

ПОДХОДЫ К ИСПОЛЬЗОВАНИЮ СИСТЕМЫ ОБЛАЧНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации», г. Минск, Республика Беларусь, сотрудник

В современном обществе, существующем в «цифровом мире», электронная цифровая подпись (ЭЦП) играет важную роль в обеспечении безопасности и придании юридической значимости электронным документам.

В Республике Беларусь порядок использования электронных документов с реквизитом в виде ЭЦП определяется законом Республики Беларусь №113-3 от 28.12.2009 «Об электронном документе и электронной цифровой подписи». Этот закон направлен на установление правовых основ применения электронных документов, определение основных требований, предъявляемых к электронным документам, а также правовых условий использования ЭЦП в электронных документах, при соблюдении которых ЭЦП в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе [1].

С учетом законодательства Республики Беларусь, стандартов в области информационных технологий и информационной безопасности был разработан прототип регистрационного центра инфраструктуры открытых ключей, который позволяет пользователям создавать электронные документы с облачной электронной цифровой подписью. Схема взаимодействия между компонентами этого центра представлена на рисунке 1.

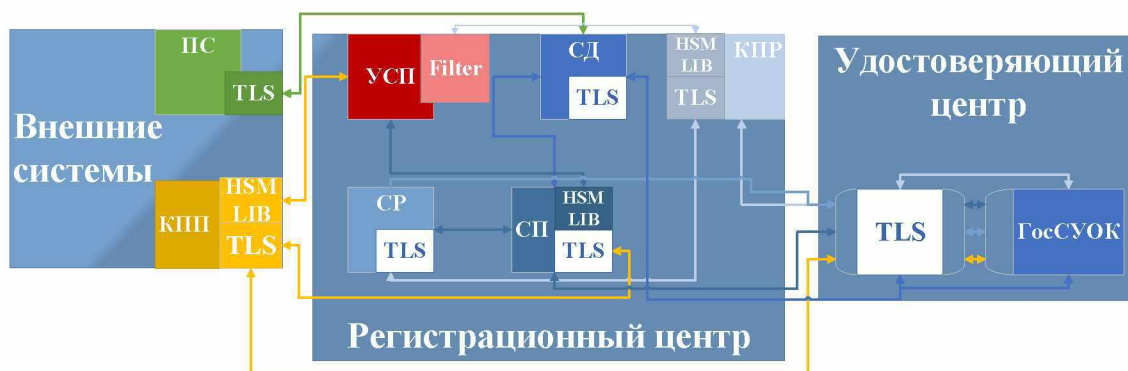


Рисунок 1 – Структурная схема взаимодействия компонентов прототипа регистрационного центра инфраструктуры открытых ключей

Использованные на рисунке 1 аббревиатуры соответствуют следующим компонентам:

- ПС – прикладная система;
- КПП – клиентская программа пользователя;
- УСП – устройство создания подписи;
- СР – сервер регистрации;
- СД – сервер документооборота;
- СП – сервер подписи;
- КПР – клиентская программа регистратора;

Использовать разработанный прототип возможно по модели представления облачных услуг в качестве программного обеспечения как услуги (Software as a Service, SaaS) или же платформы как услуги (Platform as a service, Paas).

Предлагаются следующие подходы к использованию разработанной СОП в Республике Беларусь.

1. Использование системы облачной электронной цифровой подписи в системе электронного голосования. Разработчикам системы электронного голосования предстоит решить важные вопросы, связанные с обеспечением безопасности системы. Один из таких вопросов – это процедура аутентификации избирателей. Чтобы подтвердить личность избирателя и предотвратить отказ в аутентификации, необходимо использовать надежные механизмы аутентификации. Один из наиболее надежных способов – это использование ЭЦП и сертификата открытого ключа (СОК), которые позволяют проверить подлинность подписи. Данное решение обеспечивает необходимый уровень безопасности при условии надежной защиты закрытого ключа избирателя. Обычно для хранения личных ключей используются криптографические токены, которые обеспечивают их аппаратную защиту.

Однако криптографические токены не получили широкого распространения из-за ограниченной поддержки операционных систем. Достойной альтернативой криптографическим токенам может быть использование СОП. Для безопасного функционирования системы электронного голосования с использованием СОП уже разработан протокол регистрации избирателя [2]. В рамках разработанного протокола используется облачная ЭЦП в качестве фактора аутентификации избирателей. Этот протокол представляет собой перспективное решение, так как с его помощью можно повысить защищенность и надежность систем электронного голосования. Более

широкое применение этого протокола будет способствовать повышению доверия к системам электронного голосования. Использование разработанного протокола обеспечивает защиту от следующих атак: перехват аутентификатора, угадывание и подбор аутентификатора, перехват сообщений протокола, раскрытие частных данных, повтор, «человек посередине», подделка билета аутентификации, перенаправление билета аутентификации, повторное использование билета аутентификации. Дальнейшие исследования и практические испытания разработанного протокола будут направлены на подтверждение его эффективности и применимости.

2. Использование системы облачной электронной цифровой подписи в интегрированной информационной системе «БГУИР: Университет». Использование возможностей СОИ в интегрированной информационной системе «БГУИР: Университет» [3] и других информационных системах, которые используются в системе образования, позволит решить ряд следующих задач, связанных с повышением защищенности системы и обрабатываемых с ее использованием данных:

- организация двухфакторной аутентификации пользователей (преподавателей, методистов, студентов) информационной системы;

- создание электронных документов на различных типах устройств. СОИ позволяет подписывать документы без использования физических носителей ключевой информации (НКИ). Это ускоряет процесс решения вопросов, связанных с получением подписи должностного лица. Пользователь может создавать электронный документ на более широком спектре устройств, таких как персональный компьютер, планшет, мобильный телефон;

- использование физических НКИ устанавливает ряд проблем и ограничений, таких как, отсутствие либо некорректная работа драйвера взаимодействия с НКИ на операционной системе (ОС) пользователя, отсутствие версии программного обеспечения для взаимодействия с НКИ на ОС пользователя;

- невозможность отказа от авторства. Внедрение возможности создания электронных документов с использованием облачной ЭЦП исключает возможность подмены данных, так как для выполнения операции подписания электронного документа пользователю необходимо пройти двухфакторную аутентификацию, подтвердить владение личным ключом. Например, если преподаватель аутентифицировался в своем личном кабинете из учебной аудитории, но забыл выйти из своей учетной записи после окончания занятия, то злоумышленник не сможет использовать его учетную запись для изменения оценок в электронном журнале;

- защита интеллектуальной собственности. СОП может быть использована для защиты авторских прав на объекты авторского права: научные статьи, электронные учебные и учебно-методические пособия, лекции, задания и тесты. Облачная ЭЦП обеспечивает подтверждение авторства и предотвращает возможность подделки.

3. Использование системы облачной электронной цифровой подписи в автоматизированной информационной системе «электронный рецепт». СОП в системе здравоохранения может быть применена для решения задач обеспечения безопасности и повышения эффективности обработки медицинской информации. Рассмотрим использование СОП для улучшения пользовательского опыта в автоматизированной информационной системе «Электронный рецепт» [4]. Данная система предназначена для реализации технологии обращения электронных рецептов

в системе здравоохранения Республики Беларусь. Основные функции СОП, которые можно использовать в АИС «Электронный рецепт»:

- использование учетной записи в СОП для аутентификации с помощью личного ключа пациента в информационной системе;
- создание электронного рецепта врачом, подписанного облачной ЭЦП, с помощью ПК, планшета или мобильного телефона;
- замена пластиковой карты, которая является носителем идентификатора пациента на идентификатор личного ключа пациента.

Разработанный прототип системы облачной электронной цифровой подписи предоставляет ряд преимуществ по сравнению с традиционными подходами к использованию ЭЦП. Предложенные направления использования СОП в системе электронного голосования, информационных системах образования и здравоохранения позволяют обеспечить более высокий уровень информационной безопасности, эффективность документооборота и удобство пользования. Реализация таких проектов способствует дальнейшей цифровизации государственных сервисов и повышению их доступности. Разработанная система облачной электронной цифровой подписи, при условии дальнейшей отработки и внедрения, может стать важным элементом информатизации государственного сектора Республики Беларусь.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Об электронном документе и электронной цифровой подписи. [Электронный ресурс] – Режим доступа: <https://pravo.by/document/?guid=3961&p0=N10900113>. – Дата доступа : 27.08.2024.
2. Герасимов, В. А. Использование системы облачной электронной подписи для организации электронного голосования / В. А. Герасимов, М. А. Казловский // Цифровая трансформация. – 2024. – Т. 30, № 1. – С. 52–62.
3. Марков, А. Н. Готовность учреждений высшего образования к цифровой трансформации процессов / А. Н. Марков, С. А. Мигалевич // Цифровая трансформация. – 2021. – № 2. – С. 64–68.
4. АИС «Электронный рецепт». [Электронный ресурс] – Режим доступа : <https://tncmt.by/информатизация/разработки-центра/аис-электронный-рецепт>. – Дата доступа : 27.08.2024.