Результатом выполненных работ является база данных, которая будет еще расширяться и наполняться, и по результатам которой можно будет делать как краткосрочный, так и долгосрочный прогноз подтопления той или иной территории совместив ДДЗ с наземными данными. Стоит учитывать, что любая система прогнозирования основана в первую очередь на повторяемости событий.

Главное достоинство ДДЗ при мониторинге паводковой ситуации заключается в том, что они поступают ежедневно, в реальном времени и делают возможным мониторинг паводковой ситуации основных бассейнов рек одновременно в нескольких административно-территориальных единицах СФО. В Сибирском Центре «НИЦ “Планета”» спутниковый мониторинг паводковой ситуации на сегодняшний день ведется только с оптико-электронных спутниковых систем, где главным фактором съемки являются безоблачные погодные условия. Таким образом, в условиях безоблачности картографирование ДДЗ с использованием современных технологий позволяют выделить на реках не только момент и границы выхода воды на пойму, но и определить скорость продвижения волны паводка по последовательным снимкам, что является основной тематической нагрузкой карт паводковой обстановки любого масштаба. Интеграция полученных результатов с опорными данными в ГИС позволяет представить результаты обработки в картографическом виде и оперативно передавать заинтересованным пользователям [1].

**Литература**

1. ГЕО-Сибирь-2008. Т. 3. Дистанционные методы зондирования Земли и фотограмметрия, мониторинг окружающей среды, геоэкология. Ч. 2: сб. матер. IV Междунар. научн. конгресса «ГЕО-Сибирь-2008». 22–24 апреля 2008 г. Новосибирск: СГГА, 2008. 307 с.

2. Дистанционное зондирование Земли из космоса: алгоритмы, технологии, данные: учебное пособие для слушателей молодежной школы-семинара / Сост.: А.А. Лагутин, Р.И. Райкин, Т.Н. Чимитдоржиев. Барнаул: Изд-во Алт. ун-та, 2013. 151 с.

3. *Лурье И.К., Косиков А.Г.* Теория и практика цифровой обработки изображений // Научный мир. 2003. 168 с.

4. *Чандра А.М., Гош С.К.* Дистанционное зондирование и географические информационные системы // Техносфера. 2008. 312 с.

**Monitoring and mapping of flood situation in the Siberian Federal District**

***Valeriy Nikolaevich Antonov**, Director: State Research Center "Planeta" Novosibirsk*

***O.G. Novgorodtseva**, Junior research fellow: State Research Center "Planeta" - Novosibirsk*

*The article describes the importance of the problem of flood situation and digital processing technology of multispectral data, used in the operational work in State Research Center "Planeta". The flood maps are informative enough to serve as one of the main sources of information for the regional services of the Ministry for Emergency Situation.*

*Keywords: remote sensing, mapping, technology, water level/*

**УДК 004.052.2:004.056.53**

# УСТОЙЧИВОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ. КОНЦЕПЦИЯ УСТОЙЧИВОГО ВЗАИМОДЕЙСТВИЯ

***Юрий Иванович Афанасьев**, канд. техн. наук, доц., доцент*
*кафедры математики и информатики*
*E-mail: afanasieff_jury@mail.ru*
*Московский университет им. С.Ю. Витте*
*http://www.muiv.ru*

*Необходимым условием для взаимодействия двух и более систем является их одновременное существование. Под одновременностью существования будем понимать такой промежуток времени функционирования систем, в течение которого воздействие или воздействие хотя бы одной из них повлияет на результативность другой при выполнении конкретной задачи.*

*Устойчивость как свойство любой информационной системы является фундаментальным. Данное свойство интуитивно может быть определено как некоторое постоянство, неизменность определенной структуры и поведения системы.*

*Ключевые слова: Взаимодействие, устойчивость, процессы в информационных системах, системный анализ.*

**Введение**

Взаимодействие определяет существование, структурную организацию и свойства всякой информационной системы. Взаимодействие – свойство, присущее не только материи в целом, но и всем ее состояниям и проявлениям, отдельным вещам, явлениям, процессам, их сторонам и свойствам [1].

Ю.И. Афанасьев

Первым необходимым условием для взаимодействия двух (или более) систем является их одновременное существование. Под *одновременностью существования* будем понимать такой промежуток времени функционирования систем, в течение которого воздействие хотя бы одной из них повлияет на результативность другой при выполнении конкретной задачи. Причем это влияние может быть *непосредственным*, и опосредованным, когда эффективность системы может существенно возрасти. Вторым необходимым условием для взаимодействия является наличие у рассматриваемых систем определенных свойств, которые позволили бы им осуществлять соответствующее воздействие друг на друга.

Свойство ***устойчивости*** является фундаментальным свойством любой информационной системы. Данное свойство интуитивно может быть определено как некоторое постоянство, неизменность определенной структуры (*статическая устойчивость*) и поведения системы (*динамическая устойчивость*). Применительно к информационным системам определение устойчивости было дано выдающимся русским математиком Ляпуновым А.М.: «*Устойчивость* – это способность системы функционировать в состояниях близких к равновесному, в условиях постоянных внешних и внутренних возмущающих воздействий».

**Устойчивость автоматизированных систем**

Взаимодействие неизбежно приводит к внешним и внутренним воздействиям для информационных систем, которые обязательно как следствие потребуют усиление такого свойства системы как устойчивость. По Б.С. Флейшману [2], различают активную и пассивную форму устойчивости. Активная форма устойчивости (надежность, отказоустойчивость, живучесть и пр.) присуща *сложным* системам, поведение которых основано на *акте решения.* Здесь акт решения определяется как выбор альтернатив, стремление системы достигнуть предпочтительное для нее состояние – целенаправленное поведение, а это состояние – ее целью. Пассивная форма (прочность, сбалансированность, гомеостазис) присуща *простым* системам, не способным к *акту решения*.

Так как штатный режим функционирования информационных систем, как правило, далек от равновесного, центральным элементом в данном случае является понятие *структурно-функциональной устойчивости*. При этом внешние и внутренние информационно-технические воздействия постоянно изменяют само равновесное состояние информационной автоматизированной системы. Соответственно мерой близости позволяющей решать изменяется ли поведение системы и как существенно под действием возмущения, здесь является множество выполняемых функций при взаимодействии.

После известных работ академика Глушкова В.М. развитию теории устойчивости автоматизированных систем были посвящены исследования Липаева В.В., Додонова А.Г., Кузнецовой М.Г., Горбачик Е.С. [2, 3] и целого ряда других отечественных ученых. Однако теория устойчивости в этих работах развивались лишь только с точки зрения уязвимости структуры автоматизированных систем без явного учета уязвимости поведения системы в условиях априорной неопределенности информационно-технических воздействий (в условиях взаимодействия).

Основой поддержания работоспособности автоматизированных систем в условиях информационно-технических воздействий относятся:

- недостаточная устойчивость функционирования автоматизированных систем;
- рост сложности структуры и поведения аппаратно-программных средств;
- трудность выявления количественных закономерностей, позволяющих исследовать устойчивость функционирования в условиях взаимодействия.

**В первом случае сложностью** является *недостаточная устойчивость* функционирования автоматизированной системы, которая часто оказывается ниже требуемой. Во многих случаях аппаратно-программные средства не в состоянии полностью выполнить свои функции по множеству причин. Среди этих причин:

- несогласованность реальных параметров вычислительных процессов и данных в спецификациях системного и прикладного программного обеспечения;
- переоценка современного уровня развития технологии программирования;
- переоценка возможностей современных методов и средств защиты информации, отказоустойчивости вычислительных систем (ВС) и надежности программного обеспечения (ПО).

Незнание или игнорирование названных причин приводит к снижению эффективности функционирования автоматизированных систем.

**Во втором случае сложностью** является территориальный и поведенческий рост *структуры информационной системы*.

К *особенностям структуры* автоматизированной системы относится следующее. Современные информационные системы, как правило, представляют собой территориально распределенные системы, состоящие из множества ЛВС клиент-серверной архитектуры. При этом защищенность и устойчивость функционирования аппаратных и программных средств автоматизированных систем в ряде случаев не обеспечены. Более 70% инструментальных средств разработки прикладного ПО являются зарубежными, менее 20% обладают соответствующими лицензиями производителя.

**Третья сложность** заключается *в трудности выявления количественных закономерностей*, позволяющих исследовать устойчивость функционирования автоматизированных систем в условиях взаимодействия. Дело в том, что на процессы функционирования автоматизированной системы существенно влияют факторы внешней и внутренней среды. Этими факторами в рамках рассматриваемой структуры либо принципиально невозможно управлять, либо управление происходит с недопустимым запаздыванием. Кроме того, внешняя и внутренняя среды имеют свойство неполной определенности возможных своих состояний в будущих периодах, т.е. факторы, влияющие на структуру алгоритмов функционирования автоматизированной системы, претерпевают такие изменения во времени, которые могут коренным образом изменять алгоритмы или вообще делают поставленные цели недостижимыми.

До недавнего времени для выявления указанных закономерностей функционирования автоматизированных систем использовали, главным образом, два основных подхода: *экспериментальный* (например, методы математической статистики и методы планирования эксперимента) и *аналитический* (например, методы аналитической верификации алгоритмов ПО). В противоположность экспериментальным методам, дающим возможность изучать единичный вычислительный процесс автоматизированных систем, методы аналитической

верификации алгоритмов позволяют рассматривать наиболее общие свойства вычислительного процесса, характерные для класса процессов автоматизированной системы в целом. Однако названные подходы обладают существенными недостатками. Недостатком экспериментальных методов является невозможность распространить результаты, полученные в данном эксперименте, на другой вычислительный процесс, отличающийся от изученного. Недостатком методов аналитической верификации алгоритмов ПО является трудность перехода от класса процессов автоматизированной системы, характеризуемых выводом общезначимых алгоритмических свойств, к единичному процессу, который характеризуется дополнительно соответствующими условиями функционирования (в частности, конкретными значениями параметров вычислительного процесса в условиях взаимодействия).

Следовательно, каждый из этих подходов в отдельности не достаточен для эффективного исследования устойчивости функционирования автоматизированной системы в условиях взаимодействия. Только комплексирование позволяет использовать сильные стороны обоих подходов [4], объединяет их в одно целое, и в этом случае можно получить необходимый математический аппарат для выявления требуемых количественных закономерностей.

**Комплексирование**

Проведенный анализ методов поддержания работоспособности автоматизированной системы свидетельствует о неадекватности рассмотренных способов обеспечения устойчивости в условиях взаимодействия. Взаимодействие, то есть взаимное влияние различных систем друг на друга с обязательным изменением свойств одной системы под воздействием другой исключает возможность моделирования функционирования систем традиционными методами. Возникающие при этом факторы сложности и порождаемые трудности приведены в таблице 1.

Таблица 1

| | **Фактор сложности** | **Порождаемые трудности** |
|---|---|---|
| 1 | Активность автоматизированной системы | Сложность определения предельных законов потенциальной эффективности системы |
| 2 | Сложная структура и поведение автоматизированной системы | Громоздкость и многомерность решаемых задач |
| 3 | Взаимное влияние структур данных автоматизированных систем друг на друга | Не может быть учтено моделями известных типов |
| 4 | Стохастичность поведения автоматизированной системы | Неопределенность описания поведения системы, сложность в постановке задач |
| 5 | Отклонения от штатных условий эксплуатации системы | Не могут быть учтены моделями известных типов |
| 6 | Влияние сбоев и отказов аппаратуры на поведение автоматизированной системы | Неопределенность параметров поведения системы, сложность в постановке задач |

Здесь определяющими являются факторы два и три. Они исключают возможность ограничиться моделированием общезначимых *алгоритмических свойств* автоматизированной системы в условиях взаимодействия. Однако традиционные методы поддержания работоспособности автоматизированной системы основаны на следующих подходах:

- упрощении моделирования поведения автоматизированной системы до вывода общезначимых алгоритмических свойств;

- обобщении эмпирически установленных частных закономерностей поведения автоматизированной системы.

Использование указанных подходов приводит не только к существенной погрешности результатов, но имеет и принципиальные недостатки. Недостатком аналитического моделирования поведения автоматизированной системы в условиях взаимодействия является трудность перехода от класса вычислительных процессов, характеризуемых выводом общих алгоритмических свойств, к единичному процессу, который характеризуется дополнительно условиями функционирования. Основным преимуществом модели является возможность путем изменения ее параметров описывать различные состояния системы [5].

На практике, в этом случае, традиционные математические модели поддержания работоспособности автоматизированных систем могут быть использованы только для разработки систем приближенного прогнозирования устойчивости функционирования автоматизированных систем в условиях взаимодействия.

Таким образом, значительным недостатком традиционных подходов поддержания работоспособности автоматизированных систем в условиях взаимодействия является игнорирование фактических условий реализации вычислительных процессов, что приводит к упрощенным идеальным результатам. Поэтому традиционные модели и методы поддержания работоспособности автоматизированных систем препятствуют практическому использованию расчетных решений задач обеспечения устойчивости. Очевидно, что без изменения подхода к математическому моделированию поведения автоматизированных систем невозможно обоснованное поддержание работоспособности системы.

В настоящей концепции предлагается подход на основе теории подобия, который лишен указанных недостатков и позволяет реализовать так называемый *принцип декомпозиции* автоматизированной системы в условиях взаимодействия (информационно-технического воздействия) *по структурно-функциональным признакам* [6]. В теории подобия доказывается, что множество связей между существенными для рассматриваемого поведения системы параметрами не является собственным свойством исследуемых задач. В действительности влияние отдельных факторов внешней и внутренней среды автоматизированной системы, представленных различными величинами, проявляется не порознь, а совместно. Поэтому предлагается рассматривать не отдельные величины, а их совокупности (инварианты подобия), имеющие определенный смысл для функционирования взаимодействующих информационных систем.

Теория подобия позволяет сформулировать необходимые и достаточные условия изоморфности двух моделей разрешенного поведения автоматизированных систем в условиях информационно-технических воздействий, описываемых системами однородных степенных многочленов (позиномов). Как следствие, становится возможным:

- производить аналитическую верификацию вычислительных процессов автоматизированной системы и проверять условия изоморфности;
- численно определять коэффициенты некоторого представления модели вычислительных процессов автоматизированной системы для достижения условий изоморфности.

А это позволяет контролировать семантическую корректность вычислительных процессов, обнаруживать аномалии вычислительных процессов и восстанавливать параметры вычислительных процессов автоматизированной системы, существенно влияющие на устойчивость поведения системы.

Основные положения теории подобия были сформулированы российской научной школой, главным образом, Гухманом А.А., Седовым Л.И., Вениковым В.А. [2, 3, 6]. Первоначально положения теории подобия нашли применение в теории механических и электрических процессов, а также процессов теплообмена. В конце 1980-х гг. полученные результаты теории подобия были распространены автором, под профессора Ковалева В.В., на область системного и прикладного программирования. В частности, в 1996 г. автором был разработан метод обнаружения аномалий локальных вычислительных процессов на основе применения *π-анализа уравнений и π-анализа размерностей* теории подобия. Основным результатом кандидатской диссертации автора стало обоснование и создание возможных *метрики и меры устойчивости* локальных вычислительных процессов автоматизированной системы. Это позволило разработать инженерные методики *моделирования, наблюдения, измерения и сравнения* устойчивости автоматизированных систем на основе инвариантов подобия. В частности, была получена новая методика моделирования эталонов семантически корректного локального вычислительного процесса, состоящая из следующих четырех этапов.

*Первый этап – π-анализ* моделей вычислительных процессов автоматизированной системы. Основная цель этого этапа состоит в выделении эталонов семантической корректности вычислительных процессов на основе инвариантов подобия. Процедура этапа включает следующие шаги:

1) выделение структурно-функциональных эталонов;
2) выделение временных эталонов;
3) выработка контрольных соотношений, необходимых для определения семантической корректности вычислительных процессов.

*Второй этап – алгоритмизация* получения эталонов семантической корректности вычислительных процессов. Основной его целью является получение в матричной и графической форме вероятностных алгоритмов эталонов или инвариантов подобия вычислительных процессов. Процедура этапа состоит из следующих шагов:

1) построение алгоритма эталона в форме дерева;
2) перечисление реализаций алгоритма;
3) взвешивание реализаций алгоритма (построение вероятностного алгоритма);
4) нормирование дерева алгоритма.

*Третий этап – синтез* эталонов семантической корректности вычислительных процессов адекватных целям и задачам применения автоматизированной системы. Основная цель его – синтез алгоритмических структур, образованных совокупностью последовательно выполняемых алгоритмов эталона. Данная процедура осуществляется по следующим шагам:

1) синтез структурно-функциональных эталонов;
2) синтез временных эталонов;
3) симметризация и ранжирование матриц, описывающих эталоны.

*Четвертый этап – моделирование* стохастически определенных алгоритмических структур эталонов семантической корректности вычислительных процессов автоматизированной системы. Процедура этапа включает следующие шаги:

1) анализ эмпирических эталонов семантической корректности;
2) определение вида эмпирической функциональной зависимости;
3) выработка контрольных соотношений, достаточных для определения семантической корректности вычислительного процесса.

**Предлагаемый подход и его развитие**

Для формирования модельного представления проблемы поддержания работоспособности автоматизированной системы в условиях информационно-технических воздействий воспользуемся следующими понятиями:

- система обработки данных;
- поведение системы обработки данных;
- целевое назначение системы обработки данных;
- угрозы устойчивости обработки данных;
- информационно-технические воздействия внешней и внутренней среды;
- корректирующие действия по обеспечению устойчивости (контрмеры);
- состояние системы обработки данных.

Перечисленные понятия относятся к числу первичных, неопределяемых понятий и используются в следующем смысле.

*Под системой обработки данных* понимается некоторая совокупность аппаратно-программных компонент, предназначенная для выполнения определенных функций обработки данных. Под *поведением* системы обработки данных понимается некоторая реализация вычислительного процесса во времени. При этом допускается проведение целенаправленных корректирующих действий для обеспечения требуемой устойчивости. Функциональная предназначенность системы обработки данных называется *целевым назначением*, корректирующие мероприятия – *обеспечением устойчивости*. Другими словами,

любая система обработки данных создана или создается для определенного целевого назначения и обладает некоторым защитным механизмом, настраиваемым или регулируемым средствами обеспечения устойчивости.

Под понятием *источник угроз* понимается лицо или группа лиц, которые в результате предумышленных или непредумышленных действий потенциально могут нанести определенный ущерб.

Выделяются следующие категории внутренних и внешних нарушителей. К *внутренним нарушителям* относятся:

- операторы автоматизированных рабочих мест, администраторы служб информационной безопасности, системные администраторы, администраторы баз данных, инженерный состав;
- технический персонал, работающий в зданиях, в которых размещается вычислительные средства;
- другие служащие подразделений, имеющие санкционированный доступ в здания, где расположено оборудование передачи и обработки информации.

Под *внешними нарушителями* понимаются лица, совершающие свои действия с целью нанесения ущерба системам обработки данных автоматизированной системе (съём информации, искажение информации, разрушение системного или прикладного программного обеспечения).

Выделяются три основные группы потенциальных нарушителей:

1 группа – субъекты, не имеющие доступ в пределы контролируемой зоны объекта защиты.

2 группа – субъекты, не имеющие доступ к работе со штатными средствами объекта защиты, но имеющие доступ в помещения, где они размещаются.

3 группа – субъекты, имеющие доступ к работе со штатными средствами объекта защиты.

Предположения о квалификации внутреннего нарушителя формулируются следующим образом:

А – не является специалистом в области вычислительной техники.

В – самый низкий уровень возможностей – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции при обработке информации.

С – возможности создания и запуска собственных программ с новыми функциями по обработке информации.

Д – возможность управления функционированием автоматизированной системы, т.е. воздействием на базовое программное обеспечение системы, на состав и конфигурацию оборудования.

Е – включает весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств автоматизированной системы, вплоть до включения в состав системы собственных технических средств с новыми функциями по обработке информации.

Условимся считать, что внешний нарушитель является специалистом высшей квалификации в области вычислительной техники и программного обеспечения.

Для классификации *угроз автоматизированных систем аппаратно-программные* компоненты выделяются следующим образом:

- средства вычислительной техники (далее технические средства);
- коммуникационная подсистема и сети передачи данных;
- программное обеспечение;
- технологические процессы обработки и передачи информации.

Тогда классификация угроз автоматизированных систем выглядит так:

- угрозы, связанные с применением технических средств;

- угрозы, связанные с использованием коммуникационной подсистемы и сетей передачи данных;
- угрозы, связанные с использованием программного обеспечения;
- угрозы, связанные с нарушением технологического процесса обмена данными.

Также разделим угрозы автоматизированных систем на три основные категории:
- угрозы секретности (конфиденциальности);
- угрозы доступности;
- угрозы целостности.

Разделим потоки данных автоматизированных систем на два основных типа:
- технологические данные;
- вспомогательные данные.

Под технологическими данными понимаются любые данные, обрабатываемые или хранимые в автоматизированной системе.

Под вспомогательными данными понимаются данные, порождаемые прикладным и системным программным обеспечением, например сообщения о синхронизации времени серверов баз данных, данные аудита операционных систем и т.п.

*Информационно-техническое воздействие* – это единичный акт внешнего или внутреннего информационно-технического воздействия внутренней и/или внешней среды на систему обработки данных автоматизированной системы. Воздействие приводит к изменению параметров вычислительных процессов и препятствует или затрудняет выполнение целевого назначения системы обработки данных автоматизированной системы. Совокупность таких единичных актов образует *множество информационно-технических воздействий*.

*Состояние системы обработки данных* автоматизированной системы есть некоторый набор числовых характеристик параметров вычислительных процессов. Числовые характеристики вычислительных процессов зависят от условий функционирования системы обработки данных, воздействий внутренней и внешней среды, корректирующих действий по обеспечению требуемой устойчивости и, в общем случае, от времени. Совокупность всех корректирующих действий по обеспечению устойчивости вычислительных процессов называется *множеством корректирующих мероприятий*, совокупность всех состояний системы обработки данных – *множеством состояний*.

Таким образом, будем считать, что при отсутствии воздействий, а также корректирующих мероприятий по обеспечению устойчивости каждая система обработки данных автоматизированной системы находится в работоспособном состоянии и отвечает некоторому целевому назначению. Под некоторым воздействием система обработки данных переходит в новое состояние, которое может не отвечать целевому назначению. В этом случае необходимо решить следующие задачи оперативного планирования – обеспечение устойчивости систем обработки данных автоматизированной системы непосредственно после воздействия (взаимодействия), а также задачу перспективного планирования на этапе проектирования системы обработки данных автоматизированной системы, когда требуется сделать ее устойчивой к максимальному подмножеству возможных воздействий.

В целом анализ проблемы поддержания работоспособности автоматизированной системы в условиях информационно-технических воздействий свидетельствует о целесообразности определения трех групп факторов систем обработки данных:

x – параметры вычислительных процессов;

y – внутренние и внешние информационно-технические воздействия на системы обработки данных автоматизированной системы;

*z* – корректирующие действия для обеспечения требуемой устойчивости.

Природа факторов на данном уровне рассмотрения систем обработки данных автоматизированной системы пока не существенна. Достаточно считать x, y, *z* элементами некоторых подмножеств X, Y, Z конечномерных, функциональных или других общих про-

странств. При этом целевое назначение каждой системы обработки данных автоматизированной системы состоит в том, чтобы некоторые функции или операторы на параметрах вычислительных процессов, информационно-технических воздействий злоумышленника (взаимодействия), а также определенных корректирующих действий принимали заранее заданные значения.

$$F(x, y, z) \in Q, (x, y, z) \in P. \quad (1.1)$$

Здесь F некоторый оператор, определенный на множестве $P = X \times Y \times Z$, а Q – множество требуемых значений оператора F.

**Заключение**

Поддержания работоспособности автоматизированных систем в условиях взаимодействия (информационно-технических воздействий) является важной технической проблемой и требует своего разрешения.

*Проблемная ситуация* состоит в противоречии между необходимостью поддержания работоспособности взаимодействующей автоматизированной системы в условиях информационно-технических воздействий и недостаточной проработкой моделей и методов обнаружения и парирования информационно-технических воздействий злоумышленника.

Оценка практической применимости известных моделей и методов поддержания работоспособности автоматизированных систем (N-кратное резервирование; инверсионное программирование; введение различной структурной и функциональной избыточности; перераспределение операций, структур и ресурсов вычислительных систем; восстановление работоспособности элементов; реализация различных защитных функций и пр.) свидетельствует об их ограниченной ценности и показывает, что в настоящее время повышение (сохранение) устойчивости функционирования автоматизированных систем сдерживается отсутствием адекватных математических моделей разрешенного функционирования автоматизированных систем в условиях взаимодействия (информационно-технических воздействий).

**Литература**

1. *Афанасьев Ю.И.* Теория взаимодействия. Анализ в условиях синхронизации процесса // Образовательные ресурсы и технологии. 2014. № 6. С. 47–52.

2. *Калинин В.Н., Резников Б.А., Варакин Е.И.* Теория систем и оптимального управления. Л.: Изд-во ВКА, 1979. Ч. 1. 456 с.

3. *Калинин В. Н., Резников Б.А., Варакин Е.И.* Теория систем и оптимального управления. – Л.: Изд-во ВКА, 1987. Ч. 2. 589 с.

4. *Парфенова М.Я., Руденко Ю.С.* Механизм интеграции образования, науки и производства с применением подхода диссимметрии // Образовательные ресурсы и технологии. 2013. № 2 (3). С. 67– 73.

5. *Кубова В.И., Кубова Р.М.* Обучающая модель исследования работы сердца как импульсной системы // Образовательные ресурсы и технологии. 2013. № 2. С. 40– 51.

6. *Афанасьев Ю.И., Петренко С.А* Концепция устойчивости автоматизированных систем военного назначения. Статья, депонированная в ЦВНИ МО РФ. Вып. 2(107). М.: ЦВНИ МО РФ, 2010.

**Stability of automation systems. The concept of sustainable interaction**

***Yury Ivanovich Afanasyev**, Ph.D., senior lecturer Moscow University named after S. Y. Witte*

*The first prerequisite for the interaction of two (or more) systems is their simultaneous existence. Under the simultaneous existence we mean a period of time of functioning of systems for which the effect of at least one of them will affect the effectiveness of the other in the performance of a specific task.*
*Stability property is a fundamental property of any information system. This property can be intuitively defined as a certain constancy, immutability of certain structures and system behavior.*

*Keywords: Interaction theory, stability, processes in information systems, systems analysis.*