

УДК 004.75 (004.624)

Р.В. Мещеряков, О.И. Жуковский, П.В. Сенченко, Ю.Б. Гриценко, М.М. Милихин

## Особенности архитектуры единого информационного пространства при управлении сложными технологическими процессами

Предложены решения, позволяющие обеспечить взаимодействие между компонентами автоматизированной системы управления подводной добычей с помощью береговой станции на основе параметрической модели подводного добычного комплекса (АСУ ПДК). Рассматриваются особенности архитектуры единого информационного пространства с целью объединения существующих источников данных, необходимых для совместного использования при управлении сложными технологическими процессами. В рамках проектирования архитектуры разрабатываемой системы предложено использовать сервис-ориентированный подход, предполагающий разделение системы на компоненты (сервисы). Описывается ролевая модель доступа к данным, положенная в основу определения политики безопасности.

**Ключевые слова:** единое информационное пространство, подводный добычный комплекс, автоматизированные системы управления, базы данных, сервис-ориентированная архитектура, ролевая модель доступа.

**doi:** 10.21293/1818-0442-2017-20-4-75-81

В современных условиях задача обеспечения функционирования морских сооружений и объектов нефтедобычи с использованием отечественных информационных технологий в соответствии с комплексной программой импортозамещения, принятой в Российской Федерации, на основе и с учетом опыта применения лучших мировых практик становится все более актуальной.

Исследования, представленные в данной статье, проводятся во исполнение требований Государственной программы Российской Федерации «Развитие судостроения и техники для освоения шельфовых месторождений на 2013–2030 годы». Ставится задача обеспечения работы морских сооружений и объектов нефтедобычи в части создания отечественных средств автоматизированных систем управления работой технологического оборудования объектов и систем (АСУ ТП) в соответствии с комплексной программой импортозамещения, принятой в Российской Федерации на основе и с учетом опыта использования лучших решений, существующих в мировой практике в данной предметной области.

Работа подводных добычных комплексов осуществляется удаленно с участием береговых или судовых систем дистанционного управления объектами с использованием автоматизированных рабочих мест на основе применения средств вычислительной техники и контроля состояния всей системы со стороны оператора в автоматическом, полуавтоматическом или ручном режимах.

Основной целью выполняемых исследований является обеспечение информационной поддержки проектирования дистанционного управления технологическим процессом морских сооружений и объектов нефтедобычи, используемых для освоения континентального шельфа (ДУ ТП МСОШ).

### Единое информационное пространство АСУ ПДК

Применение надежных и эффективных решений универсального рабочего места оператора сис-

тем ДУ ТП позволяет снизить численность персонала, эксплуатирующего морской добычный комплекс, за счет автоматизации процессов контроля управления береговыми и подводными техническими средствами.

Универсальность рабочего места оператора обеспечивается за счет инсталляции в компьютерные средства программного обеспечения мониторинга и управления техническими средствами и экспертной системы моделирования технологических процессов для принятия решений, после чего АРМ становится функциональным элементом добычного объекта.

Построение универсального многофункционального АРМ оператора ДУ ТП на базе распределенных вычислительных систем позволяет значительно сократить объемы кабельных трасс, уменьшить размеры пультов за счет отображения информации о контролируемом оборудовании на экранах нескольких видеомониторов, осуществлять постоянный контроль технических средств, мониторинг работы берегового и подводного (дистанционно контролируемого) оборудования.

Обеспечить полноценное управление добычными комплексами невозможно без организации электронного взаимодействия между основными компонентами ДУ ТП МСОШ. Осуществить такое взаимодействие целесообразно за счет объединения существующих источников данных в единое информационное пространство (ЕИП), представляющее собой «совокупность автоматизированных информационных ресурсов, информационно-коммуникационных технологий их формирования, ведения и использования, а также организационных механизмов, обеспечивающих технологическое взаимодействие участников проекта и удовлетворение их информационных потребностей» [1]. Под автоматизированными информационными ресурсами (АИР) будем понимать базы и банки данных, актуализация

и предоставление доступа к которым осуществляются в соответствии с установленным регламентом с помощью информационно-коммуникационных технологий.

АИР, составляющие единое информационное пространство, можно классифицировать по различным признакам. Необходимо учесть, что такие ресурсы имеют различную степень структурированности, что, в свою очередь, означает возможность разделения АИР на атомарные информационные элементы и возможность фиксации их позиции в конкретном информационном ресурсе.

Построение ЕИП производится в соответствии с концепцией «непрерывного развития и поддержки жизненного цикла» – CALS (Continuous Acquisition and Life cycle Support). Согласно данной концепции следует провести автоматизацию информационной поддержки каждого этапа жизненного цикла конкретного изделия.

Другим аспектом развития рассматриваемого единого информационного пространства является «включение в его состав интеллектуальных подсистем, обеспечивающих поддержку принятия решений. Поэтому к составу и структуре единого информационного пространства предъявляются принципиально новые требования, затрагивающие как функциональность всех компонентов программного обеспечения, так и методики работы с ними» [1].

На рис. 1 представлены структура единого информационного пространства, основывающаяся на наборе баз данных, и информационные потоки автоматизированной системы управления технологическими процессами (АСУ ТП) для проектирования дистанционного управления производственного процесса морских объектов и объектов добычи нефти, используемых для освоения континентального шельфа.

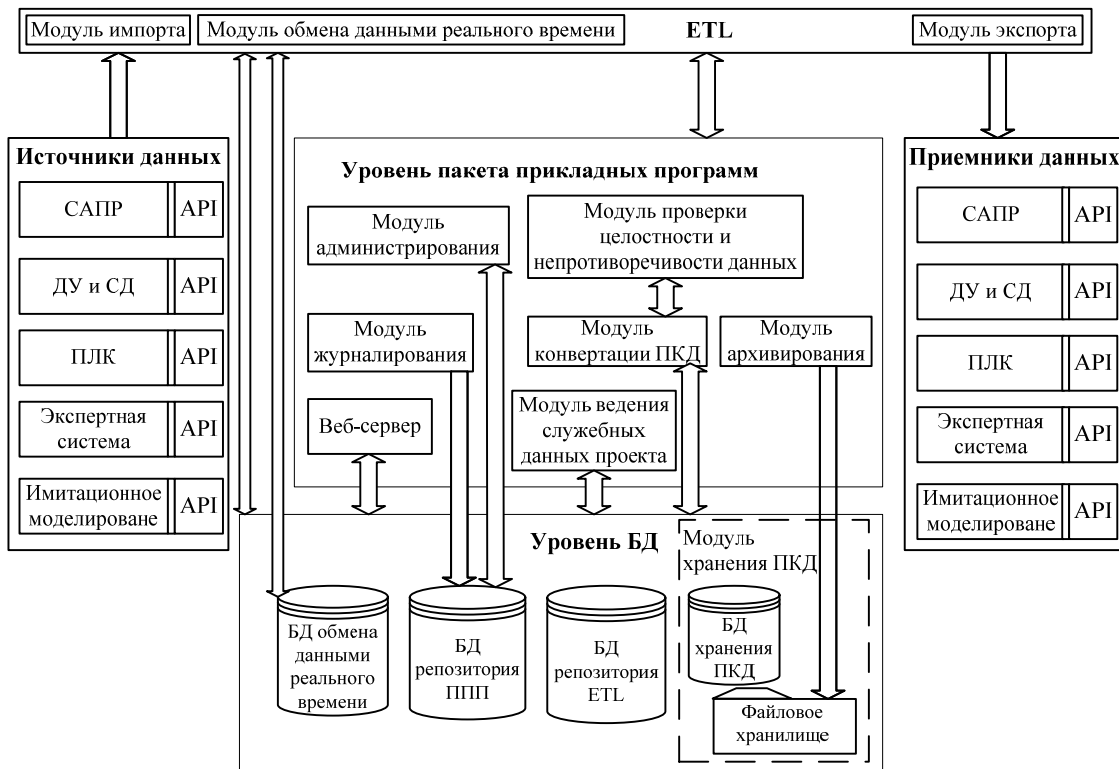


Рис. 1. Структура единого информационного пространства с набором БД

Основной задачей, встающей перед разработчиками при формировании ЕИП, является задача сопряжения данных информационных ресурсов, формируемых в различных прикладных программах. Фактически в применении к рассматриваемой предметной области необходимо реализовать информационную технологию с использованием специальных форматов обмена, которая смогла бы обеспечить интеграцию следующих программно-аппаратных комплексов:

– компонентов программного пакета АСУ ТП для проектирования дистанционного управления производственного процесса;

– экспертной системы для принятия решений диспетчерского круга;

– отладочных имитаторов;

– тренажерных комплексов для опытного образца универсального рабочего места оператора.

Как видно из рис. 1, источниками и приемниками данных являются принципиально отличающиеся друг от друга программные продукты:

1. Подсистема ДУ и СД (SCADA – Supervisory Control And Data Acquisition – диспетчерское управление и сбор данных) – подсистема диспетчерского управления (ДУ) и сбора данных (СД). Представленный программный пакет предназначен для раз-

работки и обеспечения функционирования в режиме реального времени систем, выполняющих сбор, обработку, отображение и архивирование разнородных данных об объекте управления.

2. САПР – система автоматизированного проектирования, используемая для проектирования объектов АСУ ТП.

3. Подсистема ПЛК – подсистема программируемого логического контроллера.

4. Экспертная система – программный продукт, включающий средство создания и настройки оптимизационной теоретической модели добычного комплекса. В режиме поддержки принятия решений модуль экспертной системы получает данные имитационной модели или фактические данные от объекта управления при помощи модуля сбора информации в реальном времени.

5. Модуль имитации – программное средство создания и настройки имитационных моделей. Данный модуль позволяет предоставить инструменты для описания алгоритмов формирования выходных сигналов и задания исходных условий моделирования. Модуль имитации обеспечивает расчет созданных имитационных моделей и управляет режимом их функционирования. В режиме поддержки принятия решений модуль экспертной системы получает данные имитационной модели или фактические данные от объекта управления в реальном времени. Полученные данные сравниваются с заложенными в базу знаний, и при наступлении предопределенных событий оператору выводится предупреждающее сообщение и рекомендация к действию.

#### **Формирование баз данных единого информационного пространства**

Разработка информационной технологии обеспечения взаимодействия внутри ЕИП может быть обеспечена за счет создания механизмов, направленных на формирование баз данных (БД) единого информационного пространства. Роль таких механизмов выполняют служебные модули подсистемы хранения и обмена проектно-конструкторскими данными (ПКД):

- администрирования;
- импорта/экспорта данных;
- конвертации ПКД;
- хранения ПКД;
- проверки целостности и непротиворечивости данных;
- обмена данными реального времени;
- журналирования;
- архивирования;
- ведения служебных данных проекта (данные пользователей, информация о проекте, набор правил, набор событий).

Базы данных единого информационного пространства представляются в виде «совокупности взаимосвязанных, хранящихся вместе данных при наличии такой организации и минимальной избыточности, которая допускает их использование оптимальным образом для одного или нескольких при-

ложений, при этом данные запоминаются и используются так, чтобы они были независимы от программ, использующих эти данные, а программы были независимы от способа и структуры хранения данных» [2]. Способ отражения в БД информации должен обеспечить достоверность и возможность ее прочтения, а также сохранность в сроки, установленные пользовательскими требованиями, и обеспечить возможность доступа к такой информации по состоянию на каждый рабочий день.

Формирование и ведение БД ЕИП должно основываться на выполнении определенных требований (правил), направленных на обеспечение свободного от избыточности, целостного, согласованного и бесконфликтного хранения информации сложной структуры и значительного объема. Целостность и согласованность БД можно рассматривать как соответствие информации, хранящейся в базе данных её структуре, внутренней логике, всем правилам её формирования и требованиям со стороны участников единого информационного пространства. Каждое правило, которое налагает некоторое требование (ограничение) на возможное состояние базы данных есть ограничение целостности. Порядок и соблюдение таких правил определяются регламентом ведения баз данных. Под регламентом [3] будем понимать совокупность требований, которые перечисляют и описывают по порядку этапы, которые должен предпринимать пользователь или группа пользователей для выполнения процесса с указанием (при необходимости) требуемых сроков выполнения.

На текущем этапе работ выделены следующие БД:

- БД обмена данными реального времени;
- БД хранения ПКД;
- БД репозитория пакета прикладных программ (ППП);
- БД репозитория программ обмена данными (ETL).

Под системой управления базами данных (СУБД) будем понимать «набор специальных программных приложений, предназначенных для обеспечения эффективного доступа к БД, используемый для предоставления только необходимой информации, обеспечения независимости от возможных изменений в структуре той части базы данных, которую не обрабатывает программа» [2]. В качестве СУБД подсистемы хранения ПКД и обмена данными предлагается использовать свободно распространяемую объектно-реляционную СУБД PostgreSQL. Файловое хранилище, изображенное на рис. 1, предназначено для хранения исходных файлов, полученных из источников данных, графических данных и архива журнала модуля журналирования.

Следует отметить, что данные между «Подсистемой хранения ПКД и обмена данными», источниками и приемниками данных передаются в виде XML-документов (XML – eXtensible Markup Language – расширяемый язык разметки [4]). Такие XML-документы формируются с помощью API (Application Programming Interface) – программного интерфейса,

позволяющего использовать внутренние библиотеки программ источников и приемников данных для формирования файлов выгрузки необходимого формата и загрузки данных в программу-приемник.

#### Архитектурные решения при организации взаимодействия в едином информационном пространстве

При проектировании архитектуры разрабатываемой АСУ ПДК целесообразно использовать сервис-ориентированный подход, который подразумевает декомпозицию системы на атомарные компоненты, или «сервисы», которые при условии наличия согласованных общих интерфейсов используют единые правила для определения вызова сервисов и правила взаимодействия между собой. В качестве сервиса или службы может выступать программный компонент, доступ к которому осуществляется посредством сети Интернет/Инtranет. Такой механизм реализует некоторую функцию с заранее согласованным интерфейсом.

Преимуществами использования сервис-ориентированной архитектуры (SOA – service-oriented architecture) являются [5]:

- сокращение временных и финансовых издержек, возникающих на всех этапах разработки программных приложений, вследствие упорядочивания процесса их разработки;
- модификация и адаптация к конкретной реализации существующего программного кода;
- обеспечение повышения масштабируемости и интероперабельности создаваемых программных систем;
- обеспечение реальной независимости от используемых платформ, применяемых при разработке языков программирования и другого инструментария;
- совершенствование технической поддержки, облегчение процесса управляемости и сопровождения внедряемых программных систем.

Касательно веб-ориентированных систем необходимо отметить, что наиболее эффективно принципы SOA реализуют архитектурные подходы WSA (Web Services Architecture) и REST (Representational State Transfer). Рассмотрим данные подходы в контексте построения и практической реализации сервис-ориентированной архитектуры разрабатываемой системы.

Веб-сервисы в архитектуре WSA базируются на открытых и широко используемых протоколах: HTTP, SOAP, XML, WSDL, UDDI. Представленные протоколы обеспечивают реализацию основных требований SOA, это означает, что сервис должен быть доступен для динамического обнаружения и вызову посредством UDDI, WSDL и SOAP, а также сервис должен использовать не зависящий от платформы интерфейс (XML). Протокол HTTP при этом должен обеспечивать режим функциональной совместимости (рис. 2).

WSA предоставляет способ реализации SOA, в которой службы взаимодействуют посредством обмена XML-сообщениями (XML-документами) с оп-

ределенной заранее схемой документа. Способы практической реализации веб-служб на сегодняшний день достаточно хорошо проработаны – на рынке программного обеспечения предлагаются как коммерческие, так и проприетарные и свободно распространяемые наборы веб-служб.

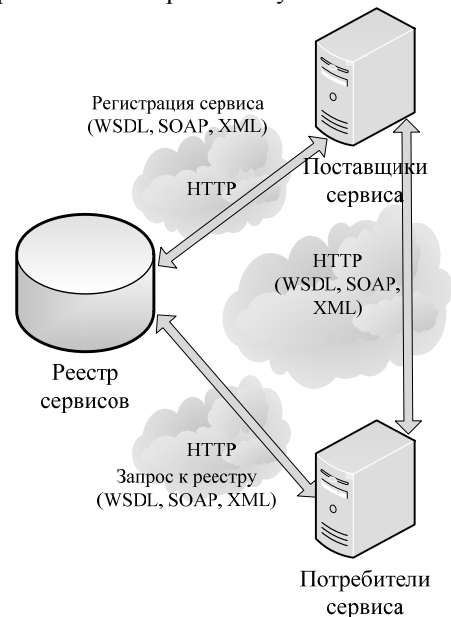


Рис. 2. Архитектура Web Services Architecture

К достоинствам рассматриваемой архитектуры можно отнести высокую степень надежности, обеспечиваемой поддержкой спецификации WS-Reliability, и достаточный уровень безопасности – поддержка спецификации WS-Security. Следует отметить, что при программной реализации приложения предполагается использование инструментальных (зачастую коммерческих) средств разработки, при отсутствии которых создать в короткие сроки простой и эффективный веб-сервис – задача достаточно сложная. Кроме этого, при разработке простых и повсеместно используемых функций веб-приложения, к которым можно отнести отображение данных и запросы на предоставление атрибутивной информации, сервис будет достаточно ресурсно-затратным: увеличится время отклика и будет отмечаться определенная избыточность передаваемых данных. При большом количестве обращений к сервису это практически гарантированно приведет к перегруженности вычислительных ресурсов и увеличению сетевого трафика. По этой причине в качестве альтернативной и более простой реализации сервис-ориентированной архитектуры рассматривают подход REST.

В REST-архитектуре (рис. 3) каждая система может быть представлена отдельными ресурсами, имеющими свое собственное состояние. При этом такая система для масштабируемости не обеспечивает хранение состояния клиентского процесса. Ресурсы представлены стандартными time-типами (типами данных, передаваемыми посредством сети Интернет с применением стандарта, описывающего

передачу различных типов данных по электронной почте). Для обеспечения доступа к конкретному ресурсу используются методы HTTP (GET, PUT, POST, и DELETE). Обеспечение передачи пакета метаданных реализуется с помощью HTTP-заголовков, представленных в виде *time*-типов. Обеспечение кеширования, прокси и авторизация также выполняются через протокол HTTP.

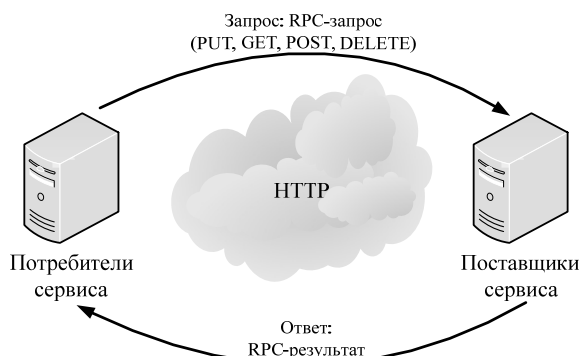


Рис. 3. Архитектура REST (Representational State Transfer)

Анализируя представленные архитектурные решения, можно сделать вывод о том, что, оптимизируя распределение функциональных задач между SOA и REST-сервисами, можно значительно повысить эффективность использования сервис-ориентированного подхода при разработке веб-сервера ЕИП. Данное решение позволяет снизить время выполнения критических для системы функций, значительно сократить сетевой трафик, а также в ряде случаев значительно снизить издержки времени на разработку проекта АСУ ТП.

#### Организация обеспечения безопасности в едином информационном пространстве

Немаловажной задачей при организации взаимодействия внутри единого информационного пространства является задача обеспечения безопасности доступа к данным. Одним из основных моментов, определяющих успешное решение данной задачи, является применение формальных моделей безопасности. Наиболее важным при этом является практическое применение формальных моделей в процессе проектировании программных систем контроля и управления доступом к объектам системы.

Модели информационной безопасности можно представить как «формальное описание политики безопасности информационной системы, заключающееся в определении условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений» [5].

В широком многообразии формальных моделей безопасности отдельное место занимают модели управления доступом к разнородным данным программной системы. Такие модели используются для решения задач разграничения прав доступа к различным базам данных электронных ресурсов единого информационного пространства.

Наиболее распространенными в практическом применении формальными моделями управления доступом являются дискреционные, мандатные и ролевые модели, представленные в [6–11]. В литературе [5, 12] подробно описываются сильные и слабые стороны таких моделей. На основании этих данных можно сделать вывод, что наиболее предпочтительным вариантом использования в рамках данного проекта является ролевая модель, которая представляет собой модифицированную и значительно усовершенствованную модель Харрисона–Руззо–Ульмана [13]. При этом необходимо отметить, что такую модифицированную модель нельзя отнести в полной мере ни к «дискреционным», ни к «мандатным» моделям. Это обусловлено тем, что управление правами доступа, реализованное на ее основе, осуществляется как на основе матрицы полномочий (прав доступа) для выделенных пользовательских ролей, так и с помощью определенных правил, регламентирующих назначение ролей конечных пользователей и их активацию непосредственно во время сеансов [5].

В описываемой ролевой модели выделяются два фундаментальных понятия: «пользователь», замещающее классическое понятие «субъект», и «роль». Под «пользователем» понимают человека, непосредственно взаимодействующего с системой и выполняющего определенный набор операций в рамках своих служебных обязанностей. Под «ролью» понимают активно действующую в программной системе некую «абстрактную сущность», для которой определен набор ограничений и логически связанных полномочий, необходимых для выполнения определенных действий в системе. Описываемый подход наиболее точно соответствует реальным условиям, при которых конечные пользователи действуют не от своего личного имени, а выполняют определенные регламентированные задачи в рамках своих обязанностей.

Таким образом, вполне логично управление правами доступа и назначение различных полномочий выделять не «реальным» пользователям (физическим лицам), а «абстрактным» ролям, фактически представляющим участников процесса обработки информации – пользователям единого информационного пространства.

При внедрении политики управления доступом, основанной на ролевой модели, процесс разбивается на две стадии:

1. Для каждой определенной роли необходимо указывать полный спектр полномочий, представляющий собой набор прав доступа к объектам системы.
2. Для каждого пользователя, зарегистрированного в системе, назначается перечень доступных ему ролей.

Использование ролевой модели при проектировании информационной технологии обеспечения взаимодействия внутри ЕИП позволит создать программное обеспечение информационной безопасности, для которого определены следующие функциональные возможности:

- наличие регламентного доступа непосредственно к базе данных и функциональной составляющей базы данных единого информационного пространства;

- обеспечение ролевого доступа к данным ЕИП на основании выделения администратором набора объектов, групп объектов, функций и организаций-подрядчиков;

- аудит активности конечных пользователей в среде ЕИП. Основным набором контролируемых действий при этом являются: создание объектов предметной области, просмотр сведений о проектных объектах, модификация атрибутивной информации, удаление данных;

- назначение конечным пользователям и группам пользователей прав на элементы пользовательского интерфейса;

- назначение следующих режимов (параметров) доступа ролям к объектам:

- 1) режим назначения прав через объекты. Такой режим целесообразно использовать при необходимости назначения нескольким ролям права на один конкретный объект;

- 2) режим назначения прав через роли. Его целесообразно использовать при назначении одной роли права на несколько объектов;

- регистрация конечного пользователя в среде единого информационного пространства;

- определение конечного пользователя как члена группы;

- определение конкретных прав каждого члена группы на доступ к проектным данным в соответствии с набором работ, в соответствии с указанной областью изделия в проекте, в соответствии с типом объектов проектируемого изделия;

- определение прав доступа к технологическим возможностям системы для членов группы, представленных как функций проекта;

- формирование критериального запроса на фильтрацию данных сеанса пользователя в соответствии с текущими правами доступа данного пользователя;

- определение набора действий с данными ЕИП, включаемых в набор аудита;

- формирование регламентных и произвольных отчетов об активности пользователей при получении доступа к объектам ЕИП и действиям над этими объектами в определенный момент времени.

Фактически ролевая модель доступа, положенная в основу определения политики информационной безопасности, является неотъемлемой частью АСУ ПДК, функционирующей в сложной организационной структуре с большим количеством пользователей, выполняющих определенный набор функций в рамках своих служебных обязанностей и наделенных в связи с этим различными правами доступа и набором полномочий. Все это соответствует современным требованиям к надежному хранению и доступу к данным единого информационного пространства.

### Заключение

В представленной работе рассмотрены некоторые ключевые моменты создания единого информационного пространства, необходимого для эффективного выполнения сложного технологического проекта. Представленный анализ возможных архитектурных решений ведения базы данных ЕИП показывает нестареющую эффективность сервис-ориентированного подхода, особенно в комплексе с веб-ориентированной организацией доступа к данным.

Анализ моделей доступа к сложноорганизованному данным представляет преимущества ролевой модели в случае многослойной структуры технологической информации, составляющей основу базы данных ЕИП.

Предлагаемые решения основаны на опыте авторов, полученном в ходе выполненных ранее крупных проектов, связанных с разработкой информационных технологий.

Работа выполнена при финансовой поддержке Минпромторга России в рамках выполнения Государственного контракта № 16411.1810190019.09.015 от 07.11.2016 г. «Разработка автоматизированной системы управления подводной добычей с помощью береговой станции на основе параметрической модели подводного добычного комплекса, разработка проекта подводного добычного комплекса и виртуального макета его системы управления».

### Литература

1. Создание единого информационного пространства машиностроительного предприятия на основе облачных технологий / А.В. Волгин, И.В. Гусев, С.В. Куликов и др. // Вестник ВГТУ. – 2012. – № 6. – С. 44–47.
2. Сенченко П.В. Организация баз данных: учеб. пособие. – Томск: Том. гос. ун-т систем управления и радиоэлектроники, 2004. – 170 с.
3. Юридический словарь [Электронный ресурс]. – Режим доступа: <http://dic.academic.ru/dic.nsf/lower/17887>, свободный (дата обращения: 28.11.2015).
4. XML. Beginning XML / Д. Хантер, Д. Рафтер и др. – М.: Вильямс, 2009. – 1344 с.
5. Гриценко Ю.Б. Геоинформационные технологии мониторинга инженерных сетей / Ю.Б. Гриценко, Ю.П. Ехлаков, О.И. Жуковский. – Томск: Изд-во ТУСУРа, 2010. – 148 с.
6. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Изд-во Урал. ун-та, 2003. – 328 с.
7. Ferraiolo D. Introduced formal model for role based access control / D. Ferraiolo, D. Kuhn // 15th national computer security conference. – Oct 13–16, 1992. – P. 554–563 [Электронный ресурс]. – Режим доступа: [http://csrc.nist.gov/groups/sns/rbac/documents/role\\_based\\_access\\_control-1992.html](http://csrc.nist.gov/groups/sns/rbac/documents/role_based_access_control-1992.html), свободный (дата обращения: 10.02.2015).
8. ISO / IEC 17799:2000 «Information technology – information security management» [Электронный ресурс]. – Режим доступа: [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/atalogue\\_detail.htm?Cnumber=33441](http://www.iso.org/iso/iso_catalogue/catalogue_tc/atalogue_detail.htm?Cnumber=33441), свободный (дата обращения: 25.05.2017).
9. LaPadula L. Secure Computer Systems: A Mathematical Model / L. LaPadula, J. Elliott [Электронный ресурс]. – Режим доступа: <http://www.albany.edu/acc/>

courses/ia/classics/bellla-padula1.pdf, свободный (дата обращения: 25.05.2017).

10. McLean John. Security models / John McLean // Encyclopedia of software engineering [Электронный ресурс]. – Режим доступа: <http://citeseerx.ist.psu.edu/view doc/summary?doi=10.1.1.34.8561>, свободный (дата обращения: 10.06.2017).

11. McLean John. The Specification and Modeling of Computer Security / John McLean // Computer. – 1990. – Vol. 23, No. 1. – P. 9–16.

12. Gritsenko Y. B. Model of role-based access to spatial data of electronic master plan / Y.B. Gritsenko, M.M. Milikhin, P.V. Senchenko, O.I. Zhukovsky // AICT 2015, Proceedings. – 2015. – P. 196–200. – doi: 10.1109/ICAICT.2015.7338545.

13. Harrison M. Monotonic protection systems / M. Harrison, W. Ruzz // Foundation of computation secure. – 1978. – P. 337–363.

**Сенченко Павел Васильевич**

Канд. техн. наук, доцент, декан  
факультета систем управления ТУСУРа  
Тел.: +7-906-947-82-83  
Эл. почта: pvs@tusur.ru

**Гриценко Юрий Борисович**

Канд. техн. наук, доцент,  
начальник инновационного управления ТУСУРа  
Тел.: +7-905-990-95-49  
Эл. почта: innovation@tusur.ru

**Милихин Михаил Михайлович**

Аспирант каф. АОИ  
Тел.: +7-999-619-38-90  
Эл. почта: milikhin@gmail.com

---

**Мещеряков Роман Валерьевич**

Д-р техн. наук, профессор,  
проректор по научной работе и инновациям ТУСУРа  
Тел.: +7 (382-2) 51-43-02  
Эл. почта: mrv@tusur.ru

**Жуковский Олег Игоревич**

Канд. техн. наук, ст. науч. сотр., доцент каф.  
автоматизации обработки информации (АОИ) ТУСУРа  
Тел.: +7-913-855-47-82  
Эл. почта: zhukol54@gmail.com

Meshcheryakov R.V., Zhukovskiy O.I., Senchenko P.V.,  
Gritsenko Yu.B., Milikhin M.M.

**Architecture features of a common information space to manage complex technological processes**

This paper presents solutions that can be used to interlink components of an automated subsea production control system for a shore station based on the parametric model of a subsea production complex. Features of architecture of a common information space for the purpose of association of the existing data sources necessary for sharing at management of difficult technological processes are considered. Based on division of a system into components (services), the service-oriented approach is discussed as the best choice in architecture design of a new system. The paper discusses the role-based data access model as the basis for the security policy.

**Keywords:** common information space, subsea production complex, automated control system, databases, service-oriented architecture, role-based access control.