МОДЕЛЬНО-АЛГОРИТМИЧЕСКОЕ И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ КОСМИЧЕСКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ

УДК 62-519; 629.3.076
DOI: 10.17586/0021-3454-2018-61-7-559-565

ФУНКЦИОНАЛЬНАЯ УСТОЙЧИВОСТЬ НАВИГАЦИОННО-ИНФОРМАЦИОННЫХ СИСТЕМ

А. Н. Королев

„НИИ КС имени А. А. Максимова“ – филиал АО „ГКНПЦ им. М. В. Хруничева“,
141091, Московская область, г. Королев, Россия
E-mail: niiks@khrunichev.com

Рассматриваются вопросы формального описания свойства функциональной устойчивости навигационно-информационных систем на основе использования понятий качества реализации выполняемых ими функций с учетом состояния доступных навигационных полей и применяемых систем подвижной радиосвязи. Под навигационно-информационной системой (НИС) понимают автоматизированную информационно-управляющую систему, предназначенную для управления одним или несколькими подвижными объектами на основе обработки данных о их местоположении, параметрах движения и состоянии. Представлена графическая интерпретация процесса обеспечения функциональной устойчивости системы. Обеспечение функциональной устойчивости НИС сводится к процессу поддержания текущего вектора качества выполнения функций НИС в требуемой зоне.

Ключевые слова: *навигационно-информационная система, функциональная устойчивость, надежность, живучесть, безопасность*

Под навигационно-информационной системой (НИС) понимают автоматизированную информационно-управляющую систему (ИУС), предназначенную для управления одним или несколькими подвижными объектами на основе обработки данных об их местоположении, параметрах движения и состоянии.

Процесс функционирования НИС заключается в выполнении совокупности функций, реализующих требования по назначению. Совокупность свойств продукции, обусловливающих ее пригодность к удовлетворению определенных потребностей в соответствии с назначением, является качеством[*], следовательно, эффективность НИС можно рассматривать как отношение качества ее функционирования к затратам. Отличительной чертой высокоэффективных НИС является значительное доминирование качества функционирования над совокупными затратами на разработку, изготовление, эксплуатацию и утилизацию системы.

Всегда существует угроза деструктивных воздействий на реальные системы со стороны

[*] ГОСТ 15467-79 Управление качеством продукции. Основные понятия. Термины и определения. Изд-во стандартов, 1991.

внешней среды, персонала или действий, вызванных конструктивными дефектами аппаратных или программных средств, отказами технических средств, недостоверностью или недостаточностью данных в информационных ресурсах системы, в результате которых система может потерять возможность выполнения требуемых функций с заданным уровнем характеристик. Обеспечение работоспособности любой сложной системы, какой является НИС, основывается на следующих постулатах:

1) любые элементы (ресурсы) системы под действием деструктивных воздействий могут переходить в состояние отказа;

2) переход элементов системы в состояние отказа не должен приводить к отказу системы в целом.

Первоначально модель создания эффективных сложных систем связывалась с обеспечением их надежного функционирования и была сформулирована Фон Нейманом в середине XX века как конструирование *„надежной системы из ненадежных элементов“* [1]. Последующие тридцать лет на основе указанной модели интенсивно развивались методы аппаратного резервирования, предусматривающие для поддержания требуемого уровня характеристик надежности введение в состав системы аппаратной избыточности путем включения запасных (резервных) элементов и связей, дополнительных по сравнению с составом системы, выполняющей те же функции в условиях отсутствия деструктивных воздействий.

С 1980-х гг. в связи с развитием и усложнением программного обеспечения ИУС значимость программных отказов как фактора ненадежности системы резко возрастает. При этом резко снижается эффективность применения ставших уже традиционными методов резервирования аппаратно-программных модулей в системе. Это обусловлено тем, что программные отказы, в отличие от аппаратных, связаны, прежде всего, с ошибками проектирования, и соответственно при резервировании тиражируются на запасные модули. Соответственно программный отказ наступает одновременно во всех идентичных модулях, решающих одну задачу, что неминуемо ведет к выходу из строя системы в целом. В это же время формируется единый подход к созданию механизмов обеспечения надежности и безопасности.

На основе принципа многоверсионного проектирования и реализации компьютерных систем вводится понятие гарантоспособных вычислений [2], а в начале XXI в. — и гарантоспособных систем, обладающих свойствами надежности, живучести и безопасности [3—5]. В результате исходная модель была преобразована в *„гарантоспособные системы из ненадежных аппаратных и программных элементов“*.

Дальнейшее развитие ИУС показало, что и эта модель имеет существенные ограничения в применении. Во-первых, кроме аппаратных и программных средств в состав системы входит ее информационное обеспечение. При полностью работоспособных средствах система может отказать вследствие снижения или потери полноты, достоверности, точности, актуальности, полезности и ценности информации. Особенно актуально это для навигационно-информационных систем, где неоднородность навигационных полей является одним из наиболее критичных факторов возникновения информационных отказов в системе. Во-вторых, автоматизированная система, в соответствии с определением, помимо средств автоматизации в свой состав включает персонал, который сам по себе, вообще говоря, является ненадежным и небезопасным. Таким образом, к ненадежным и небезопасным аппаратным средствам, ненадежным программным средствам, из которых создается НИС, следует добавить ненадежное информационное обеспечение и возможные отказы по вине персонала.

Введем понятие *ресурса*, под которым будем понимать средства, запасы, возможности, источники средств — все, что используется и расходуется в процессе функционирования НИС. Тогда все элементы НИС можно разбить на четыре типа ресурсов:

1) аппаратные — технические средства, входящие в состав НИС;

2) программные — программное обеспечение составных частей НИС;

3) информационные — информация, созданная и (или) обнаруженная, зарегистрированная, оцененная, с определенными (заданными) законами деградации и обновления [6];

4) трудовые — персонал, реализующий информационную технологию выполнения возложенных на НИС функций.

НИС относятся к классу целенаправленных систем, цель функционирования которых состоит в выполнении заданного набора функций с требуемым качеством. Сохранение (автоматическое восстановление) возможности выполнения полного или приемлемого набора функций в условиях деструктивных воздействий обеспечивается функциональной устойчивостью системы, что позволяет потребителю гарантированно доверять ее услугам. Таким образом, на современном этапе модель эффективного функционирования НИС может быть сформулирована как конструирование *„функционально устойчивых систем из ненадежных и небезопасных ресурсов“*.

Переход от надежных к функционально устойчивым системам обусловлен факторами, связанными с чрезмерным ростом размерности современных систем. Построение надежных систем базировалось на ряде допущений, которые для сложных человеко-машинных комплексов являются неоправданно сильными. К числу таких допущений относится, например, наличие биективного отображения множества векторов допустимых параметров во множество работоспособных состояний системы. Однако на практике при большом количестве параметров даже нахождение всех их в заданных пределах не гарантирует выполнения заданной функции, так как на этапе проектирования системы невозможно проверить правильность функционирования при всех возможных сочетаниях параметров, находящихся в заданных пределах, но при этом отдельные сочетания параметров способны привести к фатальным последствиям. Переход от управления ресурсами по обеспечению надежности к управлению ресурсами по обеспечению функциональной устойчивости аналогичен переходу от функциональных к терминальным методам управления объектами при выведении в заданную точку пространства [7].

В работе [8] свойство функциональной устойчивости НИС формализовано на основе понятия качества выполняемых системой функций.

Определение. НИС является функционально устойчивой на интервале времени Δt, если при любом наборе деструктивных воздействий $R_{\Delta t}$ существует хотя бы одно работоспособное распределение ресурсов НИС, обеспечивающее с учетом имеющегося на этом интервале состояния навигационного и связного полей реализацию набора функций F с уровнем качества не ниже $\mathbf{a}_{\lim}$

$$\forall\left(R_{\Delta t}\in R, e_m^N\in E_{\Delta t}^N, e_m^G\in E_{\Delta t}^G\right), \exists k^*\left(Z_{\Delta t}\right)\in K, <k^*, e_m^N, e_m^G> \Rightarrow \mathbf{a}_{k^*}\succeq \mathbf{a}_{\lim},$$

где $R_{\Delta t}$ — подмножество действующих на интервале времени Δt на НИС деструктивных воздействий из множества R деструктивных воздействий, которые могут воздействовать на систему; $E_{\Delta t}^N=\left\{e_m^N\right\}$ — подмножество уровней качества пространственно-временной идентификации объектов в НИС на интервале времени Δt, формируемое из упорядоченного конечного множества E^N уровней качества пространственно-временной идентификации объектов управления в НИС, с учетом доступных НИС навигационных полей, действующих деструктивных воздействий $R_{\Delta t}$ и перемещения объектов НИС на интервале времени Δt; $E_{\Delta t}^G=\left\{e_m^G\right\}$ — подмножество уровней качества информационного обмена в НИС на интервале времени Δt, формируемое из упорядоченного конечного множества E^G уровней качества информационного обмена в НИС, с учетом доступных НИС систем мобильной связи, деструктивных воздействий $R_{\Delta t}$ и перемещения объектов НИС на интервале времени Δt; $Z_{\Delta t}$ — подмножество

ресурсов (аппаратных, программных, информационных и трудовых), остающихся в распоряжении НИС при воздействии деструктивных воздействий $R_{\Delta t}$ на интервале времени Δt, из множества $Z=\{z_i\}$ ресурсов полностью исправной НИС; $K=\{k_l\}$, $k_l =< Z_l^1, Z_l^2, \ldots, Z_l^N >$, $Z_l^i \subset Z$ — множество распределений ресурсов НИС по N функциям набора функций F, реализующих требования по назначению; $\mathbf{a}_{k^*}$ — вектор уровня качества реализации набора функций F НИС при распределении ресурсов в ней k^* и текущих уровнях качества пространственно-временной идентификации объектов e_m^N и информационного обмена e_m^G в НИС, исходя из ее пространственно-временной конфигурации на интервале времени Δt; $\mathbf{a}_{\lim}$ — предельный уровень качества реализации набора функций F НИС, ниже которого функционирование системы не удовлетворяет требованиям по назначению.

Каждый вектор $\mathbf{a}_i$ представляет собой набор $\left\langle q_{i_1}^1, q_{i_2}^2, \ldots, q_{i_N}^N \right\rangle$ длины N (где N — количество реализуемых функций НИС в соответствии с требованиями по назначению), причем каждый элемент q_i^j представляет собой некоторый уровень качества реализации j-й функции и принадлежит множеству Q^j, которое, в свою очередь, представляет собой частично упорядоченное конечное множество возможных уровней качества реализации j-й функции $Q^j = \left\{ q_1^j, q_2^j, \ldots, q_{L_j}^j \right\}$.

Для реализуемого НИС набора функций F существует множество Q уровней качества функционирования НИС, состоящее из непересекающихся подмножеств $\left\{ Q^1, Q^1, \ldots, Q^N, \right\}$ с элементами $q_i^j \in Q^j$, $j=\overline{1,N}$, упорядоченными согласно условию

$$q_1^j \le q_2^j \le \ldots \le q_{L_j}^j, j=\overline{1,N},$$

где q_1^j — минимальный уровень качества реализации j-й функции, соответствующий невыполнению функции; $q_{L_j}^j$ — максимальный уровень качества, с которым НИС теоретически может реализовывать j-ю функцию; L_j — количество градаций уровня качества выполнения j-й функции.

Множество Q является частично упорядоченным и его удобно записывать в виде квазиматрицы N-го порядка со строками — упорядоченными множествами Q^j [9]:

$$Q = \begin{Vmatrix} q_1^1 & \cdots & q_{L_1}^1 \\ \vdots & \ddots & \vdots \\ q_1^N & \cdots & q_{L_N}^N \end{Vmatrix} = \left\| q_j^i \right\|, \; i=\overline{1,N}, \; j=\overline{1,L_i}.$$

Множество векторов уровней качества реализации набора функций F НИС $A=\{\mathbf{a}_i\}$ также является частично упорядоченным, причем для любых двух векторов $\mathbf{a}_i$ и $\mathbf{a}_j$ вектор $\mathbf{a}_i$ предпочтительнее $\mathbf{a}_j$, если для каждой задачи f_m из набора F качество ее реализации q_i^m, принадлежащее вектору $\mathbf{a}_i$, не хуже качества реализации этой функции q_j^m, принадлежащего вектору $\mathbf{a}_j$:

$$\mathbf{a}_i \succeq \mathbf{a}_j : \forall \left(q_{k_l}^l \in \mathbf{a}_i, q_{m_l}^l \in \mathbf{a}_j, l=\overline{1,N} \right) (k_l \ge m_l).$$

Кроме того, на множестве A введена метрика, такая, что расстояние между двумя векторами этого множества равно минимальной разности между индексами уровней качества реализации каждой функции из набора F, являющихся элементами этих векторов

$$\forall\left(\mathbf{a}_i,\mathbf{a}_j\in A,\mathbf{a}_i\succeq\mathbf{a}_j\right)d\left(\mathbf{a}_i,\mathbf{a}_j\right)=\min_l\left(k_l-m_l\right),q_{k_l}^l\in\mathbf{a}_i,q_{m_l}^l\in\mathbf{a}_j,L=\overline{1,N}.$$

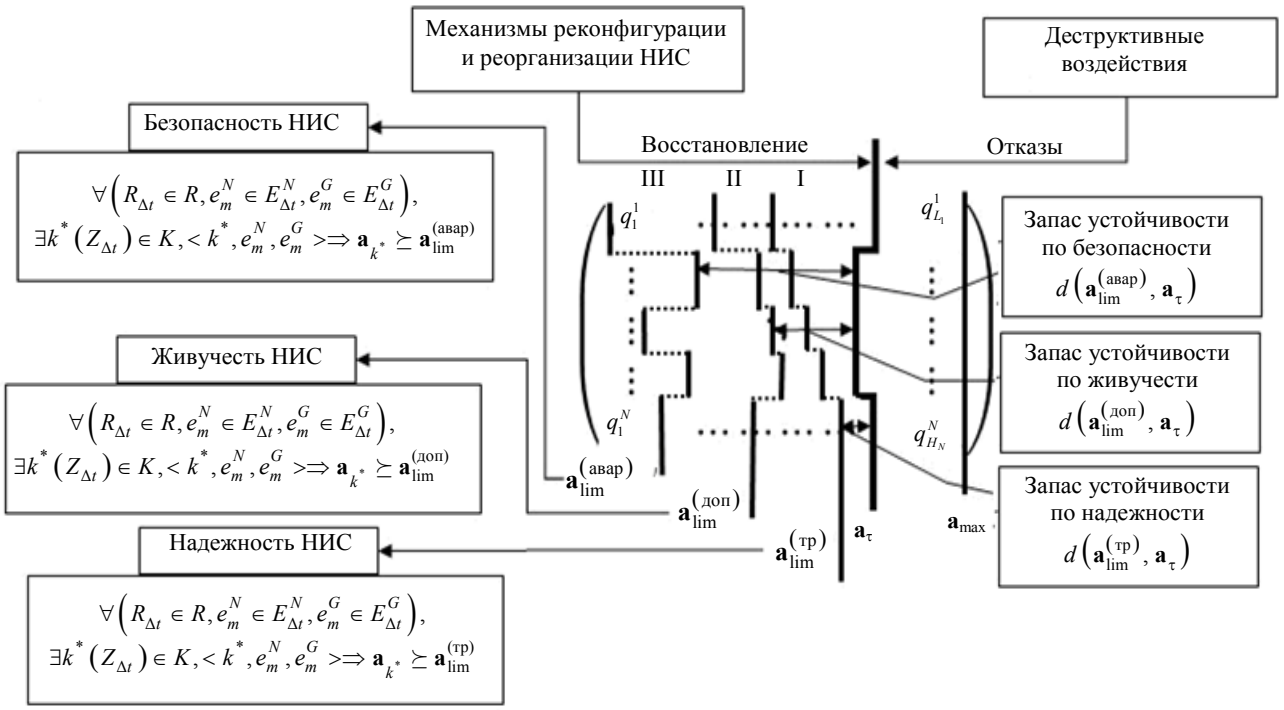
Исходя из приведенных определений можно интерпретировать $\mathbf{a}_{\lim}$ как *границу функциональной устойчивости* НИС к деструктивным воздействиям из R, а расстояние $d\left(\mathbf{a}_{\lim},\mathbf{a}\left(k^*\right)\right)$ — как *запас функциональной устойчивости* НИС для распределения ресурсов НИС k^*.

Следует отметить, что, меняя требования к границе функциональной устойчивости $\mathbf{a}_{\lim}$, можно решать локальные задачи по построению:

надежных $\left(\mathbf{a}_{\lim}=\mathbf{a}_{\lim}^{(\text{тр})}\right)$, живучих $\left(\mathbf{a}_{\lim}=\mathbf{a}_{\lim}^{(\text{доп})}\right)$ и безопасных $\left(\mathbf{a}_{\lim}=\mathbf{a}_{\lim}^{(\text{авар})}\right)$ НИС,

$\mathbf{a}_{\lim}^{(\text{тр})}$ — минимальный уровень качества реализации функций *F*, при котором НИС сохраняет во времени в установленных пределах значения всех параметров, характеризующих способность выполнять свои функции в заданных режимах и условиях эксплуатации; $\mathbf{a}_{\lim}^{(\text{доп})}$ — минимальный уровень качества реализации функций *F*, при котором НИС сохраняет способность выполнять установленный объем функций системы в заданных пределах; $\mathbf{a}_{\lim}^{(\text{авар})}$ — минимальный уровень качества реализации функций *F*, при котором НИС не создает угрозу для жизни и здоровья людей, а также для окружающей среды.

Графическая интерпретация процесса обеспечения функциональной устойчивости НИС приведена на рисунке.



На квазиматрице *Q* уровней качества реализации функций *F* НИС показаны векторы: $\mathbf{a}_{\lim}^{(\text{тр})}$, $\mathbf{a}_{\lim}^{(\text{доп})}$, $\mathbf{a}_{\lim}^{(\text{авар})}$, а также $\mathbf{a}_\tau$, определяющий уровень качества выполнения задач в текущий момент времени τ, и $\mathbf{a}_{\max}$, определяющий максимально возможный уровень качества выполнения задач при функционировании НИС.

Расстояния между вектором $\mathbf{a}_\tau$ и границами функциональной устойчивости определяют запасы устойчивости по надежности, живучести и безопасности соответственно.

Поток деструктивных воздействий вызывает отказы в НИС, в результате чего с течением времени вектор $\mathbf{a}_\tau$ сдвигается влево по квазиматрице Q, приводя к снижению запасов устойчивости или полностью к потере соответствующего свойства НИС. В результате восстановления (автоматического, на основе механизмов реконфигурации и/или реорганизации ресурсов системы, или путем введения дополнительных ресурсов извне) вектор $\mathbf{a}_\tau$ сдвигается вправо по квазиматрице Q, что, в свою очередь, приводит к восстановлению свойств или к увеличению запасов устойчивости НИС. Можно выделить три зоны, в которых перемещается вектор $\mathbf{a}_\tau$.

Если объем ресурсов и механизмов реконфигурации и/или реорганизации этих ресурсов достаточен для того, чтобы вектор $\mathbf{a}_\tau$ находился

— в зоне I — между векторами $\mathbf{a}_{\lim}^{(\text{тр})}$ и $\mathbf{a}_{\max}$ $\left(\mathbf{a}_{\lim}^{(\text{тр})} \succeq \mathbf{a}_\tau \succeq \mathbf{a}_{\max}\right)$, то система надежна;

— в зоне II — между векторами $\mathbf{a}_{\lim}^{(\text{доп})}$ и $\mathbf{a}_{\max}$ $\left(\mathbf{a}_{\lim}^{(\text{доп})} \succeq \mathbf{a}_\tau \succeq \mathbf{a}_{\max}\right)$, то система обладает живучестью;

— в зоне III — зона между векторами $\mathbf{a}_{\lim}^{(\text{авар})}$ и $\mathbf{a}_{\max}$ $\left(\mathbf{a}_{\lim}^{(\text{авар})} \succeq \mathbf{a}_\tau \succeq \mathbf{a}_{\max}\right)$, то система безопасна.

Следует отметить, что если ставится задача функционирования НИС только в зоне I, то такая НИС является системой, не допускающей редукцию, и, напротив, если она допускает функционирование также в зонах II, III — то это система с редукцией.

Таким образом, в настоящей работе для формализации описания свойства функциональной устойчивости навигационно-информационных систем сформулировано понятие вектора качества реализации выполняемых НИС функций с учетом состояния доступных навигационных полей и используемых систем подвижной радиосвязи. Показано, что процесс обеспечения функциональной устойчивости НИС сводится к поддержанию текущего вектора качества выполнения функций НИС в требуемых интервалах в заданный период времени. Для осуществления такого процесса в составе НИС необходимы специальные средства и механизмы реконфигурации и реорганизации ресурсов системы, обеспечивающие в условиях деструктивных воздействий требуемый уровень качества реализации функций НИС.

СПИСОК ЛИТЕРАТУРЫ

1. *Нейман Дж.* Вероятностная логика и синтез надежных организмов из ненадежных компонент // Автоматы / Под ред. *К. Э. Шеннона* и *Дж. Маккарти*. М.: ИЛ, 1956. С. 129—185.

2. *Авиженис А., Лапри Ж. К.* Гарантоспособные вычисления: от идеи до реализации в проектах // ТИИЭР. 1986. Т. 71, № 5. С. 8—21.

3. *Харченко В. С.* Гарантоспособность и гарантоспособные системы: элементы методологии // Радіоелектронні і комп'ютерні системи. 2006. № 5. С. 7—19.

4. *Харченко В. С.* Парадигмы и принципы гарантоспособных вычислений: состояние и перспективы развития // Радіоелектронні і комп'ютерні системи. 2009. № 2(36). С. 91—100.

5. *Теслер Г. С.* Концепция построения гарантоспособных вычислительных систем // Математичні машини і системи. 2006. № 1. С. 134—145.

6. *Ковалева Н. Н.* Информационное право России. М.: Дашков и К., 2008. 359 с.

7. *Разоренов Г. Н., Бахрамов Э. А., Титов Ю. Ф.* Системы управления летательными аппаратами (баллистическими ракетами и их головными частями): Учеб. для вузов. М.: Машиностроение, 2003. 584 с.

8. *Королев А. Н., Тарасов А. А.* О функциональной устойчивости навигационно-информационных систем // Вестн. РГГУ. Сер. „Информатика. Защита информации. Математика". 2012. № 14/12. С. 144—152.

9. *Левин В. И.* Логическая теория надежности сложных систем. М.: Энергоатомиздат, 1985. 128 с.

Сведения об авторе

Александр Николаевич Королев — канд. техн. наук, старший научный сотрудник; „НИИ КС имени А. А. Максимова“ – филиал АО „ГКНПЦ им. М. В. Хруничева“; первый заместитель директора, главный конструктор;
E-mail: niiks@khrunichev.com

Поступила в редакцию
26.02.18 г.

Ссылка для цитирования: *Королев А. Н.* Функциональная устойчивость навигационно-информационных систем // Изв. вузов. Приборостроение. 2018. Т. 61, № 7. С. 559—565.

FUNCTIONAL STABILITY OF NAVIGATION INFORMATION SYSTEMS

A. N. Korolev

A. A. Maksimov Space Systems Research Institute − Branch of Khrunichev State Research and Production Space Center JSC, 141091, Moscow Region, Korolev, Russia
E-mail: niiks@khrunichev.com

The problems of formal description of the functional stability of navigation and information systems are considered using the concepts of the quality of the functions performed by them, taking into account the status of available navigation fields and the mobile radio systems used. The navigation information system is an automated information management system designed to control one or more mobile objects based on processing of their location, traffic parameters and status. A graphic interpretation of the process of ensuring the functional stability of the system is presented. Ensuring the functional sustainability of the navigation information system is reduced to the process of maintaining the current quality vector for performing the system functions in the required area.

Keywords: information navigation system, functional stability, reliability, survivability, safety

REFERENCES

1. Von Neumann J. *Probabilistic logics and the synthesis of reliable organism from unreliable components*; Automata studies, NY, Princeton, 1956, pp. 45–98.
2. Avizhenis A.N., Lapri Zh.K. *Trudy instituta inzhenerov po elektrotekhnike i radioelektronike*, 1986, no. 5, pp. 8–21 (in Russ.)
3. Kharchenko V.S. *Radioyelektronni i komp'yuterni sistemi*, 2006, no. 5, pp. 7–19 (in Russ.)
4. Kharchenko V.S. *Radioyelektronni i komp'yuterni sistemi*, 2009, no. 2(36), pp. 91–100 (in Russ.)
5. Tesler G.S. *Matematichni mashini i sistemi*, 2006, no. 1, pp. 134–145. (in Russ.)
6. Kovaleva N.N. *Informatsionnoye pravo Rossii* (Russian Information Law), Moscow, 2008, 359 p. (in Russ.)
7. Razorenov G.N., Bakhramov E.A., Titov Yu.F. *Sistemy upravleniya letatel'nymi apparatami* (ballisticheskimi raketami i ikh golovnymi chastyami) (Control Systems of Aircraft (Ballistic Missiles and Their Head Parts)), Moscow, 2003, 584 p. (in Russ.)
8. Korolev A.N., Tarasov A.A. *RSUH/RGGU Bulletin. Records Management and Archival Studies. Computer Science. Data Protection and Information Security*, 2012, pp. 144–152. (in Russ.)
9. Levin V.I. *Logicheskaya teoriya nadezhnosti slozhnykh sistem* (Logical Theory of Reliability of Complex Systems), Moscow, 1985, 128 p. (in Russ.)

Data on author

Alexander N. Korolev — PhD, Senior Scientist; A. A. Maksimov Space Systems Research Institute − Branch of Khrunichev State Research and Production Space Center JSC; First Deputy Director, Chief Designer;
E-mail: niiks@khrunichev.com

For citation: Korolev A. N. Functional stability of navigation information systems. *Journal of Instrument Engineering*. 2018. Vol. 61, N 7. P. 559—565 (in Russian).

DOI: 10.17586/0021-3454-2018-61-7-559-565