Вестник Тюменского государственного университета.
Физико-математическое моделирование. Нефть, газ, энергетика. 2015. Том 1. № 2(2). 173-184

© С. В. СТЕПАНОВ[1], А. А. ЗАХАРОВ[2], А. В. БОЙКО[3]

[1]ТННЦ «Роснефть»
[2, 3]Тюменский государственный университет
[3]Voron70@gmail.com

УДК 519.711

ОБ ОДНОМ ПОДХОДЕ К РАЗРАБОТКЕ ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ПРОЕКТИРОВАНИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ ДОБЫЧИ НЕФТИ

AN APPROACH TO THE DEVELOPMENT OF A SOFTWARE COMPLEX FOR DESIGN PROCESS OIL RECOVERY

В данной статье рассматривается проблема создания виртуальной лаборатории на основе SaaS облака. Такая лаборатория позволяет непосредственно на производстве использовать комплекс программ (сервисов) для проектирования технологических режимов добычи нефти. Описаны три программных сервиса, включенных в облако SaaS. Сервис для разделения добычи и закачки при одновременной совместной разработке пластов. Сервис для исследования причин сложной немонотонной динамики обводнения вертикальной нефтяной скважины при обводнении. Сервис для изучения динамики газового фактора для горизонтальной нефтяной скважины в условиях образования газового конуса. Рассматриваются угрозы безопасности в виртуальных средах. Рассмотрены проблемные вопросы защиты гипервизора и сервера управления виртуальной машины. Предложены меры по организации защиты информации в виртуальных средах и облачных платформах.

This article deals with the problem of creating a virtual laboratory based on SaaS cloud. This laboratory allows you to use a set of programs (services) for the design of technological modes of oil recovery at production. The three program services included in the cloud SaaS are described. The first is the service to separate production and injection in joint development of reservoirs. The second service is to investigate the causes of the dynamics of complex non-monotonic inundation vertical oil well with a water cut. The third service is to study the dynamics of the gas factor for horizontal oil well in the conditions of gas coning. The main threats to the security of information in virtual environments and cloud platforms are shown. Problem questions of protection of the hypervisor and the server of virtual machine management are considered. Some steps for the protection of information in virtual environments and cloud platforms are suggested.

КЛЮЧЕВЫЕ СЛОВА. Технологические режимы добычи нефти, защита информации, облачные вычисления, виртуализация.

KEY WORDS. Technological regimes of oil recovery, information security tools, cloud computing, virtualization.

Введение

Задача увеличения извлечения нефти за счет расширения применения новых моделей и методов и технологий была поставлена еще в «Основных направлениях экономического и социального развития СССР на 1981-1985 годы и на период до 1990 года». Решение задачи предусматривало комплекс научных и технических и технологических мероприятий, ориентированных на создание банков гидрогеологической, геогидродинамической и гидрогеохимической информации, а также технологий моделирования, позволяющих оптимизировать процессы, связанные с разведкой, добычей и транспортировкой углеводородного сырья.

Принципиально важно отметить, что параллельно с разработкой новых моделей развивается индустрия создания программного обеспечения, позволяющая тиражировать не только отдельные системные и прикладные программы определенного назначения на разных аппаратных платформах, но и создавать информационные и вычислительные системы «под ключ» путем интеграции различных сервисов в целевые проблемно-ориентированные комплексы. Для внедрения новых моделей и технологий проектирования технологических процессов извлечения нефти непосредственно в производство особую ценность представляет концепция облачных вычислений [1], в частности SaaS (Software as a service — прикладное ПО как услуга) [2] позволяющая создавать web-ориентированные лаборатории с интерактивным доступом и к инструментам моделирования и к качественной поддержке пользователей: хранение исходных данных и результатов, визуализация процессов и т. п.

Описание облачных сервисов

Практика решения задач при проектировании и сопровождении разработки месторождения нефти и газа показывает, что возможности существующего коммерческого программного обеспечения часто являются недостаточными. В этой связи создается оригинальное программное обеспечение, например, для проектирования технологических режимов нефтяных горизонтальных скважин в подгазовых зонах [3] или для анализа заводнения [4]. Описываемые ниже сервисы облачного программного комплекса созданы для решения задач анализа и проектирования разработки нефтяных и газонефтяных месторождений компаний «СургутНефтеГаз» и «Роснефть»:

• программа «RecoveryDevision» разделение добычи/закачки при одновременной совместной разработке пластов (значительное количество месторождений представлено именно многопластовыми залежами, разрабатываемых одновременно и совместно);

• программа «WellTuner» исследование причин сложной немонотонной динамики обводнения вертикальной нефтяной скважины в условиях обводнения;

• программа «Sterkh» имитация динамики газового фактора горизонтальной нефтяной скважины в условиях образования газового конуса и при поддержании пластового давления.

Отметим, что общим моментом в реализованных сервисах появляется возможность решать прямые и обратные задачи подземной гидродинамики применительно к конкретным производственным постановкам. При этом решение обратных задач возможно как в ручном, так и в автоматическом режиме. Автоматический режим основывается на методе Нелдера−Мида с заданием начального симплекса по методу Монте-Карло. Такой подход позволяет определить глобальный экстремум оптимизационной задачи, а следовательно повысить надежность в определении управляющих параметров.

Программа «*RecoveryDevision*» — результат работы по созданию быстродействующего по сравнению с альтернативными продуктами, использующими гидродинамические модели (ГДМ) сервиса для оперативной оценки добычи и закачки по пластам при их одновременной совместной разработке.

В основе программы лежит аналитическое решение уравнения материального баланса в виде Capacitance-Resistive Models (CRM) [4; 5], которое учитывает взаимодействие добывающих и нагнетательных скважин, упругоемкость пластовой системы, влияние на добычу водоносного горизонта, объемы закачки воды и изменения забойного давления добывающих скважин. В рамках разработанного метода допускается, что решение CRM справедливо для каждого из пластов многопластовой залежи. В таком предположении задача определения коэффициентов разделения добычи и закачки сводится к решению обратной задачи, для которой невязка в целевой функции формулируется относительно суммарного по всем пластам дебита жидкости. По аналогии с расшифровкой аббревиатуры CRM, метод, разработанный на этой основе для случая нескольких пластов, мы называем CRMML (Capacitance Resistive Model for Multiplicity Layers). Для корректного учета влияния конфигурации области дренирования в модели CRMML параметры упругоемкости и взаимовлияния между скважинами представлены как монотонные положительные функции аналогичные по форме зависимости изотерме адсорбции Ленгмюра. Метод позволяет получить качественную и количественно верную картину по притокам жидкости из пластов с приемлемой погрешностью. Решение тестовых задач с использованием синтетических ГДМ показало, что относительная погрешность в коэффициентах деления добычи жидкости и закачки воды не превышает 7%.

Результаты расчетов по методу CRMML также сопоставлялись с результатами расчета на симуляторе Eclipse для участка Самотлорского месторождения. При решении оптимизационной задачи использовались фактические данные по добыче жидкости, которые также задавались в качестве граничного условия в ГДМ. На рис.1 и в таблице показаны результаты расчетов, соответствующие решению оптимизационной задачи с наименьшим значением целевой функции. Как видно из рис.1, модель CRMML позволяет воспроизвести фактические

данные по добыче жидкости за исключением интервала времени (ориентировочно) 200-300 месяцев от начала разработки участка. Отметим, что такая особенность характерна для всех вариантов расчетов. Тем не менее, как показывает сравнение коэффициентов деления добычи/закачки (таблица), полученные значения по методу CRMML качественно и количественно согласуются со значениями, полученными по ГДМ.

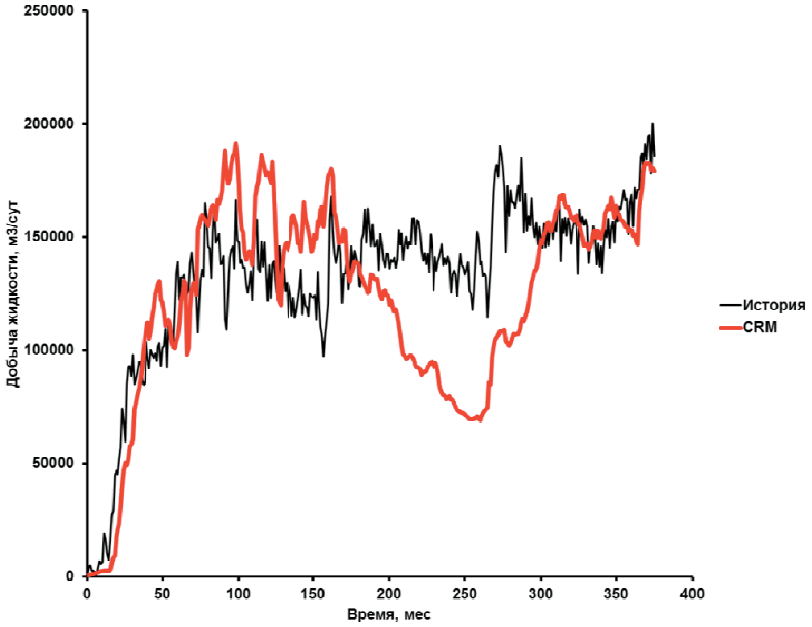


Рис. 1. Фактическая и расчетная динамики добычи жидкости

Таблица

Сравнение коэффициентов деления добычи и закачки по пластам

Модель	Доля добычи, %			Доля закачки, %		
	AB1(1-2)	AB1(3)	AB2-3	AB1(1-2)	AB1(3)	AB2-3
Eclipse	7.6	51.5	40.9	7.2	63.1	29.7
CRM	5.5	60.3	34.2	5.9	57.9	36.1

Программа «*WellTuner*» разработана для детального моделирования работы нефтяной вертикальной добывающей скважины в условиях ее обводнения. В данной программе используется модель двухфазной изотермической фильтрации нефти и воды. Особенностью численной реализации является возможность использования зависимости относительных фазовых проницаемостей (ОФП) от капиллярного числа и детальных расчетных сеток различной конфигурации в радиальном направлении, что дает возможность корректно рассчитать фильтрационное сопротивление вблизи скважины.

Использование программы «WellTuner» позволило выявить причины сложной немонотонной динамики обводнения реальных скважин [6]. На рис. 2 показаны фактическая и расчетные динамики обводненности скважины, соответствующие решениям обратной задачи с целевой функцией, учитывающей невязку по обводненности. Исходные постановки задач отличались тем, что в первом случае управляющие параметры включали свойства пласта (абсолютную проницаемость, ОФП), а во втором случае — еще и протяженность интервала перфорации.

По результатам расчетов получено, моделирование сложной немонотонной динамики обводненности скважины оказалось возможным только в предположении о том, что работающим является не весь интервал перфорации. Как видно из рис. 2а, б на расчетную динамику обводненности влияет учет модели капиллярного давления и сжимаемости. Влияние капиллярного давления проявляется в монотонности тренда кривой динамики обводненности, а сжимаемости — в амплитуде «пульсаций» обводненности. При этом величина пульсаций увеличивается с уменьшением интервала перфорации. Данный факт объясняется влиянием длины интервала перфорации на эффект от различной сжимаемости пористой среды насыщенной многофазной жидкостью. Это следует из того факта, что для заданного фактического изменения дебита жидкости при уменьшении интервала перфорации изменение давления становится более сильно выраженным как по пространству, так и во времени.

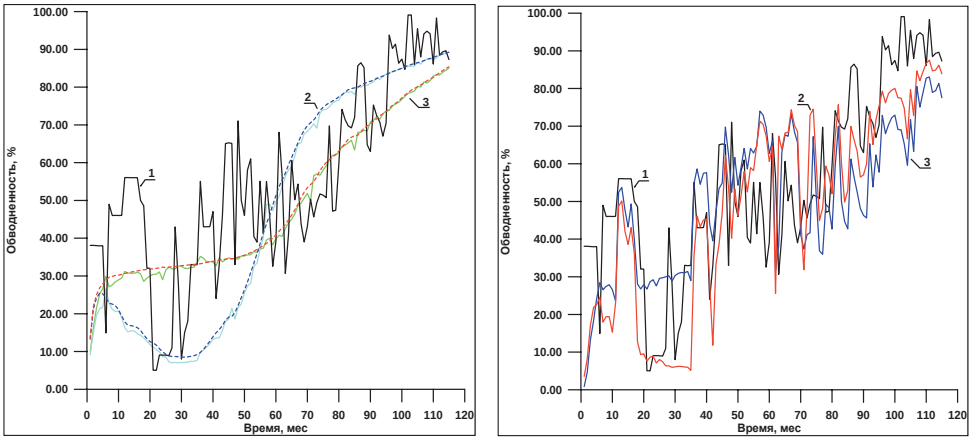


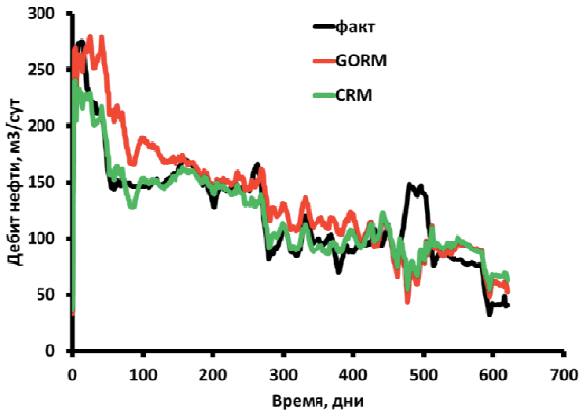
Рис. 2. Расчетные и фактическая динамики обводненности скважин:
а — перфорация 13 м, б — перфорация 7 м. 1 — факт, 2 — расчет с учетом капиллярного давления, 3 — расчет без учета капиллярного давления.
Сплошная линия — расчет с учетом сжимаемости,
пунктирная линия — расчет без учета сжимаемости

Программа «*Sterkh*» разработана для обоснования технологического режима нефтяной горизонтальной скважины в условиях образования газового конуса и поддержании пластового давления посредством закачки воды. В основе

программы лежит оригинальный численно-аналитический метод NAMGC (Numerical-Analytical Method of Gas Cone), полученный объединением упрощенной численной модели газового конуса GORM [4] и аналитической модели CRM [5].

Подробное описание численной реализации метода NAMGC, в том числе и с позиции исследования численного решения приведено в работах [7; 8]. На рис. 3 показаны фактические и расчетные динамики дебита нефти. Видно, что упрощенные модели GORM и CRM, формирующие метод NAMGC, позволяют воспроизводить достаточно сложную динамику дебита нефти. В данных примерах обращает на себя внимание тот факт, что для скважины 1 обе модели показали примерно одинаковое качество имитации дебита нефти, а для скважины 2 качество имитации по модели CRM значительно лучше, чем по модели GORM. Анализ исследований работы данных скважин показал, что влияние закачки воды в ячейках заводнения данных скважин разное, а именно для скважины 2 оно выше, чем для скважины 1, что согласуется с результатами моделирования.

а



б

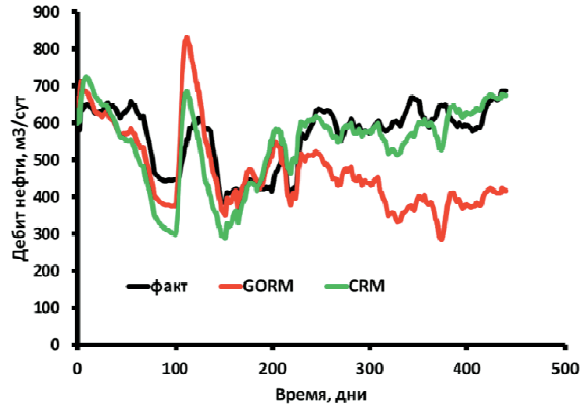


Рис. 3. Фактические и расчетные динамики дебита нефти для скважины 1 (а) и для скважины 2 (б).

В качестве облачной платформы SaaS для описанных выше сервисов выбран продукт VMware vCloud Director, использующий в своей основе платформу виртуализации VMware vSphere.

Информационная безопасность предлагаемых технологий

Пилотное внедрение комплекса показало, что одна из самых распространенных причин, по которым организации не спешат внедрять облачные IT сервисы, является безопасность исходных данных и результатов расчетов. Действительно, облачные вычисления не дают заказчику возможности контролировать не только технологические, но и собственные информационные ресурсы, а, следовательно, в такой области как подсчет запасов, где информация напрямую связана с налогообложением добывающих компаний, вопросы информационной безопасности выходят на первое место. Пользователи посылая на обработку свои данные должны быть уверены в том, что их данные обрабатываются строго в соответствии с установленным технологическим процессом, учитывающим организационные и технические требования по обеспечению безопасности.

Применение ПО виртуализации как основы облачных технологий требует существенного изменения в подходах к обеспечению информационной безопасности систем [9]. Необходимо отметить появление нового, принципиально важного объекта виртуальной инфраструктуры — гипервизора, который на практике часто игнорируется и не защищается при помощи специализированных средств. Отметим, что за счет компрометации одного только гипервизора возможен вариант получения контроля над всеми подконтрольными ему виртуальными машинами и даже всей инфраструктурой виртуализации. В качестве защиты применялись: интеграция хост-серверов со службой каталога Active Directory, использование политик сложности и устаревания паролей, стандартизация процедур доступа к управляющим средствам хост-сервера, встроенный брандмауэр хоста виртуализации, применение единого профайла политик безопасности хоста, сторонние инструменты аудита и контроля доступа к подсистемам гипервизора.

Следует отметить, что при внедрении технологий виртуализации происходят серьезные изменения в физической инфраструктуре. С точки зрения организации сети возникает такое новое понятие как виртуальный коммутатор, который обеспечивает сетевое взаимодействие виртуальных машин в пределах одного хоста виртуализации. Проблема виртуальных коммутаторов заключается в не подконтрольности внутрисетевого трафика, а также в возможности прослушивания всего сетевого трафика между виртуальными машинами. Для решения проблемы прослушивания портов использован подход к организации сетей VLAN на базе виртуальных коммутаторов, где тегирование кадров происходит на уровне хоста виртуализации еще до попадания пакетов в физическую сеть.

Виртуальная машина является самым потенциально опасным объектом виртуальной инфраструктуры с точки зрения информационной защиты ввиду ее изначальной полной незащищенности и простоты модификации данных. Кроме того, такие технологии как «живая миграция» и «мгновенные снимки»

способны послужить отличным инструментом сокрытия следов присутствия в руках злоумышленника. В частности, злоумышленник, проникнув в гостевую операционную систему виртуальной машины и имея достаточный контроль над системой управления хостом виртуализации, может скрыть следы своего пребывания путем возврата к предыдущему снимку диска виртуальной машины (снапшоту). Наконец, кража самих файлов мгновенных снимков виртуальной машины способна привести к серьезной утечке информации, поскольку они содержат в себе все последующие изменения данных на виртуальном диске и полный снимок оперативной памяти виртуальной машины с момента создания снимка. Исходя из вышесказанного, были выделены следующие основные типы угроз безопасности виртуальных сред:

1. Атака на виртуальную машину:

— из другой виртуальной машины;

— на диск и файлы конфигурации виртуальной машины;

— на сеть репликации виртуальных машин;

— на сеть и систему хранения данных содержащей файлы виртуальной машины;

— на средства резервного копирования виртуальной машины.

2. Атака непосредственно на хост (гипервизор) виртуализации:

— из физической сети;

— средствами скомпрометированного сервера управления виртуальной инфраструктурой;

— через внутренние сервисы гипервизора SSH, WEB, TELNET и др.;

— через агентов гипервизора от сторонних производителей.

3. Атака на сервер управления виртуальной инфраструктуры:

— через гостевую ОС, обеспечивающую функционирование управляющих сервисов;

— через СУБД сервера управления виртуальной инфраструктурой;

— через базу учетных записей;

— через сервис взаимодействия и мониторинга с хостами виртуализации.

4. Атака на ресурсы хоста виртуализации путем:

— неконтролируемого роста числа виртуальных машин;

— некорректного планирования разграничения пулов ресурсов;

— некорректного планирования растущих по мере заполнения виртуальных дисков ВМ;

— некорректного разграничения прав пользователей и групп виртуальной инфраструктуры.

Защита исходных данных

Для решения наиболее острой проблемы — обеспечения защиты доступа к исходным данным и результатам расчетов, хранящихся на дисках виртуальных машин и подверженных описанным выше типам угроз, было успешно опробовано решение шифрования дисков в реальном времени и доверенной загрузки виртуальных машин на базе дополнительного программного комплекса

SafeNet ProtectV. ProtectV представляет собой полное функциональное решение для шифрования данных в виртуализированных и облачных окружениях, которое позволяет осуществлять управление данными, администрирование данных и обеспечивает их прозрачность, а также помогает соблюдать требования информационной политики организации — клиента облачных IT услуг. С помощью системы шифрования ProtectV появилась возможность защитить критичные данные хранящиеся в виртуальных машинах конечных пользователей облака на протяжении всего их жизненного цикла: от момента подготовки и инициализации и до уничтожения. Среди основных особенностей решения — гранулярное и полное шифрование всех виртуальных дисков виртуальной машины. Оно поддерживает предстартовую аутентификацию и размещение отправной точки доверия на оборудовании на стороне заказчика, что обеспечивает комплексную защиту на всем протяжении жизненного цикла информации, позволяет запускать системы в многопользовательском окружении. Все виртуальные машины и соответствующие им разделы для хранения данных шифруются с применением надежного симметричного алгоритма блочного шифрования AES с длиной ключа 256 бит — сюда относятся копии дисков виртуальных машин (vmdk), их конфигурации (snapshot) и резервные копии на всех узлах и площадках аварийного восстановления. Таким образом, привилегированные пользователи и администраторы облачной инфраструктуры, без прямой санкции владельца виртуальных машин, не могут получить доступ к зашифрованным виртуальным машинам. Для осуществления надлежащего контроля и обеспечения надежного управления аудитом вне зависимости от того, где размещаются или хранятся данные, соблюдая при этом требования законодательных нормативных актов (включая PCI DSS, HIPAA) используется механизм фиксируемого контроля с подтверждением операций по управлению данными через журналы аудита.

Для автоматизированного аудита виртуальной среды на предмет наличия ошибок в конфигурации безопасности виртуальной инфраструктуре VMware vSphere нами разработан программный продукт, который использует для взаимодействия с компонентами платформы виртуализации VMware vSphere стандартный VMware vSphere SDK интерфейс. На вход программе подается адрес конкретного хоста виртуализации VMware ESX либо сервера управления всей инфраструктурой VMware vCenter и учетные данные пользователя с правами на чтение. На выходе программа генерирует отчет по состоянию защиты исследуемого объекта и выставляет общий рейтинг защищенности на соответствие одному из трех уровней защищенности, предложенных компанией производителем VMware Inc:

1. Уровень предприятия (Enterprise). Этот уровень предназначен для защиты от большинства типичных атак на виртуальную инфраструктуру и обеспечения высокого уровня защищенности конфиденциальной информации.

2. Уровень демилитаризованной зоны (DMZ). Этот уровень позволяет обеспечить надежную защиту хостов и виртуальных машин, имеющих подключение к Интернет.

3. Уровень специализированной зоны с ограниченной функциональностью (SSLF). Этот уровень призван обеспечить максимально возможную степень защиты виртуальной инфраструктуры, в том числе за счет потери определенной функциональности виртуальной инфраструктуры в пользу защищенности от самых ухищренных атак.

Отчет представляет собой детализированную таблицу, разделенную по типам угроз, свойственных виртуальной инфраструктуре, которые были предложены выше. В качестве тестов на защищенность используется отслеживание параметров конфигурации хостов, виртуальных машин, сервера управления и 64 другие, основанные на рекомендуемых регламентах производителя, платформы. В основе этих рекомендаций лежит технический документ VMware vSphere Hardening Guide, описывающий 3 уровня защищенности виртуальной инфраструктуры VMware vSphere, где каждому из этих уровней соответствует более 100 параметров объектов системы виртуализации. Все эти параметры аккумулируются и анализируются движком программы в автоматическом режиме и накладываются на заранее созданный шаблон угроз по уровню защищенности. В результате пользователь (администратор) может детально отследить, какому уровню защищенности соответствует данная виртуальная инфраструктура и на какие параметры системы следует обратить внимание для приведения ее в соответствие.

Предлагаемый программный комплекс в значительной мере повышает безопасность виртуальной инфраструктуры, однако, естественно, он не в состоянии обеспечить абсолютную защиту виртуальной среды. Следовательно, необходимо выработать и стандартизовать единый подход к обеспечению информационной безопасности в виде регламентов и стандартов, обязательно учитывая рекомендации производителя платформы виртуализации, поскольку именно технологические особенности платформы определяют необходимые меры по обеспечению безопасности.

Вывод

В рамках научного сотрудничества с Тюменским нефтяным научным центром на основе изложенных принципов авторами был выполнен пилотный проект по использованию безопасных облачных технологий для виртуальной лаборатории. В реализованном формате данная виртуальная лаборатория позволяет использовать комплекс оригинальных программ, позволяющих исследовать причины сложной немонотонной динамики обводнения скважин, определять коэффициенты деления добычи и закачки по пластам при их одновременной совместной разработке, а также прогнозировать технологический режим нефтяных горизонтальных скважин подгазовой зоны. Каждый из сервисов облачного программного комплекса также позволяет определять данные о системе «пласт−скважина», в т. ч. и в автоматическом режиме решения обратных задач.

СПИСОК ЛИТЕРАТУРЫ

1. Иванников В. П. Облачные вычисления в образовании, науке и госсекторе // Параллельные вычисления и задачи управления: пленарные доклады V Междунар. конф. М., 2010.

2. Листопад Н. И., Олизарович Е. В. Модели функционирования «облачной» компьютерной системы //Доклады БГУИР. № 3 (65). 2012. С. 23-29.

3. Мьеваттен А., Осхайм Р., Сэлид С., Груннинг О. Модель образования газового конуса и зависимости газового фактора от темпа отбора в нефтеназоносном пласте с нефтяной оторочкой, SPE 102390, 2006.

4. Sayarpour M., Zuluaga E., Kabir C. S., Lake L. W. The Use of Capacitance-Resistive Models for Rapid Estimation of Waterflood, SPE 110081, 2007.

5. Алтунин А. Е., Семухин М. В., Степанов С. В. Использование материального баланса и теории нечетких множеств для решения задачи разделения добычи при одновременной разработке нескольких пластов // Нефтяное хозяйство. 05-2012. С. 56-60.

6. Степанов С. В. Численное исследование влияния капиллярного давления и сжимаемости на динамику обводненности скважины // Нефтяное хозяйство. 08-2008. С. 72-74.

7. Степанов С. В., Степанов А. В., Елецкий С. В. Численно-аналитический подход к решению задачи оперативного прогнозирования работы нефтяной скважины в условиях образования газового конуса // Нефтепромысловое дело. 2/2013. С. 53-58.

8. Степанов С. В., Гринченко В. А., Степанов А. В., Анурьев Д. А., Долгов И. А. Сопровождение разработки подгазовой зоны с использованием различных видов гидродинамического моделирования на примере Верхнечонского месторождения // Научно-технический вестник ОАО «НК «Роснефть», 4-2013. С. 38-45.

9. Захаров А. А., Бойко А. В. Безопасность HPC для интеллектуальных месторождений //Научный сервис в сети Интернет: поиск новых решений: Труды Международной суперкомпьютерной конференции (17-22 сентября 2012 г., г. Новороссийск). М.: Изд-во МГУ, 2012. С. 63-65.

REFERENCES

1. Ivannikov, V. P. Oblachnye vychislenija v obrazovanii, nauke i gissektore // Parallelnye vychisleniia i zadachi upravlenija: Plenarnie dokladi V Mezhdunar. konf. M., 2010.

2. Listopad, N. I., Olizarovich, E. V. Modeli fuktsionirovanija "oblachnoj" komputernoj sistemy // Doklady BGUIR. № 3 (65). 2012. Pp. 23-29.

3. Mievatten, A., Oskhaim, R., Selit, S., Grunning, O. Model obrazovanija gazovogo konusa i zavisimosti gazovogo faktora ot tempa otbora v neftegazonosnom plaste s neftianoj otorochkoj, SPE 102390, 2006.

4. Sayarpour, M., Zuluaga, E., Kabir, C. S., Lake, L. W. The Use of Capacitance-Resistive Models for Rapid Estimation of Waterflood, SPE 110081, 2007.

5. Altunin, A. E., Semuhin, M. V., Stepanov, S.V. Ispol´zovanie material´nogo balansa i teorii nechetkikh mnozhestv dlia reshenija zadachi razdelenija dobychi pri odnovremennoj razrabotke neskolkikh plastov // Neftianoe khoziajstvo, 05-2002. Pp. 56-60.

6. Stepanov, S. V. Chislennoe issledovanie vlijanija kapilliarnogo davlenija i szhimaemosti na dinamiku obvodnennosti skvazhyny // Neftianoe khoziaistvo, 08-2008. Pp.72-74.

7. Stepanov, S. V., Stepanov, A. V., Eletskiy, S. V. Chislenno-analiticheskij podkhod k resheniu zadachi operativnogo prognozirovanija raboty neftianoj skvazhyny v uslovijakh obrazovanija gazovogo konusa//Neftepromislovoe delo, 2/2013. Pp. 53-58.

8. Stepanov, S. V., Grinchenko, V. A., Stepanov, A. V., Anuriev, D. A., Dolgov, I. A. Soprovozhdenie razrabotki podgazovoj zony s ispolzovaniem razlichnykh vidov gidrodinamicheskogo modelirovanija na primere Verkhnechonskogo mestorozhdenija // Nauchno-tekhnicheskii vestnik OAO "NK "Rosneft". 4-2013. Pp. 38-45.

9. Zaharov, A. A., Boiko, A. V. Bezopasnost NRS dlia intellektualnykh mestorozhdenij //Nauchnij servis v seti Internet:Poisk novykh reshenii:Trudi Mezhdunarodnoi superkompiuternoi konferentsii (17-22 September 2012, Novosibirsk). M.: Izd-vo MGU, 2012. Pp. 63-65.

Авторы публикации

Степанов Сергей Викторович — старший научный сотрудник ТННЦ «Роснефть», кандидат технических наук

Захаров Александр Анатольевич — зав. кафедрой информационной безопасности Тюменского государственного университета, доктор технических наук

Бойко Александр Васильевич — зам. начальника отдела IT-инфраструктуры ЦиТ Тюменского государственного университета

Authors of the publication

Sergey V. Stepanov — Cand.Tech.Sci., Senior Research Associate, Tyumen Petroleum Research Centre Ltd., "Rosneft" Oil Company

Alexandr A. Zaharov — Doctor of Tech.Sciences, Head of IT-security department, TSU

Alexandr V. Boyko — Deputy Head of IT-Infrastructure Department REC, Tyumen State University