Белоусов А.В., Глаголев С.Н., Рыбакова А.И., Кошлич Ю.А.

ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ВИРТУАЛЬНЫХ ЛАБОРАТОРИЙ С УДАЛЕННЫМ ДОСТУПОМ

В статье рассматриваются технологические подходы разработки и использования лабораторий с удаленным доступом. Особое внимание уделяется двум основным вопросам: организации web-базированного доступа к технологическим параметрам лабораторного оборудования и обеспечение безопасности соединения, которое заключается в организации защищенных каналов связи, разграничении прав доступа и защиты от несанкционированных вмешательств извне.

Ключевые слова: *лаборатории с удаленным доступом, web-базированный доступ, реверсивный AJAX, comet AJAX, HTML аутентификация, HMAC.*

A. Belousov , S. Glagolev, A. Rybakova , Yu. Koshlich

INFORMATION AND TECHNICAL SUPPORT FOR VIRTUAL LABORATORIES WITH REMOTE ACCESS

The article discusses the development of technological approaches and the use of laboratories with remote access. Special attention is given to two main issues: the organization of web- based the access to technological parameters of laboratory equipment and security compound, which is to organize the secure channel of communication, the delimitation of the rights of access and protection from unauthorized interference from the outside.

Keywords: *lab with remote access , web-based the access , reverse AJAX, comet AJAX, HTML authentication , HMAC.*

Информационные технологии достаточно широко проникли во все сферы образовательного процесса. Процесс обучения практически невозможно представить без информационной инфраструктуры. Одной из

важных проблем при использовании информационных технологий в образовании является проблема взаимодействия конечного пользователя с технологическим оборудованием:

Во-первых, высокий уровень информатизации учебного процесса предусматривает использование компьютерных тренажеров и моделей, которые базируются на реальном оборудовании, но никак реально не взаимодействуют с ним.

Во-вторых высокая стоимость лабораторного оборудования не всегда позволяет использовать определенные установки широкому кругу учебных заведений (например установки альтернативной энергетики и т.п.).

Возможное решение проблемы – использование на межвузовском уровне распределенных виртуальных лабораторий с удаленным доступом с высоким уровнем телекоммуникационной составляющей. Использование такого подхода позволит существенно снизить расходы на приобретение и содержание уникального лабораторного оборудования.

Предлагается следующая технологическая концепция, основанная на построении многоуровневой иерархической системы управления лабораторным оборудованием (Рис. 1). Оборудование нижнего функционального уровня (датчики температур, давления, расхода и т.п.) подключаются к соответствующим аналоговым входам программируемого логического контроллера (ПЛК). При помощи коммуникационного интерфейса EtherNet ПЛК происходит межуровневое взаимодействие между нижним и верхним функциональными уровнями. В качестве каналов связи для межуровневого взаимодействия системы удобно использовать локальные вычислительные сети учебных заведений и предприятий. Верхний функциональный уровень системы представлен двумя серверами: web-сервер и архивный SCADA-сервер.

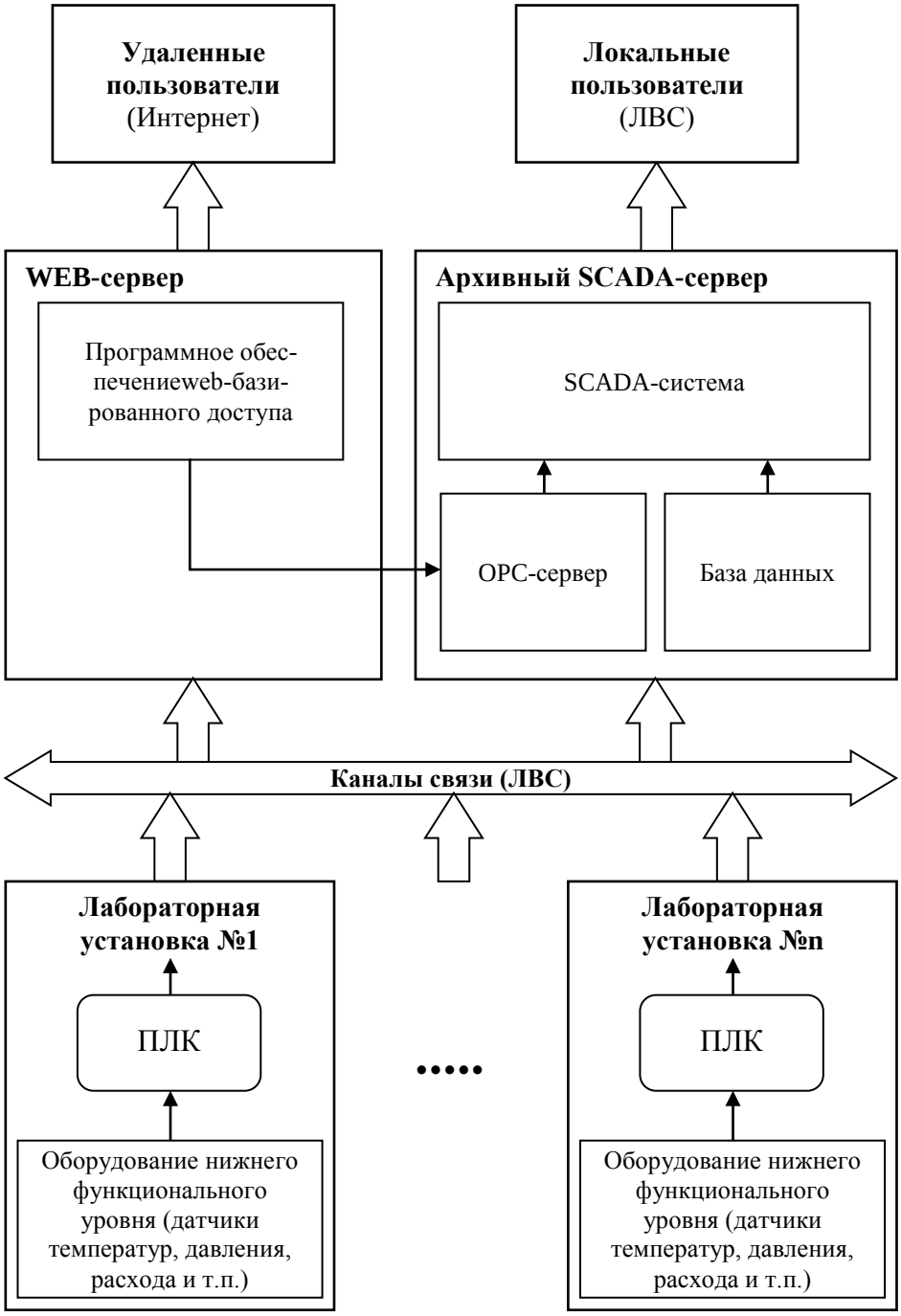

Рис. 1. Блок-схема межуровневого взаимодействия технологического оборудования виртуальных лабораторий

Техническая реализация предложенного подхода вызывает две основных сложности:

1) реализация web-базированного доступа к технологическим параметрам лабораторного оборудования [3, с. 71];
2) обеспечение безопасности соединения, которое заключается в организации защищенных каналов связи, разграничении прав

доступа и защиты от несанкционированных вмешательств извне [4, с. 62].

Обеспечение доступа для удаленных пользователей к технологическим параметрам оборудования нижнего функционального уровня является одним из ключевых моментов в организации виртуальных лабораторий с технологической точки зрения. Требование оперативности получаемых оператором данных означает, что отображение информации на стороне клиента должно происходить динамически, без необходимости полной перезагрузки страницы.

Среди наиболее распространённых в настоящее время схем функционирования веб-приложений можно выделить схемы, основанные на использовании средств Java-среды и технологий AJAX (рис. 2), в том или ином виде.

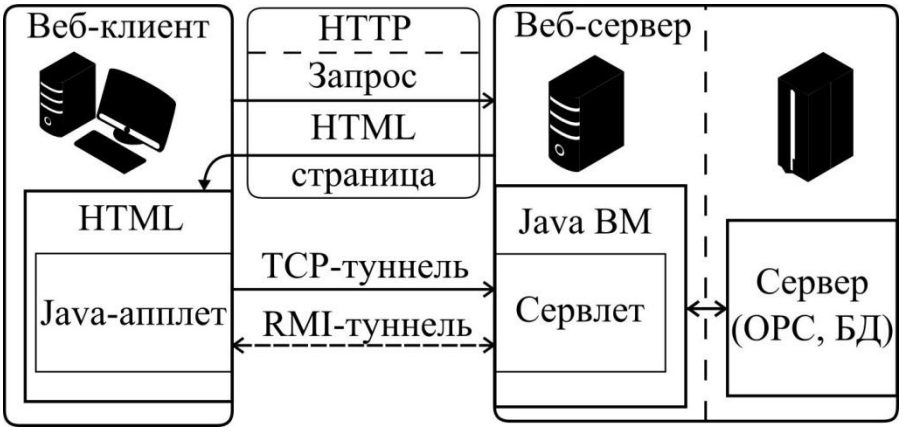

Рис. 2. Схема доступа к технологической информации посредством Java-апплета

Технологии, опирающиеся в своей реализации на Java-апплеты позволяют организовать событийно-ориентированный механизм взаимодействия с клиентом, когда данные передаются сервером непосредственно в момент изменения состояния объекта. При этом информация передаётся клиенту по отдельному TCP-каналу, открытому сервером на нестандартном порту, что создаёт трудности в работе клиентского приложения за сетевым экраном. Более того, при использовании протокола RMI (RemoteMemoryInvocation) данный порт выбирается случайным образом. Недостатком разумно считать и

необходимость использования плагина Java для браузера - одной из самых популярных мишеней для сетевых атак.

AJAX (AsynchronousJavaScriptAndXML) этих недостатков лишен (рис. 2), однако в классической реализации данная технология не позволяет серверу отправлять обновления клиентам в произвольные моменты времени, определяемые самим сервером, так как коммуникация осуществляется по протоколу HTTP 1.0 (запрос-ответ). Этот недостаток порождает необходимость регулярной отправки клиентом запросов, что значительно повышает нагрузку на сеть и аппаратную часть сервера при большом количестве обслуживаемых клиентов.

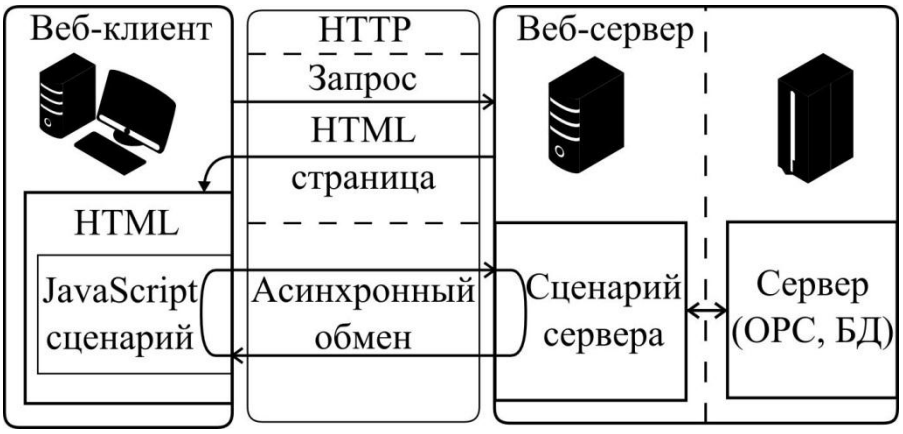

Рис.3. Схема доступа к технологической информации с использованием AJAX

Другие варианты включают в себя применение технологий .NET, таких как ASP.NET и RemoteScripting. В этих случаях, также как и с AJAX, используется только протокол HTTP, а потому невозможно добиться событийно-ориентированного обновления тонкого клиента. Основной отрицательной чертой этих подходов является их жёсткая привязка к определённой программной платформе.

Результатом изысканий путей устранения указанных недостатков явилась разработка метода, подразумевающего использование технологии реверсивного AJAX и longpoll (рисунок 3).

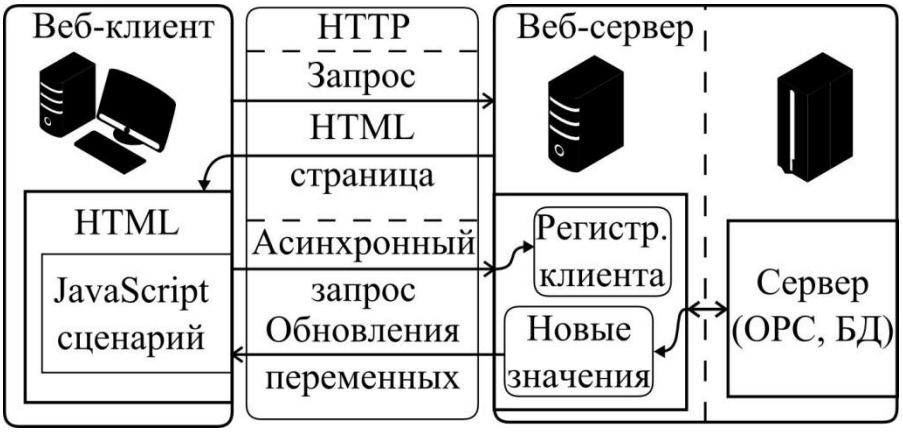

Рис.4. Событийно-ориентированный доступ на основе реверсивного AJAX

В простейшем виде схема такого клиент-серверного взаимодействия может быть описана следующим образом. После загрузки статической информации с веб-сервера (сама страница, изображения, клиентские сценарии и т.д.) клиент посылает асинхронный HTTP-запрос с информацией, определяющей его текущее состояние. Веб-сервер фиксирует это состояние, оставляя HTTP-соединения открытым - таким образом происходит регистрация конкретного клиента на следующее обновление. Серверное приложение, осуществляющее опрос датчиков объекта, уведомляет веб-сервер об очередном изменении состояния. Информация о данном изменении отсылается веб-сервером клиенту, после чего клиент закрывает HTTP-соединение.

Тот факт, что соединение может оставаться открытым продолжительное время позволяет:

1) избавить клиент от частой отправки регулярных запросов, снижая нагрузку на сеть и сервер;
2) сократить время реакции системы - клиент получает обновлённые данные без задержек, связанных с созданием нового соединения.

Реверсивность работы AJAX в данном случае объясняется переносом инициативы от клиента к серверу: сервер самостоятельно определяет моменты рассылки обновлений клиентам. При этом не требуется ни использование нестандартных портов для создания дополнительных соединений, ни каких-либо расширений браузера на стороне

клиента.Подобный подход иногда альтернативно именуют Comet AJAX, однако устоявшейся общепринятой терминологии не существует.

В итоге, оператор получает обновления состояния по протоколу HTTP, используя веб-браузер в качестве клиента. Единственным требованием является разрешённое исполнение JavaScript-сценариев в браузере, так как вся клиентская часть системы реализована именно на их основе. Данное требование практически невозможно считать обременяющим.

Что касается проблемы организации защищенного соединения, основным вопросом в решении проблемы информационной безопасности распределенных ресурсов интерактивных обучающих систем является выбор и реализация метода аутентификации web-пользователей.Наиболее распространена аутентификация пользователей посредством передачи по протоколу HTTP значений полей HTML-формы. При этом логин и пароль пользователя передаются серверу открытым текстом без модификаций, что делает схему уязвимой даже для простейших видов прослушивания трафика. Возможное хеширование пароля с помощью клиентского сценария перед его передачей на сервер никак не сказывается на практическом уровне информационной безопасности, так как хеш, в случае перехвата, может быть использован злоумышленником для повторной аутентификации [2, с. 26].

На практике эффективным способом борьбы с перехватом конфиденциальной информации является использование для её передачи защищённого канала на основе технологий криптографических протоколов SSL или TLS. Протоколы используют асимметричную криптографию для обмена ключами, а также симметричное шифрование данных для конфиденциальности и коды аутентичности для сохранения целостности сообщений.

За счёт того, что взаимодействие с сервером в процессе аутентификации происходит через защищённое соединение на основе TLS,

становится невозможным перехват конфиденциальной информации, поскольку:

1) на этапе обмена ключами пользовательский агент (веб-браузер) проверяет подлинность предоставленного сервером сертификата и удостоверяется в том, что форма аутентификации не является поддельной, препятствуя попыткам «фишинга» со стороны злоумышленника;

2) передаваемая пользовательским агентом информация шифруется с помощью временного ключа, созданного в процессе установления соединения, что исключает возможность дешифровки данных при прослушивании сетевого трафика злоумышленником. Описанное выше расширение протокола передачи HTTP за счёт SSL/TLS носит названия HTTPS.

После проверки полученных от пользовательского агента данных и его авторизации, в рамках дальнейшей коммуникации серверу необходимо идентифицировать запросы, поступающие от этого агента, в течение некоторого времени, то есть организовать временный виртуальный канал связи с агентом. Аутентификация на основе HTML-форм является общепринятым и распространённым подходом, но не стандартизована, то есть конкретный механизм идентификации запросов авторизованных пользователей не регламентируется и выбирается разработчиками веб-ресурсов на собственное усмотрение. Однако, в этой области существуют распространённые подходы и соглашения, являющиеся стандартами де-факто [1, с. 290].

Пары «запрос-ответ» протокола HTTP являются независимыми друг от друга самостоятельными транзакциями. Иными словами, протокол не отслеживает связи между отдельными запросами. Поэтому для идентификации запросов, поступающих от авторизованных агентов, в случае HTTP+HTML аутентификации используются виртуальные сессии на основе «cookie».

После проверки предоставленной информации, в случае успешной аутентификации, сервер создаёт виртуальную сессию и генерирует

временный ключ (идентификатор), который передаётся пользовательскому агенту и хранится в виде «cookie» на стороне клиента. Данный ключ, в соответствии с механизмом работы «cookie», передаётся серверу в заголовке каждого HTTP-запроса, относящегося к веб-ресурсу, до момента истечения срока действия «cookie». По значению полученного временного ключа сервер определяет сессию, к которой относится запрос (рис. 5).

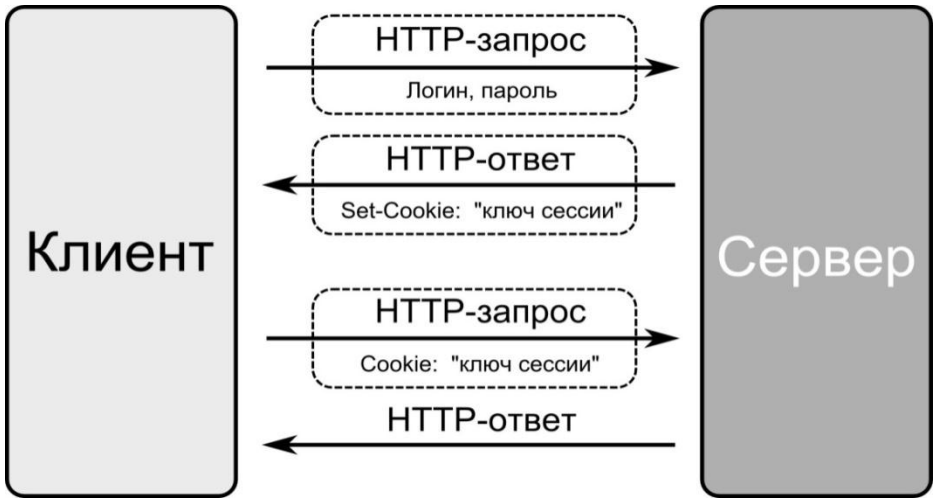

Рис. 5. Механизм идентификации запросов авторизованных агентов.

Информация, позволяющая проверить подлинность полученного ключа, и определить, к какой сессии относится полученный запрос, хранится на сервере и во избежание её перехвата по сети не передаётся. Также, в целях безопасности для передачи временных ключей не используются «cookie» с неограниченных сроком действия.

Для того, чтобы можно было гарантировать невозможность подделки ключа сессии злоумышленником, временный ключ должен удовлетворять ряду критериев. Во-первых, временный идентификатор сессии должен быть устойчив к простому перебору значений. Во-вторых, значения идентификаторов должны быть криптографически случайны. В-третьих, должны существовать способы проверки подлинности ключа сервером и обнаружения попыток модификации ключа. [2, с. 27]

Представленным критериям удовлетворяют значения, получаемые в результате хеширования текстовой строки и последующего шифрования

результата с использованием секретного ключа. Исходная текстовая строка получается путём конкатенации некоторого подмножества известных серверу данных о конкретной сессии, - этим обеспечивается верифицируемость временного ключа.

Примером такого механизма является, HMAC (hash-based message authentication code - хеш-код аутентификации сообщений) на основе алгоритма криптографического хеширования SHA1. HMAC — общее наименование механизмов шифрования, которые используют криптографические хеш-функции в сочетании с секретным ключом.

С целью использования полученного идентификатора сессии в виде «cookie» и передачи по протоколу HTTP, его необходимо преобразовать в форму ASCII-строки. Для этого полученное на выходе HMAC число представляется в 64-разрядной системе счисления base64.

Пример 64-разрядного кода аутентификации сообщения, полученного методом HMAC-SHA-1 из строки «login:datetime» с секретным ключом «SECRET_KEY», приведён ниже:

owqliFxF0h0OBL2F6dMDb8gkvjo=

Строка «login» в данном примере представляет логин авторизованного пользователя, а «datetime» дату и время создания сессии. Для того чтобы надёжно ограничить временные рамки актуальности ключа, дата и время активации добавляются к исходной строке в виде целого числа секунд, прошедших с 1 января 1970 года, то есть величины «epoch» Unix-систем.

Полученные коды аутентификации сообщений используются в составе «подписанных cookie». Строка данных «подписанных cookie» состоит из некоторого достаточного идентификатора сессии и его «подписи». Подпись представляет собой код аутентификации сообщения, полученный из достаточного идентификатора.

Наиболее простым и надёжным способом получения «подписанного cookie» является использование в качестве достаточного идентификатора некритичной составляющей пользовательских данных, например логина,

вместе с датой создания сессии, как это было сделано в предыдущем примере. Применение HMAC-SHA-1 гарантирует невозможность генерации верного кода аутентификации, если отсутствует хотя бы один из необходимых компонентов: исходная строка или секретный ключ. Исходная строка содержится в «подписанном cookie» вместе с её кодом верификации, однако секретный ключ известен только серверу и не передаётся по сети. Таким образом, до тех пор, пока секретный ключ остаётся известным только серверу, подделка такого идентификатора сессии невозможна. [2, с. 26] Таким образом, применение HTTP аутентификации пользователей на основе HTML-формы с шифрованием трафика посредством SSL/TLS позволяет организовать достаточно высокий уровень информационной безопасности ресурсов интерактивных обучающих систем с удаленным доступом.

Концепция лабораторий удаленного доступа является очень перспективной, поскольку эффективность для обучения студентов самых разных специальностей уже многократно подтверждена обширным мировым опытом. Проблемы внедрения лабораторий удаленного доступа в России усугубляется материально-техническим обеспечением учебных заведений, большой территориальной протяженностью страны и неравномерным распределением научно-технического потенциала по ее территории. Применение вышеизложенной концепции позволит значительно упростить процесс разработки и повсеместного внедрения лабораторий с удаленным доступом и сократит расходы учебных заведений на приобретение и обслуживание дорогостоящего уникального оборудования. Использование web-базированного доступа позволит использовать со стороны клиента в качестве приложения для доступа к образовательным ресурсом web-браузер, а не специализированное программное обеспечение, что делает предлагаемый подход достаточно универсальным. Электронный ресурс расположен по адресу http://ntk.intbel.ru.

Список литературных источников

1. Akhawe D. и др. Towards a formal foundation of web security // Computer Security Foundations Symposium (CSF), 2010 23rd IEEE. 2010. С. 290–304.

2. Fu K. и др. Dos and Don’ts of Client Authentication on the Web // Proceedings of the 10th USENIX Security Symposium. 2001. Т. 42.

3. Белоусов, А. В. Web-ориентированный доступ к технологической информации в системах мониторинга объектов энергопотребления / А. В. Белоусов, С. Н. Глаголев, Ю. А. Кошлич, А. Б. Быстров // Системы управления и информационные технологии. – Орел: ГУ УНПК. 2013 г. - Т. 52. № 2. С. 70-73.

4. Белоусов, А. В. Решение вопроса информационной безопасности в интерактивных обучающих системах с удаленным доступом / А. В. Белоусов, С. Н. Глаголев, Ю. А. Кошлич, А. Б. Быстров // Ученые записки ИСГЗ. – Казань: Юниверсум, 2013г. - № 1-1. С. 60-66.

Сведения об авторах:

Белоусов Александр Владимирович
Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород
Кандидат технических наук, профессор кафедры Технической кибернетики, начальник Управления информатизации и коммуникаций (УИК)
Область научных интересов: Автоматизированные системы диспетчерского управления, электроника
E-mail: ntk@intbel.ru
Тел.: +7(4722) 309-965

Глаголев Сергей Николаевич
БГТУ им. В.Г. Шухова, г. Белгород
Доктор экономических наук, профессор, ректор БГТУ им. В.Г. Шухова
Область научных интересов: разработка междисциплинарных учебных комплексов в системе «экономика и стратегия развития транспортного комплекса — управление транспортными процессами — сервис транспортных и технологических машин и оборудования»
E-mail: rector@intbel.ru
Тел.: +7(4722) 309-901

Рыбакова Анна Ивановна
БГТУ им. В.Г. Шухова, г. Белгород
Зам. начальника управления информатизации и коммуникаций, ст. преподаватель кафедры Информационных технологий
Область научных интересов: Информационные технологии и системы управления

E-mail: aribakova@intbel.ru
Тел.: +7(4722) 309-934

Кошлич Юрий Алексеевич
БГТУ им. В.Г. Шухова, г. Белгород
Аспирант кафедры Технической кибернетики, инженер УИК
Область научных интересов: Автоматизированные системы диспетчерского управления, микропроцессорная техника и электроника
E-mail: koshlich@yandex.ru
Тел.: +7 (909)200-44-58

Alexander Vladimirovich Belousov
BSTU named after VG Shukhov, Belgorod
Ph.D., Professor, Department of Technical Cybernetics , Head of Information and Communication
E-mail: ntk@intbel.ru
Tel. : +7 (4722) 309-965

Glagolev Sergey Nickolaevich
BSTU named after VG Shukhov, Belgorod
Doctor of Economics, Professor, Rector BSTU . VG Shukhov
E-mail: rector@intbel.ru
Tel. : +7 (4722) 309-901

Rybakova Anna Ivanovna
BSTU named after VG Shukhov, Belgorod
Deputy. Head of Information and Communications , Art. lecturer in Information Technology
Research interests: Information Technology and Systems Management
E-mail: aribakova@intbel.ru
Tel. : +7 (4722) 309-934

Koshlich Yuriy Alekseevich
BSTU named after VG Shukhov, Belgorod
Graduate student of Technical Cybernetics , engineer of Information and Communications
E-mail: koshlich@yandex.ru
Tel. : +7 (909) 200-44-58