Концепция поддержания работоспособности киберсистем в условиях информационно-технических воздействий

С. А. Петренко

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

В настоящей статье предлагается уточнить приведенное определение, так как устойчивость функционирования автоматизированных систем (АС) критически важных объектов (КВО) не всегда означает способность системы поддерживать равновесное состояние. Первоначально свойство устойчивости трактовали именно так, поскольку как реальное явление оно было замечено при изучении гомеостазиса (возврат в равновесное состояние при выводе из него) биологических систем. Использование аппарата системного анализа предполагает определенную адаптацию термина «устойчивость» к характерным особенностям изучаемых АС КВО в условиях информационно-технических воздействий, одним из которых являются существование *цели функционирования.* Поэтому предлагается следующее определение устойчивости: «Устойчивость функционирования АС КВО — это *способность системы, функционирующей по определенному алгоритму, достигать цели функционирования в условиях информационно-технических воздействий злоумышленника*».

Действительно, по Б. С. Флейшману [1], следует различать 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*.

Кроме того в отличие от классического равновесного подхода, центральным элементом здесь является понятие *структурно-функциональной устойчивости*. Дело в том, что штатный режим функционирования АС КВО, как правило, далек от равновесного. При этом внешние и внутренние информационно-технические воздействия постоянно изменяют само равновесное состояние. Соответственно мерой близости позволяющей решать существенно ли изменяется поведение системы под действием возмущения, здесь является множество выполняемых функций.

После работ В. М. Глушкова развитию теории устойчивости АС были посвящены исследования В. В. Липаева, А. Г. Додонова, М. Г. Кузнецовой, Е. С. Горбачик [1, 2] и целого ряда других отечественных ученых. Однако теория устойчивости в этих работах развивались лишь только с точки зрения уязвимости структуры АС без явного учета уязвимости поведения системы в условиях априорной неопределенности информационно-технических воздействий злоумышленника. В результате АС, в большинстве случаев, представляет собой пример предопределенного изменения и сохранения отношений и связей. Это сохранение призвано сохранить целостность системы в течение некоторого интервала времени в штатных условиях функционирования. Такая предопределенность имеет двойственный характер: с одной стороны обеспечивается лучшая реакция системы на штатные условия функционирования неблагоприятных воздействий, а с другой стороны, система не способна противостоять другим, априорно неизвестным информационно-техническим воздействиям злоумышленника, изменяющим ее структуру и поведение.

1. Основные сопроблемы

К основным сопроблемам поддержания работоспособности АС КВО в условиях информационно-технических воздействий относятся:

- недостаточная устойчивость функционирования АС КВО;

- рост сложности структуры и поведения аппаратно-программных средств АС КВО;
- трудность выявления количественных закономерностей, позволяющих исследовать устойчивость функционирования АС КВО в условиях воздействий.

Дадим к этим сопроблемам развернутый комментарий.

Первой (и наиболее существенной) **сопроблемой** является *недостаточная устойчивость* функционирования АС КВО, которая часто оказывается ниже требуемой. Во многих случаях аппаратно-программные средства АС КВО 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;
- деструктивное информационно-техническое воздействие факторов внешней и внутренней среды на АС КВО, особенно в условиях воздействия злоумышленников;
- 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 АС КВО. По опыту работы автора на восстановление вычислительных процессов в АС КВО расходуется более 30 % машинного времени. Более того, указанная проблема значительно обостряется в условиях информационно-технических воздействий.

Второй сопроблемой является рост сложности *структуры и поведения* АС КВО.

К *особенностям структуры* АС КВО относится следующее. Современные АС КВО, как правило, представляют собой территориально распределенные системы, состоящие из множества ЛВС клиент-серверной архитектуры. По данным автора, в состав современных АС КВО входят более:

- 15 типов ЭВМ;
- 20 типов сетевого оборудования;

- 100 сетевых протоколов;
- 20 операционных систем;
- 12 СУБД;
- 100 языков программирования;
- 10 типов средств защиты информации.

Так, например, используются следующие типы ЭВМ:

Мэйнфреймы (Эльбрус 90 Микро, а также ЭВМ на базе архитектуры IBM 370/390, представленные моделями семейства ES/9672 или S/390 IBM 3006-B01 под управлением операционных систем OS/390, MVS/ESA, VM/ESA, ОС 6.1 (БОС ЕС), ОС 7 (СВМ ЕС);

ПЭВМ (в том числе серии «Багет»), функционирующие под управлением ОС МСВС 3.0, MS Windows 98/NT/ 2000/XP, Linux Red Hat, IBM OS/2, MS DOS 6.22.

Выделенные ЭВМ, используемые для решения специальных задач защиты информации, обслуживания каналов связи, временного хранения и преобразования данных. Например, многопроцессорные ЭВМ на платформах SUN или HP под управлением ОС семейства UNIX.

При этом защищенность и устойчивость функционирования аппаратных и программных средств АС КВО в ряде случаев не обеспечены. Так, из-за определенного отставания отечественной электронной промышленности в освоении производства микропроцессоров, в ряде ЭВМ, используются зарубежные микропроцессоры. Например, в ПЭВМ серии «Багет» используется зарубежный микропроцессор R-3000, а в ЭВМ «Эльбрус 90 Микро» — микропроцессоры SPARC фирмы SUN. Более 70 % инструментальных средств разработки прикладного ПО являются зарубежными, менее 20 % обладают соответствующими лицензиями производителя. Менее 30 % используемых программных средств имеют сертификаты ФСТЭК на отсутствие недекларированных возможностей (НДВ) и защите от несанкционированного доступа по 4 классу для СВТ и 1Г классу для АС (минимальные требования по защите информации для служебного пользования). Менее 30 % программных систем прошли сертификацию в органах ФСБ.

В результате ряд требований, предъявляемых к АС КВО, оказался не учтенным. В первую очередь это касается достоверности выдаваемых данных и вероятности ошибок, устойчивости функционирования при различных информационно-технических воздействиях, а также защищенности информации. Поэтому сегодня в АС КВО возможны несанкционированные и запрещенные действия, искажение ин-

формации, нарушение хода работы или выход из строя, выдача конфиденциальной информации не допущенным к машинам лицам или зарубежным организациям, включение или выключение в не назначенное время и др.

К особенностям функционирования АС КВО относятся:

- обработка информации в территориально распределенных вычислительных системах;
- информационно-расчетный характер решения большинства вычислительных задач;
- плановая организация процесса обработки информации;
- решение задач обработки данных в реальном масштабе времени;
- жесткая временная диаграмма выполнения вычислительных работ;
- высокая точность производимых расчетов;
- частичная упорядоченность задач, препятствующая полной загрузке вычислительной системы;
- квазидетерминированный (детерминированно-стохастический) характер обработки информации, обусловленный задачами обработки данных, а также учетом возможных отклонений выполнения расчетов от штатного расписания;
- потенциальная возможность введения избыточности ресурсов и реконфигурации структуры системы для обеспечения устойчивости;
- повышенные требования к устойчивости процессов обработки данных, что объясняется невозможностью повторного решения прикладных задач.

Перечисленные *особенности структуры и поведения* АС приводят к расширению спектра угроз информационно-технического воздействия злоумышленников и определяют высокую уязвимость АС КВО.

Третья сопроблема заключается *в трудности выявления количественных закономерностей*, позволяющих исследовать устойчивость функционирования АС КВО в условиях информационно-технических воздействий злоумышленника. Дело в том, что на процессы функционирования АС КВО существенно влияют факторы внешней и внутренней среды. Этими факторами в рамках рассматриваемой структуры АС КВО либо принципиально невозможно управлять, либо управление происходит с недопустимым запаздыванием. Кроме того, внешняя и внутренняя среды имеют свойство неполной опреде-

ленности возможных своих состояний в будущих периодах, т. е. факторы, влияющие на структуру алгоритмов функционирования АС КВО, претерпевают такие изменения во времени, которые могут коренным образом изменять алгоритмы или вообще делают поставленные цели недостижимыми. Изменения, которые претерпевают факторы внешней и внутренней среды, происходят как закономерно, например, в условиях информационно-технических воздействий злоумышленника, так и случайно, поэтому в общем случае они не могут быть предсказаны точно, вследствие чего наблюдается некоторая неопределенность их значений. С другой стороны, алгоритмы и аппаратно-программные средства АС КВО, перед которыми стоит определенная цель, обладают определенным «запасом прочности» — такими особенностями, которые позволяют достигать поставленные цели при определенных отклонениях влияющих факторов внешней и внутренней среды.

До недавнего времени для выявления указанных закономерностей функционирования АС КВО 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 АС КВО, методы аналитической верификации алгоритмов позволяют рассматривать наиболее общие свойства вычислительного процесса, характерные для класса процессов АС КВО 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 АС КВО, характеризуемых выводом общезначимых алгоритмических свойств, к единичному процессу, который характеризуется дополнительно соответствующими условиями функционирования (в частности, конкретными значениями параметров вычислительного процесса в условиях информационно-технических воздействий злоумышленника).

Следовательно, каждый из этих подходов в отдельности не достаточен для эффективного исследования устойчивости функционирования АС КВО в условиях информационно-технических воздействий зло-

умышленника. Представляется, что только используя сильные стороны обоих подходов, объединив их в одно целое, можно получить необходимый математический аппарат для выявления требуемых количественных закономерностей.

2. Предлагаемый подход

Проведенный анализ методов поддержания работоспособности АС свидетельствует о неадекватности рассмотренных способов обеспечения устойчивости АС КВО в условиях информационно-технических воздействий злоумышленника. Дело в том, что эти условия придают АС КВО черты, исключающие возможность моделирования функционирования систем традиционными методами. Возникающие при этом факторы сложности и порождаемые трудности приведены в табл. 1.

Здесь определяющими являются факторы 1, 4 и 7. Они исключают возможность ограничиться моделированием общезначимых *алгорит-*

Таблица 1

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

мических свойств АС КВО в условиях информационно-технических воздействий злоумышленника. Однако традиционные методы поддержания работоспособности АС КВО основаны на следующих подходах:

- упрощении моделирования поведения АС КВО до вывода общезначимых алгоритмических свойств;
- обобщении эмпирически установленных частных закономерностей поведения АС КВО.

Использование указанных подходов приводит не только к существенной погрешности результатов, но имеет и принципиальные недостатки. Недостатком аналитического моделирования поведения АС КВО в условиях информационно-технических воздействий злоумышленника является трудность перехода от класса вычислительных процессов, характеризуемых выводом общих алгоритмических свойств, к единичному процессу, который характеризуется дополнительно условиями функционирования (параметрами вычислений, информационно-техническими воздействиями злоумышленника и корректирующими действиями). Недостатком эмпирического моделирования поведения АС КВО является невозможность распространить результаты на другие вычислительные процессы, отличающиеся от изученного параметрами функционирования АС КВО.

Поэтому на практике традиционные математические модели поддержания работоспособности АС КВО могут быть использованы только для разработки систем приближенного прогнозирования устойчивости функционирования АС КВО в условиях информационно-технических воздействий злоумышленника. Разработка требуемых систем поддержания работоспособности АС КВО затруднена и требует теоретической проработки вопросов моделирования разрешенного функционирования АС КВО в условиях информационно-технических воздействий.

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

Предлагаемый в настоящей концепции подход на основе теории подобия лишен указанных недостатков и позволяет реализовать так называемый *принцип декомпозиции* АС КВО в условиях информационно-технических воздействий злоумышленника *по структурно-функциональным признакам* [2]. 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 АС КВО, представленных различными величинами, проявляется не порознь, а совместно. Поэтому предлагается рассматривать не отдельные величины, а их совокупности (инварианты подобия), имеющие определенный смысл для функционирования АС КВО.

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

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

Это, в свою очередь, позволяет:

- контролировать семантическую корректность вычислительных процессов АС КВО в условиях воздействий путем сравнения наблюдаемых инвариантов подобия с инвариантами эталонного, изоморфного представления процессов;
- обнаруживать (в том числе в режиме реального времени) аномалии вычислительных процессов АС, возникшие в результате информационно-технического воздействия злоумышленника, а также в различных аварийных ситуациях;
- восстанавливать параметры вычислительных процессов АС, 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]. 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 именем профессора В. В. Ковалева, 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 АС КВО. Это позволило разработать инженерные методики *моделирования, наблюдения, измерения и сравнения* устойчивости выполнения военно-прикладных программ АС КВО 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 АС КВО. 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 АС КВО. Основная цель его — синтез алгоритмических структур, образованных совокупностью последовательно выполняемых алго-

ритмов 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 АС КВО. 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.

В результате в кандидатской диссертации автором была показана применимость методов теории подобия для *декомпозиции* алгоритмов вычислительных процессов *по функциональным признакам* и формирования необходимых инвариантов семантически корректного функционирования АС КВО. Наличие свойства автомодельности инвариантов подобия позволило сформировать статические и динамические эталоны семантически корректного вычислительного процесса и использовать их для инженерного решения задач контроля, обнаружения и нейтрализации аномалий локальных вычислительных процессов АС КВО.

Развитие предлагаемого подхода

Для формирования модельного представления проблемы поддержания работоспособности АС КВО 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 ИВК;
- другие служащие подразделений, имеющие санкционированный доступ в здания, где расположено оборудование передачи и обработки информации.

Под *внешними нарушителями* понимаются лица, находящиеся на службе специальных служб иностранных государств, а также преступных сообществ, совершающих свои действия с целью нанесения ущерба системам обработки данных АС КВО (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:

- A — не является специалистом в области вычислительной техники;
- B — самый низкий уровень возможностей — запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции при обработке информации;
- C — возможности создания и запуска собственных программ с новыми функциями по обработке информации;
- D — возможность управления функционированием автоматизированной системы, т. е. воздействием на базовое программное обеспечение системы, на состав и конфигурацию оборудования;
- E — включает весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств автоматизированной системы, вплоть до включения в состав СВТ 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 АС КВО 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 АС КВО 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 АС КВО на три основные категории:

- угрозы секретности (конфиденциальности);
- угрозы доступности;
- угрозы целостности.

Разделим потоки данных АС КВО на два основных типа:

- технологические данные;
- вспомогательные данные.

Под *технологическими* данными понимаются любые данные, обрабатываемые или хранимые в АС КВО.

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 АС КВО. Воздействие приводит к изменению параметров вычислительных процессов и препятствует или затрудняет выполнение целевого назначения системы обработки данных АС КВО. Совокупность таких единичных актов образует *множество информационно-технических воздействий*.

Состояние системы обработки данных АС КВО 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 АС КВО 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 задачу оперативного планирования — обеспечение устойчивости систем обработки данных АС КВО непосредственно после воздействия, а также задачу перспективного планирования на этапе проектирования системы обработки данных АС КВО, когда требуется сделать ее устойчивой к максимальному подмножеству возможных воздействий.

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

- x — параметры вычислительных процессов;
- u — внутренние и внешние информационно-технические воздействия на системы обработки данных АС КВО;
- v — корректирующие действия для обеспечения требуемой устойчивости.

Природа факторов на данном уровне рассмотрения систем обработки данных АС КВО пока не существенна. Достаточно считать x, u, v элементами некоторых подмножеств X, U, V конечномерных, функциональных или других общих пространств. При этом целевое назначение каждой системы обработки данных АС КВО состоит в том, чтобы некоторые функции или операторы на параметрах вычислительных процессов, информационно-технических воздействий злоумышленника, а также определенных корректирующих действий принимали заранее заданные значения.

$$F(x, u, v) \in Q, (x, u, v) \in P. \qquad (1.1)$$

Здесь F — некоторый оператор, определенный на множестве $P = X \times U \times V$, а Q — множество требуемых значений оператора F.

Принципы расчета устойчивости

Предлагаются следующие новые принципы расчета устойчивости функционирования АС КВО:

- *системного обеспечения устойчивости*: использование средств повышения устойчивости вычислительных процессов должно быть

нацелено на достижение максимальных показателей устойчивости при одновременном соблюдении допустимых или оптимальных затрат ограниченных ресурсов АС КВО;

- *адаптивного обеспечения устойчивости:* по мере развития и совершенствования АС КВО требования к повышению устойчивости должны пересматриваться в направлении улучшения их от допустимых к оптимальным;
- *информационного обеспечения устойчивости:* вопросы применения средств повышения устойчивости должны решаться на основе объективных количественных оценок, получаемых на начальных стадиях эксплуатации АС КВО путем расчетно-аналитических, модельных и экспертных оценок, проверяемых экспериментально на последующих стадиях;
- *автоматического обеспечения устойчивости:* стабильная тенденция разумного освобождения человека-оператора АС КВО от рутинных функций и создания условий для максимального автоматического повышения устойчивости, усиленного возможностями системного программирования.

Эти общие принципы в совокупности образуют основу предлагаемой прикладной теории поддержания работоспособности АС КВО в условиях информационно-технических воздействий на основе инвариантов подобия.

Частные принципы непосредственно связаны с разработкой и применением методов и алгоритмов контроля, коррекции и восстановления вычислительных процессов АС. К ним относятся следующие принципы:

- *постоянства функций*, означающий, что все свойства вычислительного процесса существуют в качестве функций, реализация которых упорядочена во времени и пространстве;
- *соответствия функций*, проявляющийся в общности алгоритмов вычислительных процессов и их свойств;
- *развития функций*, позволяющий рассматривать вычислительный процесс, как непрерывный процесс становления функций, в котором АС КВО приобретает все новые свойства и все больше свойств становится функциями системы;
- *активизации функций*, означающий, что в АС КВО активизация информационно-расчетных функций осуществляется за счет активного по своей природе поведения вычислительной системы и специальных программных средств повышения устойчивости;

- *компенсации функций*, обусловливающий возможность передачи функций ошибочных вычислительных процессов, неспособных к восстановлению, другим резервным компонентам АС КВО.

Возможные постановки задач

В терминах *оптимального управления* и *математического программирования* постановка задачи исследования формулируется следующим образом.

Гарантированная устойчивость. Минимаксный подход

Необходимо

1. Определить целевое назначение АС КВО вида:

$$F(x,u,\nu) \in Q, \tag{1.15}$$

где $x \in X$ — инварианты подобия вычислительных процессов АС КВО; $u \in U$ — параметры внутренних и внешних информационно-технических воздействий; $\nu \in V$ — параметры восстановления; Q — допустимая область значений цели функционирования АС КВО.

2. Определить эквивалентные условия «гарантированной устойчивости» вычислительных процессов АС КВО вида:
   - для $\forall \nu \in V, \exists x \in X, u \in U : F(x,u,\nu) \in Q$;
   - в области X x V определения многозначного отображения

$$(x,u) \to F(x,u,V), F(x,u,V) = \{F(x,u,\nu) : \nu \in V\}$$

     найдется пара (*x*, *u*) со свойством $F(x,u,\nu) \subset Q$;
   - включения $F(x,u,V) \subset Q, (x,u) \in X \times V$ совместны.

3. По некоторому *k*-му показателю устойчивости решить минимаксную задачу вида

$$\begin{gathered} g_u(x,u) = \sup_{\upsilon \in V} f_u(x,u,\nu) \to \min; \\ g_u(x,u) \le b_i, i \ne u \in I \subset IN. \end{gathered} \tag{1.16}$$

Стохастический подход

При наличии априорной или апостериорной информации о внутренних и внешних информационно-технических воздействий на АС КВО преобразовать случайное включение $F(x,u,\nu) \subset Q;$ в новое детерминированное условие. Например, одно из следующих

$$\mathrm{M}\, F(x,u,\nu) \subset Q; \tag{1.17}$$

$$\mathrm{P}\,(\, F(x,u,\nu) \subset Q;\,) \geq \mathrm{p}, \tag{1.18}$$

где M, P — символы математического ожидания и вероятности; p — заданная вероятность выполнения исходного включения.

К частным задачам исследования относятся:

1) разработать модели процессов разрешенного функционирования АС КВО;
2) разработать метод построения эталонов функционирования для контроля деструктивного информационно-технического воздействия;
3) разработать методов выявления вторжений и аномалий для поддержания работоспособности АС КВО;
4) разработать комплекс методик обнаружения деструктивных информационно-технических воздействий на вычислительную среду АС КВО и ее требуемого восстановления.

Заключение

1. Поддержание работоспособности АС КВО в условиях информационно-технических воздействий является важной технической проблемой и требует своего разрешения.
2. Оценка практической применимости известных моделей и методов поддержания работоспособности АС КВО (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 АС КВО сдерживается отсут-

ствием адекватных математических моделей разрешенного функционирования АС КВО в условиях информационно-технических воздействий.

3. *Проблемная ситуация* состоит в противоречии между необходимостью поддержания работоспособности АС КВО в условиях информационно-технических воздействий и недостаточной проработкой моделей и методов обнаружения и парирования информационно-технических воздействий злоумышленника.
4. *Научная проблема* состоит в формализации семантики вычислений для синтеза эталонов разрешенного функционирования вычислительной среды.
5. Анализ возможностей выбранного *направления исследований* на основе теории подобия свидетельствует о перспективности этого направления для решения задачи оценивания устойчивости функционирования АС КВО и задачи синтеза оптимального поведения АС КВО с требуемой устойчивостью. Предлагается поддерживать работоспособность АС КВО в условиях информационно-технических воздействий путем «расширения» исходных информационно-расчетных алгоритмов и программ некоторыми дополнительными структурно-функциональными параметрами, так называемыми инвариантами подобия, на которые накладывается ряд контрольных условий. Проверка этих условий в процессе функционирования АС позволяет контролировать допустимый ход вычислительного процесса системы в реальном масштабе времени.

Литература

1. *Калинин В. Н., Резников Б. А., Варакин Е. И.* Теория систем и оптимального управления. Л.: Изд-во ВКА, 1979. Часть 1. 456 с.
2. *Калинин В. Н., Резников Б. А., Варакин Е. И.* Теория систем и оптимального управления. Л.: Изд-во ВКА, 1987. Часть 2. 589 с.
3. *Петренко С. А., Курбатов В. А.* Политики информационной безопасности. М.: ДМК Пресс, 2006. 400 с.: ил. (Информационные технологии для инженеров).
4. *Петренко С. А., Симонов С. В.* Управление информационными рисками. Экономически оправданная безопасность. М.: ДМК Пресс, 2005. 384 с.: ил. (Информационные технологии для инженеров).