

DOI:

## WEB АРХИТЕКТУРА ОБЛАЧНОГО СЕРВИСА ДЛЯ ПРОЕКТИРОВАНИЯ И АНАЛИЗА АСУ ТП

Промыслова О.А., Промыслов В.Г.

*Институт проблем управления им. В.А. Трапезникова РАН,*

*Россия, г. Москва, ул. Профсоюзная д.65*

*vitalionics@gmail.com*

*Аннотация: В статье разбирается возможность создания интерфейса без привлечения специалистов по веб-дизайну на примере инженерного сайта Omole. Приведен пример моделирования типового канала АСУ ТП АЭС.*

Ключевые слова: АСУ ТП, архитектура, интерфейс, bootstrap, Omole.

### Введение

Веб-приложения вошли не только в повседневную практику, но стали обычными в областях, традиционно реализующих специализированный интерфейс с пользователем. Такими областями являются различные системы автоматизированного проектирования (САПР), системы моделирования и т.п. Разработчик специализированных приложений теперь почти неминуемо столкнется с проблемой создания веб-сайта поддержки, а, возможно, и прикладного интерфейса со своей программой. Для крупных проектов проблема может быть решена привлечением специалистов веб-дизайна, но для небольших проектов часто разработчики вынуждены создавать веб-интерфейс самостоятельно. В такой ситуации оказались и авторы, когда занялись созданием обучающего портала по информационной безопасности (ИБ) АСУ ТП Omole [1], совмещенного с сервисом моделирования ИБ. Перед нами были вопросы: достаточна ли функциональность веб-технологий для интерфейса САПР; можно ли создать современный сайт, не обладая талантами дизайнера, а только имея базовую подготовку технического ВУЗа? Если ответить на каждый из вопросов отдельно, то окажется, что существует множество решений «из коробки», которые покрывают конкретные аспекты создания инженерного сайта. Перечислим некоторые из них: веб-библиотеки d3 [2], google chart [3] и др. (обзор можно посмотреть, например, на ресурсе [4]), для отображения и редактирования инженерных данных; Wordpress [5], Blogspot [6] для создания простых сайтов с документацией. Однако попытка интегрировать разные продукты «из коробки» для получения собственного сервиса, вызвали у нас трудности, которые заставили искать другие решения. В статье нам бы хотелось поделиться опытом, полученным во время реализации нашего проекта.

### 1 Характеристика инженерного сайта

Во введении мы использовали понятие «инженерный сайт» явно его не определяя. Теперь попробуем на примере нашего сайта определить более точно, что представляет собой инженерный сайт в нашем понимании.

Инженерный сайт это веб-ресурс, который:

- предоставляет пользователю некоторый набор документов (статические страницы). Документы чаще всего имеют текстовый характер, возможно, с формулами и графиками. Они в основном монохромны и просты по структуре;
- отображает динамическую информацию, например, новости проекта, конференции и т.д.;
- предоставляет пользователю доступ к некоторому сервису. Входными и выходными данными сервиса может служить табличная информация, возможно, в виде графов и диаграмм.

В нашем случае входная информация являлась мультиграфом, описывающим отношения ИБ между субъектами системы, а выходная информация представляла собой пути в мультиграфе, субграфы и табличные данные.

Для себя мы решили, что небольшой проект для узкой целевой аудитории (профессионалы по ИБ) не требует изощренного дизайна, характерного для сайтов топ-компаний или коммерческих проектов рассчитанные на массовую аудиторию. Специалисты могут принять некоторые упрощения в дизайне, но в тоже время интерфейс должен быть функционален и удобен. Если понятие «функционален» означает, что должно поддерживаться отображение и навигация по определенным типам данным, то понятие «удобно» включает в себя, в том числе, и возможность работать с сервисом на различных устройствах: стационарные компьютеры, планшеты, смартфоны. Решение последней задачи не является тривиальной, если пытаться разработать интерфейс, используя базовые средства HTML. В

качестве «кирпичиков» для создания интерфейса нами выбраны пакеты Bootstrap [7], Cytoscape [8] и сервис Twitter [9].

## 2 Интерфейс инженерного сайта omole

Пакет bootstrap простой и, в тоже время, гибкий интерфейсный фреймворк, облегчающий разработку web-приложений. Его особенностями являются то, что он свободный, имеет лаконичный дизайн. Графические примитивы пакета интуитивно понятны и восходят к делению экрана на прямоугольные зоны (таблица). Важной особенностью является эффективная адаптация интерфейса для различных устройств. Нами использован данный пакет для отображения документации и задания остова (меню, общий вид) сайта. Сервис Twitter был интегрирован для создания новостной основы сайта. Данная связка является наиболее логичной с учетом того, что bootstrap разрабатывался программистами компании Twitter. Пример интерфейса сайта на мобильном устройстве приведен на рис. 1.

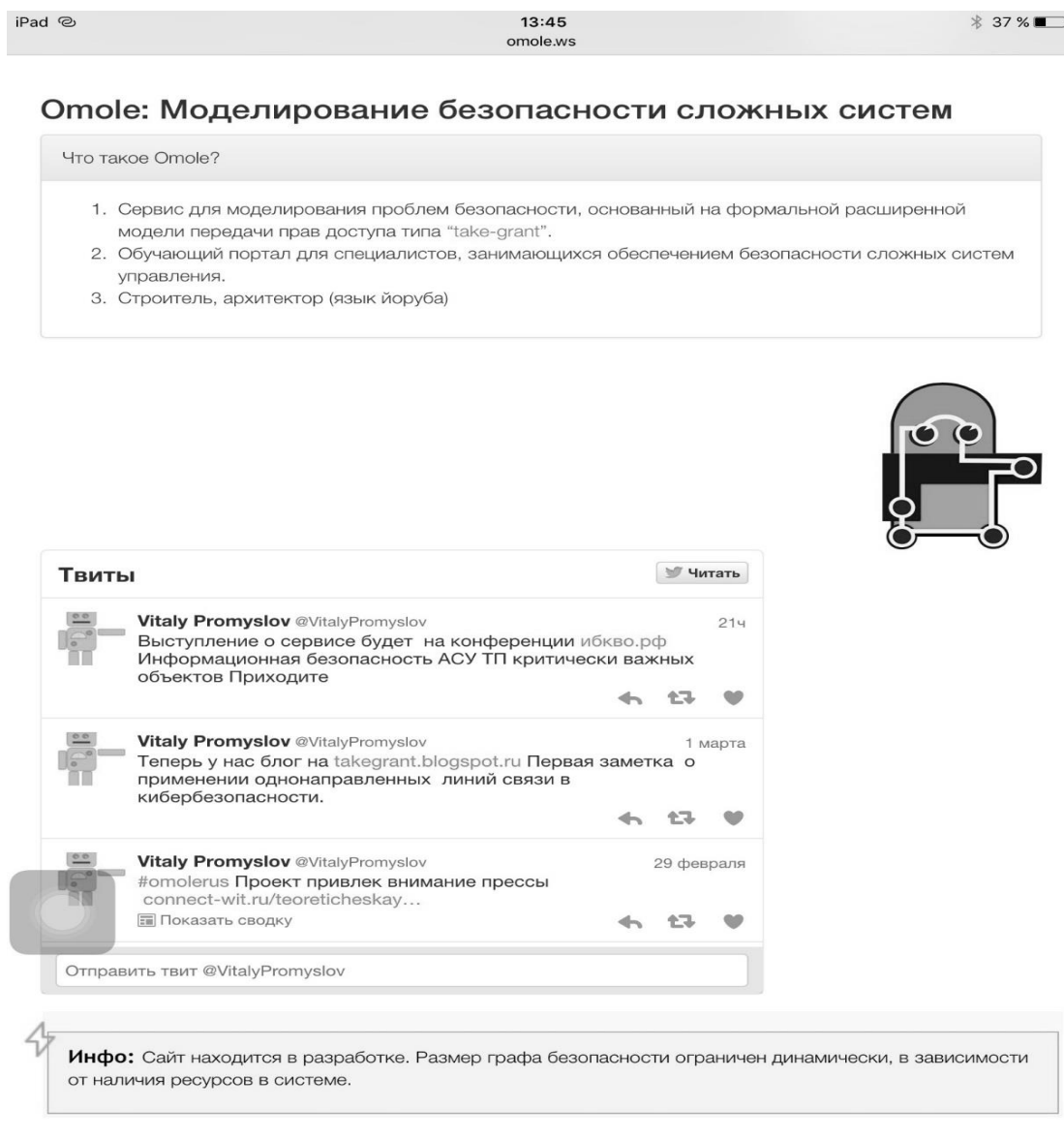


Рис. 1. Пример интерфейса заглавной страницы сайта Omole на мобильном устройстве

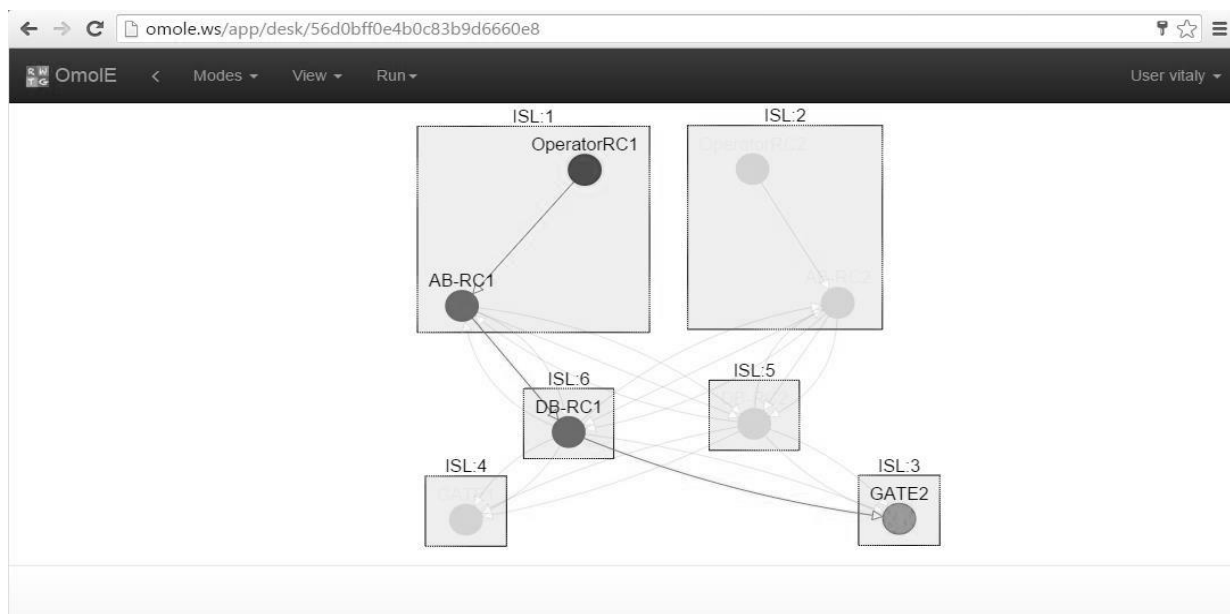


Рис. 2. Пример интерфейса работы с сервисом ИБ сайта Omole на настольном компьютере

Для обеспечения собственно моделирующего сервиса нами использован пакет Cytoscape. Его выбор оказался не столь однозначен по сравнению с использованием пакета Bootstrap. Нам приходилось выбирать, с одной стороны, между эффективной визуализацией инженерной информации, что является проблемой с ростом размера графа, а с другой стороны, удобством программирования пользовательской работы с графом. В качестве полусюв здесь может считаться оригинальный JavaScript как наиболее примитивный язык, но в то же время эффективный веб-язык и, например, пакет d3 с высокоуровневыми примитивами отображения инженерных данных. Место Cytoscape, по нашему мнению, где-то посередине. Пример интерфейса приведен на рис. 2.

### 3 Примеры синтеза архитектуры кибербезопасности АСУ ТП и анализ применимости метода

Основные этапы синтеза архитектуры кибербезопасности опишем на примере синтеза архитектуры безопасности для некоторой подсистемы АСУ ТП АЭС. Такие подсистемы, сгруппированные по контролируемому оборудованию, предназначены для реализации отдельных функций АСУ ТП, например:

- передачи команд оператора по управлению технологическими процессами и технологическим оборудованием;
- представления информации о состоянии оборудования;
- контроля состояния подсистемы;
- архивирования информации.

В примере использована реализация типового канала АСУ ТП для подсистемы, работающей под управлением платформы Operator [10].

Для анализа и синтеза архитектуры безопасности используется интегрированная модель кибербезопасности [11].

Пример более детального учета некоторых реальных характеристик системы при классификации приведен в работе [13].

#### 3.1 Описание типовой АСУ ТП

Современная АСУ ТП представляет собой распределенную по функциям и средствам систему, которая обеспечивает реализацию основных функций управления объектом, таких как:

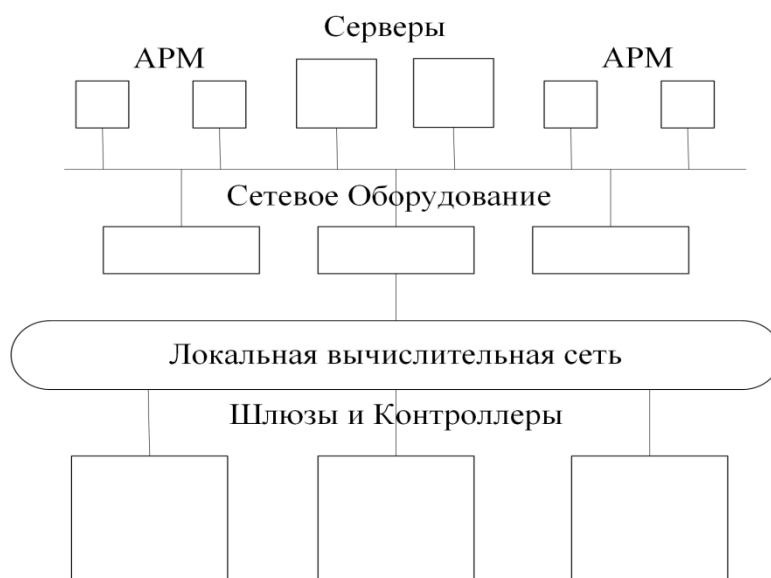
- централизованный сбор и представление оперативному персоналу объекта как обобщенной, так и детализированной информации о состоянии объекта, режимах его работы, отдельных параметров технологического процесса и состояния оборудования самой АСУ ТП (контуров измерения, арматуры, механизмов, программ управления);
- возможность дистанционного автоматизированного управления с рабочих станций (РС) технологическим оборудованием объекта;

- формирование сигнализации о нарушениях в работе, отдельных технологических систем, отдельного оборудования, о возникновении условий, требующих вмешательства персонала;
- сбор и представление информации о нарушениях пределов и условий безопасной эксплуатации, о возникновении исходных проектных событий, а также информации о состоянии критических функций безопасности;
- представление справочной и регламентной информацией персоналу объекта;
- выполнение алгоритмов функционально-группового управления оборудованием технологических систем.

Основными элементами АСУ ТП, являются: автоматизированные рабочие места, серверы, локальная вычислительная сеть (ЛВС), датчики, программируемые логические контроллеры, исполнительные механизмы.

Взаимодействие АСУ ТП с объектом управления осуществляется через шлюзы и контроллеры, подключенные к ЛВС, в которых на программном уровне обеспечивается информационная совместимость соответствующих механизмов объекта управления. Структурная схема АСУ ТП рассматриваемая в работе представлена на Рис 3. Компонентами АСУ ТП являются:

- Автоматизированные рабочие места (АРМ);
- Сервера;
- Шлюзы и контроллеры;
- Сетевое оборудование.



*Р и с . 1 Структура типовой АСУ ТП*

Автоматизированные рабочие места (АРМ) реализуются на основе одной или нескольких РС, подключаемых в зависимости от их основного функционального назначения к определенному серверу. Подключённые к одному серверу рабочие станции образуют кластеры, которые связаны с выполняемой функцией или группой контролируемого оборудования. В функции АРМ входит отображение поступающей информации в проблемно-ориентированной форме, которая зависит от задач, решаемых операторами объекта, и формирования потока команд на управление объектом от оператора к низовой автоматике (цепочка АРМ-сервер-шлюз).

Информация об объектах контроля/управления в АСУ ТП обрабатывается серверами, которые выполняют функции архивирования и сортировки информации по ее назначению. В сервере также реализуют алгоритмы автоматического управления, которые формируют независимый от оператора поток команд.

Источником информации об объекте для сервера являются данные, поступающие от шлюзов (контроллеров) в виде аналоговых, дискретных величин, характеризующих состояние объекта контроля. Обратный поток информации от сервера к шлюзу формирует команды управления.

Общий алгоритм функционирования АСУ ТП осуществляет обработку трех информационных потоков: потока сигналов контроля состояния объекта, потока команд управления оборудованием, потока сигналов диагностики и управления собственно АСУ ТП.

### 3.2 Идентификация и классификация активов

Входными данными для процедуры синтеза являются:

- идентифицированный список активов,
- назначенный целевой уровень ИБ.

Входные данные заданы таблицей (Таблица 1). В целевой архитектуре безопасности дополнительно указаны зоны ИБ для идентифицированных активов.

Активы могут быть проклассифицированы по уровням безопасности с применением как чисто экспертных, так и более формальных методов классификации. Мы использовали метод кластерного анализа признаков активов [11].

Чтобы пример оставался наглядным, в списке активов Таблицы 1 рассматриваются только программные модули. Поэтому в списке активов отсутствуют второстепенные для демонстрационной цели задачи синтеза архитектуры компоненты реальной системы: сетевое оборудование, системные блоки, встроенные источники питания, блоки контроля физического доступа к компьютеру, климатические датчики и т.п.. В примере также не рассматривается архитектура безопасности системы с резервируемыми элементами, так как схемы и методы резервирования в основном являются системно зависимыми и привязаны к конкретной реализации. Однако при моделировании реальной системы резервирование элементов должно быть учтено [13].

Т а б л и ц а 1 – Список активов типового канала АСУ ТП и целевые характеристики ИБ

Имя актива (программного модуля)	Описание	Целевой уровень ИБ	Зона безопасности
Программное обеспечение рабочей станции			
IZ	Модуль, обеспечивающий графический интерфейс с оператором	5	1
AB	Модуль, обеспечивающий логический интерфейс с оператором	5	
WWW	Веб-браузер с доступом к архиву данных через веб-сервер	5	
OS_WS	Операционная система АРМ	4	2
Программное обеспечение сервера			
ES	Модуль алгоритмов управления	3	3
DB	База данных	3	
ArchDB	Часть базы данных, ответственная за хранение архива данных на диске.	- не устанавливается для активов типа объект	
WWWserv	Веб сервер с доступом к архиву данных о состоянии оборудования.	не ниже 4	4
OS_SERV	Операционная система сервера	2	5
Gate (Шлюз, ретранслятор)	Модуль связи с контроллером оборудования	3	3

### 3.3 Информационная модель системы

Типовой канал АСУ ТП реализует следующий порядок взаимодействия между компонентами.

1. Оператор через человеко-машинный интерфейс рабочей станции (компоненты IZ и АВ), может менять состояние записей в базе данных сервера (актив DB).
2. Актив АВ периодически запрашивает состояние объекта управления (считывает записи из базы данных) и через графический и звуковой интерфейс компьютера (актив IZ) отображает их оператору.
3. Актив DB при изменении состояния записей инициирует передачу команд на контроллеры оборудования (актив Gate). Кроме того, DB запрашивает состояние оборудования у шлюза и сохраняет их в базе данных (актив ArchDB).
4. Автоматические алгоритмы управления объектом реализуются через экспертную систему (актив ES).
5. Оператор также имеет возможность получить историю состояния объекта управления, используя доступ к базе данных через веб-интерфейс (активы WWW, WWWServer).
6. Все активы функционируют на компьютерах, под управлением некоторой операционной системы, ОС (активы OS\_SERV, OS\_WS).

Все активы, кроме актива ArchDB, являются субъектами в терминах модели “take-grant” [12].

Изложенный выше алгоритм взаимодействия описывается графом безопасности, приведенным на Рис. 4.

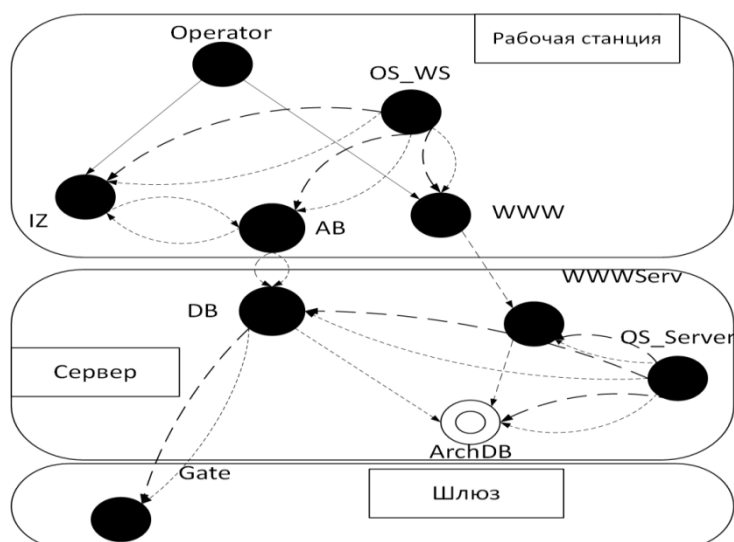


Рис. 4 - Общий вид графа безопасности для типового канала передачи информации в СББУ без учета мер защиты. Отношениям разных типов передачи информации —  $g$ ,  $r$ ,  $w$  — соответствуют сплошная, штриховая и пунктирная линии.

### Выводы

Наш пример показывает, что создание современного инженерного сайта не требует “талантов” дизайнера, и проблема может быть решена силами специалистов, занимающихся основной функциональностью ресурса. Однако следует учесть, что из-за необходимости работать на, условно, среднем и ближе к нижнему уровню веб-программирования, от специалистов требуется владения суммой веб-технологий, что не может появиться мгновенно.

### Литература

1. [www.omole.ws](http://www.omole.ws)
2. <https://d3js.org/>
3. <https://developers.google.com/chart/>
4. <http://www.sitepoint.com/15-best-javascript-charting-libraries/>
7. [www.wordpress.com](http://www.wordpress.com)
5. [www.Blogspot.com](http://www.Blogspot.com)
6. [www.getbootstrap.com](http://www.getbootstrap.com)
7. [www.cytoscape.org](http://www.cytoscape.org)

8. [www.Twitter.com](http://www.Twitter.com)
9. *Менгазетдинов Н.Э., Бывайков М.Е., Зуенков М.А и др.* Комплекс работ по созданию первой управляющей системы верхнего блочного уровня АСУТП для АЭС «Бушер» на основе отечественных информационных технологий. – М.: ИПУ РАН, 2013.
10. *Промыслов В.Г., Семенов К.В., Шумов А.С.* // Синтез архитектуры кибербезопасности для систем управления атомных электростанций. – Проблемы управления, №. 3, с. 61-71, 2019
11. *Bishop M.* "Computer Security: Art and Science," Addison Wesley, Boston, 2003
12. *Prmyslov V., Sakrutina E. and Meshcheryakov R.* "Coherence Criterion for Security Architecture of Digital Control System," 2019 International Russian Automation Conference (RusAutoCon), Sochi, Russia, 2019, pp. 1-5, doi: 10.1109/RUSAUTOCON.2019.8867615.