Моделирование информационных атак и оценки защищенности объектов риска

Назаров Алексей Николаевич; Московский физико-технический институт; 141700, Российская Федерация, Московская область, г.Долгопрудный, Институтский пер., 9; профессор, доктор технических наук; a.nazarov06@bk.ru

Нгуен Суан Тиен; Московский физико-технический институт; 141700, Российская Федерация, Московская область, г.Долгопрудный, Институтский пер., 9; аспирант; tienxuannguyen86@gmail.com

Чан Минь Хай; Московский физико-технический институт; 141700, Российская Федерация, Московская область, г.Долгопрудный, Институтский пер., 9; аспирант; minhhai.kq80@gmail.com

Аннотация.

Сегодня остро стоят вопросы обеспечения и оценки гарантированного, необходимого или допустимого уровня информационной безопасности для разных классов пользователей сервисов систем Next Generation Network (NGN). Особенно при интеграции различных средств и систем информационной безопасности и отсутствии методической основы формирования доказательной базы соответствия различным нормативно-правовым актам, требованиям регуляторов, регламентированным политикам безопасности.

Конкретные требования к мерам объектовой защиты определяются по результатам специальных исследований технических средств с учетом установленной категории защищаемого объекта в зависимости от степени конфиденциальности обрабатываемой информации и условий размещения.

Различные атаки требуют различных технологических решений по обеспечению информационной безопасности объектов атак. Поскольку количество атак и их модификаций исчисляется более, чем пятизначным числом, то разрабатываются различные классификации подходов обеспечения информационной безопасности, охватывающие группы атак.

Таким образом, методические вопросы оценки допустимого уровня информационной безопасности нуждаются в дальнейшей проработке, что предопределяет актуальность настоящей статьи.


На основе логико-вероятностного подхода разработаны логико-вероятностные модели оценки информационной безопасности объекта атаки. Модели основаны на текущем уровне знаний, возможностей противодействия атакам и позволяют учитывать технологические особенности функционирования объекта атаки, существующие нормы и правила, а также любые требования. Исследованы свойства полученных моделей в классах новых функций безопасности. Уточнено состояния достижимости приемлемого уровня безопасности объекта атаки. Сформулированы...
логические и вероятностные критерии оценки риска информационной безопасности объекта атаки. Предложена процедура оценки ценовых рисков. Показаны направления автоматизации оценки уровня риска на основе интеллектуальных решений на основе нечеткой логики и нейронных сетей в среде веб-программирования для облачных вычислений в кластере Hadoop. Сформулированы основные требования к системе для интеллектуального автоматизированного системного мониторинга демона TaskTracker_состояние и другие в кластере Hadoop.

Ключевые слова: функция защиты, логическая модель, вероятностная модель, рисе, критерий, мониторинг, Hadoop, облачные вычисления, автоматизация, программный модуль, алгоритм, объект, демон, кластер, цель, требования

Литература.


[17] Назаров А.Н. Оценка защищенности от информационных атак// Телекоммуникации, № 5, в печати.


[23] Михайлов В.А. Разработка методов и моделей анализа и оценки устойчивого функционирования бортовых цифровых вычислительных комплексов в условиях преднамеренного
Modeling of information attacks, and security risk assessment facilities

Alexey Nazarov
Professor
Moscow Institute of Physics and Technology
State University
Moscow, Russia
a.nazarov06@bk.ru

Nguyen Xuan Tien,
graduate student
Moscow Institute of Physics and Technology
State University
Moscow, Russia
tienxuannguyen86@gmail.com

Tran Minh Hai,
graduate student
Moscow Institute of Physics and Technology
State University
Moscow, Russia
minhhai.kq80@gmail.com

Abstract—On the basis of logical-probabilistic approach developed logical-probabilistic models of information security assessment of the object of attack. The models are based on the current level of knowledge to counter attacks and allow the information to take into account technological features, especially the functioning of the object of attack, regulations and any requirements. The properties of the obtained models in the grades of the new security functions. Improved reachability condition acceptable security level of the object of attack. Formulates logic and probabilistic risk assessment criteria of information security object of attack. Proposed procedure for assessing price risks. Showing the direction of automation assess the level of risk on the basis of intelligent fuzzy logic and neural networks for web development environment for cloud computing in cluster Hadoop. Formulated the main system requirements for
I. INTRODUCTION

Common approaches to the construction and study of the risk of any attack, especially in relation to objects Next Generation Network (NGN) systems, information and telecommunication systems and networks (ITSN) developed within the logical-probabilistic approach [1, 2] and tested for a variety of practical examples [3-10]. Found interesting properties bot attack risk [11-14] studied risk model [4] and received by the extreme values of the risk [15].

This special urgency, issues of security and guaranteed assessment required or acceptable level of information security for different classes of users of services ITSN, NGN. Especially with the integration of various resources and information security in the multiprotocol ITSN and the lack of methodological basis for the formation of evidence of compliance to various regulatory legal acts, the requirements of regulators, regulated security policies.

Thus, methodological issues for evaluating the acceptable level of information security need to be further developed, which determines the relevance of this article.

II. MEASURES AND MEANS OF INFORMATION SECURITY OBJECTS

It is known [16], the following measures and means of information security:

- The legal (legislative) action.
- The organizational (administrative) measures of protection.
- Software measures.
- Means of protection from unauthorized access.
- Means of identification and authentication.
- Means of access control.
- Means of the control and integrity of software and information resources.
- Means of operational control and event logging.
- Cryptographic protection of information.
- System management of information security.
- Monitoring the effectiveness of the protection system.
- Physical measures and protection of information and telecommunication systems and networks.

The specific requirements of the object to the measures of protection are determined by the results of special studies of technical means, taking into account the established categories of protected object depending on the degree of confidentiality of information processed and accommodation conditions.

Various attacks require different technology solutions to ensure information security of objects of attacks. As the number of attacks and their modifications amounts to more than five digits, the approaches developed different classifications of information security, covering a group of attacks.

Results of the analysis tables in [16] show that the current classification of subject area of information security in the Russian telecommunications examples do not have a conceptual completeness. So, the most important for special consumers requirements for cryptographic protection of information not explicitly linked to the requirements for reliability. Not investigated the mutual influence of various destabilizing factors. The table in [16] shows the summary of various subject areas unrelated. Therefore, we need new fundamental results for the formulation of the scientific problem to counter attacks on objects of ITSN, and for the analysis and synthesis of the ways and means of preventing the destabilizing impact of information.

II. RISK OF ATTACK. FUNCTIONS OF SECURITY

Destabilizing factors [1] (DF) - the immediate cause of one or more phenomena, events, a consequence of the onset of which may be a violation of the integrity, stability, and others. Negative consequences for the ITSN. Among DF should also include the destabilizing effects, which, if successful, may be the cause of human rights of users content services in various subject areas. The destabilizing factors for a particular object of attack, of course have their own specifics. DF occur in technology, communications, network structure of society, and others.

The risk of an object subjected ITSN information attack by the enemy, consists of two components: [1]

- The probability of failure of counter attack against him (hereinafter - the failure of the object) or the probability of a successful attack - and assessment (e.g., financial, material, time to repair the damage, and others.) Scale effects (damage) of a successful attack.

The results of studies to assess the damage of a successful attack are given in [1]. For any object of risk in general, there are [2,3] in the full sense of the causal system (list) security functions (Table1), which performance scheme and the results obtained are shown in Fig. 1 and Table 2. Outcomes form a complete group of incompatible events [1].

<table>
<thead>
<tr>
<th>Designation of security functions</th>
<th>Appointment of security functions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 1. Preventing the occurrence of conditions conducive to the generation of (occurrence) destabilizing factors (DF)

<table>
<thead>
<tr>
<th>$X_1$</th>
<th>Preventing the occurrence of conditions conducive to the generation of (occurrence) destabilizing factors (DF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_2$</td>
<td>Warning immediate manifestations of destabilizing factors</td>
</tr>
<tr>
<td>$X_3$</td>
<td>Detection manifested destabilizing factors</td>
</tr>
<tr>
<td>$X_4$</td>
<td>Prevention of exposure to risk in the manifested and revealed destabilizing factors</td>
</tr>
<tr>
<td>$X_5$</td>
<td>Prevention of exposure to risk on the manifest, but the undetected destabilizing factors</td>
</tr>
<tr>
<td>$X_6$</td>
<td>Detecting the impact of destabilizing factors on the subject of risk</td>
</tr>
<tr>
<td>$X_7$</td>
<td>Localization (restriction) found the impact of destabilizing factors on the subject of risk</td>
</tr>
<tr>
<td>$X_8$</td>
<td>Localization of undetected exposure to risk by destabilizing factors</td>
</tr>
<tr>
<td>$X_9$</td>
<td>Dealing with the consequences of the localized impact of the detected object on the destabilizing factors</td>
</tr>
<tr>
<td>$X_{10}$</td>
<td>Dealing with the consequences of undetected localized exposure to risk by destabilizing factors</td>
</tr>
</tbody>
</table>

Figure 1. The causal diagram of the security functions $X_1 + X_{10}$ and results of attack $H_1 + H_{10}$.

Table 2. Final events in Fig. 1

<table>
<thead>
<tr>
<th>$H_1 + H_6$</th>
<th>Defence Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H_7, H_8$</td>
<td>Defence Broken</td>
</tr>
<tr>
<td>$H_9, H_{10}$</td>
<td>Defence Destroyed</td>
</tr>
</tbody>
</table>
From Fig. 1, it follows that the logic function (L-function, L-polynomial) the risk of an attack on the object A of ITS is

\[ LY = H_1 \lor H_2 \lor \ldots \lor H_m = Y_A \lor Y_A^c , \quad m = 10 , \]

where

\[
Y_A = H_7 \lor H_8 \lor H_9 \lor H_{10} \quad \text{-(1)}
\]

logic function successful attack, and

\[
Y_A^c = H_1 \lor H_2 \lor H_3 \lor H_4 \lor H_5 \lor H_6 \quad \text{-(2)}
\]

logic function object success or failure of the risk of attack [17].

Recall that [1] under the security function will be to understand the set of homogeneous functionally activities regularly carried out in ITS various means and methods to create, maintain, and provide the conditions necessary to objectively reliable information security.

The output of each of the security functions or it is the outcome is a random event and may take two values - success or failure. As in [1] suppose that the binary logical variable \( X_j, j=1+n, n=10 \) is equal to 1 (see "1" in Fig. 1) with a probability \( P_j \) if execution of the second function of protection has led to failure of the object of risk and is equal to 0 (see "0" in Fig. 1) with probability \( Q_j = 1 - P_j \) otherwise.

From Fig. 1 and [2,17] follow relations, taking into account the "bridge circuit" causality:

\[
\begin{align*}
H_1 &= \bar{X}_1; \\
H_2 &= X_1\bar{X}_2; \\
H_3 &= X_1X_2\bar{X}_3X_4; \\
H_4 &= X_1X_2(\bar{X}_3X_4 \lor X_3X_5)\bar{X}_6\bar{X}_7\bar{X}_9; \\
H_5 &= X_1X_2(\bar{X}_3X_4 \lor X_3X_5)X_6\bar{X}_8\bar{X}_{10}; \\
H_6 &= X_1X_2X_3X_5; \\
H_7 &= X_1X_2(\bar{X}_3X_4 \lor X_3X_5)\bar{X}_6\bar{X}_7\bar{X}_9; \\
H_8 &= X_1X_2(\bar{X}_3X_4 \lor X_3X_5)X_6\bar{X}_8\bar{X}_{10}; \\
H_9 &= X_1X_2(\bar{X}_3X_4 \lor X_3X_5)\bar{X}_6\bar{X}_7; \\
H_{10} &= X_1X_2X_3X_4 \lor X_3X_5\bar{X}_6X_7,
\end{align*}
\]

(3)

Assume that a binary logical variable \( H_j, j=1+m \) is equal to 1 with probability \( PH_j \) if not come outcome (outcome failure), and is equal to 0 with a probability \( QH_j = 1 - PH_j \) otherwise. Similarly, [2] we find that the probability of the risk (P-function, P-polynomial)

\[
PY = PH_1 + PH_2QH_1 + PH_3QH_1QH_2 + \ldots \\
+ PH_mQH_1QH_2 \cdots QH_{m-1} = P_A^Y + P_A ,
\]

where

\[
P_A = P_{10} + \sum_{i=2}^{6} PH_i \prod_{j=1}^{i-1} QH_j ,
\]

probability of success of the object risk,

\[
P_A^Y = \sum_{i=7}^{10} PH_i \prod_{j=1}^{i-1} QH_j ,
\]

(4)

probability of success of attack.

General view of the LP-functions (1), (5) of successful attack with (3), their properties, their practical applicability and importance obtained and research in a number of studies [2-12, 16, 17]. At the moment, the success of the applicability of security functions is shown by the example of automation solutions to counter bot-attacks [11-13].

Security Functions for the specific objects of risk are developed and studied as the attacker, and the security service of the object of risk. Each party pursues the opposite goal. One party pursues the objective of obtaining new guidelines that take into account the negative impacts. And to properly obtain the values \( Q_j \) of (6) is usually carried out at a given value received \( P_A^Y \), as a rule, empirically. However, such a situation becomes intolerable, because currently there is a high dynamic modifications attacks and spreading their negative impacts. And to properly obtain the values \( P_A^Y \) necessary to develop new guidelines that take into account the rapid pace of improvement of attacks.

In general, the value shall be calculated on the basis of existing or achieved level of information security of the object of attack. This level is caused by the presence of existing knowledge and solutions to counter the attacks on the subject of risk. In other words, it should be calculated on the basis of known security functions.

Therefore, further research is necessary to formalize LP functions success risk object on the basis of the known security functions and to clarify the condition of achievability (6).

III. LP-FUNCTIONS OBJECT SUCCESS RISK. CLARIFICATION OF THE CONDITION OF ACHIEVABILITY
Barriers or boundaries of protection issued by the security service to counter the negative impacts of DF object risk known to perform certain security functions, impeding the implementation of the attack on the subject of risk. At the same time, technologically, one barrier can perform a number of security functions. Barrier may serve to protect against the risk of different objects.

For the purposes of confrontation attack (6) the need to ensure low $P_y^{Y_{A-HB}}$. This should be done at the current time known methods and means. In other words, the probability of success risk object (4) under certain security functions

$$P_y^{Y_{A-HB}} = 1 - P_y^{Y_{A-DOP}}$$  

(7)

it should be greater, close to 1.

We denote the corresponding binary logic variables $H_{1}^{HB}$, $H_{2}^{HB}$, ..., $H_{m}^{HB}$, $m=10$ final events that can occur when the currently known security functions $X_{1}^{HB} \div X_{10}^{HB}$ object risk. These events and well-known security functions fully comply with the scheme of causality shown in Fig. 1 and the relations (3).

From Fig. 1 and (2), (3) it follows that

$$Y = H_{1}^{HB} \lor H_{2}^{HB} \lor H_{3}^{HB} \lor H_{4}^{HB} \lor H_{5}^{HB} \lor H_{6}^{HB}$$  

(8)

where [17]

$$H_{1}^{HB} = \overline{X}_{1}^{HB},$$

$$H_{2}^{HB} = \overline{X}_{1}^{HB} \overline{X}_{2}^{HB},$$

$$H_{3}^{HB} = \overline{X}_{1}^{HB} \overline{X}_{2}^{HB} \overline{X}_{3}^{HB} \overline{X}_{4}^{HB},$$

$$H_{4}^{HB} = \overline{X}_{1}^{HB} \overline{X}_{2}^{HB} \overline{X}_{3}^{HB} \overline{X}_{4}^{HB} \overline{X}_{5}^{HB} \overline{X}_{6}^{HB},$$

$$H_{5}^{HB} = \overline{X}_{1}^{HB} \overline{X}_{2}^{HB} \overline{X}_{3}^{HB} \overline{X}_{4}^{HB} \overline{X}_{5}^{HB} \overline{X}_{6}^{HB},$$

$$H_{6}^{HB} = \overline{X}_{1}^{HB} \overline{X}_{2}^{HB} \overline{X}_{3}^{HB} \overline{X}_{4}^{HB} \overline{X}_{5}^{HB} \overline{X}_{6}^{HB},$$

and the probability of successful risk object (4) based on the circuit of Fig. 1 can be calculated as in [1] using the B-polynomial for known security functions according to the following formula [17]

$$P_y^{Y_{A-HB}} = P_y^{H_{1}^{HB}} + \sum_{i=2}^{6} P_y^{H_{i}^{HB}} \prod_{j=1}^{i-1} Q_y^{H_{j}^{HB}} =$$

$$= Q_y^{H_{1}^{HB}} + \left(1 - Q_y^{H_{1}^{HB}}\right) Q_y^{H_{2}^{HB}} +$$

$$+ \left(1 - Q_y^{H_{1}^{HB}}\right) Q_y^{H_{2}^{HB}} +$$

$$+ \left(1 - Q_y^{H_{1}^{HB}}\right) Q_y^{H_{2}^{HB}} +$$

$$+ \left(1 - Q_y^{H_{1}^{HB}}\right) Q_y^{H_{2}^{HB}} +$$

$$+ \left(1 - Q_y^{H_{1}^{HB}}\right) Q_y^{H_{2}^{HB}} +$$

$$+ \left(1 - Q_y^{H_{1}^{HB}}\right) Q_y^{H_{2}^{HB}}$$

(9)

Substituting (9) and (7) into (6) we obtain

$$P_y^{Y_{A-HB}} \geq P_y^{Y_{A-HB}}$$  

(10)

a new kind of conditions reachable.

IV. A METHOD OF MODIFYING THE KNOWN SECURITY FUNCTIONS BASED ON THEIR GRADES. EXAMPLE OF PROTECTION AGAINST INTERNET ATTACKS

The causal completeness of the [1,2] security functions is an important property of logical-probabilistic approach. But the attack will be improved. Cybercriminals will look for and use new, previously unknown DF. Accordingly, the security function may become obsolete, ignore the new DF. Leaving methodological issues modifications attacks for another study, we note that under the protection of the specific object of the attack on the risk each of the security functions can be modified (refined). For example, can change the encryption algorithm, change the settings of the firewall, it can be adopted a new legal act, etc.

Such changes are methodologically quite easily and flexibly taken into account by introducing a gradation of security functions [2,17].

By analogy with the foregoing, we assume that the binary logical variable $X_{j}^{HB}$, $j=1 \div n$, $n=10$ corresponding to the $r$-th gradation of $j$-th known security functions is equal to 1 with a probability $P_y^{Y_{j}^{HB}}$, if, because of her, execution of $j$-th known security functions has led to failure risk object, and with a probability equal to 0 otherwise.

A good example of the introduction of new grades is a new kind of conditions reachable.
To expand the functionality $X_{I^{1}}^{HB}$, $X_{12}^{HB}$, $X_{51}^{HB}$, it is possible the introduction of new grades of these security functions, putting them in line the new indexed binary logical variables according to the table 4 [17].

Table 4. New gradation, extending the functionality of the known security functions of Internet attacks

<table>
<thead>
<tr>
<th>Designation of the new graduation security functions</th>
<th>Appointment of the new graduation security functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_{11}^{HOB}$</td>
<td>Preventing an environment conducive to the generation (emergence) of Internet-based attacks on the subject of risk based on information from the Centers Computer Emergency Response</td>
</tr>
<tr>
<td>$X_{12}^{HOB}$</td>
<td>Collect information about Internet attacks, based on information from the Centers Computer Emergency Response</td>
</tr>
<tr>
<td>$X_{51}^{HOB}$</td>
<td>Finding manifestations of Internet attacks based on information from the Centers Computer Emergency Response</td>
</tr>
<tr>
<td>$X_{51}^{HOB}$</td>
<td>Preventing exposure to the risk of undetected object of Internet attacks based on information from the Centers Computer Emergency Response</td>
</tr>
</tbody>
</table>

New grading permit formally introduce new components in the L-function (8) success risk object the following method:

$$X_{1}^{HB} \cdot X_{11}^{HOB} = X_{11}^{HOB} \cdot X_{12}^{HOB} + X_{11}^{HOB} \cdot X_{12}^{HOB} \cdot X_{51}^{HOB}.$$  

(11)

$$X_{5}^{HB} \cdot X_{51}^{HOB} = X_{5}^{HOB} \cdot X_{51}^{HOB}.$$  

(12)

$$X_{5}^{HB} \cdot X_{51}^{HOB} = X_{5}^{HOB} \cdot X_{51}^{HOB}.$$  

(13)

Substituting (11) - (13) to (8) get a new L-function success risk object against the Internet attack.

Each group of gradation for $X_{j}^{HB}$ is a group of mutually exclusive events, so we can use Bayes' formula [2,17],

$$P(X_{j}^{HOB} / X_{j}^{HB}) = \sum_{r=1}^{N_{j}} P(X_{j}^{HOB} / X_{j}^{HB}) P(X_{j}^{HB} / X_{j}^{HY}).$$  

(14)

With the help of (14) specifies the expression (9) for the B-polynomial and the formula (10) for a new type of conditions reachable. Formula (14) can be used for iterative learning in the model (9) on the statistical data to clarify the current value of risk.

Consider the features of the organization of algorithmic software to calculate the results of statistical data processing in the process object of risk.

V. RISK ASSESSMENT CRITERIA OF INFORMATION SECURITY OBJECT ATTACK. PRICE RISK..

The logical condition (8) for the success of the object of risk against the attack A (L-criteria) can be written as follows:

$$Y_{A}^{HB} = 1,$$

which is performed at least one of the following conditions [17]

$$\begin{align*}
X_{1}^{HB} & = 1, \\
X_{1}^{HB} & = 1, \\
X_{2}^{HB} & = 1, \\
X_{3}^{HB} & = 1, \\
X_{4}^{HB} & = 1, \\
X_{5}^{HB} & = 1.
\end{align*}$$

(15)

Accordingly, the probability condition for the success of the object of risk against the attack A (P-criteria) is

$$P_{A}^{I^{HB}} = 1,$$

or, subject to (9)

$$Q_{A}^{HB} + \left[1 - Q_{A}^{HB} \right] Q_{2}^{HB} +
\left[1 - Q_{A}^{HB} \right] Q_{3}^{HB} Q_{4}^{HB} +
\left[1 - Q_{A}^{HB} \right] Q_{5}^{HB} \cdot Q_{6}^{HB} \cdot Q_{7}^{HB} +
\left[1 - Q_{A}^{HB} \right] Q_{8}^{HB} \cdot Q_{9}^{HB} +
\left[1 - Q_{A}^{HB} \right] Q_{10}^{HB} +
\left[1 - Q_{A}^{HB} \right] Q_{11}^{HB} +
\left[1 - Q_{A}^{HB} \right] Q_{12}^{HB} = 1.$$  

(16)

In general, the LP-criteria allow to assess the actions of the attacker, which attacks the object of risk and has a certain knowledge about the barriers used in ITSN, peculiarities of the security functions, as well as the existing vulnerabilities in them. Formally it would be written as an attacker known models (8) and (9) and some information about the security.
functions $X_1^{\text{H3B}} + X_n^{\text{H3B}}$, $n=10$. Then the value of the residual

$$\Delta P^Y_{AA} = P^Y_A - P^Y_{A-I3B},$$

(17)

where the value $P^Y_I$ obtained as a result of statistical data processing, characterizes the condition reachable objective (10) and quality of the "armor" of barriers that implement security functions of the object of risk [17].

We introduce a new indicator

$$\Delta Y_{AA} = Y_A - Y_{A-I3B}.$$ 

From (17), (18) that if, when the LP-criteria (15), (16), carried out at least one of the conditions (criterion of exhaustion of reserve risk the stability of the object)

$$\begin{cases} \Delta P^Y_{AA} < 0, \\ \Delta Y_{AA} = 1, \end{cases}$$

it indicates the presence of the stability margin of the object to the risk of attack A by the attacker [17].

Accordingly, it is necessary to put an extra attacker resource in the improvement of the attack on the object of risk.

Methodically price risk can be estimated using the following formula:

$$CY = \begin{cases} CY_{ДОП} , & \text{if carrying out criteria (15), (16),} \\ CY_{ДОП} + C , & \text{if not carrying out the criteria (15), (16),} \end{cases}$$

where $CY_{ДОП}$ - the cost of risk tolerance [1], $C$ - a term that depends on many factors specific attack, the choice of values which is an independent problem.

Interest is the development of recommendations for monitoring the risk of objects, especially in the web space

VI. MONITORING WEB-SPACE BASED ON HADOOP.

Monitoring of objects in the web-space involves regular, performed by a given program monitoring Internet sites (IP-addresses of users of the global network of sites, and others.), their information and other resources, services, both for companies and for individuals, allowing to allocate state these objects and processes occurring in them under the influence of Internet activities across the Earth. Depending on the objective function in the web-monitoring and evaluation is made and functional activity values of the Internet ecosystem, and, secondly, the conditions for the determination of corrective actions in cases where targets are problem-oriented conditions are not met.

Hadoop as the technology of distributed processing large amounts of data in the web-environment is rapidly becoming an important tool, the ability for a wide range of programmers [18].

In this regard, monitored environment Hadoop we mean an organized monitoring of the selected objects in the web-space (domain) using the capabilities of Hadoop.

Hadoop was designed to work with Big Data in the web-space. And in this regard it has a number of unique features and abilities. It is appropriate to quote [18] "Formally speaking, Hadoop - is a framework of open source, designed to create and run distributed applications that process large amounts of data."

Hadoop runs on MapReduce technology developed by Google. MapReduce is a simple yet very powerful way to process and analyze large data sets, and is particularly effective in quantities of several petabytes.

In [19] of the rather general prerequisites analyzed principles, approaches and technological procedures for organizing the monitoring. Methodological approaches to the creation of algorithms and software solutions in the environment of web-programming Hadoop for a wide class of problems of monitoring sites in the web-space. For the first time developed a cluster topology Monitoring Hadoop, having common application is schematically shown in Fig. 2.

![Monitoring Topology Cluster Hadoop](image)

Figure 2. Monitoring Topology Cluster Hadoop.

The research and algorithms of measurement attributes of monitoring facilities in the web-space to meet the requirements of unity of measurements. Developed the system requirements for the design of the monitoring cluster Hadoop [19].

VII. ASSESSMENT OF THE STATE OF THE OBJECT IN ITS MONITORING OF RISK.

The use of neuro-fuzzy approach to the creation of various automation equipment and systems, as well as decision-making are now widely represented in the various fields of science and technology. For example, in [13,14,19,20], sets out the scientific results achieved in the automation of counter malicious attacks on the Internet, including bot attack. In [22-24] studied aspects of intellectual synthesis system analysis and evaluation of the stability of the onboard computer systems to the destructive effects of electromagnetic pulses.
On the basis of neuro-fuzzy formalism created software tools to assess the state of various objects observation in different automation systems. It seems appropriate to develop approaches and guidelines for the use of this formalism to assess the state of the observed object in the web-space and identify its information model in the monitoring cluster Hadoop.

A. The requirements for intelligent system daemon TaskTraker_состояние

This daemon works with a demon DataNode_состояние taking into account the specifics of the monitoring and control systems monitoring object in the web-space [20].

In the environment developed Hadoop software daemon, which assesses the current status of the monitoring object, depending on the specifics of the monitoring and control systems monitoring object in the web-space. We are thinking that we have the solutions of establish a system of sensors that supply accurate and complete information about the dynamics of the attributes of the object monitoring.

Using the results of [20,21] proposed the following hierarchy of intelligent system daemon TaskTraker_состояние as a set of software modules of the automated system (AS) on the evaluation of the monitoring object in the web-space. By analogy with [5] daemon includes the following functional modules: the system of fuzzy production rules that describe the job identifier taking into account expert assessments; neuro-fuzzy network, which is reflected in the structure of the system of fuzzy production rules; clear self-organizing neural network (NN) to solve the problems of classification and clustering input vectors. As noted in [20,21] This hierarchy has the common use and therefore suitable for various objects based monitoring Monitoring Cluster Hadoop, shown in Fig. 2.

Basic system requirements for the AS TaskTraker_состояние monitoring object in the web-space, the presence of which is mandatory:
- Presentation of a priori experience of experts on web-monitoring of the selected object in the form of knowledge, described the system of production rules;
- The presence of base criterion for decision-making to change the attributes of the object monitoring;
- Fuzzy inference, which allows the experience of experts on web-monitoring of the selected object in the form of fuzzy production rules for initial setup information field (of interneuronal connections) fuzzy neural network;
- Plug aggregation services and service processing unstructured information of the change object attributes monitor for later analysis:
  - The ability of the NN to the classification and clustering;
  - The ability of the NN to extract knowledge about the profile and mechanism of implementation of the attributes of the object monitoring changes in the web-space;
  - The ability of the information field of the NN to the accumulation of experience in the process of teaching and learning.

The Hadoop environment should be developed software that meets the above requirements. In addition, the demon TaskTraker_состояние monitoring object in the web-space should be based on a service-oriented integration methods in terms of scalability of its functional features.

B. The mechanism of fuzzy inference

This mechanism is based on the representation of the experience of experts on web-monitoring system of fuzzy production rules of the form IF-THEN, for example, [3-5]:

\[ \Pi_1 : \text{IF } \bar{x}_1 \text{ IS } A_{11} \text{ AND } \ldots \bar{x}_n \text{ IS } A_{1n} \text{ THEN } \bar{y} \text{ IS } B_1 ; \]

\[ \Pi_2 : \text{IF } \bar{x}_1 \text{ IS } A_{21} \text{ AND } \ldots \bar{x}_n \text{ IS } A_{2n} \text{ THEN } \bar{y} \text{ IS } B_2 ; \]

\[ \ldots \]

\[ \Pi_k : \text{IF } \bar{x}_1 \text{ IS } A_{k1} \text{ AND } \ldots \bar{x}_n \text{ IS } A_{kn} \text{ THEN } \bar{y} \text{ IS } B_k , \]

where \( \bar{x}_i \) and \( \bar{y}_i \) - fuzzy input and output variables respectively, \( A_{ij} \) and \( B_j \), \( j = 1,\ldots,n \), \( i = 1,\ldots,k \), corresponding membership function.

Combining features of the NN and the fuzzy inference is one of the most promising approaches to artificial intelligence systems. As was shown in [22-24], the system compensates the basic fuzzy logic "opacity" of the NN: In the knowledge and ability to explain the results of the intelligent system, i.e. complemented by the NN. Fuzzy formalism output operates in the absence of knowledge about the attributes of objects and monitor changes to the monitoring of any objects, which is important when new attributes appear with unknown dynamics.

For the functional daemon TaskTraker_состояние monitoring object in the web-space is very important feature of such neuro-fuzzy networks as the ability to automatically generate a system of fuzzy production rules in the process of learning and self-extracting hidden patterns from data input training sample.

Algorithms for neural network training using the stochastic properties of the dynamics of changes of attributes of an object in the web-monitoring space must be based on a standard method to minimize the generalization error [21,25], based on the minimization of a quadratic functional of the residual in the training set, finding extremum target gradient density function errors using the procedure of Robbins-Monro [10,21,25,26].

VIII. THE HIERARCHY OF LEVELS AND THE WORK OF INTELLECTUAL SYSTEM DAEMON TaskTraker_состояние

The ability of the NN on classification and clustering daemon is used to solve two main tasks:
1) the classification of the input vector, for example, the feature vector object attributes change monitoring;
2) expansion of the classification of the appearance at the input of the classifier not previously encountered a combination of signs of change attributes.
Let there be at the moment the full space parcels
\[ X = \{x_1, \ldots, x_m\} \] and the full space of the
conclusions \[ Y = \{y_1, \ldots, y_n\} \]. Fuzzy causal relationship
\[ \tilde{x}_i \rightarrow \tilde{y}_j, \quad i = 1, \ldots, m, \quad j = 1, \ldots, n \] between the elements of these spaces can be represented as a matrix \( R \) with the
elements \( r_{ij}, i = 1, \ldots, m, \quad j = 1, \ldots, n \), and sending and
opinions between them can be expressed as: \( B = A \cdot R \), where
\( \cdot \) - the operation of the composition, for example, max-min-
composition.

According to [10,13,20-23] in the fuzzy inference fuzzy
expert knowledge \( A \rightarrow B \) reflects the relation \( R = A \rightarrow B \),
which corresponds to the operation of fuzzy implication.
Fuzzy relation \( R \) can be viewed as a fuzzy subset of Cartesian
product \( X \times Y \) of the full set \( X \) and conclusions \( Y \), and the
process of getting the fuzzy results \( B \) by sending the output
\( A \) and knowledge \( A \rightarrow B \) - as the compositional rule of
thumb \( B = A \cdot R = A \cdot (A \rightarrow B) \).

From the practice of [10,13,20-23] we know that the level of
accumulation of experience AS neuro-fuzzy classifier of feature vectors, the parameters change (dynamics attributes)
the Monitoring object advisable to design a three-layer fuzzy
NN (Fig. 3) with the ability to reduce (compress) the number of signs.

![Figure 3. Scheme neuro-fuzzy classifier AS.](image)

Each input vector in the space can be associated with a
formal fuzzy neuron (FN). The middle layer contains fuzzy
FN performing the operation of inference (e.g., min) of the
combinations of fuzzy statements (FS) of the first layer of the
NN to form a system of classification of fuzzy conclusions.
The third layer NN is formed from fuzzy FN "OR" (the
number of fuzzy conclusions \( \tilde{y}_j, \quad j = 1, \ldots, n \) ) and generates a
vector of output fuzzy conclusions in accordance with the
given expert system of fuzzy rules.

IX. THE MAIN STAGES OF DESIGN OF
INTELLIGENT SYSTEM DAEMON
TaskTracker_состояние.

The ability to learn intelligent system is caused by
redundancy the input information and hidden in these laws,
expand and / or modifying, altering the information model of
the object of monitoring and, as a consequence, itself neural
network in the process of monitoring the functioning of the
cluster.

Taking into account the results obtained in [23], the
following design guidelines intellectual system
TaskTracker_состояние demon in the form of the following
sequence of steps [26].

1. The decision of the classification problem for the
monitoring object the known values of attributes
(characteristics, parameters) the monitoring object of feature
elements. Storing the information obtained in the module Д-Клас-С
of daemon TaskTracker_состояние.

2. Solution of the problem of clustering the monitoring
object state changes on the grounds of such changes as the
self-development of the classification of the expansion of a
variety of known values of attributes (characteristics,
parameters) the monitoring object. Storing the information
obtained in the solution in the module Д-Кластер-С-А of
daemon DataNode_состояние.

3. Formation of a plurality of expert assessments for a
decision on the corresponding values of attributes
(characteristics, parameters) the monitoring object signs of
change. Storing the information obtained in the module Д-Э-О
of daemon DataNode_состояние.

4. Development of a program module (ПМ-Н-П-П)
daemon TaskTracker_состояние implements the fuzzy
production rules on the results of the P1 and P3.

5. Development of a program module (PM-НН-Р) daemon
TaskTracker_состояние implementing the system of neuro-
fuzzy classifier (signs of changing attributes - change the state
of an object of monitoring).

6. Development of a program module (PM-В-С) daemon
TaskTracker_состояние that implements the solution of P2 in
the form of crisp classifications based on self-learning
adaptive system - clusterer (signs of changing attributes -
change the state of an object of monitoring).

X. REQUIREMENTS FOR THE INDICATORS OF
QUALITY OF FUNCTIONING OF THE DAEMON
TaskTracker_состояние.

In general, this daemon provides continuous processing of
event data, as a rule, stochastic changes in object attributes
monitoring coming from the sensor system monitoring object
in the web-space. Since the assumed long-term (years)
monitoring the functioning of the cluster as the target function
can offer a maximum sustainability of the daemon
TaskTracker_состояние. The analytical form of objective
function requires a separate development and research,
including on the basis of the architecture of software modules and hardware monitoring cluster-specific management systems chosen subject area.

In general [26], we can offer the following limitations monitoring based on probability-time tactical and technical requirements for quality indicators of functioning daemon TaskTracker_состояние:

- Probability: \( P_{CB} \left( T_{\text{T} \cdot \text{DOP}} \leq t \right) \geq P_{CB}^{\text{T} \cdot \text{DOP}} \), where \( t \) - random time for processing of events monitoring; \( T_{\text{T} \cdot \text{DOP}} \) - permitted value of time for processing of event monitoring; \( P_{CB}^{\text{T} \cdot \text{DOP}} \) - the probability of timely processing of event monitoring; \( P_{CB} \) - permitted value probability event monitoring;

- for Expediting: \( T_{AH} \leq T_{\text{T} \cdot \text{DOP}} \cdot AH \), where \( T_{AH} \) - the average value of the time, \( T_{\text{T} \cdot \text{DOP}} \) - it permissible value;

- On the validity of \( N_{C} \leq N_{C}^{t} \) \( \text{in} S \) \( N_{H} \geq N_{H}^{t} \) \( \text{in} S \) and \( N_{A} \geq N_{A}^{t} \), where \( N_{C} \), \( N_{H} \), \( N_{A} \) - number of the analyzed scenarios of the behavior of the object of monitoring, the number of new attribute values of the object of monitoring, the number of object attributes accounted monitoring respectively; \( S \) - a lot of options state (implementation, operation, and generation) of Monitoring.; \( N_{C}^{t}, N_{H}^{t}, N_{A}^{t} \) - the number of the analyzed scenarios of the behavior of the object of monitoring, the number of new attribute values of the object of monitoring, the number of object attributes accounted monitoring \( s \)-th state respectively;

- Resource use: \( P_{\text{PEC}} \left( r \leq R_{\text{T} \cdot \text{DOP}} \right) \geq P_{\text{PEC}}^{\text{T} \cdot \text{DOP}} \), where \( P_{\text{PEC}} \) the probability of resource use in the processing of monitoring events, and \( P_{\text{PEC}}^{\text{T} \cdot \text{DOP}} \) - its permissible value, \( r \) - consume resources (hardware and software, configuration, virtual, and others.) When processing the monitoring events, and - its allowable value. Of the best practices [21] concretization can use \( P_{\text{PEC}}^{\text{T} \cdot \text{DOP}} = 0.99 \) and \( R_{\text{T} \cdot \text{DOP}} = 0.15 \) as well.

Depending on the requirements for the control system parameters specified above specific values. Probabilistic constraint can be transformed into quantile form and limit expediting - into the limit for other time points of \( t \).

To estimate quantile function of stochastic performance monitoring object attributes in the web-space daemon TaskTracker_состояние recommended to include a software module that implements a bootstrap procedure, the features of which were studied in detail in [10,20,27-29].

XI. CONCLUSION

To eliminate the gaps in the scientific fundamentals of evaluating security risks modern facilities and ITSN adequacy level of protection on the basis of logical-probabilistic approach developed new LP-model of risk assessment of the object of protection from malicious attacks ITSN. On the basis of LP-models and complete a variety of known security functions produced a new kind of conditions necessary level of reachability infosecurity object of risk in ITSN.

When modifications are known security function provides a method of extending their functionality through the mechanism of gradations. In this case, the development of LP-models of risk assessment of the security object and clarify the conditions of the reachability by using Bayesian formalism, with the possibility of organizing an algorithmic iterative learning obtained in models of statistical data in order to clarify the current value of risk.

Formulated criteria for assessing the risk of a protected object of attack and suggested guidelines for evaluating the price risk of attack.

For Monitoring Hadoop cluster topology developed and investigated the synthesis of guidelines and demons TaskTracker_состояние and DataNode_состояние responsible for the task of assessing the status of the object of observation and identification of its information model, taking into account the characteristics of cloud computing. The principles and approaches, based on neuro-fuzzy solutions that can be the basis for the design of intelligent monitoring systems of objects in the web-space.

The mechanisms of decision-making based on the formalization of a priori experience of experts in fuzzy database fuzzy production rules. Within the framework of solving the problems of classification and expansion of classification of input data about the characteristics of cloud computing. The dynamics of the object attributes monitoring investigated the possibility of neuro-fuzzy classifier in the form of a three-layer fuzzy Neural Network, consisting of the following levels:

- A system of fuzzy production rules describing the work identifier based on expert assessments;
- Neuro-fuzzy network, which is reflected in the structure of the system of fuzzy production rules;
- Self-learning neural network is a clear solution for the problem of clustering (classification) of the input data from web-space.

And the lower level solves the problem of rapid identification attribute changes, and the top - the accumulation of experience to detect the effects of such changes on the elements and nodes of the monitoring object.

An approach to the synthesis of mathematical formalization demon TaskTracker_состояние as a constrained optimization problem. Proposed restrictions in the form of inequalities, reflecting the specific cloud computing environment Hadoop.

REFERENCES

Article in a journal:


In a conference proceedings:


In a journal:


Project report:


In a conference proceedings:


[8] Nazarov, A. & Komarov, A 2013 'Intelligent analysis system cyber space on web-technologies', paper presented in the Collection of proceedings of the 7th Industry Conference "Information Society Technologies", Russia, Moscow Technical University of Communications and Informatics.

In a journal:


In a conference proceedings:


In a journal:


In a conference proceedings:


Book:


In a journal:


Book:


In a conference proceedings:


In a journal:


Doctoral thesis:


In a conference proceedings:


Book:


In a journal:


Article in a conference proceedings:


Book: