*В. М. Ничипорчук, Н. П. Цапкин*

# ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В ВЕБ-ПРИЛОЖЕНИЯХ[1]

## Введение

В настоящее время наиболее распространенными источниками информации являются веб-сайты. Большинство современных информационных сайтов поддерживаются и работают на базе систем управления веб-содержимым, которые позволяют в реальном времени размещать и обрабатывать информацию в интернет-среде.

Развитие компьютерных технологий и их использование для осуществления доверенного обмена информацией потребовало применения средств и технологий информационной безопасности, в частности средств криптографической защиты данных. Одно из таких средств — электронная цифровая подпись (ЭЦП). Механизм электронной цифровой подписи позволяет надежно идентифицировать владельца подписи, установить отсутствие искажения информации в электронном документе, а также обеспечивает неотказуемость подписавшегося [1]. На законодательном уровне в России электронная цифровая подпись приравнивается к собственноручной подписи при соблюдении ряда юридических, организационных и технических условий. Одним из таких условий для органов госуправления является применение исключительно российских средств криптографической защиты.

В связи с этим перед авторами была поставлена задача разработки средств электронной цифровой подписи в веб-приложениях с поддержкой российских криптографических стандартов. Решение задачи включало в себя следующие основные этапы: проектирование программного обеспечения электронной цифровой подписи в веб-приложениях с поддержкой российских криптографических стандартов, разработку веб-апплета и интеграцию веб-апплета в систему управления веб-содержимым.

## Особенности применения ЭЦП в веб-приложениях

Сегодня все чаще ЭЦП применяется в информационных системах при требовании юридического закрепления [2] действий пользователя. Без использования механизмов ЭЦП деятельность таких систем была бы крайне затруднена или практически невозможна. Благодаря ЭЦП в России появилась возможность широкого использования таких систем, как системы электронного документооборота, системы электронной торговли, банковские и учетные системы, системы предоставления государственных услуг, корпоративные информационные системы и многие другие. Отдельно стоит отметить важнейшую роль ЭЦП в «Концепции формирования в Российской Федерации электронного правительства до 2010 года», разработанной Министерством информационных технологий и связи РФ совместно с Министерством экономического развития и торговли РФ и Федеральной службой охраны РФ [3]. В соответствии с данной концепцией целями формирования в России электронного правительства являются:

• повышение качества и доступности предоставляемых организациям и гражданам государственных услуг, упрощение процедуры и сокращение сроков их оказания, снижение административных издержек со стороны граждан и организаций, связанных с получением государственных услуг, а также внедрение единых стандартов обслуживания граждан;

• повышение открытости информации о деятельности органов государственной власти и расширение возможности доступа к ней и непосредственного участия организаций, граждан и институтов гражданского общества в процедурах формирования и экспертизы решений, принимаемых на всех уровнях государственного управления;

[1]Статья написана в рамках НИР «Обеспечение безопасности информации в открытых распределенных вычислительных системах», заданной Государственным контрактом № П2397 в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы.

• повышение качества административно-управленческих процессов;

• совершенствование системы информационно-аналитического обеспечения принимаемых решений на всех уровнях государственного управления, обеспечение оперативности деятельности органов государственной власти и обеспечение требуемого уровня информационной безопасности электронного правительства при его функционировании.

Без использования механизма электронной цифровой подписи, включенного в инфраструктуру «электронного правительства», достижение поставленных целей невозможно. В последнее время в программной индустрии наблюдается переход от технологии классических настольных приложений к веб-приложениям, доступным из любой точки мира благодаря сети Интернет. В связи с этим все больше возрастает значимость использования средств электронной цифровой подписи в таких веб-приложениях, которые предоставляют функциональность информационных систем, требующих юридического закрепления действий пользователя, а также надежного механизма для идентификации пользователя и контроля целостности информации, передаваемой от его лица.

Согласно новейшему российскому законодательству (Приказ Министерства экономического развития Российской Федерации от 16 ноября 2009 г. № 470 г. Москва «О требованиях к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами федеральных органов исполнительной власти»), информация, публикуемая на сайтах органов государственной власти, должна быть защищена ЭЦП [4, 5]. Это означает, что имеющиеся системы управления веб-содержимым должны поддерживать средства ЭЦП российских криптографических стандартов. Однако на сегодняшний день в большинстве известных систем управления веб-содержимым данная функциональность отсутствует. На международном рынке программного обеспечения существует ряд разработок, позволяющих интегрировать в веб-приложения механизмы ЭЦП, однако ни одна из имеющихся на сегодняшний день разработок не поддерживает ЭЦП российских криптографических стандартов.

Авторами осуществлена разработка и создан опытный образец программного обеспечения, реализующий механизмы ЭЦП в веб-приложениях с поддержкой российских криптографических стандартов.

## Архитектура программного обеспечения

На рис. 1 представлена архитектура разработанного программного обеспечения. Веб-приложения построены на классической клиент-серверной архитектуре. В роли сервера выступает веб-сервер, в роли клиента — веб-браузер. На стороне сервера работает система управления веб-содержимым, в которую встроен специальный модуль, отвечающий за хранение и обработку цифровых подписей, а также за ограничение действий над электронными документами.

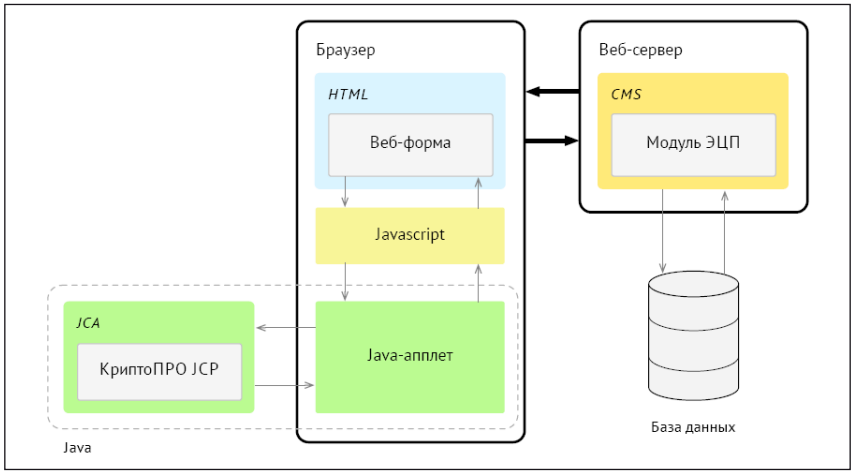


*Рис. 1. Архитектура разработанного программного обеспечения*

Содержимое веб-страницы пересылается на сторону клиента вместе с исполняемым кодом Javascript, программой Java-апплета и параметрами для настройки апплета. После этого на стороне клиента происходит инициализация и исполнение Javascript-программы и Java-апплета. Содержимое веб-страницы представлено HTML-разметкой, в которой отображается веб-форма. Содержимое веб-формы и предназначено для подписи. Javascript-программа отвечает за обработку различных событий и конфигурацию Java-апплета. Она перехватывает событие отправки данных веб-формы и вызывает Java-апплет, передавая ему всю необходимую информацию, введенную пользователем.

Для цифровой подписи Java-апплет взаимодействует с сертифицированным криптопровайдером КриптоПРО JCP [6], отвечающим за реализацию ЭЦП Российских криптографических стандартов. Взаимодействие происходит в рамках стандартной архитектуры Java Cryptographic Architecture. Java-апплет взаимодействует с Javascript-программой в обе стороны. Он позволяет уведомлять Javascript-программу о различных событиях, таких как успешная инициализация апплета или отмена решения о подписи содержимого. После подписи данных с помощью Java-апплета на стороне Javascript-программы срабатывает событие, вызванное Java-апплетом. Это событие вызывает дальнейшую отправку данных, включая цифровую подпись.

В качестве системы управления веб-содержимым (CMS) была использована CMS Drupal с открытым исходным кодом.

**Заключение**

В работе предложена архитектура, а также реализация веб-апплета, позволяющего осуществлять взаимодействие с криптопровайдером и выполнять криптографические операции с поддержкой стандартизованных российских криптоалгоритмов. Полученный апплет был встроен в систему управления сайтом для подписи содержимого электронной цифровой подписью.

Полученное решение обладает рядом преимуществ:

- кросс-платформенностью: решение протестировано на клиентских платформах Windows и MacOS;
- возможностью полностью выполняться в контексте браузера;
- возможностью поддержки смарт-карт;
- совместимостью с сертифицированным криптопровайдером КриптоПРО.

Полученные наработки нашли практическое применение в разработке сайта Управления делами Президента Российской Федерации.

Изложенные результаты получены в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы.

## СПИСОК ЛИТЕРАТУРЫ:

1. *Фергюсон Н., Шнайер Б.* Практическая криптография. Изд-во: Вильямс, 2005. — 424 с.: ил.
2. Федеральный закон Российской Федерации от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».
3. Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года. Распоряжение Правительства РФ от 27.09.2004 г.
4. Приказ Министерства экономического развития Российской Федерации от 16 ноября 2009 г. № 470 г. Москва «О требованиях к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами федеральных органов исполнительной власти».
5. Федеральный закон Российской Федерации от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».
6. СКЗИ КриптоПРО JCP. URL: http://www.cryptopro.ru/cryptopro/products/jcp/description.htm.