DOI: 10.58168/PPSPM2025_441-448
УДК 004.9

ИССЛЕДОВАНИЕ СТАНДАРТОВ ПОДПИСАНИЯ ДОКУМЕНТОВ ЭЛЕКТРОННОЙ ПОДПИСЬЮ В БРАУЗЕРЕ: АНАЛИЗ ВЗАИМОДЕЙСТВИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КРИПТОПРО И ВЕБ-ПРИЛОЖЕНИЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

А.А. Пустовалов, А.И. Заревич

ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. В статье рассматриваются проблемы интеграции программного обеспечения КриптоПро с современными веб-приложениями информационных систем. Проанализированы архитектурные особенности КриптоПро Browser plug-in, выявлены узкие места производительности и проблемы совместимости с различными браузерами. Предложены подходы к унификации API для работы с криптографическими операциями в веб-среде. Исследованы возможности оптимизации взаимодействия между клиентской и серверной частями системы при использовании российских криптографических стандартов ГОСТ.

Ключевые слова: КриптоПро, веб-приложения, цифровая подпись, ГОСТ, CSP, электронная подпись в браузере, криптографическая интеграция.

STUDY OF ELECTRONIC SIGNATURE DOCUMENT STANDARDS IN BROWSER: ANALYSIS OF INTERACTION BETWEEN CRYPTOPRO SOFTWARE AND WEB APPLICATIONS OF INFORMATION SYSTEMS

A.A. Pustovalov, A.I. Zarevich

Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract: The article examines the challenges of integrating CryptoPro software with modern web applications of information systems. Architectural features of the CryptoPro Browser plug-in are analyzed, performance bottlenecks and compatibility issues with various browsers are

identified. Approaches to API unification for cryptographic operations in the web environment are proposed. Opportunities for optimizing interaction between the client and server parts of the system when using Russian cryptographic standards GOST are explored.

Keywords: CryptoPro, web applications, digital signature, GOST, CSP, electronic signature in browser, cryptographic integration.

Переход к юридически значимому электронному документообороту создает высокие требования к надежности криптографических операций в клиентских веб-средах. В Российской Федерации использование электронной цифровой подписи (ЭЦП) регламентируется национальными стандартами ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, которые определяют алгоритмы формирования и проверки ЭЦП, а также функции хэширования.

Одним из наиболее распространенных средств реализации криптографических функций в веб-приложениях является программное обеспечение КриптоПро, включающее КриптоПро CSP (Cryptographic Service Provider) и КриптоПро ЭЦП Browser plug-in. Данные компоненты обеспечивают создание и проверку электронной подписи непосредственно в браузере пользователя, что позволяет реализовать полноценный электронный документооборот в веб-приложениях.

Однако интеграция КриптоПро с современными веб-приложениями сопряжена с рядом технических проблем, связанных с архитектурными особенностями плагина, совместимостью с различными браузерами и производительностью криптографических операций. Эти проблемы становятся особенно актуальными в контексте развития современных веб-технологий и требований к пользовательскому интерфейсу.

КриптоПро CSP представляет собой комплекс криптографических средств, обеспечивающих реализацию российских стандартов шифрования и электронной подписи. Архитектура системы включает следующие основные компоненты:

1. Криптографическое ядро – реализует алгоритмы ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012. Ядро обеспечивает выполнение базовых криптографических операций: генерацию ключей, шифрование, дешифрование, формирование и проверку электронной цифровой подписи;

Система управления ключами – обеспечивает генерацию, хранение и управление криптографическими ключами. Включает механизмы работы с контейнерами ключей, сертификатами и списками отозванных сертификатов;

2. Модуль аутентификации – реализует процедуры проверки подлинности сертификатов, включая проверку цепочки доверия и валидацию временных меток;

Интерфейс взаимодействия – предоставляет API для интеграции с прикладными программами через стандартные интерфейсы Microsoft Crypto API и PKCS.

КриптоПро ЭЦП Browser plug-in функционирует как посредник между веб-приложением и КриптоПро CSP, обеспечивая выполнение криптографических операций в браузере. Плагин состоит из следующих компонентов:

1. Модуль инициализации – отвечает за загрузку и инициализацию криптографических библиотек, проверку совместимости с установленной версией КриптоПро CSP;

JavaScript API – предоставляет интерфейс для взаимодействия веб-приложения с криптографическими функциями. API включает методы для работы с сертификатами, создания и проверки подписи, хэширования данных;

Модуль обработки сертификатов – управляет списком доступных сертификатов, их фильтрацией и отображением пользователю для выбора;

Модуль формирования подписи – реализует процедуры создания электронной подписи в различных форматах (CAdES-BES, CAdES-T, CAdES-X Long Type 1).

Плагин работает в двух режимах: синхронный режим – используется в устаревших браузерах и обеспечивает последовательное выполнение операций, асинхронный режим – применяется в современных браузерах и позволяет выполнять операции без блокировки пользовательского интерфейса.

Российское законодательство определяет использование следующих криптографических стандартов:

1. ГОСТ Р 34.10-2012 – определяет алгоритм формирования и проверки электронной цифровой подписи на основе эллиптических кривых. Стандарт поддерживает два размера ключа: 256 и 512 бит;

2. ГОСТ Р 34.11-2012 «Стрибог» – функция хэширования, обеспечивающая вычисление хэш-значения для данных произвольной длины с фиксированным размером выходного значения 256 или 512 бит;

3. ГОСТ Р 34.12-2015 «Кузнечик» – алгоритм блочного шифрования с размером блока 128 бит и длиной ключа 256 бит.

Одной из основных проблем является обеспечение совместимости плагина с различными браузерами. Современные браузеры постепенно отказываются от поддержки плагинов на основе NPAPI и ActiveX, что требует использования альтернативных технологий интеграции. С исторической точки зрения плагин эволюционировал от синхронной модели, характерной для ActiveX/NPAPI, к асинхронной, более дружелюбной к современным браузерам и требовательной к обработке ошибок и гонок состояний. При этом нормативно-правовая среда и отраслевые практики закрепляют использование ГОСТ-алгоритмов, что напрямую влияет на технологические выборы и зачастую требует нативных или доверенных реализаций.

Вариант интеграции с браузерами традиционно уязвим к атакам, эксплуатирующим браузерный контекст. Вмешательства в цепочку доставки (подмена скриптов), XSS со съемом контекстов и объектов, манипуляции параметрами API, а также повторы операций на уровне протокола — типовые угрозы, которые требуют системного внедрения контрмер: строгие политики содержания (CSP), целостные метки на ресурсы, аудит кода и статический анализ, минимизация доверенной поверхности плагина, а также протоколирование и корреляция событий на стороне сервера. Криптографическая прочность при этом должна сочетаться с корректностью следующих операций: безопасности хранения и обращения с контейнерами ключей, адекватной валидацией входных структур и защитой каналов подписи.

Разнообразие режимов и реализаций детерминирует потребность в унифицированном JavaScript-слое, абстрагирующем от различий между синхронной и асинхронной версиями плагина. Такой слой должен привести вызовы к единому асинхронному контракту, нормализовать поверхности ошибок, поддерживать обнаружение окружения и корректно маршрутизировать операции между доступными механизмами.

Публичные пакеты, такие как crypto-pro, демонстрируют подход к скрытию различий и стандартизации сценариев получения сертификатов, подписания и проверки, а также способствуют переносу кода между браузерами и версиями инфраструктуры. На уровне производительности существенный вклад дает ленивое подключение cadesplugin_api.js, встроенная повторная инициализация без блокировки интерфейса, а также кэширование результатов проверки цепочек и индексов сертификатов.

Разумная пакетизация операций (например, группировка подписаний с минимизацией контекстных переключений) и перенос тяжелых вычислений в

Web Workers позволяют снизить джиттер интерфейса. В комплексных системах дополнительно учитывается влияние корпоративных прокси и фильтров на вызовы внешних сервисов валидации.

С учетом ограничений поддержки ГОСТ в стандартном Web Crypto API разумным представляется гибридный подход: нативные механизмы браузера применяются там, где это не противоречит нормативным требованиям (к примеру, для алгоритмов хэширования отличных от ГОСТ или вспомогательных операций), тогда как формирование юридически значимой подписи и операции, требующие сертифицированных реализаций, делегируются КриптоПро.

Резюмируя подходы, был проведен сравнительный анализ всех вариантов взаимодействия программного обеспечения КриптоПро и веб-приложений информационной системы и показан в таблице 1.

Таблица 1 – Сравнение подходов к автоматизации документооборота в условиях крупного бизнеса

Критерий	Плагин КриптоПро	Унифицированный JS-слой (обертка над КриптоПро)	Гибридный подход (Web Crypto API + КриптоПро для ГОСТ)
Совместимость браузеров	Зависит от NPAPI/ActiveX и поддержки расширений; проблемы в современных браузерах	Повышенная за счет абстракции, но зависит от наличия КриптоПро и политик среды	Максимальная, браузерная нативная часть уменьшает зависимость; ГОСТ-операции остаются через КриптоПро
Соответствие ГОСТ	Полное соответствие (ГОСТ Р 34.10-2012, CAdES)	Сохраняется, так как операции делегируются КриптоПро	Сохраняется для ГОСТ-операций; часть задач — нативно в браузере через Web Crypto API

Производительность (инициализация/подпись)	Выше накладные расходы на инициализацию и доступ к хранилищам; стабильная подпись	Улучшенная за счет ленивой загрузки и кэширования; снижение лагов UI	Наилучший UX: часть операций быстро через Web Crypto API; ГОСТ — через плагин КриптоПро
Безопасность фронтенда	Требует строгих политик доставки кода, целостности и CSP; риски XSS/MITM	Дополнительные риски в обертке снижаются при код-ревью и SRI; единая обработка ошибок	Минимальные риски за счет использования нативного API
Внедрение и сопровождение	Сложнее: установка, обновления, корпоративные ограничения	Средняя сложность: единый контракт для фронтенда	Ниже порог для части функций, но требуется одновременная поддержка плагина и браузерного API
Масштабируемость сценариев	Ограничена типом плагина и политиками операционной системы и браузера	Достаточна для типовых веб-сценариев	Высокая для кроссплатформенных и мобильных браузеров

Качество интеграции оценивается по совокупности критериев, охватывающих корректность криптографических процедур, кроссбраузерную совместимость, устойчивость к нагрузке и безопасность на уровне клиент-серверного взаимодействия.

Функциональные испытания проверяют формирование и верификацию подписи в целевых форматах CAdES, корректность фильтрации и выбора

сертификатов, обработку исключительных сценариев. Совместимость оценивается на наборах браузеров и ОС с различными версиями CSP и плагинов, а также в условиях корпоративных ограничений (прокси, фильтры контента). Нагрузочные испытания фокусируются на времени инициализации, латентности операций при возрастающих объемах данных и длительных сессиях, контролируя использование памяти и деградацию отклика интерфейса.

Интеграция программного обеспечения КриптоПро с веб-приложениями информационных систем представляет собой сложную техническую задачу, требующую комплексного подхода к решению проблем совместимости, производительности и безопасности.

Анализ существующих решений показывает необходимость разработки унифицированных подходов к интеграции криптографических функций в веб-среде. Дальнейшие исследования должны быть направлены на разработку новых методов интеграции криптографических функций, адаптированных к современным веб-технологиям и требованиям информационной безопасности.

Список литературы

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. – Москва : Издательство Юрайт, 2021. – 253 с. – (Высшее образование). – ISBN 978-5-534-13960-0.

2. Григорьев, М. В. Проектирование информационных систем : учебник для вузов / М. В. Григорьев, И. И. Григорьева. — Москва : Издательство Юрайт, 2025. — 278 с. — (Высшее образование). — ISBN 978-5-534-16340-7.

3. Мельников, В. П., Клейменов, С. А., Петраков, А. М. Информационная безопасность и защита информации : учебник / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – 6-е изд., перераб. и доп. – Москва : Академия, 2020. – 336 с. – ISBN 978-5-7695-9222-5.

4. КриптоПро ЭЦП Browser plug-in – Раздел для разработчиков // cryptopro.ru. – URL: https://cryptopro.ru/products/cades/plugin/developer (дата обращения: 09.10.2025).

5. КриптоПро CADES ЭЦП Browser plug-in // Astra Linux. – URL: https://wiki.astralinux.ru/pages/viewpage.action?pageId=53645421 (дата обращения: 09.10.2025).

6. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной

цифровой подписи. – Введ. 2013-01-01. – Москва : Стандартинформ, 2012. – 24 с.

7. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. – Введ. 2013-01-01. – Москва : Стандартинформ, 2012. – 24 с.

8. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – Введ. 2016-01-01. – Москва : Стандартинформ, 2015. – 16 с.

References

1. Suvorova, G. M. Information Security: Textbook for Universities / G. M. Suvorova. – Moscow: Yurayt Publishing House, 2021. – 253 p. – (Higher Education). – ISBN 978-5-534-13960-0.

2. Grigoriev, M. V. Information Systems Design: Textbook for Universities / M. V. Grigoriev, I. I. Grigorieva. – Moscow: Yurayt Publishing House, 2025. – 278 p. – (Higher Education). – ISBN 978-5-534-16340-7.

3. Melnikov, V. P., Kleimenov, S. A., Petrakov, A. M. Information Security and Information Protection: Textbook / V. P. Melnikov, S. A. Kleimenov, A. M. Petrakov. – 6th ed., revised and enlarged. – Moscow: Academy, 2020. – 336 p. – ISBN 978-5-7695-9222-5.

4. CryptoPro EDS Browser plug-in – Developer Section // cryptopro.ru. – URL: https://cryptopro.ru/products/cades/plugin/developer (accessed: 09.10.2025).

5. CryptoPro CADES EDS Browser plug-in // Astra Linux. – URL: https://wiki.astralinux.ru/pages/viewpage.action?pageId=53645421 (accessed: 09.10.2025).

6. GOST R 34.10-2012. Information Technology. Cryptographic Information Protection. Digital Signature Generation and Verification Processes. – Effective from 2013-01-01. – Moscow: Standartinform, 2012. – 24 p.

7. GOST R 34.11-2012. Information Technology. Cryptographic Information Protection. Hash Function. – Effective from 2013-01-01. – Moscow: Standartinform, 2012. – 24 p.

8. GOST R 34.12-2015. Information Technology. Cryptographic Information Protection. Block Ciphers. – Effective from 2016-01-01. – Moscow: Standartinform, 2015. – 16 p.