S. E. Abramkin, S. E. Dushin, D. D. Sirota
Saint Petersburg Electrotechnical University «LETI»

DEVELOPMENT OF THE MATHEMATICAL MODEL OF A «RESERVOIR-GAS WELL» SYSTEM

Presents mathematical models of steady and unsteady isothermal gas filtration. For the case of pressure distribution in the bottomhole formation zone around a single well, a numerical model of gas filtration is constructed that approximates the boundary value problem by an implicit four-point scheme using a propulsion method, under the assumption of consistency of gas density and viscosity, permeability and elastic capacity of the rock. The presented model allows to calculate and predict the change in pressure distribution in the area around the well. For the numerical model obtained, an algorithm for the computer model has been developed. Using a computer model, the pressure distribution for the well, which drains the initially undisturbed formation within 30 days, is calculated. Graphs of the distribution of the pressure field, obtained when using a computer model, are given. In the simulation, boundary conditions of the first and second kind are adopted for the feed and bottom hole contours, respectively. The results obtained can be applied to the development of control systems for gas production facilities aimed at rational use of the reservoir energy and increasing the gas recovery factor.

Model of unsteady gas filtration, numerical model of gas filtration, computer model of gas filtration, distribution of pressure in a homogeneous gas reservoir

УДК 004.056.3

П. Д. Осмоловский, С. А. Романенко
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Реализация электронной подписи в подсистеме обеспечения эксплуатации и сервисного обслуживания ГАС «ВЫБОРЫ»

Описывается предложение по реализации модуля электронной подписи в подсистеме обеспечения эксплуатации и сервисного обслуживания ГАС «Выборы». Внедрение модуля позволит освободить участников взаимодействия от необходимости получать бумажные оригиналы документов для начала работы с данными. Результатом анализа архитектуры и требований подсистемы стала разработанная функциональная схема, которая легла в основу представленного решения. В статье формализованы процессы, которые планируется оптимизировать за счет использования технологии электронной подписи. Отталкиваясь от законодательных требований и проанализированных материалов, авторы аргументированно принимают решение о реализации модуля «ЭП ПОЭСО» в виде библиотеки скриптов для специализированного криптографического плагина, который доступен в браузере пользователей. Данное решение подробно описывается с использованием диаграмм, отображающих изменения процессов взаимодействия между участниками подсистемы и поясняющих структурное взаимодействие компонентов автоматизированных рабочих мест пользователей после внедрения модуля «ЭП ПОЭСО».

Электронная подпись, распределенная информационная система, электронный юридически значимый документооборот

В последнее время все чаще возникает потребность в обеспечении верификации данных, обмен которыми производится в рамках распределенных автоматизированных систем с элементами электронного документооборота. В таких системах первоисточником актуальной и достоверной информации являются бумажные документы, на основании которых вносятся изменения в данные, хранящиеся в электронном виде. С расширением количества объектов эксплуатации, автоматизируемых процессов, единиц учета растет и объем бумажных документов, своевременный централизованный сбор которых становится сдерживающим фактором эффективности

применения автоматизированной системы. Технология электронной подписи позволяет подтверждать цифровую копию документа-первоисточника и считать ее юридически равноценной оригиналу бумажного документа.

Подсистема обеспечения эксплуатации и сервисного обслуживания (далее – ПОЭСО) предназначена для автоматизации процессов учета программно-технических средств (ПТС) Государственной автоматизированной системы Российской Федерации «Выборы» (ГАС «Выборы») и сервисного обслуживания комплекса средств автоматизации Центральной избирательной комиссии Российской Федерации (далее – КСА ЦИК), восьмидесяти трех КСА избирательных комиссий субъектов Российской Федерации (далее – КСА ИКСРФ), более трех тысяч комплексов средств автоматизации территориальных избирательных комиссий (далее – КСА ТИК), более десяти комплексов средств автоматизации сервисных центров (далее – КСА СЦ), а также деятельности сервисных центров (СЦ) по обеспечению эксплуатации и сервисному обслуживанию КСА ГАС «Выборы» [1], [2].

На рис. 1 представлена структура ПОЭСО. Центральным элементом ПОЭСО являются внутренний и внешний серверы, расположенные в КСА ЦИК и обеспечивающие реализацию функциональных требований и хранение данных в структурированном виде. Для обеспечения безопасности информации серверы разделены воздушным зазором. Пользователи в КСА всех уровней работают с внутренним сервером, тогда как пользователи в СЦ работают с внешним сервером посредством «тонкого клиента», реализованного по технологии GWT, которая позволяет быстро и эффективно разрабатывать web-приложения, включающие в себя стандартные табличные формы отображения информации на языке Java. Для пользователей в КСА ЦИК также обеспечивается возможность работы с внешним сервером. Средствами ПОЭСО при участии администратора КСА ЦИК на регламентной основе (не реже двух раз в день) синхронизируются базы данных внутреннего и внешнего серверов.

Как правило, ПТС ГАС «Выборы» передаются поставщиками в СЦ и из СЦ в КСА партиями от нескольких десятков до нескольких тысяч единиц. Для каждой партии в СЦ и в КСА избирательной комиссии формируется бумажный акт приема-передачи, который должен быть представлен в КСА ЦИК. Акты приема-передачи формируются в ПОЭСО посредством ввода данных в электронном виде через клиентские приложения и распечатывания бумажных документов. Использование технологии «тонкий клиент» позволяет обеспечить наличие информации по актам приема-передачи в базе данных ПОЭСО в КСА ЦИК в момент их ввода. Однако проверить их актуальность и достоверность можно только после получения подписанных бумажных оригиналов документов. Высокая степень территориальной распределенности и организационные регламенты приводят к тому, что бумажные оригиналы документов попадают в КСА ЦИК с задержкой в несколько месяцев. Актуальной является реализация в ПОЭСО задачи хранения электронных образов бумажных оригиналов документов, проверки и подтверждения их целостности и достоверности с помощью электронной подписи, обеспечивающей юридическую значимость электронных документов. На сегодняшний день основным инструментом защиты электронных образов документов от несанкционированного изменения служит использование электронной подписи и криптографических алгоритмов [3]. Электронная подпись (ЭП) – это особый реквизит документа, который позволяет установить отсутствие искажения информации в электронном документе с момента формирования ЭП и подтвердить принадлежность ЭП владельцу. Значение реквизита получается в результате криптографического преобразования информации.

На стороне отправителя для подписи электронного образа документа вычисляется его хеш-функция, значение которой подвергается криптографическому преобразованию с использованием закрытого ключа пользователя и специального алгоритма, управляемого через криптопровайдер. Использование вместо бинарного представления значения его хеш-функции позволяет уравнять вычислительную сложность для файлов разного объема, обеспечивает совместимость алгоритмов для всех файлов, защищает содержание документа, даже если алгоритм формирования ЭП скомпрометирован. Закрытый ключ электронной подписи (ключ ЭП) позволяет генерировать электронную подпись и подписывать электронный документ. Открытый ключ электронной подписи (ключ проверки ЭП) однозначно связан с закрытым ключом ЭП и предназначен для проверки подлинности ЭП. Документом, подтверждающим принадлежность

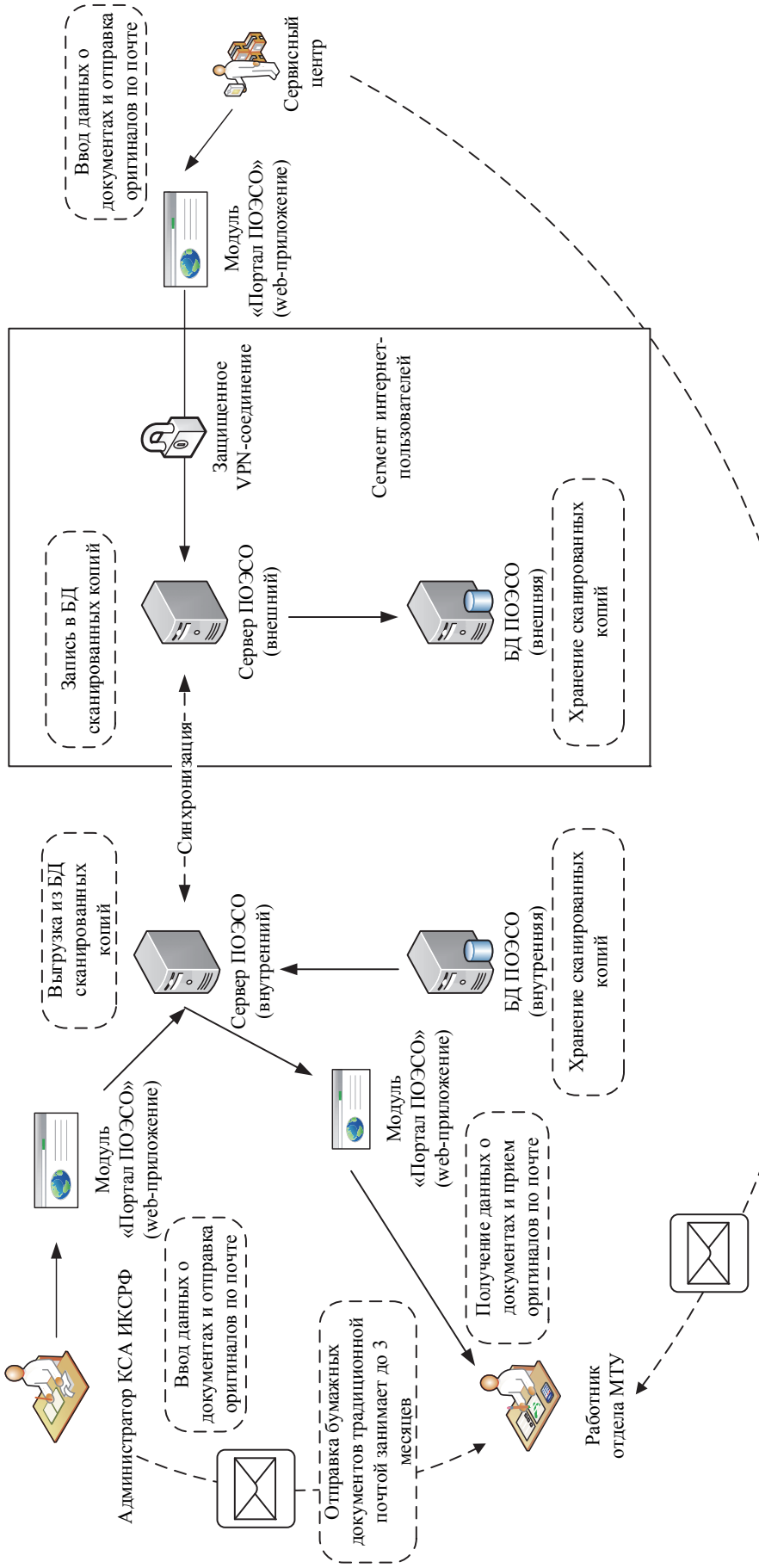
Ввод данных о документах и отправка оригиналов по почте
Сервисный центр
Модуль «Портал ПОЭСО» (web-приложение)
Защищенное VPN-соединение
Сегмент интернет-пользователей
Запись в БД сканированных копий
Сервер ПОЭСО (внешний)
БД ПОЭСО (внешняя)
Хранение сканированных копий
Синхронизация
Выгрузка из БД сканированных копий
Сервер ПОЭСО (внутренний)
БД ПОЭСО (внутренняя)
Хранение сканированных копий
Модуль «Портал ПОЭСО» (web-приложение)
Модуль «Портал ПОЭСО» (web-приложение)
Получение данных о документах и прием оригиналов по почте
Администратор КСА ИКСРФ
Ввод данных о документах и отправка оригиналов по почте
Отправка бумажных документов традиционной почтой занимает до 3 месяцев
Работник отдела МТУ

Рис. 1

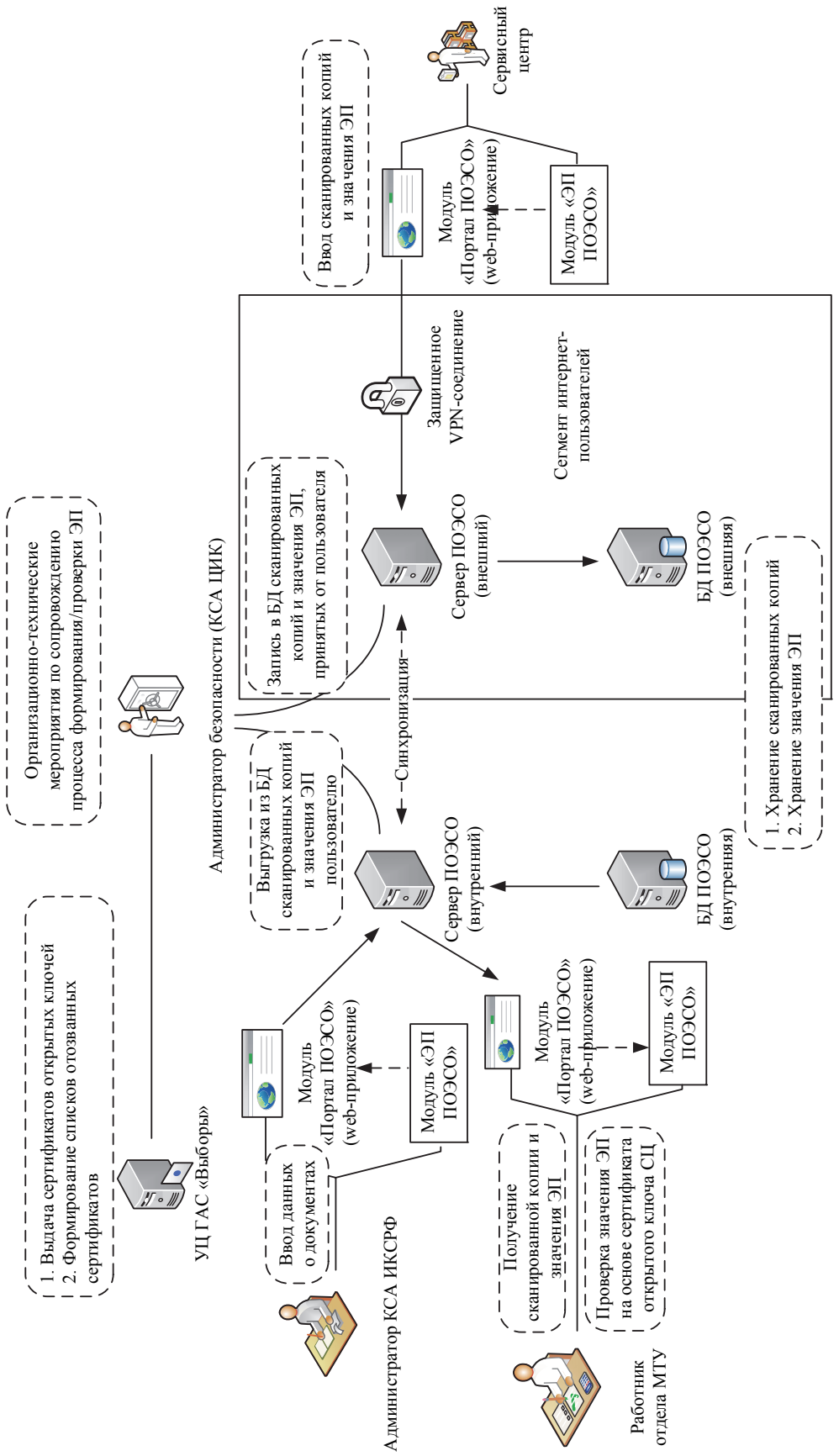
Организационно-технические мероприятия по сопровождению процесса формирования/проверки ЭП
1. Выдача сертификатов открытых ключей
2. Формирование списков отозванных сертификатов
УЦ ГАС «Выборы»
Администратор безопасности (КСА ЦИК)
Выгрузка из БД сканированных копий и значения ЭП пользователю
Запись в БД сканированных копий и значения ЭП, принятых от пользователя
Синхронизация
Сервер ПОЭСО (внутренний)
Сервер ПОЭСО (внешний)
БД ПОЭСО (внутренняя)
БД ПОЭСО (внешняя)
1. Хранение сканированных копий
2. Хранение значения ЭП
Защищенное VPN-соединение
Сегмент интернет-пользователей
Ввод сканированных копий и значения ЭП
Сервисный центр
Модуль «Портал ПОЭСО» (web-приложение)
Модуль «ЭП ПОЭСО»
Ввод данных о документах
Администратор КСА ИКСРФ
Получение сканированной копии и значения ЭП
Проверка значения ЭП на основе сертификата открытого ключа СЦ
Работник отдела МТУ

Рис. 2

закрытого и открытого ключей ЭП владельцу, является сертификат. Оборот сертификатов контролируется удостоверяющими центрами (УЦ) или их доверенными представителями. Владелец сертификата обязан хранить свой закрытый ключ в тайне.

На стороне получателя криптопровайдер дешифрует ЭП, используя открытый ключ отправителя, и сравнивает значение этой операции с вычисленным значением хеш-функции полученного образа документа. В случае совпадения факт авторства и целостности данных считают установленным.

Пригодные для формирования ЭП криптографические алгоритмы опираются либо на задачу дискретного логарифмирования (EGSA), либо на задачу разложения чисел на простые множители (RSA). Вычисления производятся на базе полей Галуа [4] или с использованием эллиптических кривых [5]. Стандарт ГОСТ Р 34.10–2012 описывает эталонный алгоритм, который, как и его предшественник, основан на свойствах эллиптических кривых, стойкость которых обеспечивается сложностью вычисления дискретного логарифма в группе точек эллиптической кривой, а также хеш-функциями, регулирующимися стандартом ГОСТ Р 34.11–2012.

По Федеральному закону от 06.04.11 № 63-ФЗ «Об электронной подписи» [6] выделяется 3 вида ЭП: простая, усиленная неквалифицированная (НЭП) и усиленная квалифицированная (КЭП). Максимально защищенной является КЭП, которая, как правило, используется на площадках электронных торгов и в системах юридически значимого документооборота, где необходимы гарантии установления авторства и целостности файла.

Функциональная схема предлагаемого решения по интеграции ЭП в подсистему ОЭСО показана на рис. 2. Основной задачей администратора безопасности является управление ключами пользователей, которое базируется на архитектуре PKI (Public Key Infrastructure) из рекомендаций стандарта X.509 в части управления сертификатами открытых ключей и должно обеспечиваться Удостоверяющим центром ГАС «Выборы» на основе продукта «КриптоПро УЦ».

Реализация данной схемы позволит участникам процессов не ждать доставки бумажных оригиналов документов в КСА ЦИК, а производить все необходимые действия с полученными из внутренней базы и проверенными модулем ЭП электронными копиями. Получение актуальных данных и возможность их использования станут доступны сотрудникам КСА ЦИК сразу же после попадания электронного образа документа и значения ЭП во внутреннюю базу данных.

При интеграции механизма электронной подписи в модуль «Портал ПОЭСО» учтены следующие технические требования:

– использование удостоверяющего центра ГАС «Выборы»;

– применение для генерации ключей, формирования и проверки ЭП, хеширования данных общего программного обеспечения, имеющего сертификаты соответствия ФСБ России и совместимого с используемыми средствами криптографической защиты информации в ГАС «Выборы»;

– учет существующей архитектуры подсистемы ОЭСО и обеспечение преемственности технический решений.

Модуль ЭП реализован в виде набора скриптов, который с помощью плагина для браузера «КриптоПро ЭЦП Browser plug-in» [7] позволяет формировать ЭП на необходимой странице web-приложения. Плагин требует наличия криптопровайдера CryptoPro CSP 4.0 [8], который включен в требования к пользовательским АРМ в ГАС «Выборы». Модуль ЭП является решением, основывающимся на сертифицированном ГОСТом алгоритме, что позволяет формировать КЭП. Достоинствами данного решения является доступность, при установленном плагине модуль запустится автоматически, а обновление происходит незаметно для пользователя. Интеграция модуля ЭП в ПОЭСО не требует изменения архитектуры и допускает прежние условия использования. Защищенность закрытого ключа пользователя обеспечена отсутствием необходимости в передаче секретной информации на сервер, что позволяет избежать серьезных издержек для проектирования и реализации системы хранения конфиденциальных данных пользователей. Продукты компании КриптоПро своевременно обновляют сертификат ФСТЭК, что позволяет использовать данные решения без рисков, связанных с потерей юридической силы цифровыми экземплярами.

После внедрения модуля «ЭП ПОЭСО» в ПОЭСО ГАС «Выборы» технология электронной подписи будет использована для учета поставки ПТС как в сервисные центры, так и на КСА ГАС «Выборы».

На рис. 3 отображена диаграмма взаимодействия участников процесса учета поставок ПТС в

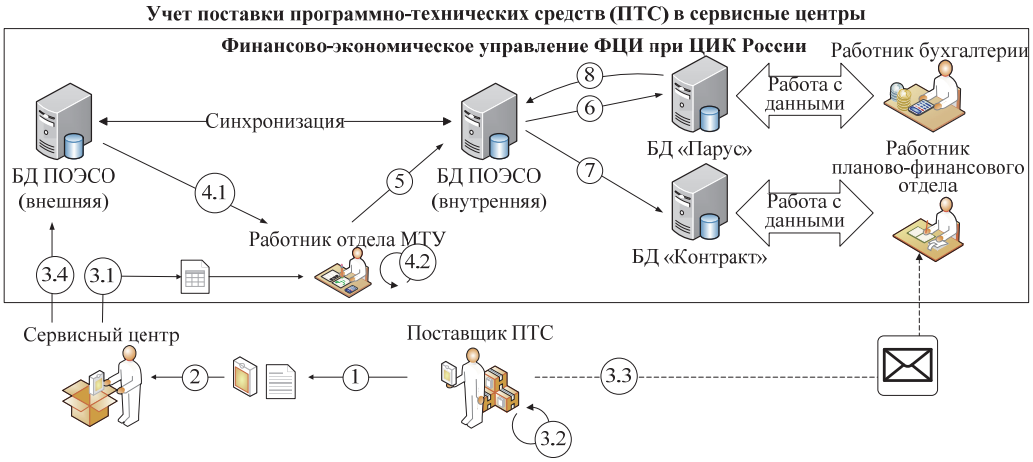

Рис. 3

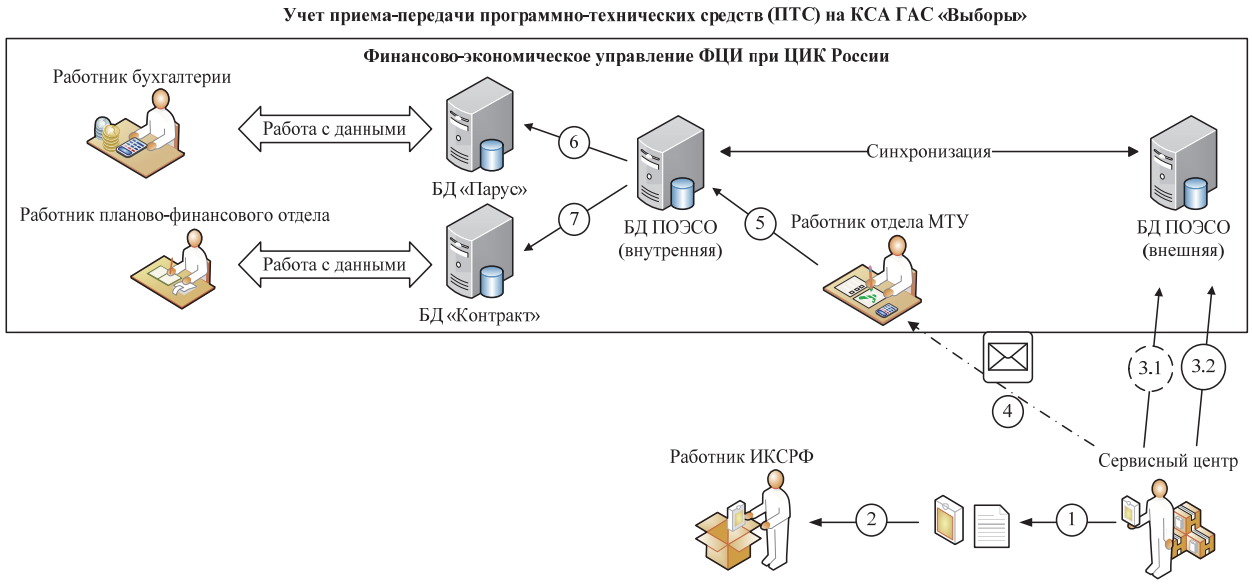

Рис. 4

СЦ. Поставщик ПТС при передаче оборудования сервисному центру оформляет товарно-транспортную накладную или акт приема-передачи (1). Бумажный оригинал документа подписывается представителем СЦ по доверенности ФЦИ при ЦИК РФ (2). Далее представитель СЦ формирует ЭП и загружает ее вместе со сканированной копией документа на внешнюю БД ПОЭСО (3.4). СЦ также отправляет спецификацию принятых ПТС отделу МТУ ФЦИ при ЦИК РФ в формате Excel (3.1). Этот файл автоматизированно проверяется с использованием специального программного обеспечения (СПО) ПОЭСО работниками отдела МТУ (4.2) после получения комплекта документов с внутреннего сервера ПОЭСО, проверенного модулем ЭП (4.1). Утвержденная спецификация автоматически размещается на внутренней БД ПОЭСО (5). Сведения об актах приема-передачи перемещаются в БД «Парус» (6), что позволяет работникам бухгалтерии ФЦИ при ЦИК РФ выдавать инвентарные номера и выгружать их в БД «Парус» (8). Сведения о принятых ПТС автоматически передаются в БД «Контракт» и становятся доступными работникам планово-финансового отдела ФЦИ из СПО ПОЭСО (7). Благодаря наличию реквизита ЭП работники планово-финансового отдела могут не дожидаться почтовой доставки бумажных оригиналов актов приема-передачи и товарно-транспортных накладных (3.3), а работать с электронными копиями, подтвержденными всеми участниками взаимодействия.

На рис. 4 отображена диаграмма взаимодействия участников процесса учета приема-передачи ПТС на КСА ГАС «Выборы».

При передаче ПТС в ИКСРФ СЦ формируют акт приема-передачи (1), который заверяется обе-

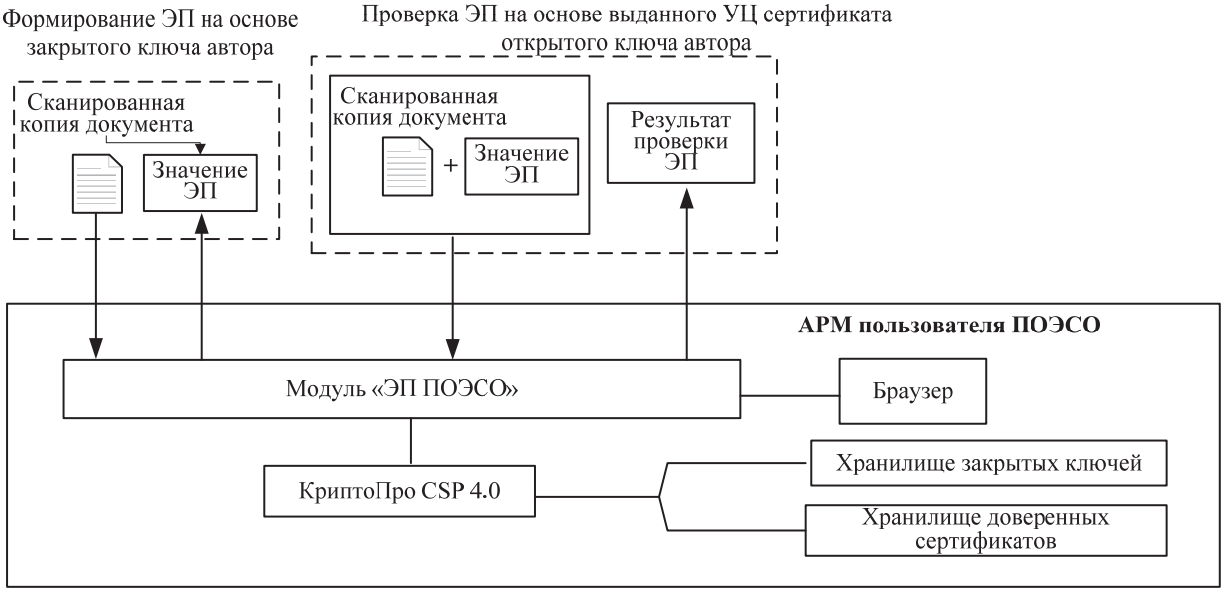

Рис. 5

ими сторонами (2). Информацию о переданном оборудовании СЦ заносят во внешнюю БД ПОЭСО (3.1), прикрепляя копию документа вместе с сформированным модулем ЭП реквизитом цифровой подписи (3.2). После синхронизации данные появляются во внутренней БД, работники отдела МТУ при ФЦИ ЦИК РФ проверяют полученный комплект с помощью модуля ЭП (5). Через некоторое время сотрудники также получают бумажный оригинал по почте (4), но наличие верифицированного цифрового образа позволяет сразу же продолжить работу с документами. Подтвержденные акты приема-передачи размещаются в БД «Парус» (6), а сведения о переданных ПТС – в БД «Контракт» (7). Работники бухгалтерии и планово-финансового отдела производят необходимые действия с использованием СПО намного быстрее, так как не надо ожидать доставки бумажных оригиналов сотрудникам отдела МТУ.

Основная версия модуля реализована на языке JavaScript стандарта EcmaScript 6 (ES6). Старые версии браузеров не поддерживают большое число функциональных возможностей ES6, для решения этой проблемы компанией КриптоПро была разработана версия плагина на стандарте ES5. Реализация дополнительных библиотек совместимости модуля ЭП позволит использовать для работы с ним практически любой браузер. На рис. 5 отображена схема взаимодействия компонентов АРМ пользователя при подписи сканированной копии документа и проверке ЭП.

Пользователь взаимодействует с ПОЭСО через браузер, который при необходимости в формировании или проверке ЭП сканированных копий документов обращается к модулю «ЭП ПОЭСО». Модуль является оболочкой для корректной работы браузера с криптопровайдером «КриптоПро CSP 4.0», имеющим доступ к хранилищам закрытых ключей и доверенных сертификатов пользователя и выполняющим требуемые криптографические операции по обработке данных. Для формирования ЭП модуль передает содержащий сканированную копию документа файл криптопровайдеру в бинарном виде, криптопровайдер получает значение закрытого ключа пользователя и на основе сертифицированных алгоритмов создает откреплённую электронную подпись. Для установления авторства и проверки целостности данных модуль передает комплект из документа и ЭП криптопровайдеру, который с помощью сертифицированных алгоритмов достоверно устанавливает факт авторства и целостности данных, отправляет ответ модулю для отображения результата проверки пользователю.

Представленное техническое и архитектурное решение построения модуля электронной подписи для ПОЭСО ГАС «Выборы» представляет собой настраиваемый механизм для организации защищенного и юридически значимого электронного документооборота. Архитектура модуля предполагает работу с многочисленными удаленными друг от друга сервисными центрами, избирательными комиссиями и представителями

ЦИК, осуществляющими взаимодействие через синхронизируемые базы данных с доступом к единому удостоверяющему центру «УЦ ГАС „Выборы“». Организация модуля в виде браузерного плагина позволяет внедрить ЭП в ПОЭСО без остановки работы пользователей. Представленное решение является универсальным для систем, использующих аналогичный набор технологий, так как предоставляет удобный интерфейс работы с криптографическими инструментами и не зависит от предметной области.

СПИСОК ЛИТЕРАТУРЫ

1. Государственная автоматизированная система Российской Федерации «Выборы» – неотъемлемая часть избирательной системы Российской Федерации. URL: http://cikrf.ru/gas/gas.pdf (дата обращения 01.03.2018).

2. Intelligent Enterprise. URL: http://cikrf.ru/gas/intelligent.pdf (дата обращения 01.03.2018).

3. Криптографические решения. От облачной подписи к доверенной среде. URL: https://goo.gl/hPXYZG. (дата обращения 01.03.2018).

4. ГОСТ Р 34.10–94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. URL: http://docs.cntd.ru/document/1200004855 (дата обращения 01.03.2018).

5. ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. URL: http://protect.gost.ru/document.aspx?control=7&id=180151 (дата обращения 01.03.2018).

6. Об электронной подписи. Федеральный закон РФ от 06.04.2011 № 63-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/.

7. КриптоПро ЭЦП Browser plug-in. URL: https://www.cryptopro.ru/products/cades/plugin (дата обращения 01.03.2018).

8. Государственная автоматизированная система Российской Федерации «Выборы». URL: http://cikrf.ru/gas/broshura_gas.pdf (дата обращения 01.03.2018).

P. D. Osmolovsky, S. A. Romanenko
Saint Petersburg Electrotechnical University «LETI»

DEVELOPMENT A DIGITAL SIGNATURE MODULE FOR THE OPERATION AND SERVICE SUPPORT SUBSYSTEM OF THE STATE AUTOMATED SYSTEM «VYBORY»

Describes the proposal on developing the digital signature module in the operation and service support subsystem of the state automated system «Vybory». The implementation of the module will eliminate the need for participants in obtaining the printed version of documents before working with data. As a result of the analysis of the subsystem architecture and requirements, a functional solution scheme was developed. The article characterizes formalized processes, which are to be optimized by using the digital signature. Attention is also given to the characteristics of its forms and the overall algorithm of its formation and verification. On the basis of the legal requirements and the analyzed materials the authors make a reasonable decision to implement the module as a script library for a special cryptographic plugin, which is accessible through the users' browser. This decision is thoroughly described by diagrams, which show the variation of cooperative processes between the subsystem participants and structural cooperation of the components of the users' automated workplaces.

Digital signature, distributed information system, legally significant electronic document flow