

# О ПОСТАНОВКЕ ЗАДАЧИ ОЦЕНИВАНИЯ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Воеводин В. А.<sup>1</sup>

DOI: 10.21681/2311-3456-2025-1-41-49

**Цель исследования:** обосновать актуальность, сформулировать и формализовать научную задачу количественного оценивания устойчивости функционирования критической информационной инфраструктуры применительно к условиям воздействия угроз нарушения ее информационной безопасности.

**Методы исследования:** системный анализ, анализ научной проблемы, формализация научных знаний, методология научного исследования.

**Полученные результаты:** сформулирована вербальная и формальная постановки научной задачи.

**Научная новизна:** предлагается авторский подход к оцениванию динамики устойчивости функционирования критической информационной инфраструктуры в условиях воздействия угроз с учетом имеющегося ресурса.

**Практическая значимость:** постановка научной проблемы может служить основой для формулирования технического задания по разработке методов, моделей и средств количественного оценивания устойчивости функционирования объектов критической информационной структуры, функционирующих в условиях воздействия угроз.

**Ключевые слова:** угрозы нарушения информационной безопасности, система восстановления функциональности, критическая информационная инфраструктура, восстанавливаемость, защищенность от угроз, возобновляемый ресурс, невозобновляемый ресурс.

## Введение

Информационная инфраструктура того или иного объекта информатизации создается для удовлетворения определенных потребностей субъектов информационных отношений (обладателей информации и операторов информационных систем) и служит активным средством в их целенаправленной деятельности. Чтобы противостоять воздействию угроз безопасности информации обладатели информации и операторы информационных систем обязаны в силу закона принимать меры по защите информации. В силу закона отдельно выделяются критические информационные инфраструктуры (КИИ). Отношения, возникающие при обеспечении устойчивости функционирования КИИ в условиях воздействия угроз, регулируются ответствующими нормативными правовыми актами.

Противник с целью нарушить функциональность объектов КИИ осуществляет как физическое воздействие по ее элементам, так и воздействие посредством воздействия помех и компьютерных атак. В совокупности эти воздействия позиционируются как воздействия угроз безопасности информации (угроз).

В результате воздействия угроз функциональность отдельных элементов может быть нарушена или они

могут быть уничтожены, что может привести к снижению устойчивости функционирования КИИ в целом ниже требуемого уровня. Генезис понятия «устойчивость функционирования КИИ» применительно к настоящей публикации рассматривается в [1].

Для обеспечения устойчивости КИИ выделяются соответствующие силы и средства, которые необходимо результативно распределить по задачам и времени. Для решения этой задачи органами управления требуется инструмент для количественного оценивания устойчивости функционирования объектов КИИ в различных условиях обстановки, в том числе и в условиях воздействия угроз.

Для успешного решения задач по оцениванию устойчивости КИИ требуется, чтобы методические потребности органов управления ИБ и соответствующий научно-методический аппарат находились в гармонии.

Применение экспериментального подхода, характерного для условий штатного применения, для оценивания устойчивости функционирования масштабных КИИ в условиях воздействия угроз требует значительного ресурса и часто неприменимо по экономическим соображениям. Поэтому основной исследовательской концепцией для оценивания

<sup>1</sup> Воеводин Владислав Александрович, кандидат технических наук, доцент, МИЭТ, Москва, Россия, E-mail: vva541@mail.ru. AuthorID: 1012813, ORCID 0009-0003-9431-1685

устойчивости функционирования применительно к условиям воздействия угроз является экспертное и математическое моделирование.

#### Анализ существующего методического обеспечения

Анализ существующих нормативных правовых актов, методических документов, приказов исполнительных органов власти 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 инструмент оценивания устойчивости КИИ ориентирован на штатные условия и базируется на приложениях теории надежности. Методы теории надежности, основаны на анализе экспериментальных и эксплуатационных данных, постоянно развиваются. Результаты фундаментальных исследований теории надежности технических систем отражены достаточно полно и глубоко в фундаментальных публикациях Б. В. Гнеденко<sup>2</sup>, И. А. Ушакова<sup>3</sup>, В. А. Каштанова<sup>4</sup> и других, признанных в этой области ученых.

Однако для оценивания устойчивости КИИ, находящейся под воздействием угроз, применение методов теории надежности не всегда оправдано и корректно. Такое ограничение связано с необходимостью учесть при оценивании устойчивости редкость событий воздействия угроз, ограниченность интервала времени их наблюдения, динамичность обстановки и самих показателей, характеризующих исходные данные, влияние поведенческой неопределенности. 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»<sup>5</sup>.

Результаты методологического исследования особенностей количественного оценивания эффективности информационных систем и технологий применительно к штатным условиям функционирования приводятся Зегждой Д. П. [2, 3]. Авторский коллектив предлагает в основу оценивания положить вероятностный подход, что для условий воздействия угроз так же не всегда является приемлемым.

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

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

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

5 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.

Отсутствие инструмента для количественного оценивания устойчивости КИИ, находящейся под воздействием угроз сдерживает развитие отношений в области обеспечения безопасности КИИ при воздействии угроз.

#### Анализ возможностей существующих научных методов

Исходными посылами, которые легли в основу анализа применимости существующих научных методов для оценивания устойчивости технических систем, функционирующих в условиях целенаправленных угроз, явились результаты осмысления деятельности по организации аудита информационной безопасности (ИБ). Почвой для такого осмысления явилось обобщение опыта преподавания учебных курсов магистратуры, в рамках которых изучались правовые и организационные основы аудита ИБ, организовывалась выпускная деловая игра по организации аудита автоматизированных систем.

Полученные общения позволили прийти к выводу о том, что существующий подход к аудиту ИБ в отношении объектов информатизации нацелен на оценивание их соответствия требованиям Регулятора, а не на количественном оценивании устойчивости их функционирования в различных условиях обстановки.

Деятельность по оцениванию устойчивости объектов КИИ, в отличие от деятельности по оценке соответствия требованиям, по своей сути является продуктивной, так как направлена каждый раз на получение объективно нового результата. Такая деятельность, в отличие от репродуктивной, нуждается в организации, то есть возникает необходимость в ее теоретическом осмыслении, а также в построении соответствующей методологии оценивания.

В основу существующего подхода к обеспечению устойчивости функционирования КИИ положены императивные нормы права. Деятельность регулируется преимущественно силой закона и подзаконных актов. Эта деятельность позиционируется как административная и относится к репродуктивной. Для организации такой деятельности инструмент для количественного оценивания устойчивости КИИ формально не требуется. К существующей инерционности и репродуктивности директивного подхода необходимо объективно добавить и то, что требования общедоступны и известны противнику (источнику угроз), который может целенаправленно планировать эффективное воздействие угроз в обход реализованных требуемых мер защиты.

Вместе с тем, опять же силой закона, обладателям информации и операторам информационных систем предписано: 1) обеспечить защиту информации; 2) не допускать воздействий на технические средства обработки информации, в результате которых

нарушается их функционирование; 3) осуществлять постоянный контроль за обеспечением уровня защищенности информации. Директивный подход в этом случае не применим, так как не обеспечивает эффективного применения соответствующих сил и средств. При исполнении перечисленных предписаний должны действовать диспозитивные нормы права, в соответствии с которыми обладателям информации и операторам информационных систем предоставляется право самостоятельно регулировать эти отношения и принимать соответствующие решения. 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 обеспечения устойчивости объектов информатизации, функционирующих в условиях воздействия дестабилизирующих факторов различной физической природы. Некоторые из таких подходов, представляющие интерес для оценивания устойчивости КИИ, приведены в трудах Д. П. Зегжды [3], И. В. Котенко [4], И. Б. Саенко [5], С. А. Коноваленко [6], С. И. Макаренко [7], Ю. И. Стародубцева [8, 9], Ю. К. Язова [10–12], И. Б. Шубинского [13–15].

Основные усилия исследователей были направлены на развитие подходов оценивания устойчивости структурно-сложных технических систем на основе парадигмы структурной и функциональной устойчивости, когда критерий отказа системы и/или элемента является бинарным. На практике задача сводилась к определению за допустимое вычислительное время доли сохранившихся работоспособных состояний, когда из строя выходит фиксированное число элементов, при этом анализ живучести проводится на стыке анализа структурной и функциональной избыточности в сочетании с вероятностными моделями объектов оценивания.

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 в штатных условиях исследовались А. М. Половко совместно с С. В. Гуровым<sup>6</sup>. В качестве предмета исследования были рассмотрены невозстанавливаемые и восстанавливаемые, нерезервированные и резервированные системы длительного и короткого времени существования.

Обобщая результаты ретроспективного анализа, можно утверждать, что основные усилия исследова-

телей были сосредоточены на оценивании устойчивости на основе исходных данных, которые характеризовали надежность элементов КИИ. Так или иначе при таком подходе к оцениванию требовались некие исторические данные (статистика). При оценивании характеристик устойчивости принималось допущение о стационарности случайного процесса, что позволяло не учитывать динамические характеристики процесса функционирования объекта оценивания, и использовать в качестве показателей усредненные оценки всего процесса. Усредненные оценки основывались на статистических наблюдениях, проводимых в стабильных условиях, которые для условий воздействия угроз чаще неприменимы из-за высокой погрешности. Обычно характеристики надежности оцениваются при проведении приемочных испытаний и приводятся в эксплуатационной документации.

Такой подход к оцениванию устойчивости в условиях воздействия угроз не всегда применим и корректен. На практике приходится иметь дело со случайными величинами, статистические характеристики которых непрерывно изменяются с течением времени либо вообще неизвестны и недоступны эксперту для наблюдения и эксперимента. Для оценивания устойчивости в этих условиях требуется специальный инструмент, который бы позволял получать оценки применительно к воздействию целенаправленных угроз, с учетом имеющегося ресурса и информационной неопределенности которая присуща противнику при планировании компьютерных атак.

Результаты проведенного анализа позволяют утверждать, что объективно наблюдается противоречивая ситуация, суть которой заключается в том, что, с одной стороны, органам управления для принятия решения требуется общепринятое методическое обеспечение для количественной оценки устойчивости функционирования КИИ, а с другой стороны, существующие научные методы и модели, без принятия грубых допущений, не могут быть использованы в качестве его теоретического фундамента.

Для разрешения противоречия требуется решить научную задачу по разработке системы методов, моделей и средств, позволяющих в графике работы органов управления ИБ получать оценки устойчивости функционирования объектов КИИ, которая бы легла методологическим фундаментом к формулированию требований к методическому обеспечению.

Анализ существующего теоретического задела подтверждает, что для условий воздействия целенаправленных угроз существуют лишь отдельные публикации, которые не объединены в единый методический аппарат, что в совокупности переводит поставленную научную задачу в статус научной проблемы.

<sup>6</sup> Половко А. М., Гуров С. В. Основы теории надежности. – СПб.: БХВ-Петербург. 2006. – 704 с.

**Вербальная постановка научной задачи**

При оценивании устойчивости КИИ с помощью моделирования следует учитывать отдельные группы факторов, которые напрямую или косвенно влияют на ее обеспечение: 1) сценарии воздействия угроз; 2) характеристики надежности элементов; 3) защищенность элементов от воздействия угроз; 4) производственные возможности системы восстановления функциональности (СВФ) субъекта КИИ; 4) схему, отображающую условия обеспечения функциональности объекта оценивания (СОФ).

Для оценивания устойчивости объекта КИИ за основу была принята концепция условий работоспособного состояния, которая была применена для оценивания концептуальных направлений решения проблемы обеспечения устойчивости сложных технических систем [13–15].

Для формальной постановки научной проблемы факторы, определяющие условия функционирования КИИ, подразделяются на две группы: 1) факторы, которые могут контролироваться лицом, принимающим решение (ЛПР), и доступны ему для управления; 2) факторы, которые по различным причинам не могут быть контролируемы ЛПР; 3) факторы, которые выведены в ограничения.

При формулировании задачи принимается, что каждый элемент оцениваемого объекта на периоде воздействия угроз может принимать одно из трех состояний: 1) *функционален* – способен выполнять требуемые функции; 2) *поврежден* – восстановление функциональности возможно через допустимый период времени восстановления, при этом расходуется имеющийся ресурс СВФ; 3) *поражен* – восстановление функциональности не целесообразно или невозможно из-за ограниченности имеющегося ресурса СВФ, в том числе и времени. Последовательный переход из одного состояния в другое позиционируется как процесс функционирования элемента и объекта КИИ в целом.

При постановке задачи принимаются ограничения: 1) считается, что если элемент попадает в состояние «уничтожен», то он так и остается в этом состоянии до конца периода оценивания; 2) требования к конфиденциальности и целостности информации выполняются на всем протяжении периода оценивания не хуже заданных; 3) возможность поражения органов управления не учитывается, т. е. вероятность сохранения ими способности формировать управленческие решения принимается равной единице.

Требуется разработать методы, модели и средства, позволяющие с учетом принятых ограничений.

**1. На первом этапе** отобразить исходные данные, характеризующие: 1) возможные сценарии воздействия противника; 2) защищенность элементов

от воздействия угроз; 3) семейство актуальных угроз; 4) выделенный для поддержания функциональности элементов ресурс; 5) надежность элементов для условий штатного применения (значения коэффициентов оперативной готовности); 6) восстанавливаемость элементов, в значения частных функций устойчивости элементов.

**2. На втором этапе** – отобразить: 1) семейство частных функций устойчивости элементов; 2) характеристики СВФ субъекта КИИ; 3) характеристики СОФ в значения функции устойчивости для всего оцениваемого объекта;

Для решения поставленной научной задачи предлагается обобщить методы теории надёжности, теории случайных функций, теории информационной безопасности на случаи, когда при оценивании устойчивости КИИ не представляется возможным принять допущения: 1) о массовости случайных явлений; 2) об эргодичности и стационарности оцениваемого случайного процесса; 3) об отсутствии поведенческой неопределенности; 4) о неограниченности ресурса СВФ.

Новизна полученных результатов заключается: 1) в усовершенствовании онтологии предметной области, позволяющей строить адекватные вербальные модели предмета исследования; 2) в оригинальной постановке научной задачи, позволяющей оценить устойчивость 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; 3) в использовании для представления исходных данных и результатов оценивания не усредненные вероятностные характеристики, как это принято для штатных условий, а функции устойчивости, отражающие зависимость параметров исходных данных и получаемого результата от времени. Такой подход позволяет снять ограничение на стационарность и эргодичность исследуемого случайного процесса; 4) 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; 5) в приложении методов управляемых полумарковских процессов для оценивания устойчивости объекта КИИ в целом на основе частных оценок функций устойчивости элементов; 6) в приложении методологии для количественного оценивания эффективности планов восстановления функциональности объекта оценивания, элементы которой получили повреждения в результате воздействия угроз;

7) в приложении разработанных методов оценивания устойчивости для обоснования распределения затрат между мероприятиями по обеспечению защищенности и восстанавливаемости элементов.

**Формальная постановка научной задачи**

Пусть заданы исходные данные, характеризующие:

**Управляемые факторы**

1. Пусть задана структура СОФ оцениваемого объекта в момент времени  $t_0$ , соответствующий начальному периоду воздействия угроз  $(0, T]$

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

где  $A(t_0) = \{a_i(t_0)\}$  – семейство узлов СОФ,  $a_i(t_0)$  – индикатор состояния  $i$ -го узла,  $i = 1, 2, \dots, N_A$ ;  $N_A$  – мощность семейства  $A(t_0)$ . Если узел  $a_i(t_0)$  функционален, то  $a_i(t_0) = 1$  и 0 в противном случае;

$L(t_0) = \{l_{ij}(t_0)\}$  – семейство ребер СОФ,  $l_{ij}(t_0)$  – индикатор состояния  $ij$ -го ребра,  $ij = 1, 2, \dots, N_L$ ;  $N_L = (N_A)^2$  – мощность семейства  $L(t_0)$ . Если ребро  $l_{ij}(t_0)$  функционально, то  $l_{ij}(t_0) = 1$  и 0 в противном случае;

Определено исходное семейство элементов (узлов и ребер) СОФ в момент времени  $t_0$

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

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

Функционирование подверженного воздействию угроз объекта оценивания характеризуется сменой состояний его элементов  $e_k(t_0) \in E(t_0)$ :

- 1) если  $k$ -й элемент на момент времени  $t$  сохранил функциональность, то  $e_k(t) = 1$ ;
- 2) 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  $t$ ;
- 3) если  $k$ -й элемент был поражен в результате воздействия угрозы, то его идентификатору безвозвратно присваивается значение  $e_k(t) = 0$ .

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

2. Семейство актуальных угроз  $U = \{u_m\}$ , где  $u_m$  – идентификатор актуальной угрозы с индексом  $m$ ,  $m = 1, 2, \dots, N_U$ ,  $N_U$  – мощность семейства актуальных угроз.

3. Семейство стационарных коэффициентов оперативной готовности элементов оцениваемого объекта

$$K_{Oz}(t_0, t_0 + t) = \{\hat{k}_{Ozk}(t_0, t_0 + t)\},$$

$t \in (0, T]$   
 $k = 1, 2, \dots, N_E$

где  $\hat{k}_{Ozk}$  – стационарный коэффициент оперативной готовности  $k$ -го элемента на интервале  $t \in (0, T]$ . Физически  $\hat{k}_{Ozk}$  отражает вероятность того, что элемент

$a_k$  проработает безотказно в течение заданного периода времени  $T$ , начиная с момента времени  $t_0$ .

4. Защищенность элементов оцениваемого объекта от воздействия актуальных угроз  $U$

$$P(u) = \prod_{k=1, 2, \dots, N_E} \prod_{m=1, 2, \dots, N_U} \{p_{k,m^*}, p_{k,m^*}, \hat{p}_{k,m^*}\},$$

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 из семейства актуальных с индексом  $u_{m^*}$ , при которой

$$p_{k,m^*} = \min_{m=1, 2, \dots, N_U} p_{k,m},$$

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

$$\hat{p}_{k,m^*} = 1 - (p_{k,m^*} + p_{k,m^*}).$$

Учитывая, что элемент может находиться только в одном из трех состояний следует, что  $p_{k,m^*} + \hat{p}_{k,m^*} + p_{k,m^*} = 1$ .

5. Оценка требуемых производственных возможностей для восстановления функциональности объекта оценивания после воздействия угроз  $u \in U$

$$T(u) = \prod_{k=1, 2, \dots, N_E} \prod_{m=1, 2, \dots, N_U} \{\tau_{k,m}\} = \prod_{k=1, 2, \dots, N_E} \prod_{m=1, 2, \dots, N_U} \{\tau_{k,m}, \hat{\tau}_{k,m}\},$$

где  $\tau_{k,m}$  – нижняя граница оценки требуемого времени восстановления функциональности элемента  $e_k$ , из всех актуальных угроз  $U$  выбирается угроза с индексом  $u_{m^*}$ , при которой

$$\tau_{k,m} = \tau_{k,m^*} = \max_{m=1, 2, \dots, N_U} \tau_{k,m};$$

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

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

6. Ресурсные возможности СВФ субъекта КИИ, выделенные для восстановления функциональности объекта оценивания в условиях воздействия угроз

$$\Theta = \{d_i, r_j\},$$

$i = 1, 2, \dots, N_D$ ,  
 $j = 1, 2, \dots, N_R$

где  $d_i$  – число единиц  $d_i$ -го возобновляемого ресурса,  $d_i$  – классификатор  $i$ -го возобновляемого ресурса,  $i = 1, 2, \dots, N_D$ ,  $N_D$  – количество классификаторов возобновляемого ресурса;  $r_j$  – число единиц  $r_j$ -го невозобновляемого ресурса,  $r_j$  – классификатор  $j$ -го невозобновляемого ресурса,  $j = 1, 2, \dots, N_R$ ,

$N_R$  – количество классификаторов (артикулов) невозобновляемого ресурса.

Обобщенная схема управляемых факторов приведена на рис. 1.

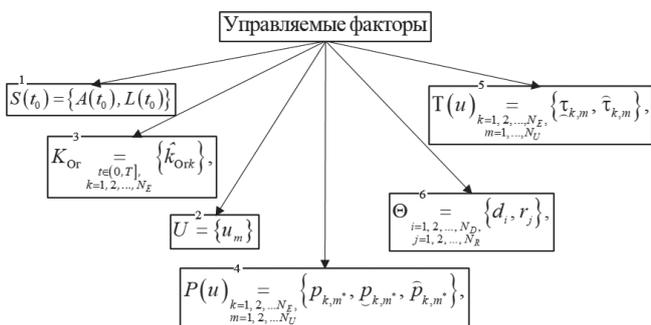


Рис. 1. Управляемые факторы, определяющие устойчивость объекта оценивания

**Неуправляемые факторы**

1. Параметры воздействия угроз по семейству элементов объекта оценивания

$$N(u) = \{\eta_{m,k,n}, \hat{\eta}_{m,k,n}\},$$

где  $\eta_{m,k,n}$  – 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

$$\eta_{m^*,k,n} = \min_{\substack{m=1,2,\dots,N_U \\ n=1,\dots,N}} \eta_{m,k,n}$$

где  $m = 1, \dots, N_U$ ,  $N_U$  – число актуальных угроз;  $k = 1, \dots, N_E$ ;  $k = 1, \dots, N_E$ ,  $N_E$  – число элементов СОФ;  $n = 1, \dots, N$ ,  $N$  – прогнозируемое число воздействий угроз;

$\hat{\eta}_{m,k,n}$  – 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

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

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

2. Оценка требуемых ресурсов для восстановления функциональности элемента, пораженного в результате воздействия угроз (формируется в результате технической разведки)

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

где  $\hat{d}_{k,m,i}$  – требуемый возобновляемый ресурс  $i$ -го типа для восстановления функциональности поврежденного элемента  $k$  при воздействии угрозы  $u_m \in U$ ,  $i = 1, 2, \dots, N_D$ ,  $N_D$  – число типов (классификаторов) возобновляемого ресурса. Из всех комбинаций индексов элементов  $k$  и угроз  $t \langle k, t \rangle$  выбирается

комбинация  $\langle k^*, m^* \rangle$ , при которой возобновляемый ресурс с индексом  $i$  имел бы максимальное число единиц учета

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

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

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

3.  $K_{Tr}$  – совокупность требований по обеспечению конфиденциальности.

4.  $\Pi_{Tr}$  – совокупность требований по обеспечению целостности.

Обобщенная схема неуправляемых факторов приведена на рис. 2.



Рис. 2. Неуправляемые факторы, определяющие устойчивость объекта оценивания

**Ограничения**

1. При оценивании устойчивости объектов КИИ принимается, что возможность поражения элементов АСУ и ИС, на практике означает их стопроцентную готовность к информационному обмену.
2. Соответствие конфиденциальности информации требованиям на всем периоде воздействия угроз  $t \in (0, T]$ ,  $K(t) \in K_{Tr}$ , где  $K(t)$  – совокупность требований по обеспечению конфиденциальности реализованных в момент времени  $t \in (0, T]$ .
3. Соответствие целостности информации требованиям на всем периоде воздействия угроз  $t \in (0, T]$ ,  $\Pi(t) \in \Pi_{Tr}$ , где  $\Pi(t)$  – совокупность требований по обеспечению целостности информации реализованных в момент времени  $t \in (0, T]$ .



Рис. 3. Обобщенная схема ограничений, которые учитываются при оценке устойчивости

**Требуется разработать**

1. Семейство методов, моделей и средств математической обработки исходных данных (оператор) –  $\mathcal{M}$ , позволяющих получать количественные оценки показателей, характеризующих устойчивость функционирования элементов оцениваемого объекта, находящихся под воздействием угроз  $u \in U$

$$\{\varphi_k(u, t)\} = \mathcal{M}\{E(t_0), U, K_{Op}, P(u), T(u, t), \Theta(t), H(u), \hat{\Theta}\},$$

$t \in (0, T]$   
 $u \in U$   
 $K(t) \in K_{Tr}$   
 $\Pi(t) \in \Pi_{Tr}$

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

2. Семейство методов, моделей и средств математической обработки исходных данных (оператор) –  $\mathcal{B}$ , характеризующих семейство функций устойчивости отдельных элементов объекта оценивания  $\varphi_k(u, t)$  и ее структуру  $S(t)$  – и позволяющие получать количественную оценку, характеризующую устойчивость функционирования объекта оценивания в целом, находящуюся под воздействием угроз  $u \in U$

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

$$= \mathcal{B}\{\mathcal{M}\{E(t_0), U, K_{Op}, P(u), T(u, t), \Theta(t), H(u, t)\}, S(t), \hat{\Theta}\},$$

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

Функциональная схема математической модели оценивания устойчивости приведена на рис. 4. Исходные данные, характеризующие условия функционирования элементов объекта оценивания, добываются для каждого отдельного элемента при использовании как детерминированных методов, так и методов экспертного оценивания. Исходные данные вводятся для каждой частной математической модели элементов объекта оценивания. Зеленым цветом обозначены исходные данные, которые могут управляться ЛПР, красным цветом – неуправляемые исходные данные. Аналогично вводятся параметры, характеризующие ограничения. Каждая частная модель элементов в соответствии с линейными операторами  $\mathcal{M}_i$  преобразует исходные данные в поле принятых ограничений в функции устойчивости отдельных элементов, которые являются исходными данными для расчета функции устойчивости объекта оценивания в целом  $\Phi(t)$ . Для чего значения функций устойчивости отдельных элементов, совместно с показателями, характеризующими СОФ и ресурсные возможности СВФ подаются на вход математической

модели объекта оценивания, которая с помощью линейного оператора  $\mathcal{B}$  осуществляет преобразование исходных данных в значения функции устойчивости объекта оценивания.

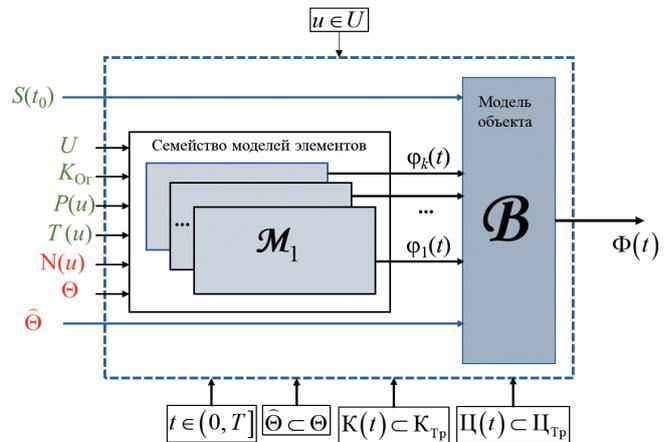


Рис. 4. Функциональная схема математической модели оценивания устойчивости

Зная количественные оценки экстремальных значений функции устойчивости и моментов времени их наступления, ЛПР представляется возможным обосновать принимаемое решение по обеспечению устойчивости функционирования объекта оценивания.

**Выводы**

В результате настоящего исследования предложены вербальная и формальная постановки научной задачи по оцениванию устойчивости функционирования объектов КИИ, элементы которых подвержены воздействию угроз их информационной безопасности. Обнаружена ограниченность существующих методов и моделей на решение задач оценивания устойчивости для условий штатной эксплуатации, которые без грубых допущений не могут быть применены для оценивания устойчивости функционирования КИИ, находящейся под воздействием угроз. Обнаружена противоречивая ситуация, когда возможности науки вступают в противоречие с потребностями практики и поставленная задача может позиционироваться как научная проблема, решение которой имеет важное экономическое значение. Для решения научной задачи были разработаны соответствующие методы и математические модели, которые опубликованы в [16–18]. Предполагается дальнейшие исследования направить на разработку формальных и экспертных методов формирования исходных данных.

При поддержке Фонда Потанина

## Литература

1. 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.
2. Зубков Е. А. Оценка киберустойчивости сетевой инфраструктуры с использованием распределенного механизма анализа и мониторинга / Е. А. Зубков, В. О. Ерастов, Д. П. Зегжда // Методы и технические средства обеспечения безопасности информации. – 2024. – № 33. – С. 14–16.
3. 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.
4. Израилов К. Е. Оценка и прогнозирование состояния сложных объектов: применение для информационной безопасности / К. Е. Израилов, М. В. Буйневич, И. В. Котенко, В. А. Десницкий // Вопросы кибербезопасности. – 2022. – № 6(52). – С. 2-21. – DOI 10.21681/23113456-6-2022-2-21.
5. Котенко И. В. Подсистема предупреждения компьютерных атак на объекты критической информационной инфраструктуры: анализ функционирования и реализации / И. В. Котенко, И. Б. Саенко, Р. И. Захарченко, Д. В. Величко // Вопросы кибербезопасности. – 2023. – № 1(53). – С. 13–27. – DOI 10.21681/2311-3456-2023-1-13-27.
6. 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.
7. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Научное издание, 2020. 337 с.
8. Стародубцев Ю. И. Концептуальные направления решения проблемы обеспечения устойчивости Единой сети электросвязи Российской Федерации / Ю. И. Стародубцев, С. А. Иванов, П. В. Закалкин // Военная мысль. – 2021. – № 4. – С. 39–49.
9. Стародубцев Ю. И. Кибероружие как основное средство воздействия на критическую инфраструктуру государств / Ю. И. Стародубцев, П. В. Закалкин, С. А. Иванов // Вестник Академии военных наук. – 2022. – № 1(78). – С. 24–32.
10. Язов Ю. К. Составные сети Петри-Маркова со специальными условиями построения для моделирования угроз безопасности информации / Ю. К. Язов, А. П. Панфилов // Вопросы кибербезопасности. – 2024. – № 2(60). – С. 53–65. – DOI 10.21681/2311-3456-2024-2-53-65.
11. Язов Ю. К., Соловьев С. В. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа. – СПб.: Научное издание, 2023. – 257 с.
12. Язов Ю. К. Основы теории составных сетей Петри-Маркова и их применения для моделирования процессов реализации угроз безопасности информации в информационных системах / Ю. К. Язов, А. В. Анищенко, А. С. Суховерхов. – Санкт-Петербург: Издательский дом «Сциентиа», 2024. – 194 с. – ISBN 978-5-605-21112-9. – DOI 10.32415/scientia\_978-5-6052111-2-9.
13. Шубинский И. Б. О функциональной безопасности сложной технической системы управления с цифровыми двойниками / И. Б. Шубинский, Х. Шебе, Е. Н. Розенберг // Надежность. – 2021. – Т. 21, № 1. – С. 38–44. – DOI 10.21683/1729-2646-2021-21-1-38-44.
14. Shubinsky I. B. Methods for ensuring and proving functional safety of automatic train operation systems / I. B. Shubinsky, E. N. Rozenberg, H. Schabe // Reliability: Theory & Applications. – 2024. – Vol. 19, No. 1(77). – P. 360–375. – DOI 10.24412/1932-2321-2024-177-360-375.
15. Shubinsky, I. B. Innovative methods of ensuring the functional safety of train control systems / I. B. Shubinsky E. N. Rozenberg, H. Schabe // Reliability: Theory & Applications. – 2023. – Vol. 18, No. 4(76). – P. 909–920. – DOI 10.24412/1932-2321-2023-476-909-920.
16. 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.
17. 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.org/10.15622/ia.23.3.1.
18. 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.

## ON THE FORMULATION OF THE TASK OF ASSESSING THE STABILITY OF THE FUNCTIONING OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

Voevodin V. A.<sup>7</sup>

**Keywords:** threats of information security violations, a system for restoring functionality, critical information infrastructure, recoverability, protection from threats, a renewable resource, a non-renewable resource.

<sup>7</sup> Vladislav A. Voevodin, Ph.D. in Technical Sciences, MIET, Moscow, Russia. E-mail: vva541@mail.ru. AuthorID: 1012813, ORCID 0009-0003-9431-1685.

**The purpose of the study:** is to substantiate the relevance, formulate and formalize the scientific task of quantifying the stability of the functioning of a critical information infrastructure in relation to the conditions of exposure to threats of violation of its information security.

**Research methods:** system analysis, analysis of a scientific problem, formalization of scientific knowledge, methodology of scientific research.

**The results obtained:** the verbal and formal statements of the scientific problem are formulated.

**Scientific novelty:** the author's approach to assessing the dynamics of the stability of the functioning of critical information infrastructure in the face of threats, taking into account the available resource, is proposed.

**Practical significance:** The developed formulation of the scientific problem can serve as the basis for the formulation of the terms of reference for the development of methods, models and tools for quantifying the stability of the functioning of objects of critical information structure operating under the influence of threats.

## References

1. Voevodin V. A. *Genezis ponjatija strukturnoj ustojchivosti informacionnoj infrastruktury avtomatizirovannoj sistemy upravlenija proizvodstvennymi processami k vozdejstvu celenapravlennoj ugroz informacionnoj bezopasnosti*. Vestnik Voronezhskogo instituta FSIN Rossii, 2023, № 2, aprel'-ijun'. – S. 30–41.
2. Zubkov E. A. *Ocenka kiberustojchivosti setевой infrastruktury s ispol'zovaniem raspredelennogo mehanizma analiza i monitoringa* / E. A. Zubkov, V. O. Erastov, D. P. Zegzhda // *Metody i tehicheskie sredstva obespechenija bezopasnosti informacii*. – 2024. – № 33. – S. 14–16.
3. Zegzhda D. P. *Kiberbezopasnost' cifrovoj industrii. Teorija i praktika funkcional'noj ustojchivosti k kiberatakam* / pod red. D. P. Zegzhdy. – M.: Gorjachaja linija – Telekom. 2022. – 560 s.
4. Izrailov K. E. *Ocenivanie i prognozirovanie sostojanija slozhnyh ob#ektov: primenenie dlja informacionnoj bezopasnosti* / K. E. Izrailov, M. V. Bujnevich, I. V. Kotenko, V. A. Desnickij // *Voprosy kiberbezopasnosti*. – 2022. – № 6(52). – S. 2-21. – DOI 10.21681/23113456-6-2022-2-21.
5. Kotenko I. V. *Podsystema preduprezhdenija komp'juternyh atak na ob#ekty kriticheskoj informacionnoj infrastruktury: analiz funkcionirovanija i realizacii* / I. V. Kotenko, I. B. Saenko, R. I. Zaharchenko, D. V. Velichko // *Voprosy kiberbezopasnosti*. – 2023. – № 1(53). – S. 13–27. – DOI 10.21681/2311-3456-2023-1-13-27.
6. Konovalenko S. A. *Metodika ocenivanija funkcional'noj ustojchivosti geterogennoj sistemy obnaruzhenija, preduprezhdenija i likvidacii posledstvij komp'juternyh atak* // *Sistemy upravlenija, svjazi i bezopasnosti*. 2023. № 4. S. 157-195. doi: 10.24412/2410-9916-2023-4-157-195.
7. Makarenko S. I. *Modeli sistemy svjazi v uslovijah prednamerennyh destabilizirujushhh vozdeystvij i vedenija razvedki*. Monografija. – SPb.: Naukoemkie tehnologii, 2020. 337 s.
8. Starodubcev Ju. I. *Konceptual'nye napravlenija reshenija problemy obespechenija ustojchivosti Edinoj seti jelektrosvjazi Rossijskoj Federacii* / Ju. I. Starodubcev, S. A. Ivanov, P. V. Zakalkin // *Voennaja mysl'*. – 2021. – № 4. – S. 39–49.
9. Starodubcev Ju. I. *Kiberoruzhie kak osnovnoe sredstvo vozdeystvija na kriticheskiju infrastrukturu gosudarstv* / Ju. I. Starodubcev, P. V. Zakalkin, S. A. Ivanov // *Vestnik Akademii voennyh nauk*. – 2022. – № 1(78). – S. 24–32.
10. Jazov Ju. K. *Sostavnye seti Petri-Markova so special'nymi uslovijami postroenija dlja modelirovanija ugroz bezopasnosti informacii* / Ju. K. Jazov, A. P. Panfilov // *Voprosy kiberbezopasnosti*. – 2024. – № 2(60). – S. 53–65. – DOI 10.21681/2311-3456-2024-2-53-65.
11. Jazov Ju. K., Solov'ev S. V. *Metodologija ocenki jeffektivnosti zashhity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa*. – SPb.: Naukoemkie tehnologii. 2023. – 257 s.
12. Jazov Ju. K. *Osnovy teorii sostavnyh setej Petri-Markova i ih primenenija dlja modelirovanija processov realizacii ugroz bezopasnosti informacii v informacionnyh sistemah* / Ju. K. Jazov, A. V. Anishhenko, A. S. Suhoverhov. – Sankt-Peterburg : Izdatel'skij dom «Scientia», 2024. – 194 s. – ISBN 978-5-605-21112-9. – DOI 10.32415/scientia\_978-5-60521112-9.
13. Shubinskij I. B. *O funkcional'noj bezopasnosti slozhnoj tehicheskoj sistemy upravlenija s cifrovymi dvojniki* / I. B. Shubinskij, H. Shebe, E. N. Rozenberg // *Nadezhnost'*. – 2021. – T. 21, № 1. – S. 38–44. – DOI 10.21683/1729-2646-2021-21-1-38-44.
14. Shubinsky I. B. *Methods for ensuring and proving functional safety of automatic train operation systems* / I. B. Shubinsky, E. N. Rozenberg, H. Schabe // *Reliability: Theory & Applications*. – 2024. – Vol. 19, No. 1(77). – P. 360–375. – DOI 10.24412/1932-2321-2024-177-360-375.
15. Shubinsky, I. B. *Innovative methods of ensuring the functional safety of train control systems* / I. B. Shubinsky E. N. Rozenberg, H. Schabe // *Reliability: Theory & Applications*. – 2023. – Vol. 18, No. 4(76). – P. 909–920. – DOI 10.24412/1932-2321-2023-476-909-920.
16. Voevodin V. A. *Model' ocenki funkcional'noj ustojchivosti informacionnoj infrastruktury dlja uslovij vozdeystvija mnozhestva komp'juternyh atak* // *Informatika i avtomatizacija*. 2023. № 22(3). S. 691–715. DOI 10.15622/ia.22.3.8.
17. Voevodin V. A. *Chastnaja polumarkovskaja model' kak instrument snizhenija slozhnosti zadachi ocenivanija ustojchivosti funkcionirovanija jelementov informacionnoj infrastruktury, podverzhenoj vozdejstvu ugroz* // *Informatika i avtomatizacija*. 2024. № 23(3). S. 611–642. doi.org/10.15622/ia.23.3.1.
18. Voevodin V. A., Krahotin N. A. *Metody ocenivanija svjaznosti neorientirovannogo duvopoljusnogo pomechennogo grafa s uchetom destruktivnogo vozdeystvija vneshnih ugroz na ego vershiny* // *Vestnik Dagestanskogo gosudarstvennogo tehicheskogo universiteta. Tehicheskie nauki*. 2024. № 51(1). S. 46–60. doi:10.21822/2073-6185-2024-51-1-46-60.

