УДК 004.056:004.058 + 620.169.2
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-69-76

Об оценивании устойчивости функционирования объектов критической информационной инфраструктуры, подверженных воздействию угроз нарушения их информационной безопасности

On assessing the operational stability of critical information infrastructure facilities affected by information security threats

Воеводин В.А.[1]*, Третьяков С.М.[2]
Voevodin V.A.[1]*, Tretyakov S.M.[2]

[1] Национальный исследовательский университет «Московский институт электронной техники», Зеленоград, Российская Федерация
[2] Военная академия связи, Санкт-Петербург, Российская Федерация
[1] National Research University of Electronic Technology, Zelenograd, Russian Federation
[2] Military Academy of the Signal Corps, Saint Petersburg, Russian Federation
** vva541@mai.ru*

Воеводин В.А.

Третьяков С.М.

Резюме. Цель. *Формализовать научную задачу количественного оценивания устойчивости функционирования объектов критической информационной инфраструктуры, подверженных воздействию угроз нарушения их информационной безопасности.* **Методы**. *Познавательные методы: системного анализа, индуктивно-дедуктивный, анализ научной задачи, формализации научных знаний, построения гипотез. Операционные методы: абстрагирование, конкретизация, сравнение, обобщение, аналогия, моделирования, методы экспертного оценивания.* **Результаты.** *Обоснована актуальность, сформулирована вербальная и формальная постановки научной задачи количественного оценивания устойчивости функционирования объектов критической информационной инфраструктуры, предложены показатели для оценивания исходных данных и получаемого результата.* **Заключение**. *Осуществлен системный анализ проблемной ситуации, что позволило выявить объективные основания актуальности решения научной задачи, осуществить ее формальную постановку, обосновать выбор управляемых и неуправляемых факторов для оценивания устойчивости, сформулировать ограничения, предложить способ учета динамики критической информационной инфраструктуры в результате воздействия угроз нарушения ее информационной безопасности.*
Abstract. Aim. *To formalise the scientific problem of quantifying the operational stability of critical information infrastructure facilities exposed to information security threats.* **Methods**. *Cognitive methods: systems analysis, induction and deduction, analysis of a scientific problem, formalisation of scientific knowledge, construction of hypotheses. Operational methods: abstraction, specification, comparison, generalisation, analogy, simulation, expert evaluation.* **Results.** *The paper substantiates the relevance, defines – both verbally and formally – the scientific problem of quantifying the operational stability of critical information infrastructure facilities, suggests indicators for assessing the input data and the result.* **Conclusions**. *The authors systematically analysed the problem, which allowed substantiating the relevance of a potential solution, formalising it, substantiating the choice of the controllable and uncontrollable factors for assessing stability, defining the restrictions, suggesting the method for taking into account the dynamics of critical information infrastructure exposed to information security threats.*

Ключевые слова: *критическая информационная инфраструктура, угрозы нарушения информационной безопасности, устойчивость функционирования, система восстановления функциональности.*
Keywords: *critical information infrastructure, information security threats, operational stability, functionality restoration system.*

Для цитирования: *Воеводин В.А., Третьяков С.М. Об оценивании устойчивости функционирования объектов критической информационной инфраструктуры, подверженных воздействию угроз нарушения их информационной безопасности // Надежность. 2025. №4. С. 69-76. https://doi.org/10.21683/1729-2646-2025-25-4-69-76*

For citation: *Voevodin V.A., Tretyakov S.M. On assessing the operational stability of critical information infrastructure facilities affected by information security threats. Dependability 2025;4: 69-76. https://doi.org/10.21683/1729-2646-2025-25-4-69-76*

Поступила: *13.09.2024* / **После доработки:** *16.03.2025* / **К печати:** *28.09.2025*
Received on: *13.09.2024* / **Revised on:** *16.03.2025* / **For printing:** *28.09.2025*

Введение

Информационная инфраструктура создается для удовлетворения потребностей субъектов информационных отношений (обладателей информации и операторов информационных систем) и служит активным средством в их целенаправленной деятельности. Противник с целью нарушить функциональность объектов критической информационной инфраструктуры (КИИ) наносит поражающие воздействия по их элементам.

В результате поражения отдельных элементов может быть нарушена их функциональность или они могут быть уничтожены, что может привести к нарушению функциональности КИИ в целом.

Для обеспечения устойчивости функционирования КИИ выделяется соответствующий ресурс, который необходимо эффективно распределить по задачам и времени. Под ресурсом понимаются выделяемые для обеспечения устойчивости объектов КИИ силы, средства и материальный ресурс. Если силы и средства могут применяться неоднократно, такой ресурс позиционируется как возобновляемый. Материальный ресурс расходуется безвозвратно и позиционируется как невозобновляемый ресурс. Для принятия решения по обеспечению устойчивости КИИ, органам управления требуется инструмент для количественного оценивания устойчивости функционирования КИИ, чтобы сравнить альтернативные варианты управленческих решений и обосновать выбор рационального.

Для успешного решения задач по обеспечению безопасности КИИ современные методические потребности органов управления в оценивании устойчивости КИИ и возможности существующего научно-методического аппарата должны находится в *гармонии*.

В результате исследований сформулированы вербальная и формальная постановки научной задачи количественного оценивания устойчивости КИИ, предложены подходы к формированию исходных данных и интерпретации получаемого результата. Новизна результатов заключается в том, что был осуществлен системный анализ проблемной ситуации, результаты которого позволили: а) выявить актуальность задачи обеспечения устойчивости КИИ, находящейся в условиях воздействия угроз; б) выявить ограниченность существующих методов поддержки принимаемых решений; в) осуществить формальную постановку задачи.

При постановке задачи обоснован выбор управляемых и неуправляемых параметров, сформулированы ограничения, предложен способ учета динамики КИИ в результате изменения обстановки.

Анализ существующих нормативных правовых актов, методических документов, приказов исполнительных органов власти (Регуляторов) и национальных стандартов позволяет утверждать, что они в совокупности и по отдельности не содержат общепринятых методических рекомендаций по количественному оцениванию устойчивости КИИ применительно к условиям воздействия угроз.

Существующий инструментарий оценивания устойчивости КИИ ориентирован на *штатные условия, зафиксированные в эксплуатационной документации,* и базируется на положениях теории надежности. Методы теории надежности, основанные на анализе экспериментальных данных, постоянно развиваются. Результаты фундаментальных исследований теории надежности технических систем отражены достаточно полно и глубоко в публикациях Б.В. Гнеденко [1], И.А. Ушакова [2], А.М. Половко и С.В. Гурова [3], В.А. Каштанова [4], И.Б. Шубинского [5, 6] и других признанных ученых.

Однако для условий воздействия угроз применение методов теории надежности для оценивания устойчивости КИИ не всегда оправдано. Такое ограничение связано с редкостью событий воздействия угроз, ограниченностью интервала времени их наблюдения, изменчивостью обстановки, поведенческой неопределенностью. Ограниченность методов теории надежности при исследовании живучести, безопасности, защищенности сложных систем и надежности программного обеспечения отмечалась И.А. Ушаковым в докладе «Надежность: прошлое, настоящее, будущее» [7].

Результаты исследования особенностей количественного оценивания эффективности информационных систем и технологий применительно к *штатным* условиям функционирования как сервисных систем приводятся Р.М. Юсуповым и А.А. Мусаевым [8]. Авторы предлагают в основу оценивания положить вероятностный подход, что для условий воздействия угроз не всегда приемлемо.

Отсутствие методического аппарата для количественного оценивания устойчивости КИИ при воздействии угроз сдерживает развитие отношений, которые возникают при обеспечении безопасности КИИ.

1. Анализ возможностей существующего методического аппарата

Особенностями существующего подхода к управлению информационной безопасностью (ИБ) является то, что для его осуществления характерны и являются преобладающими императивные нормы права. Деятельность, которая регулируется преимущественно

силой закона и подзаконных актов, позиционируется как административная и относится к репродуктивной. К существующей инерционности директивного подхода необходимо объективно добавить и то, что требования Регулятора известны противнику (источнику угроз), который может использовать эти знания и целенаправленно планировать эффективное воздействие угрозами в обход требуемых мер защиты.

Вместе с тем, опять же силой закона, обладателям информации и операторам информационных систем предписано: а) обеспечить защиту информации; б) не допускать воздействий на технические средства обработки информации, в результате которого нарушается их функционирование; в) осуществлять постоянный контроль за обеспечением уровня защищенности информации. При исполнении этих предписаний действуют диспозитивные нормы права, в соответствии с которыми обладателям информации и операторам информационных систем предоставляется право самостоятельно регулировать эти отношения. Для самостоятельного регулирования таких отношений требуется инструмент, позволяющий решить задачу количественного оценивания устойчивости функционирования соответствующих объектов информатизации.

В настоящее время известен ряд подходов к решению задачи оценивания и повышения устойчивости функционирования объектов информатизации, функционирующих в условиях воздействия дестабилизирующих факторов различной физической природы. Некоторые из таких подходов, представляющих интерес для оценивания устойчивости КИИ, приведены в трудах Д.П. Зегжды [9], И.В. Котенко, И.Б. Саенко, М.А. Кониняка, О.С. Лауты [10], А.А. Шелупанова и Р.В. Мещерякова [11, 12], С.А. Коноваленко [13], С.И. Макаренко [14, 15], Ю.И. Стародубцева, П.В. Закалкина [16], Ю.К. Язова [17], Г.Е. Черкесова, А.О. Недосекина и В.В. Виноградова [18, 19], И.А. Рябинина [20].

Основные усилия были направлены на развитие подходов к оцениванию устойчивости структурно-сложных технических систем на основе парадигмы структурной и функциональной устойчивости, когда критерий отказа системы и/или элемента является бинарным.

Вопросы обеспечения устойчивости функционирования сложных систем рассматривались и в смежных областях. Так, критерии, методы анализа и синтеза технических и информационных систем, методы обеспечения и повышения надежности, эксплуатации исследовались А.М. Половко совместно с С.В. Гуровым и приведены в [3]. В качестве предмета исследования были рассмотрены невосстанавливаемые и восстанавливаемые, нерезервированные и резервированные системы длительного и кратковременного времени существования.

Обобщая результаты ретроспективного анализа, можно утверждать, что для условий воздействия целенаправленных угроз существуют лишь отельные публикации, которые не объединены в единый методический аппарат, что в совокупности переводит поставленную задачу в статус научной проблемы. Также следует отметить, что отсутствует общепринятое официальное определение понятия «устойчивость функционирования КИИ» и место в понятийном поле термина «живучесть КИИ», поэтому приводится авторское видение этой терминологии, которое опубликовано в [21].

2. Вербальная постановка задачи

При оценивании устойчивости КИИ можно выделить отдельные группы факторов: а) устойчивость элементов (узлов и ребер), входящих в состав схемы устойчивости объекта КИИ; б) условия функционирования КИИ (сценарии воздействия угроз); в) способы применения сил и средств восстановления функциональности элементов КИИ.

Для формальной постановки задачи факторы, определяющие условия функционирования КИИ, подразделяются на две группы: а) факторы, которые могут *контролироваться* лицом, принимающим решение (ЛПР); б) факторы, которые не могут быть контролируемы ЛПР по различным причинам.

Каждый элемент оцениваемого объекта на периоде воздействия угроз может принимать три различных состояния: а) функционален – способен выполнять требуемые функции; б) поврежден – восстановление функциональности возможно через определенный промежуток времени восстановления, не превышающий момента окончания воздействия угроз; в) поражен – восстановление функциональности не целесообразно или невозможно из-за ограниченности ресурса, в том числе и временного. Последовательный переход из одного состояния в другое позиционируется как процесс функционирования элемента и объекта КИИ в целом.

3. Формальная постановка задачи

1) Управляемые факторы

Пусть задана структура информационной-телекоммуникационной сети[1] (объект критической инфраструктуры) в момент времени t_0, соответствующий началу периода воздействия угроз $(0, T]$

$$S(t_0) = \{A(t_0), L(t_0)\},$$

где $A(t_0) = \{a_i(t_0)\}$ – семейство *узлов связи* (узлов), $a_i(t_0)$ – индикатор состояния i-го узла (если узел $a_i(t_0)$ функционален, то $a_i(t_0) = 1$ или 0 в противном случае), $i = 1, 2, \ldots, N_A$; N_A – мощность семейства $A(t_0)$; $L(t_0) = \{l_{i,j}(t_0)\}$ – семейство *линий связи* (ребер), $l_{i,j}(t_0)$ – индикатор состояния i,j-й линии связи (если линия связи $l_{i,j}(t_0)$ функциональна, то $l_{i,j}(t_0) = 1$ или 0 в противном случае), $i,j = 1, 2, \ldots, N_L$; $N_L = (N_A)^2$ – мощность семейства $L(t_0)$.

[1] Концепция структурной схемы устойчивости в данном случае применяется по аналогии с ГОСТ Р МЭК 61078-2021 Надежность в технике. Структурная схема надежности.

Определено исходное семейство *элементов* объекта КИИ в момент времени t_0

$$E(t_0)=\{e_k(t_0)\}=A(t_0)\cup L(t_0)=\{\{a_i(t_0)\}\cup\{l_{i,j}(t_0)\}\},$$

где $k=1, 2, \ldots, N_E$; N_E – мощность исходного семейства элементов $E(t_0)$, $e_k(t_0)\in E(t_0)$.

Процесс функционирования подверженного воздействию угроз объекта КИИ характеризуется сменой состояний его элементов $e_k(t)\in E(t_0)$; если k-й элемент на момент времени t сохранил функциональность, то $e_k(t)=1$, если k-й элемент был поврежден, то $e_k(t)=\tau_k(t)$ где $\tau_k(t)$ – время до окончания восстановления функциональности k-го элемента на момент времени t; если k-й элемент был поражен в результате воздействия угрозы, то его идентификатору безвозвратно присваивается значение $e_k(t)=0$.

Пусть известны количественные оценки факторов, которые оказывают непосредственное влияние на устойчивость объекта КИИ:

- семейство актуальных угроз

$$U=\{u_m\},$$

где u_m – идентификатор актуальной угрозы с индексом m, $m=1, 2, \ldots, N_U$, N_U – мощность семейства актуальных угроз;

- семейство стационарных коэффициентов оперативной готовности элементов объекта КИИ

$$K_{\text{Or}}(t_0, t_0+t)\underset{\substack{t\in(0,T],\\ k=1,2,\ldots,N_E}}{=}\{\hat{k}_{\text{Or}k}(t_0, t_0+t)\},$$

где $\hat{k}_{\text{Or}k}$ – стационарный коэффициент оперативной готовности k-го элемента на интервале $t\in(0, T]$. Физически $\hat{k}_{\text{Or}k}$ отражает вероятность того, что элемент a_k проработает безотказно в течение заданного периода времени T, начиная с момента времени t_0.

Защищенность элементов объекта КИИ от воздействия угроз U

$$P(u)\underset{\substack{k=1,2,\ldots N_E,\\ m=1,2,\ldots N_U}}{=}\{p_{k,m^*}, \underset{\sim}{p}_{k,m^*}, \widehat{p}_{k,m^*}\},$$

где $p_{k,m}$ – оценка вероятности сохранения функциональности элементом с индексом $e_k(t_0)\in E(t_0)$ при воздействии угрозы с индексом $u_m\in U$. Если угроза u_m для элемента $e_k(t_0)$ является не актуальной, то $p_{k,m}=1$. Из всех актуальных угроз U для оценивания защищенности элемента с индексом e_k выбирается угроза с индексом u_{m^*}, при которой

$$p_{k,m^*}=\min_{\substack{k=1,2,\ldots N_E,\\ m=1,2,\ldots N_U}} p_{k,m},$$

где $\underset{\sim}{p}_{k,m^*}$ – вероятность *повреждения* k-го элемента при воздействии угрозы u_{m^*}; $\widehat{p}_{k,m^*}$ – вероятность *поражения* k-го элемента при воздействии угрозы u_{m^*}, при этом

$$\widehat{p}_{k,m^*}=1-\left(p_{k,m^*}+\underset{\sim}{p}_{k,m^*}\right).$$

Учитывая, что элемент может находится только в одном из трех состояний следует, что

$$p_{k,m^*}+\widehat{p}_{k,m^*}+\underset{\sim}{p}_{k,m^*}=1.$$

Оценка *требуемых* производительных *возможностей* для восстановления функциональности объекта КИИ после воздействия угроз $u\in U$

$$\mathrm{T}(u)\underset{\substack{k=1,2,\ldots,N_E,\\ m=1,\ldots,N_U}}{=}\{\tau_{k,m}\}\underset{\substack{k=1,2,\ldots,N_E,\\ m=1,\ldots,N_U}}{=}\{\underset{\sim}{\tau}_{k,m}, \widehat{\tau}_{k,m}\},$$

где $\underset{\sim}{\tau}_{k,m}$ – нижняя оценка *требуемого времени* восстановления функциональности элемента e_k, из всех актуальных угроз U выбирается угроза с индексом u_{m^*} при которой

$$\underset{\sim}{\tau}_k=\underset{\sim}{\tau}_{k,m^*}=\max_{m=1,2,\ldots,N_U}\underset{\sim}{\tau}_{k,m},$$

где $\widehat{\tau}_{k,m}$ – верхняя оценка *требуемого* времени восстановления функциональности элемента e_k, из всех актуальных угроз U выбирается угроза с индексом u_{m^*} при которой

$$\widehat{\tau}_k=\widehat{\tau}_{k,m^*}=\max_{m=1,2,\ldots,N_U}\widehat{\tau}_{k,m}.$$

Ресурсные возможности системы восстановления функциональности субъекта КИИ, выделенные для восстановления функциональности объекта КИИ в условиях воздействия угроз

$$\Theta\underset{\substack{i=1,2,\ldots,N_D,\\ j=1,2,\ldots,N_R}}{=}\{d_i, r_j\},$$

где d_i – число единиц d_i-го *возобновляемого* ресурса, d_i – классификатор i-го *возобновляемого* ресурса, $i=1, 2, \ldots, N_D$, N_D – количество классификаторов возобновляемого ресурса; r_j – число единиц r_j-го *невозобновляемого* ресурса, r_j – классификатор j-го *невозобновляемого* ресурса, $j=1, 2, \ldots, N_R$, N_R – количество классификаторов (артикулов) невозобновляемого ресурса.

2) Неуправляемые факторы

Параметры воздействия угроз по семейству элементов объекта КИИ

$$\mathrm{H}(u)=\{\underset{\sim}{\eta}_{m,k,n}, \widehat{\eta}_{m,k,n}\},$$

где $\underset{\sim}{\eta}_{m,k,n}$ – нижняя граница времени до n-го воздействия угрозы $u_m\in U$ по элементу a_k. Из всех актуальных угроз U для каждого воздействия n выбирается угроза с индексом $u_{m^*}\in U$, для которой

$$\underset{\sim}{\eta}_{m^*,k,n}=\min_{\substack{m=1,2,\ldots,N_U,\\ n=1,\ldots,N}}\underset{\sim}{\eta}_{m,k,n},$$

где $m=1, \ldots, N_U$, N_U – число актуальных угроз; $k=1, \ldots, N_E$; $k=1, 2, \ldots, N_E$, N_E – число элементов СОФ; $n=1, \ldots, N_U$, N – прогнозируемое число воздействий угроз; $\widehat{\eta}_{m,k,n}$ – верхняя граница времени до k-го воздействия

угрозы $u_m \in U$ по элементу a_k при воздействии угрозы n. Из всех актуальных угроз U для каждого воздействия n выбирается угроза с индексом $u_{m^*} \in U$, для которой

$$\hat{\eta}_{m^*,k,n} = \max_{\substack{m=1,2,\ldots,N_U,\\ n=1,\ldots,N}} \hat{\eta}_{m,k,n},$$

где m=1, …, N_U, N_U – число актуальных угроз; k=1, …, N_E; k=1, 2, …, N_E, N_E – число элементов СОФ; n=1, …, N_U, N – прогнозируемое число воздействий угроз.

Оценка требуемых ресурсов для восстановления функциональности объекта КИИ, подверженного воздействию угроз (формируется в результате технической разведки)

$$\hat{\Theta} = \left\{\hat{d}_{k,m,i}, \hat{r}_{k,m,j}\right\},$$

где $\hat{d}_{k,m,i}$ – требуемый *возобновляемый* ресурс i-го типа для восстановления функциональности поврежденного элемента e_k при воздействии угрозы $u_m \in U$, i=1, 2, …, N_D, N_D – число типов (классификаторов) *возобновляемого* ресурса. Из всех комбинаций индексов элементов k и угроз m $\langle k, m\rangle$ выбирается комбинация $\langle k^*, m^*\rangle$ при которой *возобновляемый* ресурс с индексом i имел бы максимальное число единиц учета

$$\hat{d}_i\langle k^*, m^*\rangle = \max_{\substack{k=1,2,\ldots,N_E,\\ m=1,2,\ldots,N_U}} \hat{d}_i\langle k, m\rangle,$$

$\hat{r}_{k,m,j}$ – требуемый *невозобновляемый* ресурс j-го типа для восстановления функциональности поврежденного элемента e_k при воздействии угрозы $u_m \in U$, j=1, 2, …, N_R, N_R – число типов (классификаторов) *невозобновляемого* ресурса. Из всех комбинаций индексов элементов k и угроз m $\langle k, m\rangle$ выбирается комбинация $\langle k^*, m^*\rangle$ при которой *невозобновляемый* ресурс с индексом j имел бы максимальное число единиц учета

$$\hat{r}_j\langle k^*, m^*\rangle = \max_{\substack{k=1,2,\ldots,N_E,\\ m=1,2,\ldots,N_U}} \hat{r}_j\langle k, m\rangle.$$

3) Ограничения

Соответствие конфиденциальности информации требованиям на всем периоде воздействия угроз $t \in (0, T]$

$$\mathrm{К}(t) \underset{t\in(0,T]}{\in} \mathrm{К}_{\mathrm{Тр}},$$

где К(t) – совокупность требований по обеспечению конфиденциальности реализованных в момент времени $t \in (0, T]$;

$\mathrm{К}_{\mathrm{Тр}}$ – совокупность требований по обеспечению конфиденциальности.

Соответствие целостности информации требованиям на всем периоде воздействия угроз $t \in (0, T]$

$$\mathrm{Ц}(t) \in \mathrm{Ц}_{\mathrm{Тр}},$$

где Ц(t) – совокупность требований по обеспечению целостности информации реализованных в мент времени $t \in (0, T]$;

$\mathrm{Ц}_{\mathrm{Тр}}$ – совокупность требований по обеспечению целостности.

Требуется, с учетом принятых ограничений, разработать:

Семейство методов теоретической обработки исходных данных (оператор) – $\mathcal{M}$, позволяющих получать количественные оценки показателей, характеризующих устойчивость функционирования элементов объекта КИИ, находящегося под воздействием угроз $u \in U$

$$\left\{\varphi_k(u,t)\right\} \underset{\substack{t\in(0,T]\\ u\in U\\ \mathrm{К}(t)\in\mathrm{К}_{\mathrm{Тр}}\\ \mathrm{Ц}(t)\in\mathrm{Ц}_{\mathrm{Тр}}}}{=} \mathcal{M}\left\{\begin{matrix} E(t_0), U, K_{\mathrm{Ог}}, P(u),\\ \mathrm{Т}(u,t), \Theta(t), \mathrm{Н}(u), \hat{\Theta}\end{matrix}\right\},$$

где $\{\varphi_k(u,t)\}$ – семейство функций устойчивости, характеризующих устойчивость функционирования элементов объекта КИИ, находящегося под воздействием угроз $u \in U$, $\varphi_k(u,t)$ – частная функция устойчивости k-го элемента.

2. Семейство методов теоретической обработки исходных данных (оператор) – $\mathcal{B}$, характеризующих семейство функций устойчивости отдельных элементов объекта КИИ $\varphi_k(u,t)$ и его структуру $S(t)$, позволяющих получать количественную оценку, характеризующую устойчивость функционирования объекта КИИ в целом, находящегося под воздействием угроз $u \in U$

$$\Phi(t) = \mathcal{B}\left\{\varphi_k(u,t), S(t), \hat{\Theta}\right\} =$$

$$= \mathcal{B}\left\{\mathcal{M}\left\{\begin{matrix} E(t_0), U, K_{\mathrm{Ог}}, P(u),\\ \mathrm{Т}(u,t), \Theta(t), \mathrm{Н}(u,t)\end{matrix}\right\}, S(t), \hat{\Theta}\right\},$$

где $\Phi(t)$ – функция устойчивости объекта КИИ, находящегося под воздействием угроз, $\mathcal{B}$ – оператор, позволяющий отобразить семейство частных функций устойчивости элементов объекта КИИ в функцию устойчивости объекта КИИ в целом.

Новизна полученных результатов заключается: а) в усовершенствовании онтологии предметной области, позволяющей стоить адекватные вербальные модели предмета исследования; б) в оригинальной постановке научной задачи, позволяющей оценить устойчивость объекта КИИ для условий воздействия угроз, когда методы математической статистики и теории вероятностей, которые нашли широкое применение для штатных условий, не могут быть применимы без грубых допущений; в) в использовании для представления исходных данных и результатов оценивания не усредненных вероятностных характеристик, как это принято для штатных условий, а функций, отражающих зависимость параметров исходных данных и получаемого результата от времени, что позволяет снять ограничение на стационарность и эргодичность исследуемого случайного процесса; г) применение для оценивания устойчивости отдельных элементов методов теории управляемых полумарковских процессов с *тремя* возможными состояниями, что позволяет связать частные характеристики

защищенности и восстанавливаемости элементов, подверженных угрозам, с частными оценками устойчивости их функционирования; д) в приложении методов управляемых полумарковских процессов для оценивания устойчивости объекта КИИ в целом на основе частных оценок функций устойчивости элементов; е) в приложении разработанной методологии для количественного оценивания эффективности планов восстановления функциональности объекта КИИ, элементы которого получили повреждения в результате воздействия угроз; ж) в приложении разработанных методов оценивания устойчивости для обоснования распределения затрат между мероприятиями по обеспечению защищенности и восстанавливаемости элементов.

Заключение

Таким образом, предлагаемая постановка научной задачи позволяет обобщить методы теории надежности, теории случайных функций, теории информационной безопасности на случаи, когда при оценивании устойчивости КИИ не представляется возможным принять допущения: а) о массовости случайных явлений; б) о неограниченности времени наблюдения за оцениваемым объектом; в) о стационарности сопутствующей обстановки; г) об отсутствии поведенческой неопределенности. Разработаны соответствующие методы и математические модели, которые приведены в [22-24].

При поддержке Фонда Потанина

Список литературы

1. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. М.: Наука, 1965. 524 с.

2. Ушаков И.А. Обобщенные показатели при исследовании сложных систем / И.А. Ушаков, Е.И. Литвак. М.: Знание, 1985. 128 с.

3. Половко А.М., Гуров С.В. Основы теории надежности. СПб.: БХВ-Петербург, 2006. 704 с.

4. Каштанов В.А., Медведев А.И. Теория надежности сложных систем: 2-е изд., перераб. М.: ФИЗМАТЛИТ, 2010. 608 с.

5. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 216 с.

6. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 296 с.

7. Ушаков И.А. Надежность: прошлое, настоящее, будущее: пленарный доклад на открытии конференции «Математические методы в надежности» (MMR–2000), Бордо, Франция, 2000 // Надежность: Вопросы теории и практики: сетевой журн. 2016. № 1(1). С. 17-27.

8. Юсупов Р.М. Особенности оценивания эффективности информационных систем и технологий / Р.М. Юсупов, А.А. Мусаев // Труды СПИИРАН. 2017. Вып. № 2 (51). С. 5–34.

9. Зегжда Д.П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / под ред. Д.П. Зегжды. М.: Горячая линия – Телеком, 2022. 560 с.

10. Котенко И.В. Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей / И.В. Котенко, И.Б. Саенко, М.А. Коцыняк, О.С. Лаута // Труды СПИИРАН. 2017. № 6(55). С. 160-184. DOI: 10.15622/sp.55.7

11. Шелупанов А.А. Безопасность комплексных гетерогенных систем и сетей. Теория и практика: монография // С.Ю. Исхаков, А.А. Шелупанов, Р.В. Мещеряков. Томск: Изд-во Томского государственного университета систем управления и радиоэлектроники, 2015. 119 с.

12. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем: монография / Р.В. Мещеряков, А.А. Шелупанов. Томск: Издательство В–спектр, 2007. 278 с.

13. Коноваленко С.А. Методика оценивания функциональной устойчивости гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Системы управления, связи и безопасности. 2023. № 4. С. 157-195. DOI: 10.24412/2410-9916-2023-4-157-195

14. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки : [монография]. СПб.: Наукоемкие технологии, 2020. 337 с.

15. Макаренко С.И. Информационный конфликт системы связи с системой дестабилизирующих воздействий. Часть III: Управление системой связи в условиях конфликта // Техника радиосвязи. 2021. № 1(48). С. 103-116. DOI: 10.33286/2075-8693-2021-48-103-116

16. Стародубцев Ю.И., Закалкин П.В. Структурно-функциональный анализ конфликтной ситуации между государственной системой обеспечения информационной безопасности и иностранной системой деструктивных воздействий // Вопросы кибербезопасности. 2024. № 4(62). С. 82-91. DOI: 10.21681/2311-3456-2024-4-82-91

17. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах : [монография] / Ю.К. Язов; Федеральное гос. науч. учреждение «Северо-Кавказский науч. центр высш. шк.». Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. 270 с.

18. Черкесов Г.Н., Недосекин А.О., Виноградов В.В. Анализ функциональной живучести структурно-сложных технических систем // Надежность. 2018. Том 18. № 2. С. 17-24. DOI: 10.21683/1729-2646-2018-18-2-17-24

19. Черкесов Г.Н. Описание подхода к оценке живучести сложных структур при многоразовых воздействиях высокой точности / Г.Н. Черкесов, А.О. Недосекин // Надежность. 2016. Том 16. № 2(57). С. 3–15.

20. Рябинин И.А. Надежность и безопасность структурно-сложных систем. Спб.: Политехника, 2000. 248 с.

21. Воеводин В.А. Генезис понятия структурной устойчивости информационной инфраструктуры автоматизированной системы управления производственными процессами к воздействию целенаправленных угроз информационной безопасности // Вестник Воронежского института ФСИН России. 2023. № 2, апрель–июнь. С. 30-41.

22. Воеводин В.А. Модель оценки функциональной устойчивости информационной инфраструктуры для условий воздействия множества компьютерных атак // Информатика и автоматизация. 2023. № 22(3). С. 691-715. DOI: 10.15622/ia.22.3.8

23. Воеводин В.А. Частная полумарковская модель как инструмент снижения сложности задачи оценивания устойчивости функционирования элементов информационной инфраструктуры, подверженной воздействию угроз // Информатика и автоматизация. 2024. № 23(3). С. 611-642. DOI: 10.15622/ia.23.3.1

24. Воеводин В.А., Крахотин Н.А. Методы оценивания связности неориентированного двухполюсного помеченного графа с учетом деструктивного воздействия внешних угроз на его вершины // Вестник Дагестанского государственного технического университета. Технические науки. 2024. № 51(1). С. 46-60. DOI:10.21822/2073-6185-2024-51-1-46-60

References

1. Gnedenko B.V., Beliaev Yu.K., Soloviev A.D. [Mathematical methods in the dependability theory]. Moscow: Nauka; 1965. (in Russ.)

2. Ushakov I.A., Litvak E.I. [Generalised indicators in the study of complex systems]. Moscow: Znanie; 1985. (in Russ.)

3. Polovko A.M., Gurov S.V. [Fundamentals of the dependability theory]. St. Petersburg: BHV-Peterburgl; 2006. (in Russ.)

4. Kashtanov V.A., Medvedev A.I. [Dependability theory of complex systems: 2nd edition, revised]. Moscow: Fizmatlit; 2010. (in Russ.)

5. Shubinsky I.B. [Structural dependability of information systems. Analysis methods]. Moscow: Dependability Journal; 2012. (in Russ.)

6. Shubinsky I.B. [Functional dependability of information systems. Analysis methods]. Moscow: Dependability Journal; 2012. (in Russ.)

7. Ushakov I.A. [Dependability: past, present, future: keynote speech of the opening of Mathematical Methods in Reliability (MMR-2000) conference, Bordeau, France, 2000]. *Reliability: Theory & Applications* 2016;1(1):17-27. (in Russ.)

8. Yusupov R.M., Musaev A.A. Efficiency of Information Systems and Technologies: Features of Estimation. *SPIIRAS Proceedings* 2017;2(51):5-34. (in Russ.)

9. Zegzhda D.P. [Cybersecurity of the digital industry. Theory and practice of functional resistance to cyber attacks]. Moscow: Goriachya liniya – Telekom; 2022. (in Russ.)

10. Kotenko I., Saenko I., Kotsynyak M., Lauta O. Assessment of Cyber-Resilience of Computer Networks based on Simulation of Cyber Attacks by the Stochastic Networks Conversion Method. *SPIIRAS Proceedings* 2017;6(55):160-184. DOI: 10.15622/sp.55.7

11. Shelupanov A.A., Iskhakov S.Yu., Shelupanov A.A., Meshcheryakov R.V. [Security of complex heterogeneous systems and networks. Theory and practice: a monograph]. Tomsk: Tomsk State University of Control Systems and Radioelectronics Publishing; 2015. (in Russ.)

12. Meshcheryakov R.V., Shelupanov A.A. [Comprehensive information security of automated systems: a monograph]. Tomsk: V–spektr Publishing; 2007. (in Russ.)

13. Konovalenko S. A. Methodology for assessing the functional stability of a heterogeneous system for detecting, preventing and eliminating the consequences of computer attacks. *Systems of Control, Communication and Security* 2023;4:157-195. (in Russ.). DOI: 10.24412/2410-9916-2023-4-157-195

14. Makarenko S.I. [Models of a communication system exposed to deliberate destabilising effects and intelligence: a monograph]. St. Petersburg: Naukoemkie tekhnologii; 2020. (in Russ.)

15. Makarenko S. I. Information conflict between a communication system and a system of destabilizing influences. Part III: Controlling of a communication system in conflict situation. *Radio communication technology* 2021;1(48):103-16. DOI: 10.33286/2075-8693-2021-48-103-116

16. Starodubtsev Yu.I., Zakalkin P.V. Sructural and functional analysis of the conflict situation between the state information security system and a foreign system of destructive influences. *Cybersecurity issues* 2024;4(62):82-91. DOI: 10.21681/2311-3456-2024-4-82-91

17. Yazov Yu.K. [Fundamentals of the methodology for quantifying the effectiveness of information protection in computer systems: a monograph]. Federal State Scientific Institution North Caucasus Scientific Centre of Higher Education. Rostov-on-Don: NCSCHE Publishing; 2006. (in Russ.)

18. Cherkesov G.N., Nedosekin A.O., Vinogradov V.V. Functional survivability analysis of structurally complex technical systems. *Dependability* 2018;18(2):17-24. DOI: 10.21683/1729-2646-2018-18-2-17-24

19. Cherkesov G.N., Nedosekin AO. Description of approach to estimating survivability of complex structures under repeated impacts of high accuracy. *Dependability* 2016;16(2):3-15. DOI:10.21683/1729-2646-2016-16-2-3-15

20. Ryabinin I.A. Reliability and safety of structurally complex systems. St. Petersburg: Polytekhnica; 2000. (in Russ.)

21. Voevodin V.A. [The genesis of the concept of structural resilience of the information infrastructure of an automated production process management system to the effects of targeted information security threats]. *Vestnik*

of Voronezh Institute of the Russian Federal Penitentiary Service 2023;2:30-41. (in Russ.)

22. Voevodin V. A Model for Assessing the Functional Stability of Information Infrastructure Elements for Conditions of Exposure to Multiple Computer Attacks. *Informatics and Automation* 2023;22(3):691-715. DOI: 10.15622/ia.22.3.8

23. Voevodin, V. A. On the formulation of the task of assessing the stability of the functioning of critical information infrastructure facilities. *Cybersecurity issues* 2025;1(65): 41-49. DOI: 10.21681/2311-3456-2025-1-41-49.

24. Voevodin V.A., Krahotin N.A. Methods for assessing the connectivity of an undirected bipolar labeled graph taking into account the destructive impact of external threats on its vertices. *Herald of Dagestan State Technical University. Technical Sciences* 2024;51(1):46-60. (in Russ.) DOI:10.21822/2073-6185-2024-51-1-46-60

Сведения об авторах

Воеводин Владислав Александрович – 124575, Зеленоград, корп. 901, кв. 160, Россия, НИУ «Московский институт электронной техники», доцент кафедры «Информационная безопасность», кандидат технических наук, доцент, почетный радист России; vva541@mail.ru; Известия вузов Электроника: 2024, Т.29. №3, 2024, Т.29. №2; Информатика и автоматизация 2023, Т. 22, № 3, 2024 Т 23 №3; Вестник Дагестанского государственного технического университета. Технические науки: 2024 Т 51 №1, 2023 Т50 №23, 2023 Т50 №1, 2022 Т49 №3; Вестник Воронежского института ФСИН России, 2023, № 2; Информационные технологии: 2024 Т30 №1; International Journal of Open Information Technologies: 2023. Т. 11, № 9; Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика: 2022. № 2; Системы управления, связи и безопасности. 2021. № 2.

Третьяков Сергей Михайлович – 194064, г. Санкт-Петербург, К-64, Тихорецкий проспект, д.3, Военная академия связи, доцент кафедры технического обеспечения связи и автоматизации, кандидат технических наук, доцент; smt2k@mail.ru.

About the authors

Vladislav A. Voevodin, 901, app. 160, Zelenograd, 124575, Russia, National Research University of Electronic Technology, Senior Lecturer, Department of Information Security, Candidate of Engineering, Associate Professor, Honorary Radio Operator of Russia; vva541@mail.ru; Proceedings of Universities Electronics: 2024;29(3), 2024;29(2); Computer Science and Automation 2023;22(3), 2024;23(3); Herald of Daghestan State Technical University. Technical Sciences 2024;51(1), 2023;50(23), 2023;50(1), 2022;49(3); Vestnik of Voronezh Institute of the Russian Federal Penitentiary Service 2023;2; Information technologies 2024;30(1); International Journal of Open Information Technologies 2023; 11(9); Vestnik of Astrakhan State Technical University Series: Management, computer science and informatics 2022;2; Systems of Control, Communication and Security 2021;2.

Sergey M. Tretyakov, 3, K-64 Tikhoretsky Prospekt, 194064, St. Petersburg, Russia, Military Academy of the Signal Corps, Senior Lecturer, Department of Technical Support of Communications and Automation, Candidate of Engineering, Associate Professor; smt2k@mail.ru.

Вклад авторов в статью

Воеводин В.А.: Вербальная и формальная постановки задачи.

Третьяков С.М.: Введение, анализ литературы по теме, исследование актуальности научной задачи, анализ возможностей существующего методического аппарата.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.