Андрей Е. Краснов[1], Александр С. Мосолов[2], Наталия А. Феоктистова[3]
[1]Российский государственный социальный университет,
ул. Вильгельма Пика, 4, стр. 1, Москва,129226, Россия
[2]Российский химико-технологический университет им. Д.И. Менделеева,
Миусская пл., 9, Москва, Россия
[3]Российская академия образования,
ул. Погодинская, 8, Москва, 119121, Россия
[1]e-mail: krasnovmgutu@yandex.ru, https://orcid.org/0000-0002-4075-4427
[2]e-mail: asmosolov@yandex.ru, https://orcid.org/0000-0002-3266-9505
[3]e-mail: feofamilynat@yandex.ru, https://orcid.org/0000-0002-0030-7390

ОЦЕНИВАНИЕ УСТОЙЧИВОСТИ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР К УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2021.1.09

Аннотация. Цель настоящей статьи заключается в описании методологии комплексного оценивания уязвимости критической информационной инфраструктуры (КИИ) и ее критических элементов на опасных производственных объектах, в том числе на объектах топливно-энергетического комплекса. К элементам КИИ на таких предприятиях в первую очередь следует отнести автоматизированные системы управления технологическими процессами. От нормального функционирования КИИ зависит бесперебойная работа сложных производственно-технологических процессов на критических элементах. Поэтому оценка уязвимостей в системе информационной безопасности, а также исследование стабильности системы безопасности объекта в целом позволит принять превентивные меры в отношении различного вида угроз. В рамках исследования применялись методы системного анализа (декомпозиция и синтез): при оценивании устойчивости информационной системы в целом ее иерархическая структура рассмотрена на примере графа с возможными структурными связями компонентов (активов) системы. Рассмотрены четыре вида отношений активов – полная независимость, слабая зависимость, сильная зависимость, обратная связь. Оценивание устойчивости системы в целом основано на вычислении устойчивости ее парных активов и информационной технологии рекуррентного пересчета при подключении новых компонентов. Метод имитационного моделирования применен для моделирования влияния рисков информационной безопасности на КИИ в условиях неполных и неоднозначных данных об их составляющих, логико-вероятностные методы – для оценки влияния рисков как на составляющие (активы) информационной системы, так и систему в целом с учетом иерархической связи этих активов. Для оценивания влияния базовой угрозы «технического воздействия» (информационной безопасности и системы физической защиты) на риски системы безопасности производственных объектов использовался метод Монте-Карло. Проведение мероприятий по оценке устойчивости информационных систем и стабильности систем безопасности ориентировано на критически важные объекты в медицине, образовании, промышленности, структурах государственного управления.

Ключевые слова: угроза, риск, устойчивость, стабильность, граф, отношения, независимость, слабая зависимость, сильная зависимость, обратная связь.

Для цитирования: КРАСНОВ, Андрей Е.; МОСОЛОВ, Александр С.; ФЕОКТИСТОВА, Наталия А. ОЦЕНИВАНИЕ УСТОЙЧИВОСТИ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР К УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 106–120, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1328>. Дата доступа: 18 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.09.

Andrey E. Krasnov[1], Alexander S. Mosolov[2], Nataliya A. Feoktistova[3]
[1]Russian State Social University,
Wilhelm Pik str., 4 Building 1, Moscow, 129226, Russia,
[2]D. Mendeleev University of Chemical Technology of Russia,
Miusskaya square, 9, Moscow, 125047
[3]Russian Academy of Education,
Pogodinskaya str., 8, Moscow, 119121, Russia
[1]e-mail: krasnovmgutu@yandex.ru, https://orcid.org/0000-0002-4075-4427
[2]e-mail: asmosolov@yandex.ru, https://orcid.org/0000-0002-3266-9505
[3]e-mail: feofamilynat@yandex.ru, https://orcid.org/0000-0002-0030-7390

Assessing the resilience of critical information infrastructures to information security threats

DOI: http://dx.doi.org/10.26583/bit.2021.1.09

Abstract. This paper describes the methodology for comprehensive assessment of the vulnerability of critical information infrastructure (CII) and its critical elements at hazardous production facilities, including those of the fuel and energy production. The elements of CII at such enterprises, first of all, include automated control systems for technological processes. The smooth operation of complex technological and production processes based on critical elements depends on the normal functioning of the CII. Therefore, the assessment of vulnerabilities in the information security system, as well as the study of the security system stability at the facilities as a whole, will allow taking preventive measures against various types of threats. The following methods were used in this study. Methods of system analysis (decomposition and synthesis): when assessing the resilience of an information system as a whole, its hierarchical structure is considered using the example of a graph with possible structural connections of the components (assets) of the system. Four types of asset relationships are considered (their complete independence, weak dependence, strong dependence, feedback). Assessing the resilience of the system as a whole is based on calculating the resilience of its paired assets and information technology of recurrent recalculation when new components are connected. The method of simulation modeling, in particular, for modeling the impact of information security risks on CII in conditions of incomplete and ambiguous data on their components, logical and probabilistic methods - for assessing the impact of risks both on the components (assets) of the information system, and the system as a whole, taking into account the hierarchical relationship of these assets. The Monte Carlo method was used to assess the impact of the basic threat of "technical impact" (information security and physical protection systems) on the security risks of production facilities. The implementation of measures to assess the resilience of information systems and the security systems stability is focused on critical objects in medicine, education, industry, and public administration.
Keywords: threat, risk, resilience, stability, graph, relationships, independence, weak dependence, strong dependence, feedback.
For citation: KRASNOV, Andrey E.; MOSOLOV, Alexander S.; FEOKTISTOVA, Nataliya A. Assessing the resilience of critical information infrastructures to information security threats. IT Security (Russia), [S.l.], v. 28, n. 1, p. 106–120, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1328>. Date accessed: 18 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.09.

Введение

В управлении безопасностью как больших организационно-экономических и организационно-технических систем, так и систем безопасности категорируемых предприятий топливно-энергетического комплекса ключевую роль играет управление рисками, и, в первую очередь, модели оценивания рисков (Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ, последняя редакция). Риски рассматривают как функции от вероятностей и опасностей событий, вызванных множеством угроз, а также уровней уязвимости к этим угрозам [1, 2]. Риск угрозы «технического воздействия» системе

безопасности – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и нанести ущерб организации (ГОСТ Р ИСО/МЭК 27005:2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011. – 94 с. NIST SP 800-30 Revision 1. Guide for Conducting Risk Assessments, 2012). Традиционно риски рассчитывают, как произведение вероятности наступления неблагоприятного события на величину его последствий [2–5]. Следует также отметить, что даже во многих внедренных системах информационной безопасности величины вероятностей наступления неблагоприятных событий рассчитывают, как произведение оценок вероятностей реализации каждой из угроз, считая их независимыми событиями, что совершенно не верно для общего случая.

В последнее время весьма плодотворными оказались подходы, в которых риски рассматривают как нечеткие категории, а их оценивание предлагают проводить на основе функций принадлежности теории нечетких множеств [6, 7], а также смешанного нечетко-вероятностного анализа [8].

Развиваются также гибридные модели информационной безопасности систем, включающие как факторный анализ рисков, так и особенности управленческих и технических решений в области противодействия [9].

Тем не менее, еще в работе [2] отмечалась важность агрегирования оценок рисков различной природы для сложных систем, а также возрастание сложности контроля безопасности в системах с разнородными рисками из-за увеличения взаимозависимости различных системных структурных составляющих и утраты контроля за их безопасностью. Поэтому независимо от того, как рассчитывается риск (на основе вероятностного подхода, или на основе теории нечетких множеств), главным является оценивание его связи с иерархией информационной системы, относящейся к критической информационной инфраструктуре (КИИ) в соответствии с 187-ФЗ от 26.07.2017.

Основная гипотеза настоящего исследования состоит в том, что для оценивания влияния угроз на системообразующие составляющие защищаемой информационной системы, а также систему в целом эффективным будет новое вводимое понятие – устойчивость к угрозам информационной безопасности. Это позволяет воспользоваться результатами, полученными в работах по формализации синдромной диагностики заболеваний [10], привлечь нейросетевые технологии агрегирования для оценивания качества функционирования многопараметрических объектов и процессов [11], а также – эффективности функционирования организации по ключевым показателям ее деятельности [12, 13].

Целью настоящей статьи является создание методологии, позволяющей оценивать влияние рисков информационной безопасности на КИИ в условиях неполных и неоднозначных данных об их составляющих, а главное – влияние рисков как на составляющие (активы) информационной системы, так и систему в целом с учетом иерархической связи этих активов. Конкретными активами могут быть серверы и локальные сети, подключенные к компьютерам лабораторные установки.

1. Постановка задачи исследования

Рассмотрим трехуровневую иерархическую структуру отношений (связей) составляющих (активов, ресурсов) $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, $\boldsymbol{A}_3$, $\boldsymbol{A}_4$, $\boldsymbol{A}_5$ информационной системы (ИС), представленных в виде однонаправленного графа (рис. 1).

Из приведенного на рис. 1 графа видно, что каждый последующий уровень ИС агрегирует подсистемы предыдущего уровня. Естественно, что отношения активов могут быть более сложными, включая и обратные связи. Такие связи рассмотрим позже.

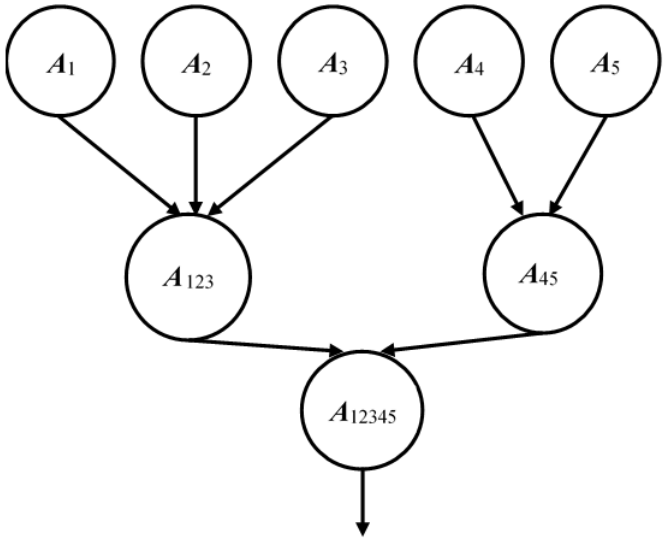

Рис. 1. Граф иерархических уровней связей активов ИС
Fig. 1. Graph of hierarchical levels of links between IS assets

Пусть заданы коэффициенты $K_c(\boldsymbol{A}_n)$, $K_i(\boldsymbol{A}_n)$ и $K_a(\boldsymbol{A}_n)$ («важности») критериев *конфиденциальности* (*confidentiality*), *целостности* (*integrity*) и *доступности* (*availability*) каждого актива $\boldsymbol{A}_n$ (n = 1, 2, …, N) в произвольных балльных шкалах (3-х балльной, 5-ти балльной). Пусть также экспертно заданы:

$\mu_c(T|\boldsymbol{A}_n)$ и $\mu_c(V|\boldsymbol{A}_n)$ – мера (степень) реализации *угрозы безопасности* (*security threat*) и мера (степень) *уязвимости* (*vulnerability*) конфиденциальности актива $\boldsymbol{A}_n$ соответственно;

$\mu_i(T|\boldsymbol{A}_n)$ и $\mu_i(V|\boldsymbol{A}_n)$ – мера (степень) реализации *угрозы безопасности* и мера (степень) *уязвимости* целостности актива $\boldsymbol{A}_n$ соответственно;

$\mu_a(T|\boldsymbol{A}_n)$ и $\mu_a(V|\boldsymbol{A}_n)$ – мера (степень) реализации *угрозы безопасности* и мера (степень) *уязвимости* доступности актива $\boldsymbol{A}_n$ соответственно.

Значения всех мер μ заданы в интервале $(0 \div 1)$.

Определим меры *риско*в (*risk*) конфиденциальности, целостности и доступности актива $\boldsymbol{A}_n$ (n = 1, 2, …, N) в виде нечеткого И:

$$\mu_c(R|\boldsymbol{A}_n) = k_c(\boldsymbol{A}_n)\ \mu_c(T|\boldsymbol{A}_n)\ \mu_c(V|\boldsymbol{A}_n); \quad (1)$$

$$\mu_i(R|\boldsymbol{A}_n) = k_i(\boldsymbol{A}_n)\ \mu_i(T|\boldsymbol{A}_n)\ \mu_i(V|\boldsymbol{A}_n);$$

$$\mu_a(R|A_n) = k_a(\boldsymbol{A}_n)\ \mu_a(T|\boldsymbol{A}_n)\ \mu_a(V|\boldsymbol{A}_n),$$

где

$$k_c(\boldsymbol{A}_n) = K_c(\boldsymbol{A}_n)/[K_c(\boldsymbol{A}_n) + K_i(\boldsymbol{A}_n) + K_a(\boldsymbol{A}_n)]; \quad (2)$$

$$k_i(\boldsymbol{A}_n) = K_i(\boldsymbol{A}_n)/[K_c(\boldsymbol{A}_n) + K_i(\boldsymbol{A}_n) + K_a(\boldsymbol{A}_n)];$$

$$k_a(\boldsymbol{A}_n) = K_a(\boldsymbol{A}_n)/[K_c(\boldsymbol{A}_n) + K_i(\boldsymbol{A}_n) + K_a(\boldsymbol{A}_n)],$$

а меры угроз безопасности и меры уязвимости будем считать независимыми.

Тем самым в (1) все три меры $\mu_c(R|\boldsymbol{A}_n)$, $\mu_i(R|\boldsymbol{A}_n)$ и $\mu_a(R|A_n)$ рисков R (конфиденциальности, целостности и доступности) для актива $\boldsymbol{A}_n$ (n = 1, 2, …, N) определены произведением нормированных коэффициентов (2) важности этих критериев

на меры реализации соответствующих угроз и меры уязвимости конфиденциальности, целостности и доступности.

Задача заключается в том, чтобы оценить влияние рисков на агрегаты ($\boldsymbol{A}_{123}$, A_{45}, $\boldsymbol{A}_{12345}$) всех уровней, формируемых из соответствующих ресурсов с учетом однонаправленных связей графа, представленного на рис. 1.

2. Устойчивости агрегатов информационной системы к угрозам информационной безопасности

2.1. Устойчивости активов

Будем считать, что риски конфиденциальности, целостности и доступности не являются независимыми, и будем рассчитывать значение риска для каждого актива $\boldsymbol{A}_n$ (n = 1, 2, …, N), используя рекурсию [12]:

$$\mu_{ci}(R|\boldsymbol{A}_n) = \mu_c(R|\boldsymbol{A}_n) + \mu_i(R|\boldsymbol{A}_n) - \mu_c(R|\boldsymbol{A}_n)\,\mu_i(R|\boldsymbol{A}_n)]; \quad (3)$$

$$\mu_{cia}(R|\boldsymbol{A}_n) = \mu_{ci}(R|\boldsymbol{A}_n) + \mu_a(R|\boldsymbol{A}_n) - \mu_{ci}(R|\boldsymbol{A}_n)\,\mu_a(R|\boldsymbol{A}_n).$$

Тогда из (3) получим выражение для расчета совокупной меры риска для каждого актива $\boldsymbol{A}_n$:

$$\mu_{cia}(\boldsymbol{A}_n) = \mu_c(\boldsymbol{A}_n) + \mu_i(\boldsymbol{A}_n) + \mu_a(\boldsymbol{A}_n) - \quad (4)$$

$$- \mu_c(\boldsymbol{A}_n)\,\mu_i(\boldsymbol{A}_n) - \mu_c(\boldsymbol{A}_n)\,\mu_a(\boldsymbol{A}_n) - \mu_i(\boldsymbol{A}_n)\,\mu_a(\boldsymbol{A}_n) + \mu_c(\boldsymbol{A}_n)\,\mu_i(\boldsymbol{A}_n)\,\mu_a(A_n).$$

Полученное выражение имеет простой физический смысл: первые три слагаемых оценивают результирующую степень риска конфиденциальности, целостности и доступности без учета их зависимости, вторые три слагаемые учитывают вклад их двойных корреляций, а последнее слагаемое – вклад тройной корреляции.

Предположим, что динамика реализации одиночной угрозы безопасности конфиденциальности, целостности и доступности, связанных с динамикой активности *ACT(t) (activity)* угроз и противодействия *C(t) (counteraction)* им, описывается для каждой составляющей актива $\boldsymbol{A}_n$ простейшей кинетической зависимостью, которая согласуется с качественной моделью, предложенной в [5]:

$$\frac{d\mu}{dt} = -\frac{\mu}{\tau} + AVT(t) - C(t) = -\frac{\mu}{\tau} + \Delta ACT(t),\ \mu(t_0) = 0,\ \Delta ACT_{max} = \frac{1}{\tau}, \quad (5)$$

где τ – время релаксации угрозы в отсутствии ее активности, t_0 – случайное время начала реализации угрозы, ΔACT – скомпенсированная активность угрозы за счет принятия мер противодействия.

Заметим, что среди базовых угроз, законодательно закрепленных регулятором (Министерство энергетики РФ) в структуре процедуры категорирования объектов топливно-энергетического комплекса (ТЭК), угроза «технического воздействия» встречается в более чем 75% случаев («Методические рекомендации по анализу уязвимости производственно-технологического процесса и выявлению критических элементов объекта, оценке социально-экономических последствий совершения на объекте террористического акта и антитеррористической защищенности объекта при проведении категорирования и составлению паспорта безопасности объекта топливно-энергетического комплекса». Минэнерго России. М.: 2012). При этом речь идет о воздействии на автоматизированные системы управления технологическими процессами (АСУ ТП) критических элементов. В качестве потенциального нарушителя рассматривается и руководитель установки, который действует совместно с представителем соответствующей службы.

Поэтому можно предположить, что динамика активности угроз зависит от субъекта, участвующего в технологическом информационном процессе.

Рассмотрим случай, когда характерное время изменения активности много меньше времени τ, а активность угрозы изменяется «скачком» (от 0 до ΔACT) и продолжается некоторое характерное время, большее τ. Тогда (5) имеет аналитическое решение:

$$\mu(t) = \tau \Delta ACT \left[1 - \exp\left(-\frac{t-t_0}{\tau}\right)\right], \quad (6)$$

где $\mu(t)$ – мера риска для составляющей актива.

Из (6) следует, что при $\Delta ACT = \Delta ACT_{max}$:

$$\mu(t) = \left[1 - \exp\left(-\frac{t-t_0}{\tau}\right)\right], \text{ а } \mu_{max} = 1. \quad (7)$$

Исходя из (7), величину $1 - \mu(t) = \exp\left(-\frac{t-t_0}{\tau}\right)$ будем рассматривать, как *степень устойчивости* к угрозам – с ростом степени реализации угрозы (от 0 до 1) степень устойчивости падает (от 1 до 0).

Далее, по аналогии с (7) и используя (4) введем степени $s_{cia}(\boldsymbol{A_n})$ устойчивости (*sustainability, resilience*) к угрозам каждого актива $\boldsymbol{A}_n$ (n = 1, 2, …, N):

$$s_{cia}(\boldsymbol{A}_n) = 1 - \mu_{cia}(\boldsymbol{A}_n). \quad (8)$$

2.2. Устойчивости агрегатов активов

Рассмотрим возможные методы оценивания степеней устойчивости к угрозам агрегатов всех иерархических уровней графа информационной системы, представленного на рис. 2.

Для расчёта введем для всех активов $\boldsymbol{A}_n$ (n = 1, 2, …, N) коэффициенты $K(\boldsymbol{A}_n)$ их «весомости», а нормированные коэффициенты их значимости пересчитаем по аналогии с (2):

$$k(\boldsymbol{A}_n) = K(\boldsymbol{A}_n) / \sum_{n=1}^{N} K(\boldsymbol{A}_n). \quad (9)$$

При расчетах будем учитывать случаи отношений элементов агрегатов из [11].

2.3. Устойчивость агрегата при полностью независимых активах

Определим степень устойчивости агрегата $\boldsymbol{A}_{123}$, как:

$$s_{cia}(\boldsymbol{A}_{123}) = k(\boldsymbol{A}_1)\, s_{cia}(\boldsymbol{A}_1) + k(\boldsymbol{A}_2)\, s_{cia}(\boldsymbol{A}_2) + k(\boldsymbol{A}_3)\, s_{cia}(\boldsymbol{A}_3), \quad (10)$$

$$k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) = 1,$$

$$s_{cia}(\boldsymbol{A}_{45}) = k(\boldsymbol{A}_4)\, s_{cia}(\boldsymbol{A}_4) + k(\boldsymbol{A}_5)\, s_{cia}(\boldsymbol{A}_5),$$

$$k(\boldsymbol{A}_4) + k(\boldsymbol{A}_5) = 1.$$

В этом случае выход из строя одного из элементов агрегата (обнуление его устойчивости) не приведет к потере устойчивости всего агрегата.

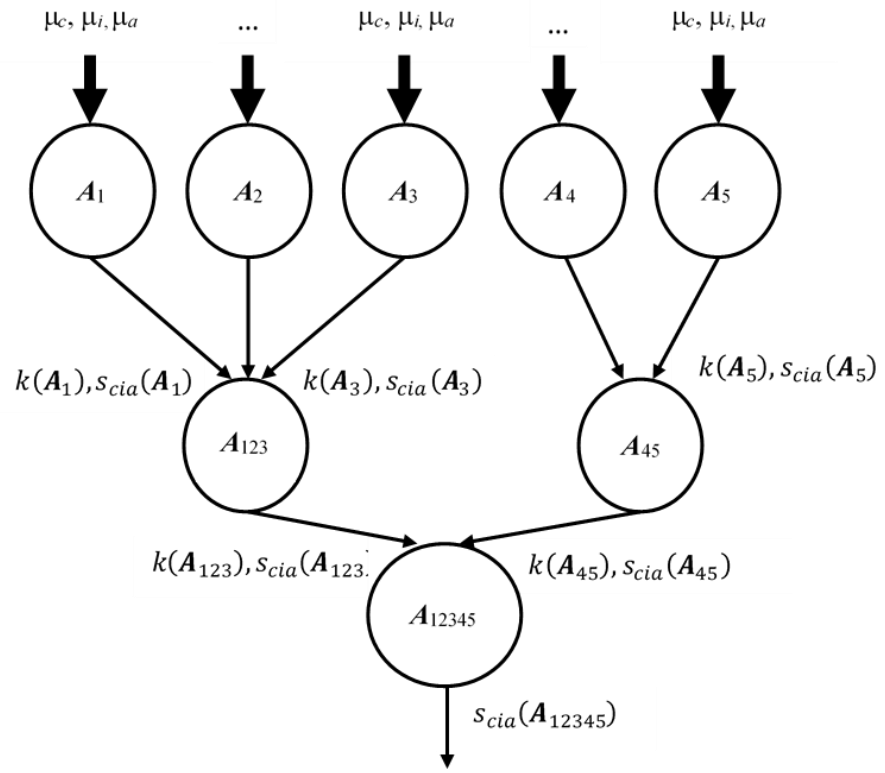

Рис. 2. Граф расчета устойчивости агрегатов ИС
Fig. 2. Graph for calculating the stability of IS aggregates

2.4. Устойчивость агрегата при слабой зависимости активов

Определим степень устойчивости таких агрегатов на основе рекурсии парных взаимодействий (корреляций) их элементов. Так, для агрегата $\boldsymbol{A}_{123}$ (рис. 2):

$$s_{cia}(\boldsymbol{A}_{12}) = \frac{k(\boldsymbol{A}_1)\, s_{cia}(\boldsymbol{A}_1) + k(\boldsymbol{A}_2)\, s_{cia}(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_2)}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)}, \tag{11}$$

$$k(\boldsymbol{A}_{12}) = k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2), k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) = 1.$$

$$s_{cia}(\boldsymbol{A}_{123}) = \frac{k(\boldsymbol{A}_{12})\, s_{cia}(\boldsymbol{A}_{12}) + k(\boldsymbol{A}_3)\, s_{cia}(\boldsymbol{A}_3) - k(\boldsymbol{A}_{12})k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_{12})s_{cia}(\boldsymbol{A}_3)}{k(\boldsymbol{A}_{12}) + k(\boldsymbol{A}_3) - k(\boldsymbol{A}_{12})k(\boldsymbol{A}_3)} =$$

$$= \frac{k(\boldsymbol{A}_1)\, s_{cia}(\boldsymbol{A}_1) + k(\boldsymbol{A}_2)\, s_{cia}(\boldsymbol{A}_2) + k(\boldsymbol{A}_3)\, s_{cia}(\boldsymbol{A}_3)}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_3) - k(\boldsymbol{A}_2)k(\boldsymbol{A}_3) + k(\boldsymbol{A}_1)\, k(\boldsymbol{A}_2)\, k(\boldsymbol{A}_3)} - \tag{12}$$

$$- \frac{k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_2) + k(\boldsymbol{A}_1)k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_3) + k(\boldsymbol{A}_2)k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_3)}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_3) - k(\boldsymbol{A}_2)k(\boldsymbol{A}_3) + k(\boldsymbol{A}_1)\, k(\boldsymbol{A}_2)\, k(\boldsymbol{A}_3)} +$$

$$+ \frac{k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_3) +}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_3) - k(\boldsymbol{A}_2)k(\boldsymbol{A}_3) + k(\boldsymbol{A}_1)\, k(\boldsymbol{A}_2)\, k(\boldsymbol{A}_3)}.$$

Первое слагаемое в (12) соответствует отсутствию зависимости активов, второе – их парным корреляциям, а третье – тройным корреляциям.

Корреляция или слабое взаимодействие дает значительный синергетический эффект повышения устойчивости агрегата. Рассмотрим этот синергетический эффект $\Delta s_{cia}(\boldsymbol{A}_{45})$, например, для агрегата $\boldsymbol{A}_{45}$:

$$\Delta s_{cia}(\boldsymbol{A}_{45}) = \frac{k(\boldsymbol{A}_4)\, s_{cia}(\boldsymbol{A}_4) + k(\boldsymbol{A}_5)\, s_{cia}(\boldsymbol{A}_5) - k(\boldsymbol{A}_4)k(\boldsymbol{A}_5)s_{cia}(\boldsymbol{A}_4)s_{cia}(\boldsymbol{A}_5)}{k(\boldsymbol{A}_4) + k(\boldsymbol{A}_5) - k(\boldsymbol{A}_4)k(\boldsymbol{A}_5)} -$$

$$- \frac{k(\boldsymbol{A}_4)\, s_{cia}(\boldsymbol{A}_4) + k(\boldsymbol{A}_5)\, s_{cia}(\boldsymbol{A}_5)}{k(\boldsymbol{A}_4) + k(\boldsymbol{A}_5)} . \quad (13)$$

Максимальный синергетический эффект – увеличение площади под поверхностью $\Delta s_{cia}(\boldsymbol{A}_{45})$ достигается при $k(\boldsymbol{A}_4) = k(\boldsymbol{A}_5) = 0.5$.

При слабом взаимодействии потеря устойчивости одним из активов также не приводит к потере устойчивости агрегата.

2.5. Устойчивость агрегата при сильной зависимости активов

На содержательном уровне сильное взаимодействие активов обусловлено их полной взаимозависимостью. Определим степень устойчивости агрегатов при сильном взаимодействии их парных элементов, как:

$$s_{cia}(\boldsymbol{A}_{12}) = \frac{k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_2)}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)}. \quad (14)$$

Тогда для агрегата $\boldsymbol{A}_{123}$ получим:

$$s_{cia}(\boldsymbol{A}_{123}) = \quad (15)$$

$$= \frac{k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_2) + k(\boldsymbol{A}_1)k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_3) + k(\boldsymbol{A}_2)k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_3)}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_3) - k(\boldsymbol{A}_2)k(\boldsymbol{A}_3) + 2\,k(\boldsymbol{A}_1)\,k(\boldsymbol{A}_2)\,k(\boldsymbol{A}_3)} -$$

$$\frac{2\,k(\boldsymbol{A}_1)k(\boldsymbol{A}_2)k(\boldsymbol{A}_3)s_{cia}(\boldsymbol{A}_1)s_{cia}(\boldsymbol{A}_2)s_{cia}(\boldsymbol{A}_3)}{k(\boldsymbol{A}_1) + k(\boldsymbol{A}_2) + k(\boldsymbol{A}_3) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_2) - k(\boldsymbol{A}_1)k(\boldsymbol{A}_3) - k(\boldsymbol{A}_2)k(\boldsymbol{A}_3) + 2\,k(\boldsymbol{A}_1)\,k(\boldsymbol{A}_2)\,k(\boldsymbol{A}_3)}.$$

Так, при $k(\boldsymbol{A}_1) = k(\boldsymbol{A}_2) = k(\boldsymbol{A}_3)$ и $s_{cia}(\boldsymbol{A}_1) = s_{cia}(\boldsymbol{A}_2) = s_{cia}(\boldsymbol{A}_3) = 1$ получим $s_{cia}(\boldsymbol{A}_{123}) \cong 1$. При $s_{cia}(\boldsymbol{A}_1) = 0$, $s_{cia}(\boldsymbol{A}_2) = s_{cia}(\boldsymbol{A}_3) = 1$ получим $s_{cia}(\boldsymbol{A}_{123}) \cong 0.02$.

Тем самым, выход из строя одного актива приводит к потере устойчивости агрегата.

2.6. Устойчивость подсистем с обратной связью.

На рис. 3 приведен граф элементарной подсистемы с обратной связью (*feedback*).

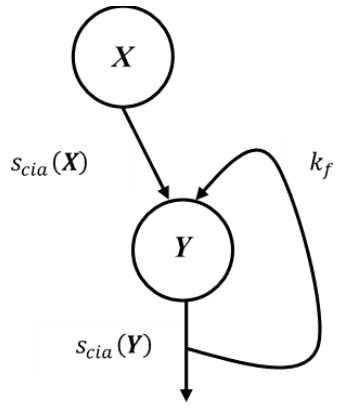

Рис. 3. Граф элементарной подсистемы с обратной связью
Fig. 3. Elementary Subsystem Graph with Feedback

В соответствии с (12) выход подсистемы $s_{cia}(\boldsymbol{Y})$ связан с ее входом $s_{cia}(\boldsymbol{X})$ уравнением:

$$s_{cia}(\boldsymbol{Y}) = \frac{s_{cia}(\boldsymbol{X})}{1 - k_f[1 - s_{cia}(\boldsymbol{X})]}, \quad (16)$$

где k_f – коэффициент обратной связи ($k_f \leq 1$).

Из (16) следует, что обратная связь увеличивает устойчивость подсистемы. На рис. 4 приведен пример отклика $s_{cia}(\boldsymbol{Y})$ данной подсистемы на входное воздействие $s_{cia}(\boldsymbol{X})$ при разных коэффициентах k_f обратной связи.

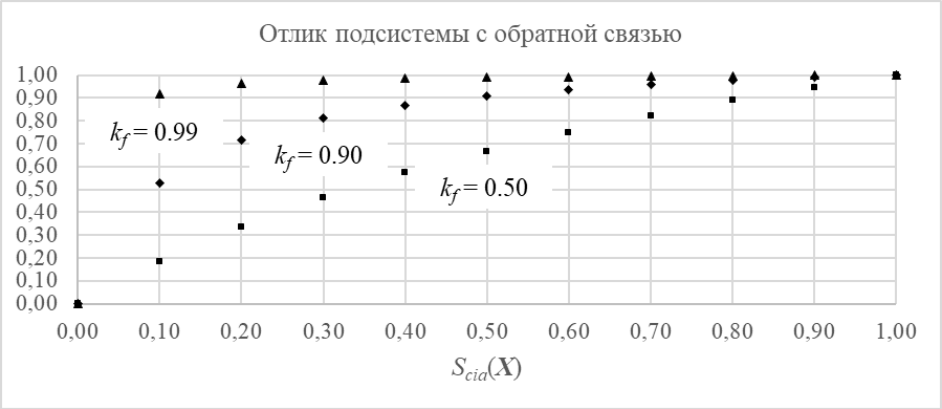

Рис. 4. Увеличение устойчивости подсистемы за счет обратной связи
Fig. 4. Increasing the stability of the subsystem due to feedback

На рис.5 приведен граф подсистемы $\boldsymbol{A}_{45}$, агрегирующей два актива и имеющей обратную связь с коэффициентом k_f. При этом активы могут быть связаны как слабой, так и сильной зависимостями.

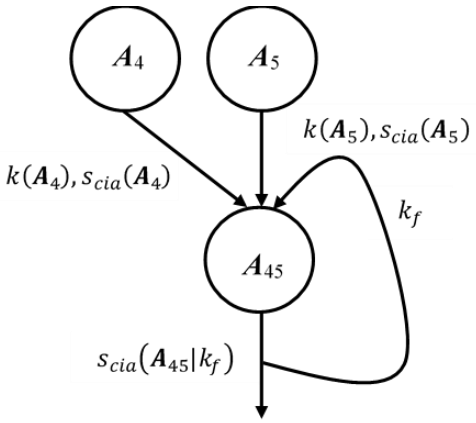

Рис. 5. Граф парной подсистемы с обратной связью
Fig. 5. The graph of the paired subsystem with feedback

В соответствии с (11) и (15) выход $s_{cia}(\boldsymbol{A}_{45})$ подсистемы $s_{cia}(\boldsymbol{A}_{45})$ связан с ее входами $s_{cia}(A_4)$ и $s_{cia}(A_5)$ уравнением:

$$s_{cia}(\boldsymbol{A}_{45}|k_f) = \frac{s_{cia}(\boldsymbol{A}_{45})}{1 - k_f[1 - s_{cia}(\boldsymbol{A}_{45})]}, \quad (17)$$

где устойчивость парного агрегата рассчитывается в соответствии с (12).

Как видно из (17) обратная связь увеличивает устойчивость агрегированной подсистемы наряду с синергизмом (12), обусловленным взаимодействием ее элементов. На рис. 6 приведена поверхность синергетического эффекта, обусловленного обратной связью (для случая слабой зависимости, $k_f = k(A_4) = k(A_5) = 0.5$), описываемая уравнением:

$$\Delta s_{cia}(\boldsymbol{A}_{45}|k_f) = s_{cia}(\boldsymbol{A}_{45}|k_f) - s_{cia}(\boldsymbol{A}_{45}|k_f = 0). \quad (18)$$

Обратная связь увеличивает синергетический эффект дополнительно к парному взаимодействию.

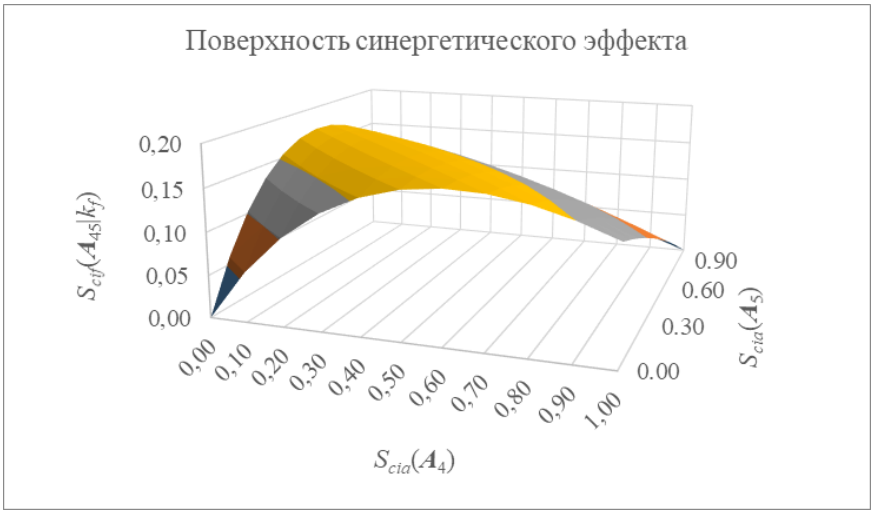

Рис. 6. Поверхность синергетического эффекта устойчивости для парной агрегированной подсистемы с обратной связью.
Fig. 6. Surface of the synergistic effect of resistance for paired aggregated subsystem with feedback.

3. Обсуждение результатов

Из приведенного рассмотрения следует, что наиболее подвержены риску взаимозависимые активы ИС, у которых потеря устойчивости хоты бы одного из них приводит к потере устойчивости всех подсистем или агрегатов, состоящих их этих активов. Поэтому в практическом отношении необходимо хотя бы дублирование таких подсистем.

Так, например, безмасштабные сети очень устойчивы к случайным повреждениям или внешним случайным воздействиям [14]. Однако, у таких сетей существует своеобразная «Ахиллесова пята» – целенаправленное повреждение одного или нескольких узлов с большим числом связей ведет к дезинтеграции сети [15]. Например, хакер может существенно повредить WWW, если выведет из строя один или несколько сайтов с большим числом связей.

При определении приоритетной комбинации отказов в результате развития аварийной ситуации, предполагается проектирование физических барьеров, которые будут «караулить» возможную аварийную ситуация.

Поэтому дублирование в информационных системах является «зеркальным» мероприятием для обеспечения информационной безопасности и безопасности объекта в целом.

Независимые активы ИС, или ресурсы, связанные слабой зависимостью, устойчивы к рискам, приводящим к потерям устойчивости хоты бы одного из активов, или даже

нескольких активов. В то же время, слабая зависимость активов дает синергетический эффект – эффект повышения ее устойчивости.

Зависимости активов, формируемые в ИС с помощью обратных связей, наряду с их слабыми зависимостями также повышают устойчивость систем.

Полученные результаты согласуются с работами в области новой парадигмы, отражающей, в отличие от редукционизма, важность рассмотрения современных сетевых систем [16] и проблем безопасности сложных технических объектов [17] на системном уровне. Основной вывод – необходимо изучать не только отдельные составляющие таких объектов, но, главным образом, их связи.

Рассмотренный материал можно аппроксимировать применительно к критическим элементам объектов ТЭК (Методические рекомендации Минэнерго России от 10.10.2012). В соответствии с методикой определения категории потенциальной опасности, по каждому объекту ТЭК в результате анализа уязвимости производственно-технологических процессов выделяются критические элементы (КЭ).

Очевидно, что к выделенным критическим элементам ТЭК специалисты вправе отнести объекты КИИ по ФЗ 187 от 26.07.2017, в частности, автоматизированные системы управления технологическими процессами, которые обеспечивают функционирование КЭ.

Устойчивость агрегатов информационной системы к угрозам информационной безопасности в каждый конкретный момент времени позволяет сделать вывод о стабильности информационной системы на исследуемом интервале времени.

Аналогично понятию устойчивости системы информационной безопасности будет полезно ввести понятие «стабильности»: взаимосвязь мер уязвимости системы информационной безопасности со «стабильностью» внешнего контура системы безопасности очевидна. Рассмотрим эту аналогию.

Под «стабильностью», в числовом выражении (в интервале от 0 до 1), подразумевается степень безопасности системы, характеризующая способность элементов системы безопасности штатно реагировать на воздействия внешних факторов, направленных на разрушение системы. Рассмотрим понятие стабильности ИС на примере элемента КИИ, описываемого графом на рис. 1, связывающего активы или ресурсы $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, $\boldsymbol{A}_3$, $\boldsymbol{A}_4$, $\boldsymbol{A}_5$.

Для каждого ресурса $\boldsymbol{A}_n$ (n = 1, 2, …, N) можно определить степень его стабильности, оценив критерии КД($\boldsymbol{A}_n$), КЦ($\boldsymbol{A}_n$) и КЗ($\boldsymbol{A}_n$) стабильности, как показатели достаточности, целостности и значимости, и их важности *Imp*(КД($\boldsymbol{A}_n$)), *Imp*(КЦ($\boldsymbol{A}_n$)) и *Imp*(КЗ($\boldsymbol{A}_n$)), соответственно. При этом физический смысл критериев КД, КЦ и КЗ стабильности определяются как:

КД – критерий достаточности (набор функциональных возможностей ресурса достаточен для того, чтобы соответствовать заданному уровню оценки эффективности системы при наличии необходимого перечня таких возможностей). Определяется с использованием программного продукта САПР «Амулет» [18–19];

КЦ – критерий целостности (условия существования и степень надежности ресурса). Определяется экспертами в интервале от 0 до 1, где 0 – не надежно, а 1 – надежно;

КЗ – критерий значимости (важность функционирования данного ресурса для функционирования системы в целом). Чем выше степень зависимости системы от данного элемента, тем более уязвимым является данная область контроля.

Тогда, определив значения каждого критерия и их важности, вычислим степень стабильности (*stability*) ресурса по формуле:

$$St(\boldsymbol{A}_n) = Imp\big(\text{КД}(\boldsymbol{A}_n)\big)\cdot \text{КД}(\boldsymbol{A}_n) + Imp\big(\text{КЦ}(\boldsymbol{A}_n)\big)\cdot \text{КЦ}(\boldsymbol{A}_\text{n}) + \\ + Imp\big(\text{КЗ}(\boldsymbol{A}_n)\big)\cdot\big(1-\text{КЗ}(\boldsymbol{A}_n)\big). \quad (19)$$

Для данного определения также вводятся ограничения типа (2) на сумму важностей критериев КД(R_n), КЦ(R_n) и КЗ(R_n): $Imp(\text{КД}(\boldsymbol{A}_n)) + Imp(\text{КЦ}(\boldsymbol{A}_n)) + Imp(\text{КЗ}(\boldsymbol{A}_n)) = 1$.

Степень стабильности системы должна быть не менее 0,95, т.е. допускается отклонение от полной стабильности не больше, чем на 5%.

Пример. Определим степень стабильности ресурса $\boldsymbol{A}_n$. Для этого экспертным методом назначим важность критериев, как приведено в табл. 1.

Таблица 1. Важность критериев стабильности

Обозначение	**Значение**
$Imp(\text{КД}(\boldsymbol{A}_n))$	0,40
$Imp(\text{КЦ}(\boldsymbol{A}_n))$	0,35
$Imp(\text{КЗ}(\boldsymbol{A}_n))$	0,25

Затем с помощью программного продукта САПР «Амулет» определим значение КД($\boldsymbol{A}_n$), как 0,95. С помощью метода экспертной оценки [20] определим надежность КЦ($\boldsymbol{A}_n$) данного ресурса, как 0,65. Проанализировав систему в целом, оценим значение КЗ($\boldsymbol{A}_n$) ресурса, как 0,85. Полученные данные приведены в табл. 2.

Таблица 2. Результаты оценки важности и значений критериев стабильности

Важность критериев		**Значения критериев**	
Обозначение	**Значение**	**Обозначение**	**Значение**
$Imp(\text{КД}(\boldsymbol{A}_n))$	0,40	КД($\boldsymbol{A}_n$)	0,95
$Imp(\text{КЦ}(\boldsymbol{A}_n))$	0,35	КЦ($\boldsymbol{A}_n$)	0,65
$Imp(\text{КЗ}(\boldsymbol{A}_n))$	0,25	КЗ($\boldsymbol{A}_n$)	0,85

Затем, оценим степень стабильности ресурса:

$$St(\boldsymbol{A}_n) = 0{,}40 \cdot 0{,}95 + 0{,}35 \cdot 0{,}65 + 0{,}25 \cdot (1 - 0{,}85) = 0{,}65.$$

Как видно, полученное значение стабильности ниже допустимого. Поэтому необходимо обеспечить наибольшую безопасность данному ресурсу.

Логично, что, исходя из важности критериев, разумно вносить изменения на те активы системы, которые увеличат значения критериев с наибольшей важностью (в рассматриваемом примере – коэффициент КД) [21, 22].

После анализа системы и увеличения ее безопасности были получены следующие значения коэффициентов (табл. 3).

Таблица 3. Результаты оценки важности и значений коэффициентов с увеличенной безопасностью

Важность коэффициентов		**Значения коэффициентов**	
Обозначение	**Значение**	**Обозначение**	**Значение**
$Imp(\text{КД}(\boldsymbol{A}_n))$	0,40	КД($\boldsymbol{A}_n$)	0,98
$Imp(\text{КЦ}(\boldsymbol{A}_n))$	0,35	КЦ($\boldsymbol{A}_n$)	0,95
$Imp(\text{КЗ}(\boldsymbol{A}_n))$	0,25	КЗ($\boldsymbol{A}_n$)	0,08

При этом степень стабильности ресурса равна 0,95: (0,4*0,98+0,35*0,95+0,25*(1-0,08) = 0,9545).

Заметим, что степень стабильности системы в целом, с учетом всех ресурсов и их связей возможно также рассчитывать по вышеизложенной методике оценивания устойчивости системы.

Заключение

Предложенный подход не является методикой организации связей ресурсов ИС для обеспечения ее информационной безопасности. Однако, при наличии установленных связей между активами системы, он позволяет провести оценивание устойчивости как ее информационных подсистем, так и системы в целом к всевозможным угрозам информационной безопасности. Хотя в работе и рассмотрены простейшие примеры структур связей активов ИС, показано, что четыре вида их отношений (независимость, слабая зависимость, сильная зависимость, обратная связь) позволяют рекуррентно вычислять устойчивость систем при любых структурах связей. Поскольку в основе устойчивости находятся модели рисков и угроз, то полученная модель устойчивости может быть применена к их различным модификациям.

Предложенный подход, связывающий устойчивость элементов системы информационной безопасности с ее устойчивостью для разных видов связей элементов, позволяет также оценивать и стабильность как отдельных элементов системы, так и системы в целом.

Кроме того, оценивание стабильности системы способно повлиять на формирование дополнительно к комплексу компенсационных мероприятий средств и систем физической защиты таблицы результатов предпроектных расчетов устойчивости в границах АСУ ТП соответствующего критического элемента КИИ.

СПИСОК ЛИТЕРАТУРЫ:

1. Wawrzyniak D. (2006) Information Security Risk Assessment Model for Risk Management. In: Fischer-Hübner S., Furnell S., Lambrinoudakis C. (eds) Trust and Privacy in Digital Business. TrustBus 2006. Lecture Notes in Computer Science. Vol. 4083. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/11824633_3.
2. Кононов А.А., Котельников А.П., Черныш К.В. Оценка защищенности критически важных объектов на основе построения моделей событий рисков. Труды ИСА РАН. Т. 62, Вып. 4, 2012. С. 69–75. URL: http://www.isa.ru/proceedings/images/documents/2012-62-4/t-4-12_69-75.pdf. (дата обращения: 01.11.2020).
3. Liu S., Kuhn R., Rossman H. Understanding insecire IT: Practical risk assessment. IT Professional Magazine. V. 11, no. 3, 2009. P. 57–59. DOI: https://doi.org/10.1109/MITP.2009.62.
4. Shukla N., Kumar S. A comparative study on information security risk analysis practices // Special Issue of International Journal of Computer Applications. P. 28–33, 2012.
5. Bandopadhyay S., Sengupta A., Mazumdar C. A quantitative methodology for information security control gap analysis," Proceedings of the 2011 International Conference on Communication, Computing & Security – ICCCS '11, 2011. DOI: https://doi.org/10.1145/1947940.1948051.
6. Shapiro Arnold F., Koissi Marie-Claire. Risk Assessment Applications of Fuzzy Logic. Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries, 2015. – 112 p. URL: https://www.soa.org/globalassets/assets/Files/Research/Projects/2015-risk-assess-apps-fuzzy-logic.pdf (дата обращения: 01.11.2020).
7. Ana Paula Henriques de Gusmão, Lúcio Camara e Silva, Maisa Mendonça Silva, Thiago Poleto, Ana Paula Cabral Seixas Costa. Information security risk analysis model using fuzzy decision theory // International Journal of Information Management. V. 36, Issue 1, 2016. P. 25–34. DOI: https://doi.org/10.1016/j.ijinfomgt.2015.09.003.
8. Abdo H., Flaus J-M. A mixed fuzzy probabilistic approach for risk assessment of dynamic systems //IFAC-PapersOnLine. V. 48, Issue 3, 2015. P. 960–965. DOI: https://doi.org/10.1016/j.ifacol.2015.06.207.
9. Sami Haji, Qing Tan, Rebeca Soler Costa. A Hybrid Model for Information Security Risk Assessment. International Journal of Advanced Trends in Computer Science and Engineering. Vol. 8, no. 1, 2019. P. 100–106. DOI: https://doi.org/10.30534/ijatcse/2019/1981.12019.
10. Krasnova T.N., Kryukova I.P., Krasnov A.E. et al. Principles of formalization of the syndrome diagnosis used in an automated system of management of patients. Biomed Eng. V. 32, 1998. P. 140–147. DOI: https://doi.org/10.1007/BF02369144.
11. Краснов А.Е., Сагинов Ю.Л., Феоктистова Н.А. Количественное оценивание качества многопараметрических объектов и процессов на основе нейросетевой технологии. В сб. научных трудов Всероссийской конференции «Информационные технологии, менеджмент качества, информационная

безопасность» (IT&MQ&IS-2015) - (20–25 мая 2015 г.). Учебно-научная база КБГУ в Приэльбрусье (п. Эльбрус). Приложение к журналу «Качество. Инновации. Образование». Т. 2, № 5, 2015. С. 97–108. URL: http://quality-journal.ru/wp-content/uploads/2016/07/ITMQIS-2015.pdf. (дата обращения: 01.11.2020).

12. Краснов А.Е., Надеждин Е.Н., Никольский Д.Н., Калачев А.А. Нейросетевой подход к проблеме оценивания эффективности функционирования организации на основе агрегирования показателей ее деятельности. Информатизация образования и науки, № 1 (33), 2017. С. 141–154. URL: https://informika.ru/pechatnye-izdaniya/zhurnal-informatizaciya-obrazovaniya-i-nauki/arhiv-vypuskov/2017/vypusk-n33/. (дата обращения: 01.11.2020).
13. Krasnov A., Pivneva S. (2021) Hierarchical Quasi-Neural Network Data Aggregation to Build a University Research and Innovation Management System. In: Murgul V., Pukhkal V. (eds) International Scientific Conference Energy Management of Municipal Facilities and Sustainable Energy Technologies EMMFT 2019. EMMFT 2019. Advances in Intelligent Systems and Computing. V. 1259. Springer, Cham. P. 12–15. DOI: https://doi.org/10.1007/978-3-030-57453-6_2.
14. Albert R., Barabasi A.-L. Statistical mechanics of complex networks. Rev. Mod. Phys. V. 74, Issue 1, 2002. P. 47–97. DOI: https://doi.org/10.1103/RevModPhys.74.47.
15. Barabási A.-L. The network takeover. Nature Phys. V. 8, 2012. P. 4–16. DOI: https://doi.org/10.1038/nphys2188.
16. Евин И.А. Введение с теорию сложных сетей. Компьютерные исследования и моделирование. Т. 2, № 2, 2010. С. 121–141. DOI: https://10.20537/2076-7633-2010-2-2-121-141.
17. Мосолов А.С. Универсальная технология проектирования систем инженерно-физической защиты «АМУЛЕТ» с заданным уровнем эффективности. М.: НИЯУ «МИФИ». 2013. – 200 с.
18. Мосолов А.С., Беляева Е.А., Бадиков А.В. Изучение универсального метода проектирования систем инженерно-технической защиты объектов. М.: НИЯУ «МИФИ». 2010. – 84 с.
19. Беляева Е.А., Кузоятов О.П., Мосолов А.С., Новиков Ю.В. Способ проектирования системы комплексной безопасности объекта. Патент RU 2219576 C2. Заявка RU 2002105932, 05.03.2002. Опубликовано 20.12.2003. Бюл. № 35. МПК G06F 17/00.
20. Саати Т. Принятие решений. Метод анализа иерархий. М.: Радио и связь, 1993. – 278 с.
21. Акинин Н.И., Губина Т.А., Мосолов А.С. Алгоритм метода определения приоритетного сценария развития аварийной ситуации на объекте защиты. Кокс и химия: журнал. М.: Металлургиздат, 2019. С. 41–49.
22. Губина Т.А., Мосолов А.С., Мосолов А.А. Система оценки безопасности опасного производственного объекта. Патент RU 2709155 C1. Заявка RU 2019107954, 02.04.2019. Опубликовано 16.12.2019. Бюл. № 35. МПК G06Q 10/06.

REFERENCES:

[1] Wawrzyniak D. (2006) Information Security Risk Assessment Model for Risk Management. In: Fischer-Hübner S., Furnell S., Lambrinoudakis C. (eds) Trust and Privacy in Digital Business. TrustBus 2006. Lecture Notes in Computer Science. Vol. 4083. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/11824633_3.
[2] Kononov A. A., Kotelnikov A. P., Chernysh K. V. Security assessment of critical objects based on the construction of risk event models. Trudy ISA RAN. V. 62, Issue 4, 2012. P. 69–75. URL: http://www.isa.ru/proceedings/images/documents/2012-62-4/t-4-12_69-75.pdf (accessed: 01.11.2020) (in Russian).
[3] Liu S., Kuhn R., Rossman H. Understanding insecire IT: Practical risk assessment. IT Professional Magazine. Vol. 11, no. 3, 2009. P. 57–59. DOI: https://doi.org/10.1109/MITP.2009.62.
[4] Shukla N., Kumar S. A comparative study on information security risk analysis practices. Special Issue of International Journal of Computer Applications. P. 28–33, 2012.
[5] Bandopadhyay S., Sengupta A., Mazumdar C. A quantitative methodology for information security control gap analysis," Proceedings of the 2011 International Conference on Communication, Computing & Security – ICCCS '11, 2011. DOI: https://doi.org/10.1145/1947940.1948051.
[6] Shapiro Arnold F., Koissi Marie-Claire. Risk Assessment Applications of Fuzzy Logic. Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries, 2015. – 112 p. URL: https://www.soa.org/globalassets/assets/Files/Research/Projects/2015-risk-assess-apps-fuzzy-logic.pdf (accessed: 01.11.2020).
[7] Ana Paula Henriques de Gusmão, Lúcio Camara e Silva, Maisa Mendonça Silva, Thiago Poleto, Ana Paula Cabral Seixas Costa. Information security risk analysis model using fuzzy decision theory // International Journal of Information Management. V. 36, Issue 1, 2016. P. 25–34. DOI: https://doi.org/10.1016/j.ijinfomgt.2015.09.003.

[8] Abdo H., Flaus J-M. A mixed fuzzy probabilistic approach for risk assessment of dynamic systems //IFAC-PapersOnLine. V. 48, Issue 3, 2015. P. 960–965. DOI: https://doi.org/10.1016/j.ifacol.2015.06.207.
[9] Sami Haji, Qing Tan, Rebeca Soler Costa. A Hybrid Model for Information Security Risk Assessment. International Journal of Advanced Trends in Computer Science and Engineering. V. 8, no. 1, 2019. P. 100–106. DOI: https://doi.org/10.30534/ijatcse/2019/1981.12019.
[10] Krasnova T.N., Kryukova I.P., Krasnov A.E. et al. Principles of formalization of the syndrome diagnosis used in an automated system of management of patients. Biomed Eng. V. 32, 1998. P. 140–147. DOI: https://doi.org/10.1007/BF02369144.
[11] Krasnov A.E., Saginov Yu.L., Feoktistova N.A. Quantitative assessment of the quality of multiparameter objects and processes based on neural network technology. Sbornik nauchnyh trudov Vserossijskoj konferencii «Informacionnye tekhnologii, menedzhment kachestva, informacionnaya bezopasnost'» (IT&MQ&IS-2015) - (20–25 maya 2015 g.). Uchebno-nauchnaya baza KBGU v Priel'brus'e (p. El'brus). Prilozhenie k zhurnalu «Kachestvo. Innovacii. Obrazovanie». T. 2, no. 5, 2015. S. 97–108. URL: http://quality-journal.ru/wp-content/uploads/2016/07/ITMQIS-2015.pdf (accessed: 01.11.2020) (in Russian).
[12] Krasnov A.E., Nadezhdin E.N., Nikolsky D.N., Kalachev A.A. A neural network approach to the problem of assessing the efficiency of an organization's functioning based on the aggregation of its performance indicators. Informatizaciya obrazovaniya i nauki, № 1 (33), 2017. S. 141–154. URL: https://informika.ru/pechatnye-izdaniya/zhurnal-informatizaciya-obrazovaniya-i-nauki/arhiv-vypuskov/2017/vypusk-n33/ (accessed: 01.11.2020) (in Russian).
[13] Krasnov A., Pivneva S. (2021) Hierarchical Quasi-Neural Network Data Aggregation to Build a University Research and Innovation Management System. In: Murgul V., Pukhkal V. (eds) International Scientific Conference Energy Management of Municipal Facilities and Sustainable Energy Technologies EMMFT 2019. EMMFT 2019. Advances in Intelligent Systems and Computing. V. 1259. Springer, Cham. P. 12–15. DOI: https://doi.org/10.1007/978-3-030-57453-6_2.
[14] Albert R., Barabasi A.-L. Statistical mechanics of complex networks. Rev. Mod. Phys. V. 74, Issue 1, 2002. P. 47–97. DOI: https://doi.org/10.1103/RevModPhys.74.47.
[15] Barabási A.-L. The network takeover. Nature Phys. V. 8, 2012. P. 14–16. DOI: https://doi.org/10.1038/nphys2188.
[16] Evin I.A. Introduction to complex network theory (in Russian). Kompyuternye issledovaniya I modelirovanie. V. 2, no. 2, 2010. P. 121–141. DOI: https://10.20537/2076-7633-2010-2-2-121-141 (in Russian).
[17] Mosolov A.S. Universal technology for designing systems of engineering and physical protection "AMULET" with a given level of efficiency. M.: NIYAU «MIFI», 2013. – 200 p. (in Russian).
[18] Mosolov A.S., Belyaeva E.A., Badikov A.V. Study of a universal method for designing systems for engineering and technical protection of objects. M.: NIYAU «MIFI», 2010. – 84 p. (in Russian).
[19] Belyaeva E.A., Kuzoyatov O.P., Mosolov A.S., Novikov Yu.V. A method for designing an integrated security system for an object. Patent RU 2219576 C2. Application RU 2002105932, 05.03.2002. Published 20.12.2003, bull. No. 35. IPC G06F 17/00 (in Russian).
[20] Saati T. Decision-making. Hierarchy analysis method. M.: Radio i svyaz', 1993. – 278 s. (in Russian).
[21] Akinin N.I., Gubina T.A., Mosolov A.S. Algorithm of the method for determining the priority scenario for the development of an emergency at the protected object (in Russian). Koks i himiya: zhurnal. M.: Metallurgizdat, 2019. S. 41–49 (in Russian).
[22] Gubina T.A., Mosolov A.S., Mosolov A.A. Safety assessment system for a hazardous production facility. Patent RU 2709155 C1. Application RU 2019107954, 02.04.2019. Published 16.12.2019, bull. No. 35. IPC G06Q 10/06 (in Russian).

Поступила в редакцию – 16 ноября 2020 г. Окончательный вариант – 12 февраля 2021 г.
Received – November 16, 2020. The final version – February 12, 2021.