# Научная статья по теме “Разработка и внедрение средств электронной подписи в подсистеме обеспечения эксплуатации и сервисного обслуживания ГАС”Выборы"

## Аннотация

В данной статье проведено исследование возможности внедрения модуля электронной подписи в подсистему обеспечения эксплуатации и сервисного обслуживания ГАС “Выборы”. Было предложено решение, основанное на проектировании и реализации браузерного плагина для формирования электронной подписи. Для проверки целостности документов планируется использовать алгоритм на сервере, что позволит централизировать этот процесс и сократить нагрузку на клиентов. В связи с ограничениями, связанными с требованиями ПОЭСО ГАС “Выборы”, в качестве основного инструмента формирования и проверки ЭП выбран криптопровайдер от компании КриптоПро, обладающий сертификацией Федеральной службы по техническому и экспортному контролю и ФСБ РФ.

## Введение

В данной работе необходимо исследовать проблему разработки и внедрения средств электронной подписи в подсистеме обеспечения эксплуатации и сервисного обслуживания ГАС “Выборы”. Объектом исследования является Электронная подпись в документообороте представленной информационной системы, а предметом - свойства электронной подписи, обеспечивающие контроль целостности данных и верификации документооборота в ПОЭСО ГАС “Выборы”.  
Целью исследования является прояснение деталей проектирования и реализации модуля ЭП для верификации документов, участвующих в документообороте ПОЭСО ГАС “Выборы”.

### Задачи

* Анализ функциональной структуры и программной архитектуры ПОЭСО ГАС “Выборы”
* Изучение видов ЭП, алгоритмов ее формирования, готовых решений с учетом требований
* Выбор способа реализации ЭП в ПОЭСО ГАС “Выборы”

Разработка и внедрение программных модулей электронной подписи в подсистеме обеспечения эксплуатации и сервисного обслуживания Государственной автоматизированной системы «Выборы» является актуальной проблемой дальнейшего развития проекта ввиду отсутствия средств защиты и верификации документооборота в системе на данный момент. Решение проблемы позволит ввести контроль целостности документов, находящихся в системе. Усиленная квалифицированная электронная подпись подтверждается сертификатом от аккредитованного удостоверяющего центра и во всех случаях приравнивается к бумажному документу с «живой» подписью, что гарантирует юридическую силу ЭП, а также защищает информацию от атак с целью подмены содержимого.

## Обзор предметной области

### Выбор алгоритма для криптографической защиты документов

В 2012 году был принят новый российский стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи, ГОСТ Р 34.10-2012. Он, как и его предшественник, основан на свойствах эллиптических кривых, стойкость которых обеспечивается сложностью вычисления дискретного логарифма в группе точек эллиптической кривой, а также хэш-функциями, регулирующимися стандартом ГОСТ Р 34.11-2012.

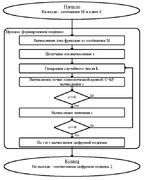
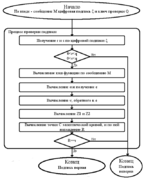
Схема формирования ЭП:  


Схема проверки подписи:  


Необходимо использовать именно этот алгоритм для возможности применения ЭП как средства подтверждения личности лица, подписавшего документ.  
### Сравнение вариантов программной реализации выбранного алгоритма формирования ЭП ##### Серверная - Подпись документов и верификация ЭП на сервере Данный вариант подразумевает использование сервера как основного регулятора процесса. Для подписи клиент будет вынужден передать данные на сервер, что не является безопасным подходом. Такая ЭП с большой вероятностью потеряет свою юридическую силу из-за нарушений законодательства РФ, регулирующего хранение закрытых ключей пользователя. Это решение можно отнести к “облачным”, в этой области на рынке представлено несколько продуктов, один из которых - КриптоПро DSS.

##### “Толстый клиент”

Эта реализация требует установки приложения каждому клиенту системы. Приложение сможет получать необходимые документы с сервера, или с локального диска, формировать ЭП и отправлять их в систему. Проверку ЭП можно проводить на сервере, где будут храниться открытые ключи пользователей, либо в приложении, для чего клиент должен будет получать документ, ЭП и открытый ключ предполагаемого автора.

##### Плагин для браузера

Данная реализация требует поддержки браузером JavaScript плагинов, наличие у каждого клиента CryptoPro CSP версии выше 3.6. Плагин будет получать доступ к сертификату пользователя и документ из ПОЭСО ГАС “Выборы”, ЭП будет формироваться в браузере клиента и отправляться непосредственно в систему.

##### Использование стороннего продукта

На данный момент наиболее удачным сторонним решением явяется Adobe Acrobat Pro, который позволяет формировать ЭП для документов в формате [.pdf]. Решение требует наличие лицензии на данный продукт, а также сертификата от удостоверяющего центра.

#### Критерии сравнения аналогов

##### Расширяемость

Критерий подразумевает оценку последующего развития ПОЭСО ГАС “Выборы”, увеличение нагрузки на серверную часть и базу данных.

##### Доступность

Подразумевает отсутствие сложностей при установке, использовании и обновлении модуля.

##### Безопасность

Критерий оценивается по количеству потенциальных рисков подмены или предоставления некорректных данных.

##### Масштабируемость

Возможность выделения в ПОЭСО ГАС “Выборы” модулей и из размещение на отдельных серверных узлах для увеличения производительности системы в целом.

#### Таблица сравнения по критериям

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Критерий | Серверная | “Толстый клиент” | Плагин для браузера | Adobe Acrobat Pro |
| Расширяемость | Низкая | Средняя | Высокая | Низкая |
| Доступность | Высокая | Низкая | Высокая | Средняя |
| Безопасность | Низкая | Высокая | Высокая | Низкая |
| Масштабируемость | Средняя | Высокая | Высокая | Низкая |

#### Выводы

По итогам анализа можно заметить, что каждое решение обладает своими преимуществами и недостатками. Серверная реализация позволит использовать проверенный сервер для формирования ЭП и верификацию документов, что исключит возможность подлога, так как данные будут заранее загружены в систему, но обновление данных о сертификатах будет затруднено. “Толстый клиент” является безопасным и отделенным от системы модулем, что позволит клиенту работать с модулем ЭП, даже если в системе произойдет сбой. Но возникают проблемы с первичной установкой, а также обновлением модуля. Плагин для браузера является гибким решением, так как пользователь будет уверен в безопасности своего закрытого ключа. Модуль сможет обновляться без действий клиента, но при отказе системы модуль также станет недоступным. Продукт компании Adobe является универсальным решением, которое может стабильно работать вне зависимости от состояния ПОЭСО ГАС “Выборы”, также пользователи смогут использовать его для просмотра и редактирования документов. Недостаток в том, что данное решение подразумевает использование прикрепленной ЭП для конкретного расширения файлов, что противоречит техническому заданию на разработку модуля ЭП ПОЭСО ГАС “Выборы”.

## Выбор метода решения

В результате сравнения аналогов реализации модуля ЭП для подсистемы обеспечения эксплуатации и сервисного обслуживания Государственной автоматизированной системы «Выборы» наиболее удачным вариантом архитектуры приложения для формирования ЭП стал модуль в виде плагина для браузера. При успешной реализации данного подхода клиент сможет подписывать документы, не покидая окно браузера, в котором открыта ПОЭСО ГАС “Выборы”, что не изменит интерфейс взаимодействия с системой. Закрытый ключ пользователя останется в безопасности, а система не будет отягощена работой с электронной подписью.  
Проверка электронных подписей должна производится на сервере, где будут храниться сертификаты с открытыми ключами пользователей. Для обеспечения актуальности предоставляемой сервером информации необходимо обновлять статус подписи раз в сутки. Для выбранного алгоритма шифрования существует несколько программных реализаций, среди которых решения от КриптоПро и Крипто-КОМ. Необходимо учесть, что по требованию Государственной автоматизированной системы «Выборы» на все клиентские машины устанавливается криптопровайдер КриптоПро CSP, таким образом остановимся на этом продукте и рассмотрим варианты реализации на его базе.

## Описание метода решения

Для формирования электронной подписи в ПОЭСО ГАС “Выборы” необходимо внедрить плагин, работа которого будет заключаться в следующем: + Получение доступа к работе с сертификатом пользователя + Получение документа из специального поля на странице загрузки документа + Получение списка отклоненных сертификатов + Формирование ЭП с помощью алгоритма из библиотеки криптопровайдера КриптоПро CSP + Загрузка документ и ЭП в систему

Для проверки электронной подписи необходимо при каждом обращении к документу проверять время его последней проверки на сервере, в случае, если оно превышает 24 часа, необходимо запускать повторную проверку, которая позволит убедиться в целостности данных, либо покажет, что подпись невалидна. Также необходимо осуществлять первичную проверку подписи документов при их загрузке в ПОЭСО ГАС “Выборы”. Работа алгоритма проверки заключается в следующем:  
+ Обращение к Удостоверяющему центру ГАС “Выборы” и получение сертификата ключа проверки электронной подписи пользователя, загрузившего документ + Хэширование бинарного представления документа + Расшифровка ЭП, прикрепленной к проверяемому документу, с помощью открытого ключа пользователя + Сравнение полученных хэшей документа, положительный ответ в случае их идентичности, в ином случае отрицательный.

## ## Исследование метода решения

## Заключение

В результате выполнения работы было проведено исследование возможности внедрения средств электронной подписи в подсистему обеспечения эксплуатации и сервисного обслуживания ГАС “Выборы”. Проведенное исследование позволило разобрать утвержденные ГОСТом криптографические алгоритмы, которые позволяют формировать электронную подпись. Изучены готовые программные решения, удовлетворяющие требованиям Законодательства РФ, а также лучшие практики реализаций подобных модулей. На основании проведенного исследования реализован модуль, работающий на базе плагина для браузера КриптоПро.

## Список литературы

http://www.altell.ru/legislation/standards/gost-34.10-2012.pdf  
https://ru.wikipedia.org/wiki/ГОСТ\_Р\_34.10-2012