_2$ - this relation of inclusion of sets specifies the relation of partial preference on the sets of security signatures $S_1 \succcurlyeq_S S_2$ or $S_1 \preccurlyeq_S S_2$ (and similarly on their respective protection systems: $ISS_1 \succcurlyeq^S ISS_2$ or $ISS_1 \preccurlyeq^S ISS_2$).

2. If $S_1 \cap S_2 = \emptyset$, then comparison based on inclusion of sets is not applicable.

3. If $S_1 \cap S_2 \neq \emptyset$, but $S_1 \not\supseteq S_2$ or $S_1 \not\subseteq S_2$, then a comparison based on inclusion of sets is also not applicable.

To improve the safety of CII, case 1 shows how a consistent "improvement" of the efficiency of protection based on asymptotic control is associated with the addition of new signatures to the monitoring systems [13].

However, there may be different situations corresponding to case 2. This can be the result of aggregating multiple signatures into one (building a template signature), or the result of identifying (and removing) "inefficient" or less efficient signatures and replacing them with others, which is especially important if resources are limited.

In this case, it is not the sets of signatures that are considered, but the corresponding security events (since the signature is considered as a result of the aggregation of security events). Further comparison of sets of safety events is performed, if possible, as a comparison of sets.

For example, let Ai be the set of security events corresponding to the set of signatures S_i: $A_i = \theta\ (S_i)$.

If it is true that: $A_1 \supset A_2$ or $A_1 \subset A_2$ - then the set inclusion relations establish for the security systems (and the corresponding signature sets) the preference relation $S_1 \succcurlyeq_S S_2$ or $S_1 \preccurlyeq_S S_2$ (Fig.2).

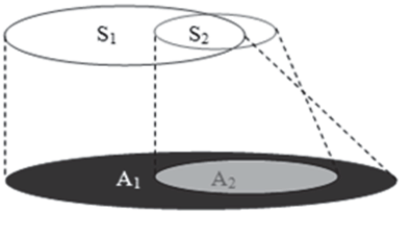

Fig. 2. The case when one set of security events is a subset of another set

In other situations, there may be different ways to make comparisons that are not so obvious. If $S_1 \cap S_2 = \emptyset$ (Fig.3.), then to exclude possible inaccuracies, we also consider the sets of corresponding security events. In this case also have that $A_1 \cap A_2 = \emptyset$, and for a "rough estimate" of sets of signatures as the metric of a plurality of security events use the power of the corresponding plurality $\|A_i\| = |A_i|$.

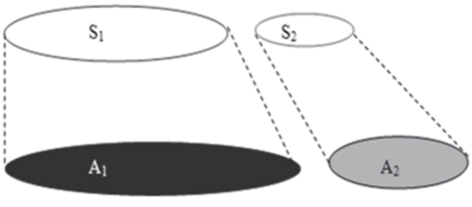

Fig. 3. The case when one set of security events is a subset of another set

This linear metric corresponds to the addition of probabilities of security events, which is not applicable here, since the events are independent, but they are combined.

However, as a justification for this rough estimate, we consider the probability of $\mathrm{P_I}(\mathbf{A})$ indicating the incident by group $\mathbf{A}$ of the corresponding combined security events. We will assume that all security events are equally significant for detecting an incident (assumption P-4) and that the probabilities of such events are approximately the same.

An incident is indicated if at least one security event is detected and, respectively $\mathrm{P_I}(\mathrm{A}) = 1 - \mathrm{P}(\overline{\mathrm{A}})$, where $\mathrm{P}(\overline{\mathrm{A}})$ the probability that no security event from A=($a_1, a_2, \ldots a_n$) occurs.

Then $\overline{\mathrm{A}} = (\bar{a}_1 \cup \bar{a}_2 \cup \bar{a}_2 \ldots \cup \bar{a}_n)$ the product of independent events and $\mathrm{P}(\overline{\mathrm{A}}) = \prod_1^n (1 - p(a_i)) = (1-p)^n$, where $p \approx p(a_i)$ the probabilities of events a_i if they are equal (or is the average of these probabilities). This shows that $\mathrm{P_I}(\mathrm{A}) = 1 - (1-p)^n$ as n grows, it monotonically increases (Fig.4).

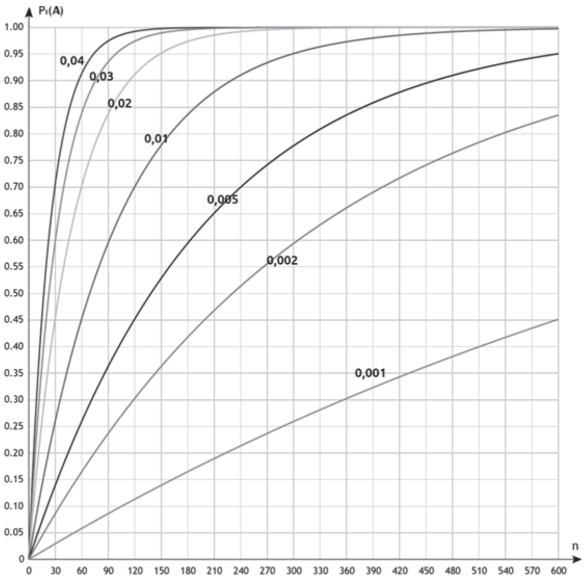

Fig. 4. Changes in the nature of the dependence of the probability of indicating an incident $\mathrm{P_I}(\mathbf{A})$ on the number of observed safety events n at various probabilities p (0.001 → 0.04) of these events occurring

Obviously, for large numbers of security events *n*, changes in $\mathrm{P_I}(\mathbf{A})$ will be small, and they can be ignored in the traditional assessment of residual risks, but in the case of CII, any improvement will be significant.

Note that it is possible to reduce the exponent in the function: $\mathrm{P_I}(\mathrm{A}) = 1 - (1-p)^{n-r}$, where r denotes the minimum number of security events necessary to ensure the desired quality of incident indication in accordance with the Bernoulli sequential test scheme.

Then, to determine $\|\mathrm{A}_1\| \geqq \|\mathrm{A}_2\|$ or $\|\mathrm{A}_1\| \leqq \|\mathrm{A}_2\|$, one can simply compare by the number of security events. And within the framework of the assumptions made: first, as noted above, each signature indicates no more than one incident, and, secondly, the significance of all signatures for indicating incidents is the same, i.e. all signatures are equally effective for detecting incidents, we will accordingly get: $\mathrm{S}_1 \succcurlyeq_{\mathrm{S}} \mathrm{S}_2$ or $\mathrm{S}_1 \preccurlyeq_{\mathrm{S}} \mathrm{S}_2$.

Note that the first assumption is obvious, since we consider a single-element set of incidents. The second assumption is a very strong restriction, but it is acceptable, since only events that are "strongly" related to the incident are selected as a security event (the corresponding correlation indicators are sufficiently noticeable not to be ignored).

If $\mathrm{S}_1 \cap \mathrm{S}_2 \neq \emptyset$, respectively, and $\mathrm{A}_1 \cap \mathrm{A}_2 \neq \emptyset$, but $\mathrm{A}_1 \not\supseteq \mathrm{A}_2$ or $\mathrm{A}_1 \not\subseteq \mathrm{A}_2$, then for comparison of sets of signatures and mapping them to appropriate protection systems different variants are possible, in some embodiments, it is possible to neglect the contribution of the security event $\mathrm{A}_1 \cap \mathrm{A}_2$, if it is relatively small (this assumption is valid for a large number of security events described by signatures, since the contribution of each event is relatively small).

If $\|\mathrm{A}_1\| >> \|\mathrm{A}_1 \cap \mathrm{A}_2\|$ and $\|\mathrm{A}_2\| \approx \|\mathrm{A}_1 \cap \mathrm{A}_2\|$, it is advisable to compare sets of security events B1=A1 and $\mathrm{B}_2 = (\mathrm{A}_1 \cap \mathrm{A}_2)$ and $\mathrm{B}_1 \supseteq \mathrm{B}_2$, which obviously reduces to the above variant (Fig.5).

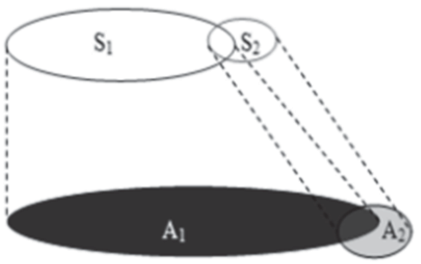

Fig. 5. The case when $\|\mathbf{A}_2\| \approx \|\mathbf{A}_1 \cap \mathbf{A}_2\|$

If $\|\mathbf{A}_2\| >>> \|\mathbf{A}_1 \cap \mathbf{A}_2\|$ and $\|\mathbf{A}_1\| \approx \|\mathbf{A}_1 \cap \mathbf{A}_2\|$ coincides, then it is useful to compare sets of security events B2=A2 and B1= (A1∩A2) and B1⊆B2 that obviously also comes down to the above variant (Fig 6).

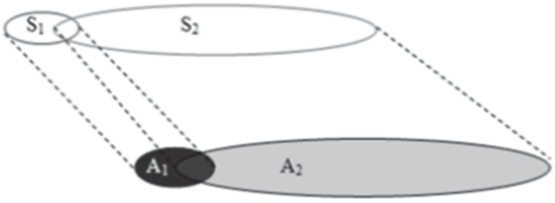

Fig. 6. The case when $\|\mathbf{A}_1\| \approx \|\mathbf{A}_1 \cap \mathbf{A}_2\|$

If $\mathrm{A}_1 \cap \mathrm{A}_2 \neq \emptyset$, it is possible to compare the sets $\mathrm{B}_1 = \mathrm{A}_1 \backslash (\mathrm{A}_1 \cap \mathrm{A}_2)$ and $\mathrm{B}_2 = \mathrm{A}_2 \backslash (\mathrm{A}_1 \cap \mathrm{A}_2)$ then $\mathrm{B}_1 \cap \mathrm{B}_2 = \emptyset$ and $\|\mathrm{B}_1\| \geqq \|\mathrm{B}_2\|$ or $\|\mathrm{B}_1\| \leqq \|\mathrm{B}_2\|$, and accordingly $\mathrm{S}_1 \succcurlyeq_{\mathrm{S}} \mathrm{S}_2$ or $\mathrm{S}_1 \preccurlyeq_{\mathrm{S}} \mathrm{S}_2$ (fig. 7).

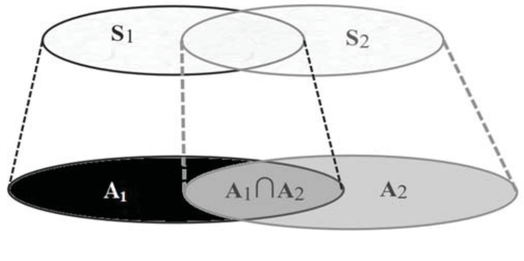

Fig. 7. Common case of correlation of a set of security events

Taking into account the established assumptions and restrictions for the introduced preference $\succcurlyeq_S$ relation, it can be argued that:

$ISS_1 \succcurlyeq^S ISS_2$ if $S_1 \succcurlyeq_S S_2$

$ISS_1 \preccurlyeq^S ISS_2$ if $S_1 \preccurlyeq_S S_2$

$ISS_1 =^S ISS_2$ if $S_1 \succcurlyeq_S S_2$ and $S_1 \preccurlyeq_S S_2$.

Despite the low accuracy of estimates, the approach described above has a remarkable property – all ISS's are comparable to each other. However, the assumption (P-4) that the significance of all signatures as indicators of an incident is the same is too strong and not always correct. In addition, the entered ratio allows you to compare ISS's for only one incident.

V. Considering the significance of signatures in determining partial order on sets of security event signatures

A more universal method is the use of correlation analysis used in the methods of applied statistics [14]. This allows the comparison to be made more accurate (removing the constraints of the assumption (P-4) about the equal significance of security events). However, keep in mind that these methods are more time-consuming and require a large amount of statistics. Unfortunately, this is not always possible and not always technically feasible.

Paired or partial correlation coefficients can be considered as factors of importance in the process of additive convolution of criteria, in contrast to the above-described convolution with the same weight equal to 1.

The use of these factors as metrics to assess the relationships between various security events, as well as the coefficient of multiple correlation to assess the relationship of security events and incidents.

In other words, as an assessment of the "degree of connectivity" between security events and incidents, in accordance with their definition as dependent events, we can consider the correlation between them.

In our case, the connectivity of a security event and an incident is determined by their paired correlation coefficient. If there are several security events ($a_1,....a_n$) that indicate an Is incident, then the multiple correlation coefficient is an indicator of connectivity (tightness) between these events and the incident $\rho_{\mathrm{I}\cdot\, a1,....an}$ [15].

$$\rho_{\mathrm{I}\cdot\, a1,....an} = 1 - \frac{|R|}{R_{00}}\,. \qquad (1)$$

Where R is the correlation matrix $R = \{\rho_{i,i}\}$;

$|R|$ is the determinant of this matrix;

R_{00} is an algebraic complement for $\rho_{0,0}$.

The correlation matrix is defined as:

$$R = \begin{pmatrix} \rho_{0,0} & \cdots & \rho_{0,an} \\ \vdots & \ddots & \vdots \\ \rho_{an,0} & \cdots & \rho \end{pmatrix}\,, \qquad (2)$$

here $\rho_{i,j} = \rho_{ai,aj}$ are paired correlation coefficients for i,j=1,…,n, and $\rho_{0,0}$=$\rho_{\mathrm{I,I}}$ and all $\rho_{i,i}$=1.

Since security events are independent, multicolleriality is absent (rows are linearly independent), then $\rho_{i,j} = 0$ for $i \neq j$.

The multiple correlation coefficients can be used as a metric to assess the performance of the signature set S_k:

$$\|\theta(S_k)\| = \|A_k\| = \rho_{\mathrm{I}\cdot A_k} = \rho_{\mathrm{I}\cdot\, a1,....an}$$

The coefficient of determination is also used as an indicator of proximity:

$$D = (\rho_{\mathrm{I}}\,*)^2$$

A necessary condition for correlation analysis is a linear regression relationship between the parameter being explained and the explanatory factors.

For the problem under consideration, the explained parameter is incident I, and the explanatory factors are signatures (aggregated security events).

As suggested in [9], we will consider all the variables of this linear regression as dichotomous (binary), taking values: 1 - if an event (incident) happened, 0 - otherwise.

When comparing binary variables ind on a dichotomous scale, the measure of the correlation is the Pearson association coefficient φ. The value of the coefficient $\rho_{i,j} = \rho_{ai,aj} = \varphi$ lies in the range of +1 and -1. In general form, the formula for the empirical calculation of the correlation coefficient of dichotomous variables x=a_i and y = y=a_j [16]:

$$\varphi = \frac{p_{xy} - p_x p_y}{\sqrt{p_x(1-p_x)p_y(1-p_y)}} \qquad (3)$$

Where:

p_x — is an estimate of the probability of occurrence of the event x=ai.

p_y — is an estimate of the probability of occurrence of the event y=aj,

p_{xy} — is an estimate of the probability of occurrence of events x and y simultaneously.

Example of calculation φ based on the conjugacy table based on observation results [16]:

TABLE I. Example of calculation φ

Event a_i	Event a_j		∑
	Yes	*No*	
Yes	*a*	*b*	*a+b*
No	*c*	*d*	*c+d*
∑	*a+c*	*b+d*	*n=a+b+c+d*

$$\varphi = \frac{ad - bc}{\sqrt{(a+b)(b+d)(a+c)(c+d)}} \qquad (4)$$

Other connection indicators calculated from this table are also known, for example, the Yula association coefficient [16]:

$$q = \frac{ad-bc}{ad+bc} \tag{5}$$

In the considered case of asymptotic control, a gradual change in the information security system is assumed, as a result of a sequential change in the set of monitored safety events. To assess the influence of individual factors (in our case, security events), partial correlation coefficients are used, when the values of all other factors are fixed [16]. The method of sequential inclusion (or exclusion) of security events allows you to choose from a possible set of events exactly those that will improve the quality of the information security system.

When a new security event ai is introduced, which has the highest absolute value of the partial correlation coefficient with the incident with a fixed influence of the previously introduced security events: $\rho_{\mathrm{I}\cdot ai|a1,\ldots,ai-1,ai+1\ldots an}$. In the general case, it is possible to consider the inclusion (or exclusion) of the group of security events, $a_{i+1}, \ldots, a_{i+l}$ ($l<n$), then the partial correlation coefficient of the l-th order is used.

When additional security events are introduced, the coefficient of determination (multiple correlation) should increase (the more, the better), and the residual variance should decrease. Therefore, we can conduct relations of preference $\succcurlyeq_{\mathrm{R}}$, comparison of $\mathrm{S_i}$ signatures based on the entered metric $\|\theta(\mathrm{S_k})\| = \rho_{\mathrm{I}\cdot \mathrm{A_k}}$ and, respectively, $\succcurlyeq^{\mathrm{R}}$ for comparison of protection system ($\mathrm{ISS_i}$):

$\mathrm{ISS_1} \succcurlyeq^{\mathrm{R}} \mathrm{ISS_2}$ if $\mathrm{S_1} \succcurlyeq_{\mathrm{R}} \mathrm{S_2}$

$\mathrm{ISS_1} \preccurlyeq^{\mathrm{R}} \mathrm{ISS_2}$ if $\mathrm{S_1} \preccurlyeq_{\mathrm{R}} \mathrm{S_2}$

$\mathrm{ISS_1} =^{\mathrm{R}} \mathrm{ISS_2}$ if $\mathrm{S_1} =_{\mathrm{R}} \mathrm{S_2}$.

VI. SUMMARY

Using the metric $\|\theta(\mathrm{S_r})\|=\|\mathrm{A_r}\|$ (introduced for $\succcurlyeq^{\mathrm{S}}$ or $\succcurlyeq^{\mathrm{R}}$) as a universal one is limited by the fact that the variants of the order relation described above are quite correct only for the case of one incident. In the case of multiple incidents, a set of incidents detected by the security system of the same significance can be considered as a single global incident $\mathrm{I}=\{\mathrm{I_1},\mathrm{I_2},\ldots,\mathrm{I_m}\}$.

However, comparison of protection systems should take into account the effectiveness of detection of each incident. Then we can consider the problem of multicriteria choice, where the detection efficiency of each Ir acts as a separate criterion (i.e., the restrictions of the assumptions P-1 and P-3 are removed). The vector criterion $(\mathrm{S_1},\mathrm{S_2},\ldots,\mathrm{S_m})$ will be used to compare the protection systems by signature sets.

For vector criteria, different approaches are possible, in particular, convolutions (aggregation) of the initial data can be used [17].

Also, the introduced relation $\succcurlyeq^{\mathrm{S}}$ or $\succcurlyeq^{\mathrm{R}}$ can be extended to the general case for a set of incidents if the occurrence of any incident is considered as a single incident I. In the general case, the comparison is performed only as a comparison of vectors of the same dimension $(\mathrm{S_1^i},\mathrm{S_2^i},\ldots,\mathrm{S_m^i})$ and $(\mathrm{S_1^j},\mathrm{S_2^j},\ldots,\mathrm{S_m^j})$, then $(\mathrm{S_1^i},\mathrm{S_2^i},\ldots,\mathrm{S_m^i}) \succcurlyeq (\mathrm{S_1^j},\mathrm{S_2^j},\ldots,\mathrm{S_m^j})$ if $\mathrm{S_r^j} \succcurlyeq_{\mathrm{S}} \mathrm{S_r^j}$ for any r (or $\mathrm{S_r^j} \succcurlyeq_{\mathrm{R}} \mathrm{S_r^j}$), otherwise the vectors are incomparable.

However, it should be borne in mind that with asymptotic control, we improve the quality of protection gradually, making consistent changes and, therefore, we can assume that in most cases this will be associated with one very specific incident.

It should be noted that, taking into account the possibility of the dynamics of the development of the composition of the indicated incidents, one should simultaneously assume the immutability of the protected object and the environment (since their change can reduce a lot of incidents). In particular, it should be assumed that the transition from one threat model to another, based on a change in the composition of incidents, occurs with the same composition of protection mechanisms.

The asymptotic approach to information security management uses consistent improvement of the quality of the security system. The article discusses various options for quality assessment to determine the improvement (direction of development) of the properties of security systems. The basis of these estimates is the order ratio on the set of various security systems.

The considered variants of the order relation make it possible to compare the protection systems with each other and thereby estimate the improvement of their properties in the process of asymptotic control. And if the use of the relation $\succcurlyeq^{\mathrm{R}}$ seems to be more accurate, then for $\succcurlyeq^{\mathrm{S}}$ one can note its simplicity and versatility.

However, note that as mentioned above a critical information infrastructure (CII) in different areas in different countries can be assigned to completely different objects, but, despite this, all these objects have some common features that determine the specificity of the CII from the point of view of security [18], including in relation to modeling methods [19].

REFERENCES

[1] Khoffman L. Modern Methods of Information Protection. Moscow: Sov. radio Publ; 1980. 262 p. (in Russ.)

[2] GOST R ISO/MEK 15408-1-2013 Information technology. Security techniques. Evaluation criteria for IT security. Part 2. Security functional components. Moscow: Standartinform Publ.; 2014. (in Russ.)

[3] Erokhin S.D., Petukhov A.N., Pilyugin P.L. Principles and Tasks of Asymptotic Security Management of Critical Information Infrastructures. T-Comm. 2019;13(12):29□35. (in Russ.) DOI:10.24411/2072-8735-2018-10330.

[4] Online Browsing Platform. ISO/IEC 27005:2018(en) Information technology. Security techniques. Information security risk

[5] Erokhin S., Petukhov A., Pilyugin P. Event-based Security Policy and Formal Model of Critical Information Infrastructures Protecting Mechanism. Proc. of Telecom. Universities. 2019;5(4):99–105. (in Russ.) DOI:10.31854/1813-324X-2019-5-4-99-105

[6] Erokhin S.D., Petukhov A.N., Pilyugin P.L. Effectiveness of Active Monitoring of Network Security Events. Elektrosviaz. 2020;2:46–51. (in Russ.) DOI:10.34832/ELSV.2020.3.2.007.

[7] Methodical Recommendations for Categorizing Critical Information Infrastructure Objects Belonging to Subjects of Critical Information Infrastructure Operating in the Field of Communications. Documentary Telecommunication Association, 26th June 2019. (in Russ.) Available from: http://www.rans.ru/images/metrecKII.pdf [Access 7th September 2020]

[8] GOST R ISO MEK/TO 18044-2007 Information technology. Security techniques. Information security incident management. Moscow: Standartinform Publ.; 2014. (in Russ.)

[9] Masich G.F. Intrusion Detection System - IDS. Institute of Continuous Media Mechanics of the Ural Branch of Russian Academy of Science. 2016. (in Russ.) Available from: https://www.icmm.ru/uchebnaya-deyatelnost/lektsii/514-ids [Access 7th September2020]

[10] https://www.icmm.ru/uchebnaya-deyatelnost/lektsii/514-ids

[11] Lozhkovskii A.G., Kaptur V.A., Verbanov O.V., Kolchar V.M. Mathematical Model of Packet Traffic. Vestnik Nat. tech. university "KhPI". 2011;9:113–119. (in Russ.) Available from: http://repository.kpi.kharkov.ua/handle/KhPI-Press/10831 [Access 7th

[12] Shelukhin O.I. Network Anomalies. Detection, Localization, Forecasting. Moscow: Goriachaia liniia Telekom Publ.; 2019. 448 p. (in Russ.)

[13] Novikova E.S., Bekeneva Ya.A., Shorov A.V., Fedotov E.S. A Survey of Security Event Correlation Techniques for Cloud Computing Environment Security. Information and Control Systems. 2017; 5 (90): 95-104. (in Russ.) DOI:10.15217/issn1684-8853. 2017.5.95

[14] Petukhov A.N., Pilyugin P.L. Methods and Tools for Modeling the Security of Critical Information Infrastructures. Proceedings of 2nd All-Russian Conference on Modern Signal Processing Technologies, 11-12 December 2019, Moscow, Russia. Moscow: Moscow Scientific and Technical Society Radio Engineering, Electronics and Communications named after A.S. Popov Publ.; 2019. (in Russ.)14. Förster E., Rönz B. Methods of Correlation and Regression Analysis. Moscow: Finans i i statistika Publ.; 1983. 304 p. (in Russ.)

[15] Kramer G. Mathematical Methods of Statistics. Moscow: Mir Publ.; 1975. 648 p. (in Russ.)

[16] Ermolaev O.Yu. Mathematical Statistics for Psychologists. Moscow: Moscow Psychological and Social Institute Publ., Flinta Publ.; 2003. 336 p. (in Russ.)

[17] Podinovskiy V.V. Ideas and Methods of the Theory of the Importance of Criteria. Moscow: Nauka Publ.; 2019. 103 p. (in Russ.)

[18] Framework for Improving Critical Infrastructure Cybersecurity. // National Institute of Standards and Technology, USA, April, 16, 2018

[19] Erokhin S., Petukhov A., Pilyugin P. Critical Information Infrastructures Security Modeling. 2019 24th Conference of Open Innovations Association (FRUCT), Moscow, Russia, 2019, pp. 82-88.