http://dx.doi.org/10.35596/1729-7648-2024-30-1-52-62

Оригинальная статья
Original paper

УДК 004.056:342.722:351.771

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ ОБЛАЧНОЙ ЭЛЕКТРОННОЙ ПОДПИСИ ДЛЯ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

В. А. ГЕРАСИМОВ, М. А. КАЗЛОВСКИЙ

Научно-исследовательский институт технической защиты информации (г. Минск, Республика Беларусь)

Поступила в редакцию 17.11.2023

Аннотация. Статья посвящена вопросам проблематики аутентификации избирателей в системах электронного голосования и созданию описания модели системы, которая предназначена для организации электронного голосования с использованием системы облачной подписи как надежного решения для аутентификации. В рамках исследования формализовано понятие электронного голосования и приведен перечень его этапов. Отмечены проблемы существующих систем аутентификации избирателей в системах электронного голосования. Обоснованы преимущества электронной цифровой подписи как наиболее надежного способа аутентификации, указаны недостатки такого подхода и предложены возможные пути их устранения. Описаны компоненты системы облачной подписи и приведена схема протокола активации подписи, который используется в процессе выработки электронной цифровой подписи. Представлено описание разработанного протокола регистрации избирателя в системе электронного голосования. Продемонстрирована возможность использования системы облачной подписи в рамках протокола регистрации избирателя в системе электронного голосования. Проведен анализ стойкости предлагаемого протокола к известным атакам.

Ключевые слова: система облачной подписи, электронное голосование, протокол аутентификации, электронная цифровая подпись, протокол активации подписи, защита персональных данных.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. 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. http://dx.doi.org/10.35596/1729-7648-2024-30-1-52-62.

USING A CLOUD-BASED ELECTRONIC SIGNATURE SYSTEM FOR ORGANIZING ELECTRONIC VOTING

VYACHESLAV A. HERASIMAU, MAKSIM A. KAZLOUSKI

Scientific Research Institute of Technical Protection of Information (Minsk, Republic of Belarus)

Submitted 17.11.2023

Abstract. The article is devoted to the research on the issues of voter authentication in electronic voting systems and the creation of a description of a system model that is designed to organize electronic voting using a cloud signature system as a reliable authentication method. Within the framework of the study, the concept of electronic voting is formalized and a list of stages. The shortcomings of existing voter authentication systems are noted. The advantages of an electronic digital signature as the most reliable method of authentication are substantiated, the disadvantages of this approach are indicated and possible ways to eliminate them are proposed. The components of the cloud signature system are described and a diagram of the signature activation protocol, which is used in the process of generating an electronic digital signature, is provided. A description of the developed voter re-

gistration protocol in the electronic voting system is presented. The possibility of using a cloud signature system as part of the voter registration protocol in the electronic voting system is demonstrated. An analysis of the resistance of the proposed protocol to known attacks is carried out.

Keywords: cloud signature system, electronic voting, authentication protocol, electronic digital signature, signature activation protocol, personal data protection.

Conflict of interests. The authors declare no conflict of interests.

For citation. Herasimau V. A., Kazlouski M. A. (2024) Using a Cloud-Based Electronic Signature System for Organizing Electronic Voting. *Digital Transformation.* 30 (1), 52–62. http://dx.doi.org/10.35596/1729-7648-2024-30-1-52-62 (in Russian).

Введение

В настоящее время активно происходит цифровизация многих сфер общественной жизни. Так, существует тенденция использования электронного голосования при проведении избирательных кампаний. Электронное голосование имеет ряд важных преимуществ перед обычным, в том числе повышение уровня доверия к результатам, уменьшение стоимости организации выборов, увеличение явки избирателей. При этом важно, чтобы криптографические протоколы, лежащие в основе системы электронного голосования, а также архитектура этой системы гарантировали защиту от известных типов атак. Необходимо понимать, что такие события, как нарушение анонимности избирателей, раскрытие промежуточных итогов голосования до его завершения, отказ в обслуживании избирателя, серьезно снизят доверие общества к подобной форме проведения выборов. Поэтому наиболее разумным видится постепенное внедрение электронного голосования, в первую очередь для тех категорий граждан, которые по объективным причинам не могут проголосовать на избирательном участке.

Реализация надежной системы электронного голосования ставит перед ее разработчиками важные вопросы, связанные с выбором криптографических механизмов и архитектурных решений, необходимых для обеспечения требуемых от системы свойств безопасности. Одним из таких вопросов является организация процедуры аутентификации избирателя. Необходимо использовать надежные механизмы аутентификации, которые позволят организаторам и наблюдателям подтвердить личность избирателя, а также гарантируют, что избиратель не сможет отрицать прохождение аутентификации в системе электронного голосования.

Наиболее надежный способ – организация аутентификации на основе предъявления избирателем электронной цифровой подписи (ЭЦП) и сертификата открытого ключа (СОК), с помощью которого можно проверить действительность предъявляемой подписи. Такое решение будет обеспечивать требуемый уровень гарантий безопасности, но только в том случае, когда обеспечена надежная защита личного ключа избирателя. Как правило, для хранения личных ключей используются криптографические токены, которые обеспечивают их аппаратную защиту. Однако на текущий момент они не имеют широкого распространения, что связано со сравнительно небольшим списком поддерживаемых ими операционных систем. Достойной альтернативой подобным решениям может служить система облачной электронной подписи (СОП), в основе которой лежит аппаратное устройство создания подписи (УСП). УСП отвечает за генерацию и безопасное хранение личных ключей большого количества пользователей.

Цель исследования, результаты которого представлены в статье, состояла в проведении анализа организации процедуры аутентификации в системах электронного голосования, разработке с учетом результатов этого анализа модели системы электронного голосования с использованием облачной электронной цифровой подписи, а также в оценке стойкости заложенного в основу этой модели механизма регистрации избирателя к известным типам атак.

Аутентификация в системах электронного голосования

При проведении обычного голосования аутентификация избирателя выполняется по сильному удостоверению[1] личности (паспорту или иному аналогичному документу) путем сличения пер-

[1] Информационные технологии и безопасность. Инфраструктуры аутентификации: СТБ 34.101.87–2022 [Электронный ресурс]. Режим доступа: https://apmi.bsu.by/assets/files/std/bias-spec130.pdf. Дата доступа: 26.10.2023.

сональных данных из удостоверения с данными, которые внесены в составленные организаторами голосования списки избирателей. Такой метод аутентификации обладает достаточно высоким уровнем надежности: атаковать его возможно только в случае появления нечестного регистратора (лица, которое отвечает за проведение аутентификации и выдачу избирателю бюллетеня для голосования), который будет выдавать бюллетени отсутствующим в списках или предъявляющим недействительные удостоверения личности избирателям. Недостатком описанного метода аутентификации являются значительные трудности проведения аудита процедуры регистрации: доказать или опровергнуть факт нечестных действий регистратора практически невозможно.

В электронном голосовании выделяют три основных этапа: регистрация, голосование и подсчет голосов. Аутентификация избирателя обычно осуществляется на этапе регистрации. Предполагается, что в ходе этого этапа избиратель подтверждает свою личность, после чего регистрационная комиссия проверяет, имеет ли данный избиратель право голосовать, и, в случае положительного решения, осуществляет выдачу избирателю бюллетеня. Бюллетень в данном контексте – некоторый объект произвольного формата, который избиратель предъявляет на этапе голосования для того, чтобы его голос был учтен на этапе подсчета голосов. Как правило, вопрос организации процедуры аутентификации избирателей в рамках описания системы электронного голосования подробно не обсуждается. Другими словами, обычно предполагается, что избиратель каким-либо образом подтверждает свою личность перед получением бюллетеня, но не описывается механизм организации этого подтверждения. Тем не менее надежность схемы аутентификации напрямую влияет на безопасность системы электронного голосования в целом.

На практике аутентификация в системах электронного голосовании может быть организована различными способами. В швейцарской системе голосования CHVote предполагается рассылка секретных кодов в виде обычного письма, которое направляется по адресу регистрации избирателя. В дальнейшем избиратель использует один из полученных кодов (код голосования) для прохождения аутентификации на базе протокола идентификации Шнорра [1]. Понятно, что подобная система не может гарантировать подлинность личности избирателя, ведь конверт с реквизитами может быть перехвачен в процессе его доставки. В Российской Федерации при организации электронного голосования аутентификация проводилась через Единый портал государственных услуг Российской Федерации[2]. Успешно пройдя аутентификацию, избиратель получал от портала подписанный токен идентификации, который в дальнейшем предъявляется для участия в процедуре голосования. Однако такой подход тоже не может считаться надежным [2]. С одной стороны, противники могут аутентифицироваться под видом избирателя, если он использует одинаковый пароль для всех сайтов или допустил попадание вредоносного программного обеспечения на свое устройство для голосования (персональный компьютер, смартфон). С другой стороны, избиратель может утверждать, что не использовал портал для аутентификации и не принанимал участия в голосовании, а отданный от его лица голос сформирован посторонним лицом, которому оператор портала раскрыл аутентификационные данные избирателя.

Приведенные примеры еще раз подтверждают, что для организации надежной процедуры аутентификации необходимо использовать исключительно криптографические механизмы [3], при этом важно обеспечить надежную защиту секрета аутентификации. Одним из наиболее естественных вариантов является аутентификация с использованием ЭЦП. В рамках данного подхода предполагается, что избиратель имеет доступ к контейнеру, в котором хранится его личный ключ. Используя пароль от контейнера, избиратель может сформировать запрос на аутентификацию, в котором предоставит регистратору доказательство владения личным ключом: выработает с его помощью подпись некоторого набора данных определенного формата. Регистратор может воспользоваться СОК избирателя, чтобы провести проверку действительности его ЭЦП. Успешное прохождение проверки означает, что избиратель прошел аутентификацию и может быть допущен к участию в голосовании.

Описанный подход имеет несколько серьезных преимуществ. Во-первых, существуют строгие требования к защите личного ключа, которые снижают вероятность успешной аутентификации противника от лица избирателя даже в том случае, когда противник смог получить доступ к контейнеру с личным ключом. Удостоверяющие центры, осуществляющие выпуск СОК, как прави-

[2] Описание протокола ДЭГ к выборам, голосование на которых состоится 17, 18 и 19 сентября 2021 г. [Электронный ресурс]. Режим доступа: https://vybory.gov.ru/resources/static/materials/9/deg2021_protocol.pdf. Дата доступа: 26.10.2023.

ло, требуют использовать аппаратный криптографический токен, который имеет строгие ограничения на число неуспешных попыток аутентификации владельца. Во-вторых, ЭЦП, сформированная с помощью личного ключа избирателя, гарантирует невозможность отказа от авторства. Другими словами, так как доступ к личному ключу есть только у его владельца, то избиратель не сможет заявить, что кто-то другой вместо него прошел аутентификацию и принял участие в голосовании. В-третьих, такая процедура аутентификации обладает достаточной прозрачностью, поскольку при регистрации используется открытый ключ, который связан с выпущенным удостоверяющим центром СОК. Поэтому при валидации результатов голосования наблюдатели могут установить связь между открытым ключом в запросе на аутентификацию и конкретным лицом, на имя которого был выдан сертификат.

Есть у такого подхода и свои недостатки. Во-первых, далеко не каждый избиратель имеет желание и возможность приобрести аппаратный криптографический токен и корректно сконфигурировать его. Более того, большинство токенов не способны взаимодействовать с мобильными операционными системами (Android, IOS), а ряд избирателей обладают персональными вычислительными устройствами только на этих платформах. В качестве возможного механизма, который может устранить указанный недостаток, можно предложить использование СОП. В этом случае личный ключ избирателя будет храниться на специальном аппаратном токене – УСП. УСП может хранить личные ключи множества избирателей, а его механизмы безопасности спроектированы таким образом, что даже администраторы УСП никогда не смогут получить доступ к хранящимся на нем личным ключам. Использование СОП позволит избирателю проходить аутентификацию в системе электронного голосования без аппаратного криптографического токена. В следующем разделе статьи рассмотрены архитектура СОП, механизмы обеспечения безопасности процесса выработки подписи, а также предложен вариант реализации этих механизмов. Во-вторых, при использовании личного ключа для аутентификации возникает вопрос защиты персональных данных его владельца. Данный недостаток связан с принципом функционирования инфраструктуры открытых ключей: пользователь генерирует личный ключ, строит по нему открытый ключ, формирует заявку на выпуск СОК, указывает в ней свои персональные данные и подписывает ее с помощью личного ключа; рассмотрев заявку, удостоверяющий центр выпускает СОК, в котором указываются как открытый ключ пользователя, так и его персональные данные; в дальнейшем СОК используется при проверке ЭЦП, которые пользователь выработал на своем личном ключе. К сожалению, явное использование сертификата избирателя в рамках аутентификации при регистрации на участие в электронном голосовании недопустимо, так как для соответствия требованиям по проверяемости системы все запросы к регистратору и его ответы должны быть общедоступными. Но в этом случае СОК избирателя, а, следовательно, и его персональные данные (фамилия, имя, отчество, личный номер паспорта и др.) тоже будут общедоступными, что противоречит действующему законодательству. Чтобы устранить указанный недостаток, в разделе статьи «Протокол регистрации избирателя на основе облачной электронной подписи» представлен протокол регистрации избирателя, который не будет использовать СОК избирателя в явном виде, а также рассмотрены вопросы безопасности указанного протокола и его интеграции в СОП.

Архитектура системы облачной электронной цифровой подписи

В основе облачных систем лежит понятие облачных вычислений. По определению, предложенному Национальным институтом стандартов и технологий США (NIST), облачные вычисления – модель по обеспечению повсеместного, удобного сетевого доступа к общему объединению конфигурируемых вычислительных ресурсов, которые могут быть быстро выделены и предоставлены [4]. Облачные вычисления относятся как к приложениям, которые предоставляются как услуги через интернет, так и к оборудованию, системному программному обеспечению в центрах обработки данных. При этом под облачной услугой (сервисом) понимается услуга, предоставляющая доступ к облачным ресурсам ее потребителям. СОП предназначена для дистанционного создания электронного документа с использованием для подписи личного ключа подписанта под его контролем.

Личный ключ подписанта хранится в удаленном программно-аппаратном УСП, и подписант с помощью определенных механизмов получает доступ к своему личному ключу. Личный ключ

подписанта хранится в структуре данных, которая называется «слот». Чтобы выработать значение подписи электронного документа, подписанту необходимо выполнить следующие действия:

1) открыть сессию со слотом;

2) установить защищенное соединения между приложением подписанта и устройством создания подписи;

3) пройти процесс аутентификации в слоте пользователя УСП.

После перечисленных действий подписант получает доступ к своему слоту и может выполнять действия, которые определены ролевой моделью доступа к СОП. СОП состоит из компонентов, позволяющих обеспечить безопасную выработку электронной подписи[3]:

– сервера подписи (СП), предназначенного для генерации и хранения личных ключей подписантов, выработки ЭЦП под контролем подписантов от их лица;

– УСП – составного компонента СП, который является аппаратным средством криптографической защиты информации;

– сервера документооборота (СД), предназначенного для создания и проверки электронного документа;

– клиентской программы (КП), предназначенной для взаимодействия подписанта с компонентами системы облачной подписи;

– сервера регистрации (СР), отвечающего за регистрацию и деактивацию аккаунтов подписантов в СОП;

– прикладной системы (ПС) – внешнего компонента по отношению к системе облачной подписи, отвечающего за загрузку, разработку, хранение и отображение подписываемых документов.

Основными функциями СОП являются:

– инициализация УСП для дальнейшей эксплуатации в СОП;

– регистрация пользователя и закрепление слота для выработки облачной электронной подписи за пользователем;

– выпуск СОК;

– установка пароля для отзыва СОК;

– отзыв СОК по паролю;

– отзыв СОК по ключу;

– смена PIN от слота пользователя;

– удаление слота пользователя;

– разблокировка слота пользователя;

– выработка значения облачной электронной подписи.

Для того чтобы подписант был уверен, что документ, который он подписывает с помощью СОП, не был модифицирован, обычно предлагается применять определенные механизмы, гарантирующие возможность использования личного ключа подписанта только под его контролем. К таким механизмам относится протокол активации подписи[4] (ПАП), представляющий собой последовательность определенных шагов, при выполнении которых подписант получает документ с ЭЦП, выработанной с помощью облачных технологий. При этом выработка ЭЦП происходит на аппаратной части СОП – УСП. Использование ПАП для выработки значения ЭЦП является ключевым для того, чтобы гарантировать подписанту, что кроме него никто не сможет выработать подпись на его личном ключе, находящемся в УСП.

Использование ПАП в СОП позволяет получить защиту от ряда атак: перехват аутентификатора, угадывание аутентификатора, подбор аутентификатора, перехват сообщений протокола, раскрытие приватных данных, повтор сеанса, противник посередине, вредоносные программы, подделка билета аутентификации, перенаправление билета аутентификации, повторное использование билета аутентификации, подделка вторичного аутентификатора, перехват вторичного аутентификатора, подмена ответов, кража сеанса.

Авторами статьи разработан собственный вариант ПАП, не только удовлетворяющий всем необходимым механизмам безопасности, но и пригодный для интеграции с используемой сегодня в нашей стране ПС. Схема протокола с компонентами СОП представлена на рис. 1.

[3] Отчет о составной части ОКР «Совершенствование инфраструктуры открытых ключей на основе современных веб-технологий».

[4] Облачная электронная цифровая подпись: протокол активации подписи [Электронный ресурс]. Режим доступа https://elib.bsu.by/handle/123456789/303664. Дата доступа: 10.11.2023.

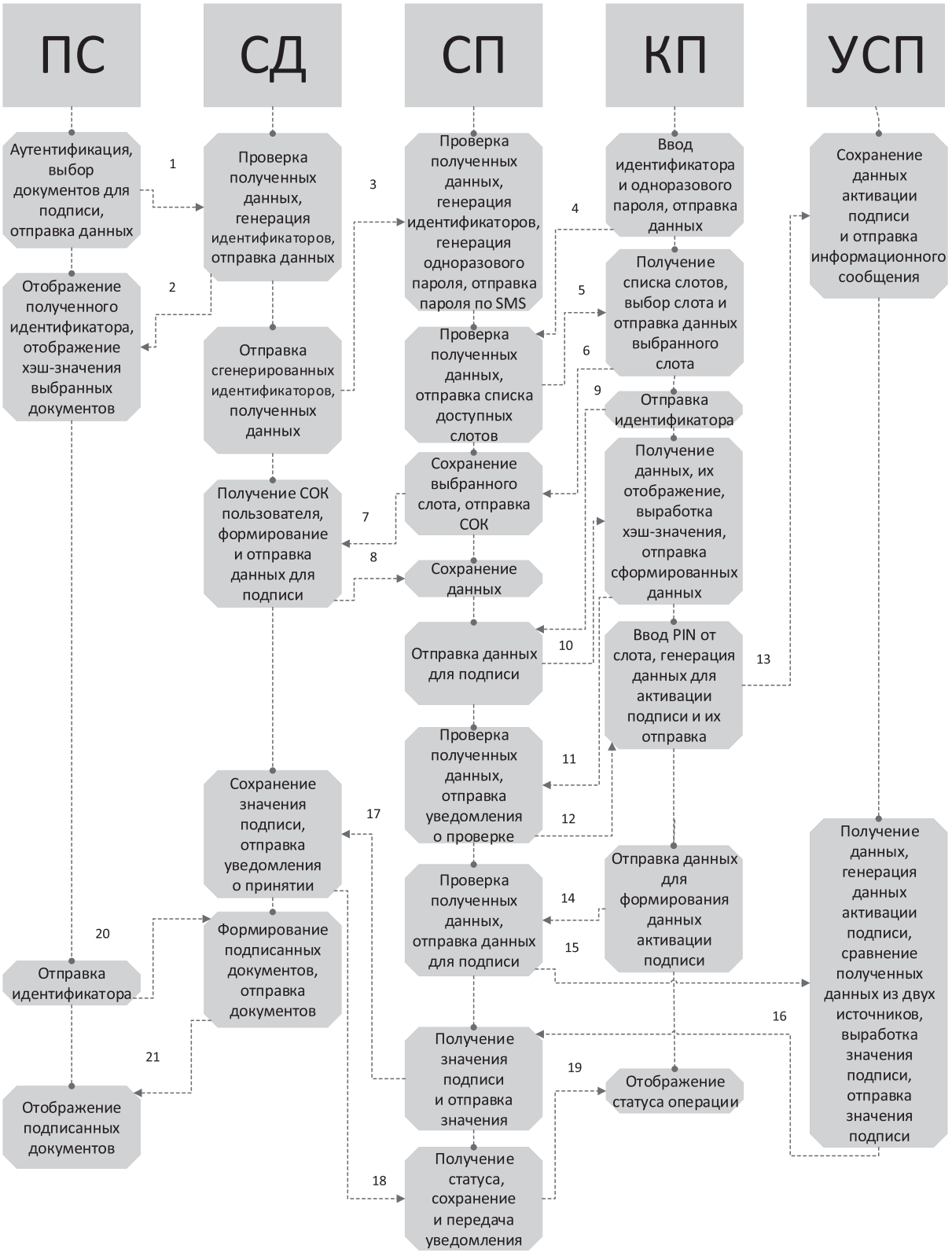

Рис. 1. Протокол активации подписи
Fig. 1. Signature activation protocol

Протокол регистрации избирателя на основе облачной электронной подписи

Как уже упоминалось в разделе «Аутентификация в системах электронного голосования», протокол регистрации избирателя перед системой электронного голосования должен удовлетворять ряду требований:

1) обеспечивать минимальную вероятность успешного прохождения аутентификации третьим лицом;

2) не раскрывать персональных данных избирателя;

3) обеспечивать невозможность отрицания избирателем факта прохождения аутентификации;

4) позволять провести аудит процедуры регистрации любого избирателя;

5) иметь адекватную вычислительную сложность, позволяющую использовать протокол на практике.

В предлагаемом протоколе регистрации избирателя участвуют две стороны: КПГ – клиентская программа для голосования (клиентское приложение, которое используется пользователем для регистрации и участия в голосовании); ЦИК – центральная избирательная комиссия (сервер, выполняющий аутентификацию пользователя, желающего зарегистрироваться в качестве избирателя).

Сделаем ряд предположений, необходимых для успешной работы протокола.

1. Пользователь имеет криптографический токен, на котором хранится его долговременный личный ключ *static_priv_client*. По этому ключу построен долговременный открытый ключ пользователя *static_pub_client*, для которого удостоверяющим центром выпущен СОК *cert_client*. Сертификат *cert_client* хранится на том же персональном устройстве пользователя, на которое установлена КПГ.

2. Криптографический токен, на котором хранится долговременный личный ключ пользователя *static_priv_client*. Токен умеет вырабатывать с его помощью ЭЦП по алгоритму выработки подписи *SIGN*, который также использует КПГ.

3. СОК *cert_client* содержит в своем составе компонент *subject*, в котором расположены персональные данные, позволяющие однозначно идентифицировать пользователя (как минимум там содержатся фамилия, имя, отчество и личный номер паспорта).

4. ЦИК имеет криптографический токен, на котором хранится его долговременный личный ключ *static_priv_cec*. По этому ключу построен долговременный открытый ключ ЦИК *static_pub_cec*, для которого удостоверяющим центром выпущен СОК *cert_cec*.

5. В КПГ «вшит» СОК ЦИК *cert_cec* в качестве доверенного сертификата.

6. Канал связи между КПГ и ЦИК обеспечивает конфиденциальность, целостность и подлинность передаваемых сообщений (например, используется протокол TLS с аутентификацией ЦИК перед КПГ с помощью *cert_cec*).

7. Каждое голосование имеет уникальный идентификатор голосования *id_vote.* Список доступных на текущий момент времени идентификаторов голосования поступает в КПГ от ЦИК. Пользователь выбирает идентификатор голосования, в котором хочет принять участие перед началом процедуры регистрации.

Предлагаемый протокол регистрации состоит из двух этапов: на первом КПГ отправляет в ЦИК набор данных, которые необходимы для аутентификации и регистрации избирателя, на втором ЦИК отправляет в КПГ ответ, содержащий либо подтверждение регистрации, либо сообщение об ошибке.

Первый этап протокола выполняется на стороне КПГ, состоит из четырех шагов, по завершении которых КПГ отправит в ЦИК сообщение, содержащее необходимые для проведения аутентификации пользователя и его регистрации в качестве избирателя данные.

1. На шаге 1.1 КПГ с помощью алгоритма *GenKeyPair* генерирует пару эфемерных ключей: *eph_priv* – эфемерный личный ключ, *eph_pub* – эфемерный открытый ключ. В качестве алгоритма генерации пары ключей *GenKeyPair* может выступать алгоритм из СТБ 34.101.45–2013 (п. 6.2.2).

2. На шаге 1.2 КПГ с помощью алгоритма *H* вычисляет хэш-значение *h_sub* от компонента *subject* из принадлежащего пользователю СОК *cert_client.* В качестве алгоритма хэширования *H* может выступать алгоритм из СТБ 34.101.31–2020 (п. 7.8) или из СТБ 34.101.77–2020 (разд. 7) в зависимости от требуемого уровня стойкости.

3. На шаге 1.3 КПГ с помощью алгоритма *SIGN* вырабатывает подпись *s_data* от полученного на шаге 1.2 хэш-значения *h_sub* и уникального идентификатора голосования *id_vote* с использованием сгенерированного на шаге 1.1 эфемерного личного ключа *eph_priv*. В качестве алгоритма выработки подписи *SIGN* может выступать алгоритм из СТБ 34.101.45–2013 (п. 7.1.3).

4. На шаге 1.4 КПГ обращается к криптографическому токену, который с помощью алгоритма *SIGN* вырабатывает подпись *s_key* от полученного на шаге 1.3 значения подписи *s_data* и полученного на шаге 1.1 эфемерного открытого ключа *eph_pub* с использованием долговременного личного ключа пользователя *static_priv_client*. В качестве алгоритма выработки подписи *SIGN* может выступать алгоритм из СТБ 34.101.45–2013 (п. 7.1.3).

5. После завершения шагов 1.1–1.4 КПГ отправляет в ЦИК пять объектов: полученный на шаге 1.1 эфемерный открытый ключ *eph_pub*, полученное на шаге 1.2 хэш-значение *h_sub*, выработанные на шагах 1.3 и 1.4 значения подписей *s_data* и *s_key* соответственно, и уникальный идентификатор голосования *id_vote*.

Второй этап протокола выполняется на стороне ЦИК, состоит из четырех шагов, по завершении которых ЦИК отправит в КПГ или облегченный сертификат *cvc*, содержащий эфемерный открытый ключ пользователя *eph_pub*, или сообщение об ошибке аутентификации.

1. На шаге 2.1 ЦИК проверяет действительность идентификатора голосования *id_vote*: если данный идентификатор отсутствует в списке идентификаторов активных голосований, то протокол завершается с ошибкой ***bad_vid***. Далее ЦИК проверяет действительность хэш-значения *h_sub*: если данное хэш-значение отсутствует в списке хэш-значений компонентов *subject* из СОК избирателей, допущенных к участию в голосовании *id_vote*, то протокол завершается с ошибкой ***bad_hsub***. Наконец, ЦИК извлекает долговременный открытый ключ *static_pub_client* из СОК *cert_client*, хэш-значение компонента *subject* которого равно *h_sub*.

2. На шаге 2.2 ЦИК с помощью алгоритма *VERIFY* проверяет корректность значения ЭЦП *s_data*, при этом в качестве подписанных данных выступают *s_data* и *eph_pub*, а в качестве открытого ключа – долговременный открытый ключ пользователя *static_pub_client*. Если подпись признана некорректной, то протокол завершается с ошибкой ***bad_lsign***. В качестве алгоритма проверки подписи *VERIFY* может выступать алгоритм из СТБ 34.101.45–2013 (п. 7.1.4).

3. На шаге 2.3 ЦИК с помощью алгоритма *VERIFY* проверяет корректность значения ЭЦП *s_key*, при этом в качестве подписанных данных выступают *h_sub* и *id_*vote, а в качестве открытого ключа – эфемерный открытый ключ пользователя *eph_pub*. Если подпись признана некорректной, то протокол завершается с ошибкой ***bad_esign***. В качестве алгоритма проверки подписи *VERIFY* может выступать алгоритм из СТБ 34.101.45–2013 (п. 7.1.4).

4. На шаге 2.4 ЦИК обращается к криптографическому токену, который с помощью алгоритма *SIGN* вырабатывает подпись *cv_sign* от набора данных, который, в том числе, включает идентификатор ЦИК *cec_id*, эфемерный открытый ключ пользователя *eph_pub*, хэш-значение *h_sub*, идентификатор голосования *id_vote*, дату выпуска сертификата *start* и дату окончания действия сертификата *end*, с использованием долговременного личного ключа ЦИК *static_priv_cec*. В качестве алгоритма выработки подписи *SIGN* может выступать алгоритм из СТБ 34.101.45–2013 (п. 7.1.3).

5. После завершения шагов 2.1–2.4 ЦИК отправляет в КПГ облегченный сертификат *cvc*, который представляет собой пару, состоящую из набора подписанных на шаге 2.4 данных и значения их подписи *cv_sign*, полученного на этом же шаге.

Протокол регистрации избирателя может быть записан в следующей краткой форме:

1. КПГ→ ЦИК: *eph_priv, eph_pub || h_sub || s_data || s_key || id_vote*
1.1. *eph_priv, eph_pub ← GenKeyPair()*
1.2. *h_sub←H(cert_client.subject)*
1.3. $s\_data \leftarrow SIGN_{eph\_priv}(h\_sub \,||\, id\_vote)$
1.4. $s\_key \leftarrow SIGN_{static\_priv\_client}(s\_data \,||\, eph\_pub)$
2. ЦИК→КПГ: *cvc = ((cec_id || eph_pub || h_sub || id_vote || start || end), cv_sign)*
2.1. Проверить корректность *id_vote* и *h_sub*
2.2. $VERIFY_{static\_pub\_client}(s\_key, s\_data \,||\, eph\_pub)$
2.3. $VERIFY_{eph\_pub}(s\_data, h\_sub \,||\, id\_vote)$
2.4 $cv\_sign \leftarrow SIGN_{static\_priv\_cec}(cec\_id \,||\, eph\_pub \,||\, h\_sub \,||\, id\_vote \,||\, start \,||\, end)$

Таким образом, успешное завершение шагов 2.2 и 2.3 означает, что пользователь, обладающий уникальным идентификатором *h_sub*, запросивший у ЦИК регистрацию своего эфемерного открытого ключа *eph_pub* в качестве ключа для участия в голосовании *id_vote*, подтвердил как обладание ассоциированным с идентификатором *h_sub* долговременным личным ключом *static_priv_client* (через подпись *s_key*), так и обладание эфемерным личным ключом *eph_priv*

(через подпись *s_data*). Это значит, что владелец СОК *cert_client* действительно изъявил желание принять участие в голосовании *id_vote* и имеет подходящую для этого пару эфемерных ключей (*eph_priv*, *eph_pub*). Соответственно, ЦИК может выпустить облегченный сертификат *cvc*, который необходим для обеспечения доверия со стороны всех субъектов системы электронного голосования к вырабатываемым избирателем ЭЦП.

После успешного завершения протокола регистрации избирателя КПГ владеет как эфемерным личным ключом *eph_priv*, который позволяет вырабатывать ЭЦП для любых сообщений, так и облегченным сертификатом *cvc*, с помощью которого любой участник системы электронного голосования сможет выполнить проверку корректности выработанной подписи и убедиться в успешном прохождении данным избирателем процедуры регистрации. Таким образом, полученный набор из личного ключа *eph_priv* и сертификата *cvc* является необходимым и достаточным условием для того, чтобы избиратель смог принять участие в электронном голосовании. При этом не имеет значения, какая именно система электронного голосования используется, потому что его применение для подтверждения права голоса избирателя возможно для любого протокола голосования, быть может с небольшой тривиальной модификацией.

Отметим, что на шаге 1.4 протокола регистрации КПГ обращается к криптографическому токену для выработки ЭЦП. Это может быть как обычный аппаратный токен (например, идентификационная карта или криптографический токен в формате USB-носителя), подключенный к устройству с запущенной КПГ, так и аппаратное УСП, которое функционирует в рамках СОП. Во втором случае процедура выработки ЭЦП несколько усложняется. КПГ сформирует документ, содержащий, согласно требованиям протокола, необходимые для подписи данные, после чего пользователь должен будет выполнить необходимые действия, которые приведены в описании ПАП: аутентифицироваться перед ПС, загрузить сформированный документ и пройти все шаги, необходимые для подписания данного документа. После получения ПС подписанного документа (последний шаг ПАП) пользователь сохраняет его и указывает путь к файлу в КПГ. КПГ извлекает из полученного файла нужную для регистрации подпись *s_key*. Таким образом, разработанный протокол регистрации избирателя может использоваться как для персонального аппаратного токена, так и для аппаратного УСП.

Рассмотрим защиту приведенного протокола регистрации избирателя от основных криптографических атак на протоколы аутентификации.

1. *Перехват аутентификатора*. Для аутентификации пользователя используется подпись *s_key*, которая вырабатывается с помощью долговременного личного ключа *static_priv_client*. В качестве аутентификатора выступает личный ключ, хранящийся на аппаратном криптографическом токене. Для доступа к ключу владелец должен пройти аутентификацию перед токеном, которая осуществляется путем ввода пароля. Если несколько раз будет введен неверный пароль, токен перейдет в состояние блокировки, в котором невозможно выполнение любых операций с личным ключом. Таким образом, защита организована с помощью аппаратных методов, реализованных в используемом токене.

2. *Угадывание и подбор аутентификатора.* Личный ключ *static_priv_client* выбирается равновероятно из множества чисел от 1 до $\approx 2^{256}$ (при минимально допустимом уровне стойкости $l = 128$). Вероятность угадать или подобрать ключ в подобной ситуации пренебрежимо мала.

3. *Перехват сообщений протокола.* Канал связи между КПГ и ЦИК защищен с помощью протокола TLS. Даже при перехвате противником всех сообщений протокола он не сможет определить ни общий мастер-ключ, который формируется по результатам выполнения протокола, ни секреты, использующиеся во время выполнения протокола.

4. *Раскрытие приватных данных.* Любые данные между КПГ и ЦИК передаются по защищенному TLS-соединению, при этом для организации данного соединения используется односторонняя аутентификация (ЦИК аутентифицируется перед КПГ), поэтому персональные данные пользователя не требуются. Использование защищенных соединений гарантирует для передаваемых по ним данным конфиденциальность, контроль целостности и подлинности криптографическими методами.

5. *Повтор.* Для раскрытия содержимого TLS-соединений (т. е. раскрытия сообщений протокола регистрации избирателя) противнику требуется провести успешную атаку на протокол TLS. На текущий момент для корректно сконфигурированного протокола (разрешены только надеж-

ные криптонаборы, включены дополнительные расширения приветственных сообщений) TLS версии 1.2 не существует известных атак.

6. *Противник посередине.* Использование протокола TLS для защиты соединения между сторонами протокола регистрации избирателя обеспечивает защиту от атаки типа «противник посередине». Противник может попытаться выдать себя за КПГ перед ЦИК, однако, так как протокол состоит из запроса к ЦИК и ответа ЦИК на данный запрос, никакую дополнительную информацию извлечь таким образом не получится.

7. *Подделка билета аутентификации.* В качестве билета аутентификации, полученного в результате выполнения протокола регистрации избирателя, выступает выпущенный ЦИК облегченный сертификат. В дальнейшем данный сертификат используется для того, чтобы участники системы электронного голосования смогли проверить ЭЦП, которые были выполнены с помощью личного ключа *eph_priv*. Для подделки облегченного сертификата необходимо знание личного ключа ЦИК, защита которого обеспечивается криптографическим токеном, на котором он хранится.

8. *Перенаправление билета аутентификации.* Облегченный сертификат, являющийся билетом аутентификации, содержит уникальный идентификатор голосования. Поэтому данный билет будет действительным только при использовании для участия в электронном голосовании, которое имеет указанный в билете идентификатор.

9. *Повторное использование билета аутентификации.* Для использования билета аутентификации (облегченного сертификата) противнику необходимо знание личного ключа *eph_priv*, так как для доказательства успешной аутентификации пользователь должен предъявить два объекта: ЭЦП, выработанную с помощью *eph_priv*, и облегченный сертификат.

Заключение

1. По результатам исследований, посвященных проблематике аутентификации избирателей в системах электронного голосования, были выявлены недостатки популярных механизмов аутентификации и обоснована необходимость использования механизма аутентификации на основе электронной цифровой подписи. Отмечены недостатки данного механизма и предложены пути их решения.

2. Предложена архитектура системы облачной электронной цифровой подписи и разработан протокол активации такой подписи, который играет ключевую роль в обеспечении безопасности личного ключа подписанта.

3. Разработан протокол регистрации избирателя, предназначенный для его аутентификации в системе электронного голосования с получением подтверждения прохождения аутентификации, которое необходимо для участия в голосовании. Предложенный протокол поддерживает возможность использования системы облачной электронной цифровой подписи для формирования аутентификационных данных.

4. Предложенный протокол, использующий облачную электронную цифровую подпись в качестве метода аутентификации избирателей, представляет собой перспективное решение, способное улучшить безопасность и надежность систем электронного голосования. Более широкое применение данного протокола будет способствовать повышению доверия к системам электронного голосования. Однако необходимы дальнейшие исследования и практические испытания для подтверждения эффективности и применимости предложенного механизма.

Список литературы / References

1. CHVote Protocol Specification. *Cryptology ePrint Archive*. Available: https://eprint.iacr.org/2017/325 (Accessed 25 October 2023).
2. Vakarjuk J., Snetkov N., Willemson J. (2022) Russian Federal Remote E-voting Scheme of 2021 – Protocol Description and Analysis. *EICC '22: Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference*. https://doi.org/10.1145/3528580.3528586.
3. Abu-Shanab E., Khasawneh R., Alsmadi I. (2013) Authentication Mechanisms for E-Voting. *Human-Centered System Design for Electronic Governance*. https://doi.org/10.4018/978-1-4666-3640-8.ch006.
4. Theuermann K., Tauber A., Lenz T. (2019) Mobile-Only Solution for Server-Based Qualified Electronic Signatures. *ICC 2019 – 2019 IEEE International Conference on Communications*. http://dx.doi.org/ 10.1109/ICC.2019.8762076.

Вклад авторов

Герасимов В. А. определил цели и задачи исследований, разработал протокол активации подписи в системе облачной подписи, сформулировал заключение и выполнил научное редактирование статьи.

Казловский М. А. сформулировал введение, описал проблематику аутентификации в системах электронного голосования, разработал протокол регистрации избирателя в системе электронного голосования с помощью системы облачной подписи и обосновал его надежность.

Authors' contribution

Herasimau V. A. determined the goals and objectives of the research, developed a signature activation protocol in the cloud signature system, formulated the conclusion and carried out scientific editing of the article.

Kazlouski M. A. formulated the introduction, described the problems of authentication in electronic voting systems, developed a voter registration protocol in the electronic voting system using a cloud signature system and substantiated its reliability.

Сведения об авторах

Герасимов В. А., сотр. Научно-исследовательского института технической защиты информации, магистрант каф. информационных технологий автоматизированных систем, Белорусский государственный университет информатики и радиоэлектроники

Казловский М. А., сотр. Научно-исследовательского института технической защиты информации, асп. каф. математического моделирования и анализа данных, Белорусский государственный университет

Information about the authors

Herasimau V. A., Employee of the Scientific Research Institute of Technical Protection of Information, Master's Student at the Department of Information Technologies of Automated Systems, Belarusian State University of Informatics and Radioelectronics

Kazlouski M. A., Employee of the Scientific Research Institute of Technical Protection of Information, Postgraduate at the Department of Mathematical Modeling and Data Analysis, Belarusian State University

Адрес для корреспонденции

220088, Республика Беларусь,
г. Минск, ул. Первомайская, 26, корп. 2
Научно-исследовательский институт
технической защиты информации
Тел.: +375 17 294-01-71
E-mail: vger@niitzi.by
Герасимов Вячеслав Александрович

Address for correspondence

220088, Republic of Belarus,
Minsk, Pervomayskaya St., 26, build. 2
Scientific Research Institute
of Technical Protection of Information
Tel.: +375 17 294-01-71
E-mail: vger@niitzi.by
Herasimau Vyacheslav Alexandrovich