

## ОПРЕДЕЛЕНИЕ КАТЕГОРИИ УСТОЙЧИВОСТИ ДЛЯ РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

**А. А. Толмачев<sup>1</sup>, М. А. Прохоров<sup>2</sup>, А. С. Андрианов<sup>2</sup>**

<sup>1</sup>Военная академия воздушно-космической обороны имени Маршала Советского Союза Г. К. Жукова,  
г. Тверь, Российская Федерация

<sup>2</sup>Военно-космическая академия имени А. Ф. Можайского,  
г. Санкт-Петербург, Российская Федерация

*В настоящее время космические системы и средства стали одним из основных инструментов обеспечения боевой и повседневной деятельности вооруженных сил развитых государств мира. В современных условиях космические системы встают в ряд стратегических компонент, устойчивость функционирования которых критична для сохранения военно-стратегического равновесия. Анализ конфликтов последних десятилетий показал тенденцию к смещению противоборства в космическую сферу и киберпространство. Космические системы и средства позволяют существенно повысить боевые возможности войск, а государство, не обладающее возможностью использования средств вооруженной борьбы, размещенных в воздушно-космической сфере, или допустившее просчеты в политике развития и использования своих космических систем и средств, будет обречено на гарантированное поражение в будущих военных конфликтах. Обороноспособность и безопасность Российской Федерации непосредственно зависят от состояния и возможностей средств стратегического предупреждения о подготовке к агрессии, начале ракетно-ядерного нападения, а также качества всестороннего обеспечения космическими силами и средствами армии и флота в мирное и военное время. В связи с этим появилась необходимость осуществить корректировку содержания категории устойчивости функционирования распределенных автоматизированных систем управления.*

*Ключевые слова: требование, устойчивость, разведзащищенность, распределенная автоматизированная система управления, космические системы, информационное противоборство, космические средства.*

### Введение

Особая роль в концепциях войн нового поколения отводится космическим системам и средствам (КСС). Уже сегодня КСС стали одним из основных инструментов стратегического сдерживания и обеспечения боевой и повседневной деятельности вооруженных сил развитых государств мира [1]. Анализ опыта применения космических систем обеспечения боевых действий показывает, что, во-первых, КСС позволяют существенно повысить боевые возможности войск (примерно в 1,5–2,0 раза), и, во-вторых, государство, не обладающее возможностью использования средств вооруженной борьбы, размещенных в воздушно-космической сфере, или допустившее просчеты

в политике развития и использования своих КСС, будет обречено на гарантированное поражение в будущих военных конфликтах [2].

Безопасность и обороноспособность Российской Федерации непосредственно зависят от возможностей и состояния средств стратегического предупреждения о подготовке к агрессии, начале ракетно-ядерного нападения, а также качества всестороннего обеспечения космическими силами и средствами армии и флота в мирное и военное время.

Таким образом, в современных условиях КСС встают в ряд стратегических компонент, паритет в которых критичен для сохранения военно-стратегического равновесия.

Реализация возможностей КСС обеспечения боевых действий, боевого применения войск (сил) ВС РФ во многом определяется качественным состоянием технической основы их системы управ-

ления – распределенными автоматизированными системами управления (РАСУ), посредством которых осуществляется управление орбитальными группировками космических аппаратов военного и двойного назначения [3].

В связи с важностью решаемых задач к РАСУ предъявляются жесткие требования по качеству функционирования, а именно по их устойчивости. Таким образом, необходимо определить содержание категории устойчивости процесса функционирования РАСУ, входящей в состав КСС.

### Определение категории устойчивости распределенных автоматизированных систем управления

С общефилософской точки зрения устойчивость задает меру изменчивости. В результате превышения меры происходит скачкообразный переход – революция с последующими качественными изменениями той или иной системы. Рассматривая этот процесс в рамках функционирования РАСУ, революцию процесса справедливо воспринимать как деструкцию, то есть переход к непригодно новому состоянию, разрушение заданных, необходимых свойств [4].

В процессе функционирования на РАСУ оказывают влияние дестабилизирующие факторы, к которым относят [5]:

- эксплуатационно-технические отказы элементов системы;
- стихийные и преднамеренные воздействия на элементы системы;
- естественные помехи, приводящие к искажению информации.

РАСУ считается устойчивой, когда под действием дестабилизирующих факторов, приводящих к снижению эффективности, осуществляется чисто тождественное изменение или так называемое ноль-преобразование. Порождение тождественного преобразования происходит при помощи компенсирующих механизмов.

Под компенсирующим механизмом понимают свойство или совокупность свойств, реализующие процессы, посредством которых нейтрализуются негативные последствия воздействий с целью сохранения устойчивости системы [6].

Исходя из обозначенных выше факторов, воздействующих на системы, выделяют следующие свойства, реализующие компенсирующие механизмы в распределенных РАСУ:

- 1) живучесть;
- 2) надежность;
- 3) помехоустойчивость.

Механизм, компенсирующий воздействие факторов на РАСУ, представлен на рис. 1.

Очевидна интегральная природа свойства устойчивости. Таким образом, под устойчивостью понимается способность РАСУ функционировать в условиях воздействия определенного подмножества факторов, т.е. способность системы компенсировать те или иные изменения, вызванные тем или иным фактором.

Согласно ГОСТ 34.003-90 под устойчивостью РАСУ как системы военного назначения понимается комплексное свойство, характеризующееся живучестью, помехоустойчивостью и надежностью.

В современных условиях вследствие тотальной информатизации общества в целом и вооруженных сил в частности все чаще наблюдается смещение противоборства в информационную сферу (киберпространство). В связи с этим все больше в практику внедряются принципы информационного противоборства. Несомненным лидером на этом пути являются США. В рамках концепции информационного противоборства предполагается бороться с системами управления при помощи информационного оружия, в частности ориентированного на поражение аппаратно-программных средств систем передачи, хранения и обработки информации, функционирующих в киберпространстве [7].

В связи с возможностью подавления систем управления без риска скомпрометировать атакующую сторону (информационная операция по срыву Иранской ядерной программы Stuxnet проведена

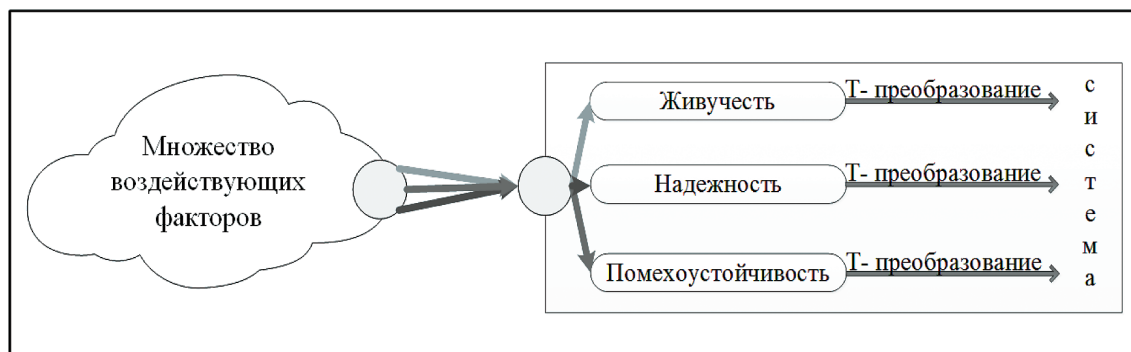


Рис. 1. Компенсирующие механизмы РАСУ

в 2010 году, однако до сих пор доподлинно не известны организаторы операции) наибольшее развитие получили средства специального программно-математического воздействия, которые объединяют возможности алгоритмического и программного информационно-технического оружия [7].

Для успешного проведения информационной операции необходимо осуществление разведывательных действий в отношении системы-цели (добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей). Для вскрытия критически важных характеристик систем-целей в США развернуты глобальные комплексы компьютерной разведки (рис. 2) [8, 9].

Результаты, полученные в [10], наглядно показывают зависимость успешности информацион-

ного воздействия от свойства разведзащищенности элементов РАСУ (рис. 3).

Здесь  $P_1$  – значение вероятности программно-аппаратной доступности инфокоммуникационной сети;  $P_2$  – значение вероятности аппаратной доступности технических каналов утечки информации;  $T$  – время готовности злоумышленника к воздействию.

Руководствуясь концепцией информационного противоборства, необходимо внести корректировку в категорию устойчивости РАСУ. Устойчивость детерминирована не только надежностью, живучестью и помехоустойчивостью, но и разведзащищенностью, то есть способностью скрыть особенности системы управления, что не позволит противнику подобрать такое воздействие, действие которого невозможно будет обра-

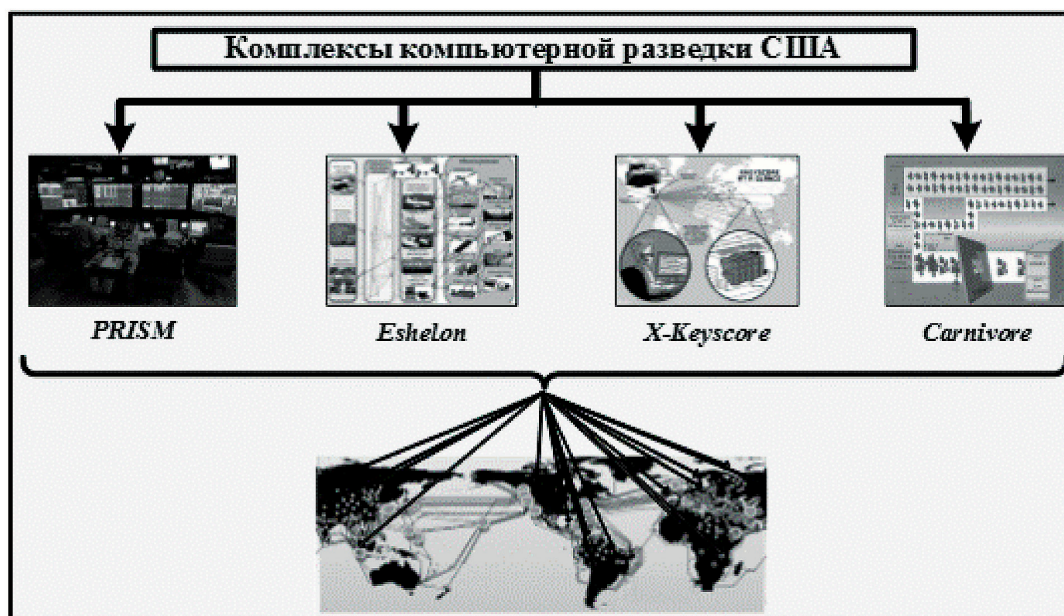


Рис. 2. Компьютерные комплексы разведки США

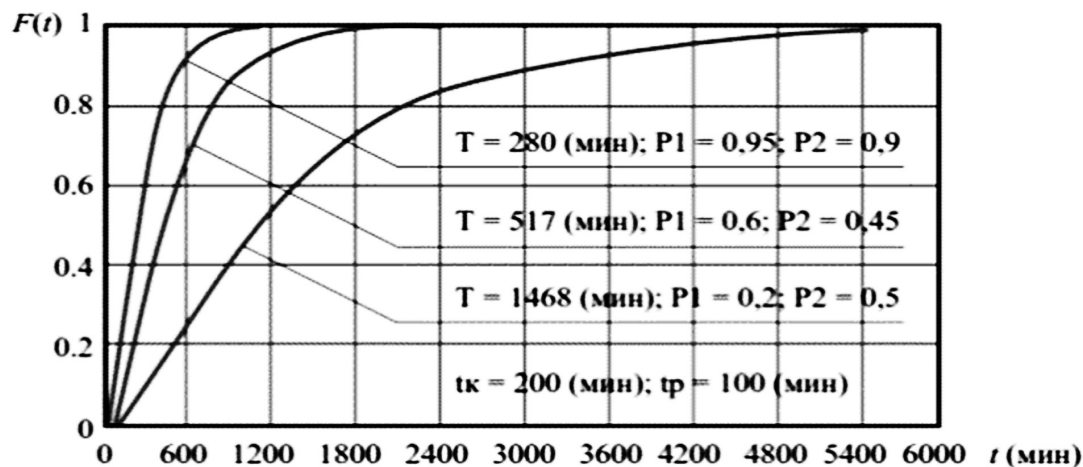


Рис. 3. Семейство функций распределения вероятности готовности противника к информационному воздействию при различной программно-аппаратной и аппаратной защищенности

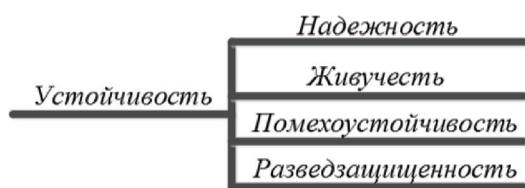


Рис. 4. Дерево атрибутивного свойства устойчивости РАСУ

тит в ноль-преобразование при помощи компенсаторских механизмов РАСУ.

Таким образом, устойчивость функционирования РАСУ должна характеризоваться атрибутивными свойствами, представленными на рис. 4.

### Заключение

Проведенный анализ показал прямую зависимость успешности реализации информационно-технического воздействия на РАСУ от свойства разведзащищенности системы. В связи с этим обозначилась необходимость корректировки категории устойчивости РАСУ и дополнения ее атрибутивным свойством разведзащищенности.

### Список литературы

1. Российский Институт Стратегических Исследований [Электронный ресурс]. – Режим доступа: <http://riss.ru>.
2. Чашин С. В., Вечеркин В. Б., Гончаров А. М. Алгоритм оценивания живучести комплексов систем автоматизации и его элементов в условиях деструктивных воздействий // Телекоммуникационные технологии. 2016. № 14. С. 122–125.
3. Мануйлов Ю. С., Петушков А. М., Новиков Е. А. Управление целевым применением космической навигационной системы по технологии гибких стратегий. СПб. : ВКА имени А. Ф. Можайского. 2007. 176 с.
4. Прохоров М. А. Оценивание устойчивости центра управления полетом космических аппаратов в условиях деструктивных воздействий // Труды II Межвузовской научно-практической конференции «Проблемы технического обеспечения войск в современных условиях». СПб., 2017. С. 160–163.
5. Иванов А. К. Проектирование устойчивой АСУ : учеб. пособие. Ульяновск : УлГТУ, 2002. 144 с.
6. Артюхов В. В. Общая теория систем: самоорганизация, устойчивость, разнообразие, кризисы. М. : Книжный дом «ЛИБРОКОМ», 2009. 224 с.
7. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292–376.
8. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты : монография. СПб. : Свое издательство, 2013. 166 с. : ил.
9. Коцыняк М. А., Кулешов И. А., Кудрявцев А. М. Киберустойчивость информационно-телекоммуникационной сети. СПб. : Бостон-спектр, 2015. 150 с.
10. Евглевская Н. В., Привалов Ан. А., Привалов Ал. А. Модель процесса подготовки злоумышленника к информационному воздействию на автоматизированные системы управления железнодорожным транспортом // Бюллетень результатов научных исследований. 2012. С. 17–25.

*История статьи*

*Поступила в редакцию 6 марта 2018 г.*

*Принята к публикации 5 апреля 2018 г.*

## DETERMINATION OF STABILITY CATEGORY FOR DISTRIBUTED AUTOMATED CONTROL SYSTEMS

**A. A. Tolmachev<sup>1</sup>, M. A. Prohorov<sup>2</sup>, A. S. Andrianov<sup>2</sup>**

<sup>1</sup>Military Aerospace Defense Academy, Tver, Russian Federation

<sup>2</sup>Military Space Academy, Saint Petersburg, Russian Federation

*At present, space systems and means became one of the main instruments of ensuring fighting and daily activity of Armed forces of the developed states of the world. In modern conditions space systems rise in a row strategic a component which stability of functioning it is critical for maintaining strategic balance. The analysis of the conflicts of the last decades has shown a tendency to confrontation shift to the space sphere and a cyberspace. Space systems and means allow to raise significantly fighting opportunities of troops, and the state which doesn't have potential of use of the means of armed struggle placed in the aerospace sphere, or allowed miscalculations in policy of development and use of the space systems and means,*

*will be doomed to the guaranteed defeat in future military conflicts. The defense capability and safety of the Russian Federation directly depend on a state and opportunities of means of strategic warning of preparation for aggression, the beginning of nuclear missile attack and also quality of comprehensive providing with space forces and means of army and fleet in peace and wartime. In this regard there was a need to carry out correction of content of category of stability of a funktsionirovaniye of the distributed automated control systems.*

*Keywords: demand, stability, intelligence protection, distributed automated control system, space systems, information confrontation, space assets.*

## References

1. Rossijskij Institut Strategicheskikh Issledovanij [Russian Institute for Strategic Studies]. – www: <http://riss.ru>. (In Russian)
2. Chashchin S. V., Vecherkin V. B., Goncharov A. M. *Algoritm ocenivaniya zhivuchesti kompleksov sistem avtomatizatsii i ego ehlementov v usloviyah destruktivnykh vozdeystvij* [Algorithm for estimating the survivability of complexes of automation systems and its elements under destructive influences] / *Telekommunikacionnye tekhnologii*. 2016. no. 14. pp. 122–125. (In Russian)
3. Manujlov YU. S., Petushkov A. M., Novikov E. A. *Upravlenie celevym primeneniem kosmicheskoy navigacionnoy sistemy po tekhnologii gibkih strategij* [Management of the target application of the space navigation system using flexible strategy technology]. Saint-Petersburg, VKA imeni A. F. Mozhajskogo. 2007. 176 p.
4. Prohorov M. A. *Ocenivanie ustojchivosti centra upravleniya poletom kosmicheskikh apparatov v usloviyah destruktivnykh vozdeystvij* [Estimation of the stability of the space flight control center under the conditions of destructive influences] [Trudy konferencii II Mezhvuzovskoj nauchno-prakticheskoy konferencii «Problemy tekhnicheskogo obespecheniya vojsk v sovremennykh usloviyah»] 2017, pp. 160–163. (In Russian)
5. Ivanov A. K. *Proektirovanie ustojchivoj ASU: Uchebnoe posobie* [Designing a sustainable control system]. Ul'yanovsk, UIGTU, 2002. 144 p.
6. Artyuhov V. V. *Obshchaya teoriya sistem: Samoorganizatsiya, ustojchivost', raznoobrazie, krizisy* [General theory of systems: Self-organization, sustainability, diversity, crises]. Moscow, Knihnyj dom «LIBROKOM», 2009. 224 p.
7. Makarenko S.I. *Informacionnoe oruzhie v tekhnicheskoy sfere: terminologiya, klassifikatsiya, primery* [Information weapons in the technical sphere: TNM, classification, examples]. *Sistemy upravleniya, svyazi i bezopasnosti*, 2016, no. 3, pp. 292–376. (In Russian)
8. Makarenko S. I., Ivanov M. S., Popov S. A. *Pomekhozashchishchennost' sistem svyazi s psevdosluchajnoj perestrojkoj rabochej chastoty. Monografiya* [Interference immunity of communication systems with pseudo-random working frequency tuning]. Saint-Petersburg, Svoe izdatel'stvo Publ., 2013. 166 p. (In Russian)
9. Kocynyak M. A., Kuleshov I. A., Kudryavcev A. M., *Kiberustojchivost' informacionno-telekommunikacionnoj seti* [Cyber resistance of the information and telecommunications network]. Saint-Petersburg, Boston-spektr Publ., 2015. 150 p.
10. Evglevskaya N. V., Privalov An. A., Privalov Al. A. *Model' processa podgotovki zloumyshlennika k informacionno-mu vozdeystviyu na avtomatizirovannye sistemy upravleniya zheleznodorozhnym transportom* [Model of the process of preparing an attacker for information impact on automated railway management systems]. *Byulleten' rezul'tatov nauchnykh issledovanij*, 2012, pp. 17–25. (In Russian)

**Article history**

Received 6 March 2018

Accepted 5 April 2018