ВЕСТНИК РОССИЙСКОЙ АКАДЕМИИ НАУК, 2023, том 93, № 6, с. 512–517

С КАФЕДРЫ ПРЕЗИДИУМА РАН

ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ ПРОБЛЕМЫ ЦИФРОВИЗАЦИИ ПРЕДПРИЯТИЙ НЕФТЕГАЗОВОГО КОМПЛЕКСА

© 2023 г. В. Б. Бетелин[a],*, В. А. Галкин[b],, Р. Д. Гимранов[c],*****

[a]*Федеральный научный центр "Научно-исследовательский институт системных исследований РАН", Москва, Россия*

[b]*Сургутский филиал Федерального научного центра "Научно-исследовательский институт системных исследований РАН", Сургут, Россия*

[c]*Публичное акционерное общество "Сургутнефтегаз", Сургут, Россия*

**E-mail: betelin@niisi.msk.ru*

***E-mail: val-gal@yandex.ru*

****E-mail: gimranov_rd@mail.ru*

Поступила в редакцию 11.05.2023 г.
После доработки 11.05.2023 г.
Принята к публикации 27.05.2023 г.

В статье обсуждается проблема обеспечения гарантированного штатного функционирования цифровых систем в нефтегазовой отрасли России в условиях санкционной войны США и Евросоюза с этой отраслью. Для её решения предлагается использовать аппаратные и программные средства со встроенными интеллектуальными механизмами самоконтроля и самокоррекции. Запреты на поставки суперкомпьютеров для гидродинамических расчётов предлагается парировать применением вычислительных методов, основанных на точных решениях и грубых сетках.

Ключевые слова: цифровая система управления, штатное функционирование, интеллектуальные средства самоконтроля и самокоррекции, гидродинамические расчёты, точные решения гидродинамических уравнений на грубых сетках.

DOI: 10.31857/S0869587323060038, **EDN:** HYYSMZ

О проблеме штатного функционирования цифровых систем управления в нефтегазовой отрасли. Санкционная война США и стран Евросоюза – это, по сути, война с нефтегазовой отраслью России, отраслью, которая вносит решающий вклад в формирование государственного бюджета, в том числе таких его статей, как образование, здравоохранение, социальное обеспечение, оборона. Так, в 2021 г. чистая прибыль ПАО "Сургутнефтегаз" и ПАО "Роснефть" составила 513 млрд руб. и 883 млрд руб. при численности персонала 118 тыс. и 315 тыс. человек соответственно. Цель санкционной войны – создать условия, которые приведут к сокращению объёмов продаж российских нефтегазовых компаний и, как следствие, к снижению их вклада в государственный бюджет.



БЕТЕЛИН Владимир Борисович – академик РАН, научный руководитель ФНЦ "НИИСИ РАН". ГАЛКИН Валерий Алексеевич – доктор физико-математических наук, директор Сургутского филиала ФНЦ "НИИСИ РАН". ГИМРАНОВ Ринат Дамирович – кандидат экономических наук, начальник управления информационных технологий ПАО "Сургутнефтегаз".

Одно из таких создаваемых Западом условий – запрет на поставки в Россию высокотехнологичных продуктов компаний Intel, HP, Cisco, Simens, Microsoft, SAP и др., на основе которых построены цифровые системы управления российскими нефтегазовыми компаниями, например, суперкомпьютеров для гидродинамического моделирования процессов движения флюидов в нефтеносных пластах (такие суперкомпьютеры – неотъемлемая часть современных технологий управления нефтедобычей). Парировать эту угрозу можно путём разработки отечественных математических методов и программных систем гидродинамического моделирования, основанных на использовании точных решений на грубых сетках [1]. Эти решения позволяют существенно снизить требования к производительности суперкомпьютера, который может быть реализован российскими разработчиками на основе отечественных комплектующих.

При оценке возможных последствий запрета поставок зарубежных компьютеров и программного обеспечения, используемых в системах цифрового управления предприятием, необходимо учитывать и то обстоятельство, что в зарубежной программной и аппаратной продукции присутствуют и будут присутствовать ошибки (уязвимости), которые могут стать причиной проникновения вирусов, нарушающих штатное функционирование как самой продукции, так и цифровых систем управления предприятием, сформированных на её основе. В итоге сбои приведут к нарушению штатного функционирования и всей нефтегазовой компании. Другими словами, хотя коммерческие аппаратные и программные продукты упоминавшихся западных компаний обладают наилучшими показателями по соотношению производительности и стоимости, они обеспечивают при этом только экономически приемлемый для компаний-производителей уровень безопасности и надёжности, который недостаточен для цифровых систем управления предприятиями нефтегазовой отрасли, относящихся к категории систем с критической миссией.

Например, в документе компании Intel (№ 326767-004 от сентября 2012 г.) декларируется: «...корпорация Intel *снимает с себя всякую ответственность*, (курсив авторов), которая может возникнуть при ненадлежащем функционировании продуктов корпорации в *“системах с критической миссией”*». В документе № 324209-012 той же компании декларируется: “корпорация Intel официально заявляет, что продукты, описанные в документации, *могут содержать дефекты или ошибки, которые могут вызвать отклонения реального поведения продуктов* от поведения, описанного в опубликованных спецификациях”.

Ошибки (уязвимости) были, есть и будут присутствовать не только в зарубежных, но и в отечественных коммерческих программных и аппаратных продуктах, поскольку процесс их проектирования представляет собой последовательность построения их представлений на различных языках, таких, например, как язык спецификаций, языки Cu, RTL и др., которые должны быть алгоритмически эквивалентны. Однако проблема эквивалентности двух алгоритмов алгоритмически неразрешима, то есть невозможно формально доказать алгоритмическую эквивалентность различных представлений этих продуктов. Следовательно, указанные представления могут быть алгоритмически не эквивалентны, что, собственно, и служит источником ошибок. Речь идёт о неэквивалентности представления программного продукта на языке спецификаций его конечному представлению на машинном языке конкретного компьютера, то есть наблюдается как раз “отклонение реального поведения продуктов от поведения, описанного в опубликованных спецификациях”. Именно поэтому Федеральный закон ФЗ-187 “О безопасности критической инфраструктуры РФ” допускает возможность инцидентов, то есть кибератак на эту инфраструктуру, базирующуюся на коммерческих зарубежных и отечественных программных и аппаратных продуктах, уровень уязвимостей в которых обеспечивается на уровне приемлемом лишь для производителя этих продуктов. Пример тому – ошибка цифровой системы управления налоговой службы, которая в ряде случаев делала налогоплательщика налоговым должником перед государством в размере... одной копейки за счёт дефекта алгоритма округления.

Уязвимости коммерческой аппаратуры и программного обеспечения как зарубежного, так и отечественного относятся к категории не декларируемых производителем возможностей, которые не могут быть компенсированы на более высоких программных уровнях, но могут служить средством злоумышленного перехвата управления и нештатного функционирования цифровой системы управления критически важными объектами нефтегазовых компаний. Примером такого злоумышленного перехвата стало заражение вирусом Stuxnet и нештатного функционирования по этой причине цифровой системы управления на основе контроллеров фирмы Simens центрифуг иранской подземной фабрики по обогащению урана. В результате были физически разрушены более тысячи центрифуг.

В этой связи необходимо отметить, что именно такие довольно массовые контроллеры фирмы Simens используются в российских цифровых системах управления нефтедобычей и транспорти-

ровкой нефти, что, несомненно, несёт реальную угрозу их функционированию. Вирусы типа Stuxnet имеют высокий уровень скрытности распространения, вторжения и воздействия, поскольку созданы на основе детальных знаний о возможностях и уязвимостях как среды распространения (Microsoft), так и среды применения – программного обеспечения контроллеров Simens. Такие детальные знания о перечнях и особенностях обнаруженных зарубежными производителями уязвимостей российским специалистам недоступны, что не позволяет ни достоверно оценить реальный уровень безопасности и надёжности киберинфраструктуры нефтегазовых компаний, ни сколь-нибудь эффективно противостоять атакам вирусов типа Stuxnet.

Достаточно очевидно, что вирус, аналогичный Stuxnet, может быть создан и на основе детальных знаний о возможностях и уязвимостях коммерческих отечественных программных и аппаратных продуктов, поскольку они, как и зарубежные, обеспечивают уровень вероятности ошибок, приемлемый только для производителя, а для него первичен показатель производительность/стоимость. То есть функционирование цифровой системы управления на основе коммерческой аппаратуры и программного обеспечения, зарубежного или отечественного, чревато неустранимой угрозой самому процессу цифровизации нефтегазовой отрасли. Эти технологии не могут гарантировать штатного функционирования созданных на их основе цифровых систем управления предприятиями, независимо от наличия допущенных в процессе их разработки ошибок и внешнего злоумышленного использования уязвимостей.

Для обеспечения штатного функционирования таких уязвимых цифровых систем необходимо встроить непосредственно в их аппаратуру и программное обеспечение средства обнаружения вторжения и парирования последствий, что предполагает функциональную избыточность и в аппаратуре, и в программном обеспечении. Эта избыточность должна обеспечить контроль функционирования цифровой системы управления, предотвратить или нейтрализовать последствия деструктивных воздействий различного рода, в том числе и кибератак. Для этого и в аппаратуре, и в программном обеспечении должны быть реализованы средства самоконтроля, отслеживания и коррекции ключевых параметров управления предприятием или промышленным оборудованием. Такие средства должны охватывать элементную базу, средства вычислительной и коммуникационной техники, операционную систему, прикладные программы, которые собственно и реализуют алгоритмы управления. Например, в прикладной программе – это построение и отображение профилей выполнения программ, утверждения о поведении программ (статические или динамические при наличии в утверждении переменных), проверка временны́х ограничений на выполнение фрагмента программы [2].

Этот очевидно избыточный с коммерческой точки зрения дополнительный комплекс аппаратных и программных средств должен гарантировать штатное функционирование цифровых систем управления в нефтегазовой отрасли, несмотря на кибератаки, отказы аппаратных и программных компонент и даже возможные проявления ошибок реализации.

Госкорпорацией “Ростех” совместно с ведущими институтами РАН и вузами страны сформирована заявка на создание комплексной научно-технической программы полного цикла “Комплексная разработка и производство доверенных интеллектуальных программно-аппаратных платформ на основе отечественных электронных компонентов и программного обеспечения” (шифр: “Флагман-РЭК”). Эта заявка поддержана экспертным советом по приоритетному направлению Стратегии научно-технологического развития России “Переход к цифровым, интеллектуальным производственным технологиям, роботизированным системам, новым материалам и способам конструирования, создание систем обработки больших данных, машинного обучения и искусственного интеллекта”. Основная цель программы “Флагман-РЭК” – парирование угроз перехвата управления и нештатного функционирования систем с критической миссией (СКМ), в том числе промышленного оборудования добычи, транспортировки и переработки нефти и газа, атомных энергетических установок, тепловых, газовых и гидравлических турбин, электрогенераторов и электроподстанций, авиационного и железнодорожного транспорта; сложных технических объектов, к которым относятся предприятия нефте- и газодобычи, их транспортировки и переработки, тепловые, атомные и гидроэлектростанции, энергосистемы, аэропорты и железнодорожные узлы, банки.

Средство достижения основной цели – разработка и серийное производство не имеющих аналогов в мире доверенных интеллектуальных цифровых систем управления СКМ и всех их составляющих (электронная компонентная база, средства вычислительной техники, программные продукты) для обеспечения штатного функционирования в условиях внешних деструктивных воздействий с целью перехвата управления. Синергетический эффект достижения основной цели – крупносерийное производство в нашей стране элементной базы и вычислительной техники

на её основе, то есть возрождение радиоэлектронной отрасли России.

О математических проблемах моделирования нефтеносных залежей и разработке адекватных вычислительных методов. Важнейшей задачей математического моделирования в нефтегазовом секторе топливно-энергетического комплекса является повышение коэффициента извлечения нефти из матрицы нефтесодержащей породы, представляющей собой пористую среду, в микроструктуре которой содержатся флюиды различной природы.

Как правило, технология вычислений в решении индустриальных задач в существенной мере опирается на подгоночные параметры, специфические для конкретной установки. Поэтому весьма важно иметь точно решаемые задачи уравнений гидродинамики, позволяющие сформулировать квалифицированное заключение о работоспособности вычислительных комплексов, возможности переноса результатов моделирования на конструкции с принципиально различающимися параметрами.

В ряде проектов расчёт позволяет обсуждать только один объект, для которого уже выполнена настройка расчётных параметров, поэтому огромное значение имеет наличие библиотеки точных нестационарных решений уравнений гидродинамики в условиях сложной геометрии. Более того, эта библиотека может служить основой малоразмерных кусочных аппроксимаций течений аналогично сплайнам[1], позволяя существенно снизить вычислительную нагрузку за счёт использования грубых сеток с прецизионными решениями в межсеточном пространстве.

Прогресс в этих технологиях связывается в настоящее время только с увеличением размерности сеточных аппроксимаций и, как следствие, с ростом требований к производительности, а значит, росту стоимости супер-ЭВМ. В конечном счёте это приводит к увеличению числа и производительности параллельно работающих микропроцессоров. Поскольку производительность микропроцессора в основном определяется технологическим уровнем его производства, то, по сути дела, в настоящее время прогресс в вычислительных технологиях на основе сеточных аппроксимаций большой размерности определяется прогрессом в области микроэлектронных технологий. Отставание в области микроэлектроники влечёт за собой отставание в технологиях моделирования на основе сеточных аппроксимаций большой размерности.

Масштаб задач, имеющих практическую значимость. О сложности этих задач говорят следующие факты:

• геометрические размеры нефтеносной залежи характеризуются кубом со стороной порядка десятка километров;

• нефтесодержащие флюиды располагаются в каналах пористой матрицы залежи с характерными размерами сечений порядка микрометров со значительной неоднородностью физико-химических характеристик на масштабах залежи;

• получение экспериментальных данных для реальных объектов – достаточно дорогостоящий процесс, а сами данные характеризуются большим разбросом параметров проб, извлекаемых из скважины на поверхность;

• работа предприятия нефтегазовой отрасли связана со сложной логистикой, опирающейся на обработку значительных информационных потоков с сопутствующими требованиями к информационной и физической безопасности производственного цикла.

В связи с масштабом высокотехнологичной задачи возникает проблема управления динамикой нефтесодержащих флюидов в пористой среде. Создание реальных моделей месторождений затруднен в отсутствие глубокого и детального изучения фильтрационно-ёмкостных свойств материала матрицы, в том числе его основных параметров – характерных размеров порового пространства, его топологической связности на реальных масштабах залежи.

В течении многофазных жидкостей типично образование локальных зон – структур, заполненных жидкостью одной фазы. Это явление специфично для процесса выдавливания нефти посредством воды или газа. Причиной служит существенное различие коэффициентов вязкости жидкостей. Обычно вода и газ обтекают “целики” нефти, которые остаются неподвижными в матрице среды. Одним из способов выделения “структур” служит формирование пространственно-временных областей, в которых макроскопические параметры состояния системы приобретают сингулярности, априори не включённые в язык описания системы. В этом случае имеет место неполнота языка математической модели, приводящая к понятиям обобщённых решений и требующая уточнения постановки исходной задачи. По существу, зачастую это означает отсутствие корректности рассматриваемых задач в исходной постановке.

Масштабы вычислительной трудоёмкости требуют для решения реальных задач моделирования течения в $\sim 10^{18}$ каналах. Традиционные подходы опираются на сеточные, проекционные

[1] Сплайн – функция в математике, область определения которой разбита на конечное число отрезков, на каждом из которых она совпадает с некоторым алгебраическим многочленом. (*Прим. ред.*)

методы, которые по своей природе весьма затратны с точки зрения их реализации на вычислительной технике, поскольку основная нагрузка, связанная с процессами вычисления, падает на последовательный обход узлов сетки с неминуемым накоплением ошибок в экспериментальных данных и неустранимых ошибок в вычислительных операциях. В конечном счёте гонку в этой области деятельности определяют размерность вычислительных сеток (количество узлов сетки), что неумолимо диктует гонку в области суперкомпьютерных технологий. При этом возможность верификации проектных расчётов крайне ограничена и вызывает существенные сомнения в их применимости в широком диапазоне параметров течения. Существенный вклад в эффективное понижение размерности вычислительных аппроксимаций и уменьшение ошибок округления может внести использование точных решений между узлами грубых сеток.

В связи с вышеизложенным перспективным направлением исследований представляется разработка оптимизационных процедур аппроксимации решений с помощью комбинаций точных решений на грубых сетках, что по своей сути близко к конструированию специализированных искусственных нейронных сетей. Эта идеология является синтетическим обобщением классического метода “первых интегралов” в теории дифференциальных уравнений для понижения размерности дифференциальных систем.

На этом направлении получены практические результаты, позволяющие выявить тонкую структуру нестационарных трёхмерных вихревых гидродинамических течений. В частности, разрабатывается иерархия моделей, реализованная на основе малоразмерных эффективных алгоритмов с использованием отечественной вычислительной техники средней производительности, обеспечивающих точность, необходимую для практической работы. Иерархия моделей включает в себя локальный анализ структуры керна и гидродинамику в нём флюидов на основе малоразмерных вычислительных алгоритмов.

Разработана методика “сшивки” решаемых задач по иерархии масштабов, соответствующих реальным размерам залежи. Эта методика положена в основу программного комплекса анализа связности порового пространства и определения таких его основных характеристик, как пористость, проницаемость, длина каналов, связность порового пространства, трещиноватость, гранулометрический состав породы, соотношение и количество связных и закрытых каналов, удельная поверхность, соотношение пор и матрицы породы.

Проблемы импортозамещения и цифровой трансформации промышленных предприятий. Промышленное производство характеризуется длительным циклом капиталоёмкости. Жизненный цикл активов составляет годы и десятилетия. Это накладывает свои особенности на организационный капитал предприятия – организационную структуру, правила управления процессами, информационные системы, стандарты, компетентность руководителей и специалистов. Такие особенности сложно сочетаются с подходами цифровизации, которая предполагает быструю смену технологий, создание продуктов и услуг с высокой долей нематериальных активов, необходимость быстрого и регулярного дополнительного профессионального обучения [3].

В настоящее время проблемы цифровой трансформации промышленных предприятий отягощены задачей импортозамещения: нужно в достаточно короткий срок – за несколько лет – заменить программное и аппаратное обеспечение производителей из недружественных стран, в основном членов НАТО, на отечественные аналоги. Необходимость импортозамещения и угрозы кибербезопасности действующих программно-аппаратных компонентов из недружественных стран усиливают риски устойчивости работы промышленных предприятий в условиях цифровой трансформации [4]. В особенности это актуально для сложных ситуаций, требующих качественных управленческих решений.

Наиболее выигрышные подходы к успешному решению задач импортозамещения и цифровой трансформации должны учитывать вышеперечисленные особенности и опираться на объединяющие решения, дающие синергетический эффект. Одним из таких подходов мы считаем создание и использование продуктов, созданных по полному циклу – от исследований до промышленного использования. Полный цикл вполне естественен как для промышленных компаний, так и для предприятий сферы информационных технологий. Необходимо выявлять области, где работы полного цикла будут наиболее эффективны, и инициировать перспективные проекты. Причём на исследовательской фазе цикла, особенно при необходимости фундаментальных исследований, требуется активное участие бюджетных и ведомственных исследовательских организаций, включающих такие проекты в государственные программы. Чем ближе к промышленному использованию, тем существенней должна быть роль в работах промышленного предприятия. Такой подход соответствует задачам достижения национального технологического суверенитета, так как способствует получению и развитию отечественных результатов интеллектуальной деятельности (технологий, архитектур, стандартов, опытных образцов).

Одним из конкретных направлений применения подхода полного цикла выступает создание защищённых, самовосстанавливающихся программно-аппаратных комплексов, как универсальных, так и специализированных под конкретные производственные задачи. Программа “Флагман-РЭК” в полной мере отвечает условиям эффективной реализации проектов полного цикла в области достижения национального технологического суверенитета.

ЛИТЕРАТУРА

1. *Бетелин В.Б., Галкин В.А.* О проблеме снижения размерности сеточных аппроксимаций // Успехи кибернетики. 2021. № 4. С. 75–77.
2. *Бетелин В.Б., Исаев В.М.* О создании доверенных интеллектуальных программно-аппаратных платформ на основе отечественных электронных компонентов и программного обеспечения // Оборонная наука – экономике России. М.: Оружие и технологии, 2021. С. 114–119.
3. *Ананьин В.И., Зимин К.В., Гимранов Р.Д., Лугачев М.И., Скрипкин К.Г.* Реальное время управления предприятием в условиях цифровизации // Бизнес-информатика. 2019. № 1. С. 7–17.
4. *Гимранов Р.Д.* Группировка угроз и рисков экономической безопасности цифрового предприятия нефтегазовой отрасли: ситуационный подход // Креативная экономика. 2020. № 7. С. 1291–1310.