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.

Общие подходы к построению и исследованию риска любой атаки, прежде всего в отношении объектов Next Generation Network (NGN) систем, информационно-телекоммуникационных систем и сетей (ИТКС) разработаны рамках логико-вероятностного подхода [1, 2] и проверены на различных практических примерах [3-10]. Обнаружены интересные свойства риска бот-атаки [11-15], исследованы модели риска [4] и получены экстремальные значения риска [16].

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 требований. 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 TaskTraker_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.

[1 Nazarov, A 2007, ′Estimation of information safety level of modern infocommunication networks on basis of logic-probability approach′, Automation and Remote Control, July 2007, Volume 68 Issue 7, 2007, pp. 1165-1176, USA, doi: 10.1134/S0005117907070053.

[2] Nazarov, A 2010, ′Logical-and-probabilistic model for estimating the level of information security of modern information and communication networks′, Telecommunications and Radio Engineering, Vol. 69, no 16, pp. 1453-1463, USA, doi: 10.1615/TelecomRadEng.v**69**.i**16**.60.

[3] Nazarov, A. & Klimanov, M. 2010, ′Estimating the informational security level of a typical corporate network′, Automation and Remote Control , Volume 71 Issue 8, 2010, pp. 1550-1561.

Article in a conference proceedings:

[4] Nazarov, A. & Klimanov, M 2009, ′Characteristic analysis of logic and probabilistic model of information security′, paper presented in the Collection of proceedings of of International Workshop on Distributed Computer and Communication Computer and Communication Networks (DCCN-2009), Sofia, Bulgaria, October 5-9, 2009, pp. 154-164. Published by Research and Development Company "Information and Networking Technologies", Russia, Moscow.

[5] Назаров А.Н., Климанов М.М. Оценка уровня безопасности DNS-серверов// Документальная электросвязь, 2011- № 21.- С. 54-57.

[6] Грудинов С.А., Комаров А.А., Назаров А.Н. и др. CyberCop: Отчёт о НИР «Глобальная система противодействия неправомерным действиям в киберпространстве» (1-й этап, Соглашение по гранту Сколково № 87 от 02.11.2012г.), ООО «Группа Айби», исх. № 8 от 25.02.2013.- 285 с.

[7] Назаров А.Н., Климанов М.М. Использование логико-вероятностного подхода при оценке риска DDOS атаки// Сборник ежегодных научных трудов Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2014), М.: ИПУ РАН.-2014 г.- С. 444-451.

[8] Назаров А.Н., Комаров А.А. Интеллектуальная система анализа кибербезопасности в пространстве на web-технологиях/ Доклад на 7-ой Отраслевой конференции «Технологии информационного общества». МТУСИ. 20.02.2013г.

[9] Назаров А.Н., Туреев С.Ф. Оценка уровня информационной безопасности компьютерной сети при сетевой атаке // T-comm.-2013.- № 10.- С. 78-80.

[10] Назаров А.Н., Комаров А.А. Интеллектуальная система кибербезопасности в пространстве на WEB-технологиях // T-comm.-2013.- № 10.- С. 81-84.

[11] A.Nazarov, S. Tureev. LOGIC AND PROBABILISTIC MODEL OF INFORMATION SECURITY FOR RISK ASSESSMENT OF THE OBJECT UNDER BOTNET ATTACKS// Proceedings of

International Conference “Distributed Computer and Communication Networks: Control, Computation, Communications (DCCN-2013), Moscow, Russia, October 07-10, 2013, pp. 276-283. Published by JSC TECHNOSPHERA, Moscow, 2013.

[12] А.А.Комаров, А.Н.Назаров Функциональные требования к системе обнаружения и противодействия ботнет-атакам на корпоративные сети // Техника средств связи, серия «Техника телевидения», 2013г., с. 140-151.

[13] Сачков И.К., Назаров А.Н. Автоматизация противодействия бот-атакам// T-comm.-Т.8.- 2014.-№ 6.- С. 5-9.

[14] Nazarov, A 2012 'Botnet tracking and global threat intelligence - behavior approaches to identifying distributed botnets', paper presented at the IEEE / Collection of proceedings of the Cybersecurity Summit (WCS), 2012 Third Worldwide, New Dehli, 30-31 Oct. 2012. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6780878&newsearch=true&queryText=Botnet%20tracking%20and%20global%20threat%20intelligence%20-%20behavior%20approaches%20to%20identifying%20distributed%20botnets

[15] Назаров А.Н., Сычев К.И. Модели и методы расчёта показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. – 2-е изд., перераб. и доп. – Красноярск: Изд-во ООО "Поликом", 2011. – 491 с.: ил.

[16] Назаров А.Н. О возможности классификации объектов информационной безопасности сети общего пользования на основе логико-вероятностного подхода// Электронный журнал «Вычислительные сети. Теория и Практика («Network journal. Theory and Practice») BC/NW 2013, № 2(23):11.1http://network-journal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=23&pa=11&ar=1

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

[18] Чак Лэм. Hadoop в действии. – М.: ДМК Пресс, 2012.-424 с.

[19] Волков Д.А., Назаров А.Н., Назаров М.А. Глобальная угроза – Теневой Интернет// Сборник ежегодных научных трудов Международной конференции «Управление развитием крупномасштабных систем» (MLSD’2014), М.: ИПУ РАН.-2014 г.- С.452-459.

[20] Назаров А.Н. О подходах к созданию интеллектуальной системы анализа атак из Интернета//Сборник материалов XII Всероссийского совещания по проблемам управления (ВСПУ-2014), ИПУ РАН, 2014.- С.9208-9215.

[21] Михайлов В.А., Мырова Л.О., Царегородцев А.В. Интеллектуальная система анализа и оценки устойчивости БЦВК к деструктивному воздействию ЭМИ // Электросвязь, № 8, 2012.- с. 36-39.

[22] Воскобович В.В., Михайлов В.А., Мырова Л.О., Царегородцев А.В. Системный подход к созданию методологии анализа и оценки устойчивости к деструктивному воздействию ЭМИ // Технологии ЭМС.-2012.-№ 1(40).- С.51-58.

[23] Михайлов В.А. Разработка методов и моделей анализа и оценки устойчивого функционирования бортовых цифровых вычислительных комплексов в условиях преднамеренного

воздействия сверхкоротких электромагнитных излучений, автореферат диссертация на соискание ученой степени доктора технический наук, ОАО «НИИ «Аргон», 2014.- 45 с.

[24] Овсянников А.В., Байда Ю.А., Лаврентьев В.С. информационные алгоритмы обучения нейронных сетей // Труды БГТУ.Сер. физ.-мат. Наук и инфор. Вып. XII. 2004. С.110-113.

[25] Фомин В.Н. Рекуррентное оценивание и адаптивная фильтрация. – М.: Наука. Гл. ред. физ.-мат. лит., 1984.- 288 с.

[26] Назаров А.Н. Назаров М.А., Пантюхин Д.В., Покрова С.В., Сычев А.К. Автоматизация процедур мониторинга в web-пространстве на основе нейро-нечеткого формализма// T-comm.-Т.9-2015.- № 8.- С. 26-33.

[27] Вишняков Б.В., Кибзун А.И. Применение метода бутстрепа для оценивания функции квантили // Автоматика и телемеханика, № 11, 2007.-с. 46-60.Article in a conference proceedings:

[28] Гаев Л.В. Рандомизированная оценка результатов имитационных экспериментов/ СПб., Сборник докладов Конференции «ИММОД-2003», 2003.- 5 с.

[29]. Галамбош Я. Асимптотическая теория экстремальных порядковых статистик. М.: Наука, 1984.
.

Modeling of information attacks, and security risk assessment facilities

Alexey Nazarov
Professor
Moscow Institute of Physics and Technology
State University
Moscow, Russia
Expert ITU
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**

intelligent automated system monitoring daemon TaskTraker_состояние and others in cluster Hadoop.

Keywords- security function, logic model, probabilistic model, risk, criterion, monitoring, Hadoop, cloud computing, automation, software programming module, algorithm, object, daemon, cluster, target, requirements

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 assesment 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 1. Security Functions

Designation of security functions	Appointment of security functions

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

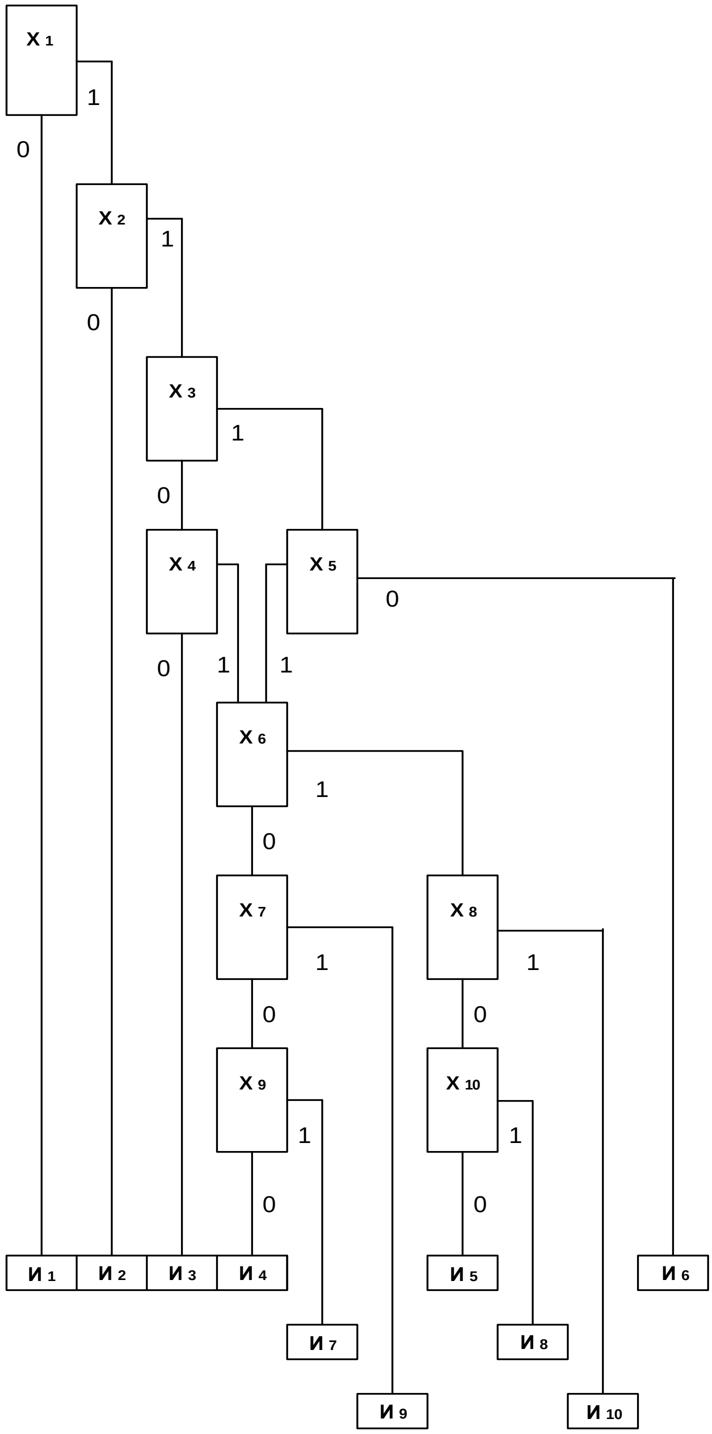

Figure 1. The causal diagram of the security functions $X_1 \div X_{10}$ and results of attack $И_1 \div И_{10}$.

Table 2. Final events in Fig. 1

$И_1 \div И_6$	Defence Provided
$И_7, И_8$	Defence Broken
$И_9, И_{10}$	Defence Destroyed

From Fig. 1, it follows that the logic function (L-function, L-polynomial) the risk of an attack on the object A of ITSN is

$$LY = И_1 \vee И_2 \vee \ldots \vee И_m = Y_A \vee Y_{\overline{A}}, \; m = 10,$$

where

$$Y_A = И_7 \vee И_8 \vee И_9 \vee И_{10} \quad - \qquad (1)$$

logic function successful attack, and

$$Y_{\overline{A}} = И_1 \vee И_2 \vee И_3 \vee И_4 \vee И_5 \vee И_6 \, - \qquad (2)$$

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 ITSN 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, $j = 1 \div n, n = 10$ 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:

$$\begin{gathered}
И_1 = \overline{X}_1; \\
И_2 = X_1 \overline{X}_2; \\
И_3 = X_1 X_2 \overline{X}_3 \overline{X}_4; \\
И_4 = X_1 X_2 \left(\overline{X}_3 X_4 \vee X_3 X_5\right) \overline{X}_6 \overline{X}_7 \overline{X}_9; \\
И_5 = X_1 X_2 \left(\overline{X_3} X_4 \vee X_3 X_5\right) X_6 \overline{X}_8 \overline{X}_{10}; \\
И_6 = X_1 X_2 X_3 \overline{X_5}; \\
И_7 = X_1 X_2 \left(\overline{X_3} X_4 \vee X_3 X_5\right) \overline{X}_6 \overline{X}_7 X_9; \\
И_8 = X_1 X_2 \left(\overline{X_3} X_4 \vee X_3 X_5\right) X_6 \overline{X_8} X_{10}; \\
И_9 = X_1 X_2 \left(\overline{X_3} X_4 \vee X_3 X_5\right) \overline{X_6} X_7; \\
И_{10} = X_1 X_2 \left(\overline{X_3} X_4 \vee X_3 X_5\right) X_6 X_8,
\end{gathered} \qquad (3)$$

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

$$\begin{aligned}
PY &= PИ_1 + PИ_2 QИ_1 + PИ_3 QИ_1 QИ_2 + \ldots \\
&\quad \ldots + PИ_m QИ_1 QИ_2 \cdots QИ_{m-1} = P_A^Y + P_A,
\end{aligned}$$

where

$$P_{\overline{A}} = PИ_1 + \sum_{i=2}^{6} PИ_i \prod_{j=1}^{i-1} QИ_j \, - \qquad (4)$$

probability of success of the object risk,

$$P_A^Y = \sum_{i=7}^{10} PИ_i \prod_{j=1}^{i-1} QИ_j \, - \qquad (5)$$

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. Security functions are developed and implemented each of the parties on the basis of the above measures and means of information security facilities.

The object of the risk is considered sufficiently protected [1,2] when considering the possibility of potential barriers to overcome probability of a successful attack (the probability of the risk, the probability of failure or the risk of insecurity object) is less than the allowable value, i.e.

$$P_З^Y \geq 1 - P_{A-ДОП}^Y \, - \quad \text{achievability condition,} \qquad (6)$$

where $P_З^Y$ - the probability of a successful attack confrontation (protected by the probability of failure of the attack, probability of success risk object) the object of the risk.

Estimation of protection of specific objects $P_З^Y$ using the conditions of achievability (6) is usually carried out at a given value received $P_{A-ДОП}^Y$, 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 $P_{A-ДОП}^Y$ 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 $P^{Y}_{A-ДОП}$ **.** 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

$$P^{Y}_{\underline{A}-ИЗВ} = 1 - P^{Y}_{A-ДОП} \qquad (7)$$

it should be greater, close to 1.

We denote the corresponding binary logic variables $И^{ИЗВ}_{1}, И^{ИЗВ}_{2}, \ldots, И^{ИЗВ}_{m}$, $m = 10$ final events that can occur when the currently known security functions $X^{ИЗВ}_{1} \div X^{ИЗВ}_{10}$ 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

$$Y^{ИЗВ}_{\underline{A}} = И^{ИЗВ}_{1} \vee И^{ИЗВ}_{2} \vee И^{ИЗВ}_{3} \vee$$
$$\vee И^{ИЗВ}_{4} \vee И^{ИЗВ}_{5} \vee И^{ИЗВ}_{6}, \qquad (8)$$

where [17]

$$И^{ИЗВ}_{1} = \overline{X}^{ИЗВ}_{1},$$

$$И^{ИЗВ}_{2} = X^{ИЗВ}_{1} \overline{X}^{ИЗВ}_{2},$$

$$И^{ИЗВ}_{3} = X^{ИЗВ}_{1} X^{ИЗВ}_{2} \overline{X}^{ИЗВ}_{3} \overline{X}^{ИЗВ}_{4},$$

$$И^{ИЗВ}_{4} = X^{ИЗВ}_{1} X^{ИЗВ}_{2} \left(\overline{X}^{ИЗВ}_{3} X^{ИЗВ}_{4} \vee X^{ИЗВ}_{3} X^{ИЗВ}_{5}\right) \bullet$$
$$\bullet \overline{X}^{ИЗВ}_{6} \overline{X}^{ИЗВ}_{7} \overline{X}^{ИЗВ}_{9},$$

$$И^{ИЗВ}_{5} = X^{ИЗВ}_{1} X^{ИЗВ}_{2} \left(\overline{X}^{ИЗВ}_{3} X^{ИЗВ}_{4} \vee X^{ИЗВ}_{3} X^{ИЗВ}_{5}\right) \bullet$$
$$\bullet X^{ИЗВ}_{6} \overline{X}^{ИЗВ}_{8} \overline{X}^{ИЗВ}_{10},$$

$$И^{ИЗВ}_{6} = X^{ИЗВ}_{1} X^{ИЗВ}_{2} X^{ИЗВ}_{3} \overline{X}^{ИЗВ}_{5},$$

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]

$$P^{Y}_{\underline{A}-ИЗВ} = PИ^{ИЗВ}_{1} + \sum_{i=2}^{6} PИ^{ИЗВ}_{i} \prod_{j=1}^{i-1} QИ^{ИЗВ}_{j} =$$

$$= Q^{ИЗВ}_{1} + \left(1 - Q^{ИЗВ}_{1}\right) Q^{ИЗВ}_{2} +$$

$$+ \left(1 - Q^{ИЗВ}_{1}\right)\left(1 - Q^{ИЗВ}_{2}\right) Q^{ИЗВ}_{3} Q^{ИЗВ}_{4} +$$

$$+ \left(1 - Q^{ИЗВ}_{1}\right)\left(1 - Q^{ИЗВ}_{2}\right) \bullet$$

$$\bullet \left[Q^{ИЗВ}_{3} \left(1 - Q^{ИЗВ}_{4}\right) + \left(1 - Q^{ИЗВ}_{3}\right) \left(1 - Q^{ИЗВ}_{5}\right) \right] \bullet$$

$$\bullet Q^{ИЗВ}_{6} Q^{ИЗВ}_{7} Q^{ИЗВ}_{9} +$$

$$+ \left(1 - Q^{ИЗВ}_{1}\right)\left(1 - Q^{ИЗВ}_{2}\right) \bullet$$

$$\bullet \left[Q^{ИЗВ}_{3} \left(1 - Q^{ИЗВ}_{4}\right) + \left(1 - Q^{ИЗВ}_{3}\right) \left(1 - Q^{ИЗВ}_{5}\right) \right] \bullet$$

$$\bullet \left(1 - Q^{ИЗВ}_{6}\right) Q^{ИЗВ}_{8} Q^{ИЗВ}_{10} +$$

$$+ \left(1 - Q^{ИЗВ}_{1}\right)\left(1 - Q^{ИЗВ}_{2}\right) \left(1 - Q^{ИЗВ}_{3}\right) Q^{ИЗВ}_{5}. \qquad (9)$$

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

$$P^{Y}_{3} \geq P^{Y}_{\underline{A}-ИЗВ} \text{ -} \qquad (10)$$

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 $X^{НОВ}_{jr}$, $j = 1 \div n, n = 10$ corresponding to the $r-$th gradation of $j-$th known security functions is equal to 1 with a probability $P^{НОВ}_{jr}$, 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 feature to prevent Internet attacks, formed on the basis of national centers to respond to computer incidents. These centers are established in each country. They are designed to monitor, combat malicious Internet attacks and dissemination of information on such attacks to all interested organizations.

To expand the functionality $X_1^{\text{ИЗВ}}$, $X_3^{\text{ИЗВ}}$, $X_5^{\text{ИЗВ}}$, 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

Designation of the new graduation security functions	Appointment of the new graduation security functions
$X_{11}^{\text{НОВ}}$	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
$X_{12}^{\text{НОВ}}$	Collect information about Internet attacks, based on information from the Centers Computer Emergency Response
$X_{31}^{\text{НОВ}}$	Finding manifestations of Internet attacks based on information from the Centers Computer Emergency Response
$X_{51}^{\text{НОВ}}$	Preventing exposure to the risk of undetected object of Internet attacks based on information from the Centers Computer Emergency Response

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

$$X_1^{\text{ИЗВ}\vee\text{НОВ}} = X_1^{\text{ИЗВ}} \vee X_{11}^{\text{НОВ}}\,\overline{X_{12}^{\text{НОВ}}} \vee \overline{X_{11}^{\text{НОВ}}}\,X_{12}^{\text{НОВ}} \vee \\ \vee X_{11}^{\text{НОВ}}\,X_{12}^{\text{НОВ}}, \tag{11}$$

$$X_3^{\text{ИЗВ}\vee\text{НОВ}} = X_3^{\text{ИЗВ}} \vee X_{31}^{\text{НОВ}}, \tag{12}$$

$$X_5^{\text{ИЗВ}\vee\text{НОВ}} = X_5^{\text{ИЗВ}} \vee X_{51}^{\text{НОВ}}. \tag{13}$$

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

Each group of gradation for $X_j^{\text{ИЗВ}}$ is a group of mutually exclusive events, so we can use Bayes' formula [2,17].

$$P\left(X_{jr}^{\text{НОВ}} \big/ X_j^{\text{ИЗВ}}\right) = \frac{P\left(X_{jr}^{\text{НОВ}}\right)P\left(X_j^{\text{ИЗВ}} \big/ X_{jr}^{\text{НОВ}}\right)}{\sum\limits_{r=1}^{N_j} P\left(X_{jr}^{\text{НОВ}}\right)P\left(X_j^{\text{ИЗВ}} \big/ X_{jr}^{\text{НОВ}}\right)}. \tag{14}$$

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:

$$Y_{\overline{A}}^{\text{ИЗВ}} = 1,$$

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

$$\left\{\begin{array}{c} \overline{X}_1^{\text{ИЗВ}} = 1, \\ X_1^{\text{ИЗВ}}\,\overline{X}_2^{\text{ИЗВ}} = 1, \\ X_1^{\text{ИЗВ}}\,X_2^{\text{ИЗВ}}\,\overline{X}_3^{\text{ИЗВ}}\,\overline{X}_4^{\text{ИЗВ}} = 1, \\ X_1^{\text{ИЗВ}}\,X_2^{\text{ИЗВ}}\left(\overline{X}_3^{\text{ИЗВ}}\,X_4^{\text{ИЗВ}} \vee X_3^{\text{ИЗВ}}\,X_5^{\text{ИЗВ}}\right)\bullet \\ \bullet\,\overline{X}_6^{\text{ИЗВ}}\,\overline{X}_7^{\text{ИЗВ}}\,\overline{X}_9^{\text{ИЗВ}} = 1, \\ X_1^{\text{ИЗВ}}\,X_2^{\text{ИЗВ}}\left(\overline{X}_3^{\text{ИЗВ}}\,X_4^{\text{ИЗВ}} \vee X_3^{\text{ИЗВ}}\,X_5^{\text{ИЗВ}}\right)\bullet \\ \bullet\,X_6^{\text{ИЗВ}}\,\overline{X}_8^{\text{ИЗВ}}\,\overline{X}_{10}^{\text{ИЗВ}} = 1, \\ X_1^{\text{ИЗВ}}\,X_2^{\text{ИЗВ}}\,X_3^{\text{ИЗВ}}\,\overline{X}_5^{\text{ИЗВ}} = 1. \end{array}\right. \tag{15}$$

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

$$P_{\overline{A}-\text{ИЗВ}}^{Y} = 1,$$

or, subject to (9)

$$\begin{array}{l} Q_1^{\text{ИЗВ}} + \left(1 - Q_1^{\text{ИЗВ}}\right)Q_2^{\text{ИЗВ}} + \\ + \left(1 - Q_1^{\text{ИЗВ}}\right)\left(1 - Q_2^{\text{ИЗВ}}\right)Q_3^{\text{ИЗВ}}\,Q_4^{\text{ИЗВ}} + \\ + \left(1 - Q_1^{\text{ИЗВ}}\right)\left(1 - Q_2^{\text{ИЗВ}}\right)\bullet \\ \bullet\left[Q_3^{\text{ИЗВ}}\left(1 - Q_4^{\text{ИЗВ}}\right) + \left(1 - Q_3^{\text{ИЗВ}}\right)\left(1 - Q_5^{\text{ИЗВ}}\right)\right]\bullet \\ \bullet\,Q_6^{\text{ИЗВ}}\,Q_7^{\text{ИЗВ}}\,Q_9^{\text{ИЗВ}} + \left(1 - Q_1^{\text{ИЗВ}}\right)\left(1 - Q_2^{\text{ИЗВ}}\right)\bullet \\ \bullet\left[Q_3^{\text{ИЗВ}}\left(1 - Q_4^{\text{ИЗВ}}\right) + \left(1 - Q_3^{\text{ИЗВ}}\right)\left(1 - Q_5^{\text{ИЗВ}}\right)\right]\bullet \\ \bullet\left(1 - Q_6^{\text{ИЗВ}}\right)Q_8^{\text{ИЗВ}}\,Q_{10}^{\text{ИЗВ}} + \left(1 - Q_1^{\text{ИЗВ}}\right)\left(1 - Q_2^{\text{ИЗВ}}\right)\bullet \\ \bullet\left(1 - Q_3^{\text{ИЗВ}}\right)Q_5^{\text{ИЗВ}} = 1. \end{array} \tag{16}$$

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 $X_1^{ИЗВ} \div X_n^{ИЗВ}$, $n=10$. Then the value of the residual

$$\Delta P_{\bar{A}A}^{Y} = P_3^{Y} - P_{\bar{A}-ИЗВ}^{Y}, \qquad (17)$$

where the value P_3^Y 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

$$\Delta Y_{\bar{A}A} = Y_{\bar{A}} Y_A .$$

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)

$$\begin{cases} \Delta P_{\bar{A}A}^{Y} < 0, \\ \Delta Y_{\bar{A}A} = 1, \end{cases}$$

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 very 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.

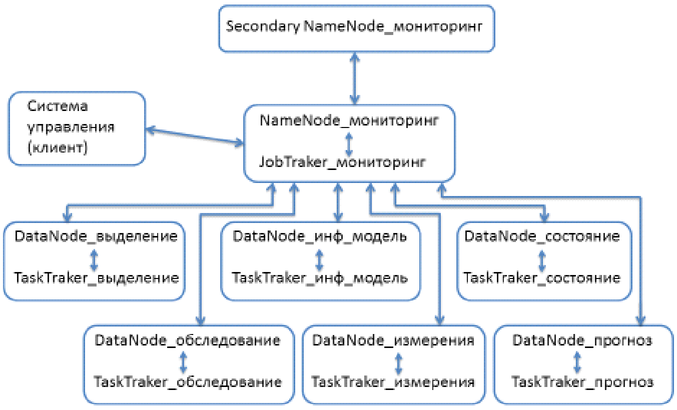

Figure 2. Monitoring Topology Cluster Hadoop.

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 aggregatsionnye 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]:

Π_1 : IF $\tilde{x}_1$ IS A_{11} AND … $\tilde{x}_n$ IS A_{1n}, THEN $\tilde{y}$ IS B_1;

Π_2 : IF $\tilde{x}_1$ IS A_{21} AND … $\tilde{x}_n$ IS A_{2n}, THEN $\tilde{y}$ IS B_2;

…

Π_k : IF $\tilde{x}_1$ IS A_{k1} AND … $\tilde{x}_n$ IS A_{kn}, THEN $\tilde{y}$ IS B_k,

where $\tilde{x}_i$ and $\tilde{y}_i$ - fuzzy input and output variables respectively, A_{ij} and B_i, $j = 1,\ldots,n$, $i = 1,\ldots,k$, 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 demon 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 HIERARHY 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 $X=\{\tilde{x}_1,\ldots,\tilde{x}_m\}$ and the full space of the conclusions $Y=\{\tilde{y}_1,\ldots,\tilde{y}_n\}$. Fuzzy causal relationship $\tilde{x}_i \to \tilde{y}_j$, $i=1,\ldots,m$, $j=1,\ldots,n$ between the elements of these spaces can be represented as a matrix R with the elements r_{ij} , $i=1,\ldots,m$, $j=1,\ldots,n$, and sending and opinions between them can be expressed as: $B=A\bullet R$, where $\bullet$ - the operation of the composition, for example, max-min-composition.

According to [10,13,20-23] in the fuzzy inference fuzzy expert knowledge $A\to B$ reflects the relation $R=A\to B$, 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 $A\to B$ - as the compositional rule of thumb $B=A\bullet R=A\bullet(A\to B)$.

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.

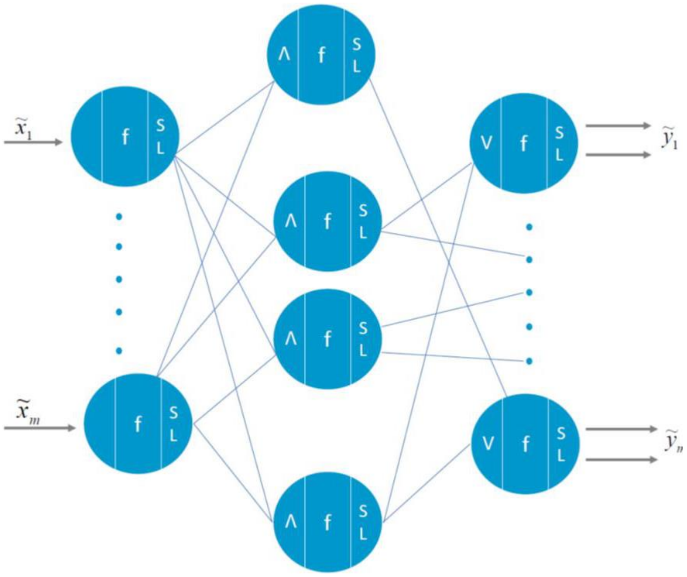

Figure 3. Scheme neuro-fuzzy classifier AS.

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 $\tilde{y}_j$, $j=1,\ldots,n$) 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 TaskTraker_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 TaskTraker_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 vectors. Storing the information obtained in module Д-Клас-С of daemon TaskTraker_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-HH-R) 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-B-C) 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: $P_{CB}\left(t \le T^{\text{ДОП}}\right) \ge P_{CB}^{\text{ДОП}}$, where t - random time for processing of events monitoring; $T^{\text{ДОП}}$ - permitted value of time for processing of event monitoring; P_{CB} - the probability of timely processing of event monitoring; $P_{CB}^{\text{ДОП}}$ - permitted value probability event monitoring;

- for Expediting: $T_{AH} \le T_{AH}^{\text{ДОП}}$ where T_{AH} - the average value of the time, $T_{AH}^{\text{ДОП}}$ - it permissible value;

- On the validity of $N_C \ge \max\limits_{s\in S} N_c^s$, $N_H \ge \max\limits_{s\in S} N_H^s$ and $N_A \ge \max\limits_{s\in S} N_A^s$, 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^s, N_H^s, N_A^s- 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: $P_{PEC}\left(r \le R^{\text{ДОП}}\right) \ge P_{PEC}^{\text{ДОП}}$ where P_{PEC} the probability of resource use in the processing of monitoring events, and $P_{PEC}^{\text{ДОП}}$ - 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 $P_{PEC}^{\text{ДОП}} = 0{,}99$ and $R^{\text{ДОП}} = 0{,}15$ 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 TaskTraker_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 TaskTraker_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 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:

[1 Nazarov, A 2007, ′Estimation of information safety level of modern infocommunication networks on basis of logic-probability approach′, Automation and Remote Control, July 2007, Volume 68

Issue 7, 2007, pp. 1165-1176, USA, doi: 10.1134/S0005117907070053.

[2] Nazarov, A 2010, ′Logical-and-probabilistic model for estimating the level of information security of modern information and communication networks′, Telecommunications and Radio Engineering, Vol. 69, no 16, pp. 1453-1463, USA, doi: 10.1615/TelecomRadEng.v**69**.i**16**.60.

[3] Nazarov, A. & Klimanov, M. 2010, ′Estimating the informational security level of a typical corporate network′, Automation and Remote Control , Volume 71 Issue 8, 2010, pp. 1550-1561.

Article in a conference proceedings:

[4] Nazarov, A. & Klimanov, M 2009, ′Characteristic analysis of logic and probabilistic model of information security′, paper presented in the Collection of proceedings of of International Workshop on Distributed Computer and Communication Computer and Communication Networks (DCCN-2009), Sofia, Bulgaria, October 5-9, 2009, pp. 154-164. Published by Research and Development Company "Information and Networking Technologies", Russia, Moscow.

Article in a journal:

[5] Nazarov, A. & Klimanov, M 2011, ′Assessing the level of security DNS-servers′, Documentary telecommunications, no 21, pp. 54-57.

Project report:

[6] Grudinov, S., Komarov, A.& Nazarov, A 2012, The global system of counteraction to illegal actions in cyberspace, Stage 1, the grant agreement Skolkovo number 87 from 02.11.2012, Russia, LLC Group-IB, unpublished.

Article in a conference proceedings:

[7] Nazarov, A. & Klimanov, M 2013 Использование логико-вероятностного подхода при оценке риска DDOS атаки//, paper presented in the annual Collection of scientific works of International conference Managing the development of large-scale systems" (MLSD'2014), Institute of control Sciences RAS, pp. 444-451.

[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.

Article in a journal:

[9] Nazarov, A. & Tureev, S 2013 ′Assessing the level of information security of the computer network at the network attack′, T-comm – Telecommunications and Transport, no. 10, pp. 78-80.

[10] Nazarov, A. & Komarov, A 2013, ′Intelligent cybersecurity in space on WEB technologies′, T-comm – Telecommunications and Transport, no. 10, pp. 81-84.

Article in a conference proceedings:

[11] Nazarov, A. & Tureev, S 2013 ′Logic and probabilistic model of information security for risk assessment of the object under botnet attacks′, paper presented in the Collection of proceedings of the International Conference "Distributed Computer and Communication Networks: Control, Computation, Communications (DCCN-2013), Moscow, Russia, October 07-10, 2013, pp. 276-283. Published by JSC TECHNOSPHERA, Russia, Moscow.

Article in a journal:

[12] Komarov, A. & Nazarov, A 2013, ′Functional requirements for a system to detect and counter the botnet attacks on corporate networks′, // Technique of communication, series "Television Technique", pp. 140-151.

[13] Sachkov, I. & Nazarov, A. 2014, ′Automation bot counter-attacks′, T-comm – Telecommunications and Transport, vol. 8, no. 8, pp. 5-9.

Article in a conference proceedings:

[14] Nazarov, A 2012 ′Botnet tracking and global threat intelligence - behavior approaches to identifying distributed botnets′, paper presented at the IEEE / Collection of proceedings of the Cybersecurity Summit (WCS), 2012 Third Worldwide, New Dehli, 30-31 Oct. 2012. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6780878&newsearch=true&queryText=Botnet%20tracking%20and%20global%20threat%20intelligence%20-%20behavior%20approaches%20to%20identifying%20distributed%20botnets

Book:

[15] Nazarov, A & Sychev, K 2011, Models and methods for calculating the indicators of quality of functioning of the equipment units and structural parameters of the network the next generation networks, 2th edn, LLC Policom, Russia, Krasnoyarsk.

Article in a journal:

[16] Nazarov, A 2013, ′Objects of the possibility of classification of information security PSTN logic-based probabilistic approach′, Network journal. Theory and Practice» BC/NW, no 2(23):11.1http://network-journal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=23&pa=11&ar=1

[17] Nazarov A 2016, ′Assessment of security from information attacks′, Telecommunications, no 5, in press.

Book:

[18] Chuck, L 2012, Hadoop in action, DMK Press, Moscow.

Article in a conference proceedings:

[19] Volkov, D., Nazarov, A. & Nazarov, M 2014, ′A global threat - the dark web′, paper presented in the annual Collection of scientific works of International conference Managing the development of large-scale systems" (MLSD'2014), Institute of control Sciences RAS, pp. 452-459.

[20] Nazarov, A 2014 ′On approaches to the development of an intelligent system for the analysis of attacks from the Internet′, paper presented in the Collection of proceedings of the XII all-Russian conference on control problems (EVERYTHING-2014), Institute of control Sciences RAS, pp. 9208-9215.

Article in a journal:

[21] Mikhailov, V., Myrova, L.& Tsaregorodtsev, A 2012, ′Intelligent system of analysis and evaluation of onboard digital computer system's resistance to destructive electromagnetic effects′, Electrosvyaz, no. 8, pp. 36-39.

[22] Voskobovich, V., Mikhailov, V., Myrova, L.& Tsaregorodtsev, A 2012, ′Systematic Approach to development of the Methodology of infocommunication system's Analysis and Evaluation of Resistance to Destructive electromagnetic effects′, EMC Technology, no. 1(40), pp. 51-58.

Doctoral thesis:

[23] Mikhailov, V 2014, Development of methods and models for analysis and evaluation of the sustainable functioning of onboard digital computer complexes in the conditions of intentional exposure of ultrashort electromagnetic radiation, doctoral thesis, JSC "Research Institute "Argon", Moscow.

Article in a conference proceedings:

[24] Ovsyannikov, A., Bayda, J.& Lavrent'ev V 2004, ′Information the learning algorithms of neural networks′, Proceedings of BSTU. Ser. Phys.-Mat. Science and information, vol. XII, pp. 110-113.

Book:

[25] Fomin, V. 1984 Kalman and adaptive filtering, Nauka. CH. ed. Fiz.-Mat. lit., Moscow.

Article in a journal:

[26] Nazarov, A., Nazarov, M., Pantiuhin, D, Pokrova, S., & Sychev, A 2015, ′Automation of monitoring processes in web-based

neuro-fuzzy formalism′, T-comm – Telecommunications and Transport, vol. 9, no. 8, pp. 26-33.

[27] Vishnyakov, B. & Kibzun, A 2007, ′Application of the bootstrap method for estimation of the quantile function′, Automatics and telemechanics, no. 11, pp. 46-60.

Article in a conference proceedings:

[28] Gaev L. V. Randomizearray evaluation of the results of simulation experiments/ St. Petersburg, The proceedings of the Conference "IMMOD-2003", 2003.- 5 P.

Book:

[29]. Galambos, Y 1984, Asymptotic theory of extreme order statistics, Nauka, Moscow.