(19) Евразийское патентное ведомство

(21) 202392403 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2023.12.05

(22) Дата подачи заявки
2022.02.27

(51) Int. Cl. ***H04L 9/40*** (2022.01)

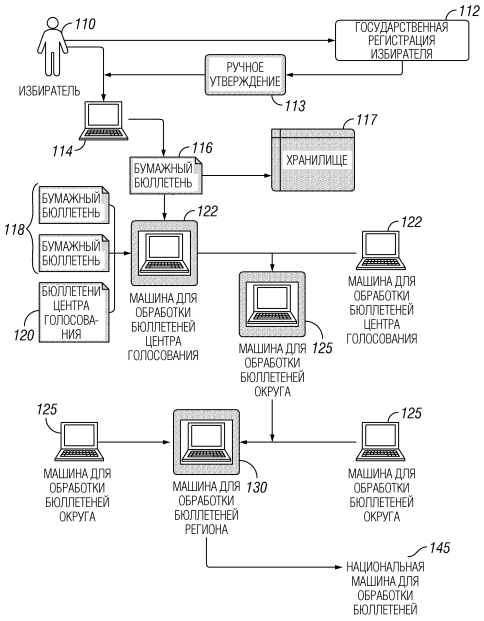
(54) СИСТЕМА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ГОЛОСОВАНИЯ

(31) **63/154,070**
(32) **2021.02.26**
(33) **US**
(86) **PCT/US2022/070854**
(87) **WO 2022/183220 2022.09.01**

(71)(72) Заявитель и изобретатель:
ДАЙ ГОРДОН РОБЕРТ (US)

(74) Представитель:
Медведев В.Н. (RU)

(57) Настоящее изобретение предоставляет средство и способ проведения безопасного, наблюдаемого и проверяемого процесса голосования и систему, предоставляющую пользу, надежность и целостность упомянутой системе, в результате чего избиратели могут взаимодействовать с системой голосования и избирательным органом, и аудиторы могут взаимодействовать с системой голосования и органом, чтобы одновременно предоставлять прозрачность и безопасность, в целом. В частности, настоящая система предоставляет возможность легкости идентификации избирателя, идентификации голоса, безопасности голоса и избирателя, также как аутентификацию подачи голоса и верификацию в эффективной и модифицируемой конструкции голосования, который остается изменяемым избирателем в течение определенного периода перед подачей голоса) и верифицируемой избирателем и верифицирующим объектом-сущностью в течение определяемых периодов после подачи голоса или дня голосования. Кроме того, настоящая система предоставляет уникальное средство обеспечения целостности системы для системы посредством поддержки раздельных механизмов и серверов для "дублируемых" операций в целях поддержки безопасности, проверки и наблюдения.



202392403 A1

202392403 A1

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

2420-579341EA/042

СИСТЕМА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ГОЛОСОВАНИЯ

Область техники, к которой относится изобретение

Центральными целями ядра программного обеспечения "Accountable Democracy" являются предоставление гарантий избирателям (и диспетчерам по обработке голосов), что 1) индивидуальные голоса избирателей учитываются и точно подсчитываются, 2) голоса всех участвующих избирателей учитываются и точно подсчитываются и 3) неавторизованные голоса не включаются и 4) неавторизованные голоса исключаются в подсчетах избирательного органа. Вторичные цели включают в себя предоставление удобства голосования заблаговременно до дня выборов, возможности или возможностей для избирателя изменить свое мнение в течение конкретного интервала времени после своего голосования, уведомление избирателя о том, что голос или голоса были приняты, предоставление необязательной квитанции, показывающей, за кого человек проголосовал, способность видеть свой голос в режиме онлайн с момента ввода избирателем своего голоса до выборочного момента времени после выборов, легкость пересчетов и существенно повышенная безопасность и надежность. Вышеуказанные цели достигаются посредством предоставления программного обеспечения для подсчета голосов, которое одновременно является в равной степени прозрачным и безопасным. В то время как прозрачность может казаться конфликтующей с безопасностью, этот уникальный проект системы достигает обеих целей одновременно.

Уровень техники

Существует множество новых приложений системы программного обеспечения, доступных в настоящее время и/или разрабатываемых и тестируемых, которые относятся к выборам, включающим в себя регистрацию избирателя, процесс голосования и различные функции наблюдения. Несколько важных аспектов голосования рассматриваются посредством такого программного обеспечения, которые будут благоприятствовать участию в процессе голосования голосующей общественности. Настоящий прикладной программный интерфейс (API) используется такими приложениями, чтобы выполнять хранение бюллетеней и подсчет, в то же время предоставляя цельный, эргономичный пользовательский интерфейс для облегчения многих аспектов процесса голосования. В настоящем изобретении, ролью системы и способа использования является предоставление внутренней поддержки для таких приложений, которая является прозрачной, неизменяемой, невзламываемой (т.е., нередактируемой) и проверяемой, в то же время предоставляя непрерывный доступ избирателя к предоставленным на рассмотрение бюллетеням.

Invote, предоставленный компанией Scytl, описывает текущий уровень техники реализуемых систем голосования и проблемы безопасности, устраняемые посредством каждой из них. Система Scytl является известным дополнением в отрасль программного обеспечения для голосования с точки зрения конфиденциальности и безопасности,

однако, она является значительно менее прозрачной и, следовательно, предоставляет меньшую пользу по сравнению с представленным проектом Accountable Democracy.

В системе Scytl, общественность не может непосредственно верифицировать целостность системы Scytl (т.е., что система является безопасной и не взломана), после того как бюллетени принимаются сервером подсчета голосов. Хотя эта система предоставляет способ для избирателей (a) верифицировать свою личность (например, посредством цифровых сертификатов, электронного ID, двойного фактора, биометрии, третьесторонних систем аутентификации и т.п.) и (b) предоставляет возможность подписи бюллетеня избирателя. В то время как система Scytl может подтверждать, что бюллетени избирателей были приняты, после того как бюллетень избирателя был передан серверу подсчета, цифровые (подтверждающие) подписи удаляются, и связь бюллетеня с избирателем, и системой регистрации избирателя, необратимо теряется, когда все данные шифруются и помещаются в цифровой ящик для бюллетеней. Этот ящик для бюллетеней является "смешанным" и "перетасованным", таким образом, отдельные избиратели не могут быть привязаны к бюллетеню. Очевидно, дополнительные (поддельные) бюллетени могут вводиться в систему необнаруженными, хотя идентификация и шифрование/дешифрование проводится посредством цифровых ключей голосования, каждый для законно поданных голосов, незаконное содержимое цифрового ящика для бюллетеней может быть добавлено, чтобы легитимировать ящики для бюллетеней, таким образом, разбавляя или превосходя законные голоса, тем самым, создавая "электронное" наполнение ящика для бюллетеней фальшивыми бюллетенями, когда отсутствует возможность учета между подачей бюллетеней и избирателями. Также, если злоумышленники получают ключи дешифрования, бюллетени могут быть модифицированы, и результаты выборов могут быть изменены - все получается в результате отсутствия непрерывной способности отслеживать путь от отдельных избирателей до их бюллетеней, делая систему "непроверяемой". Что еще важно отметить, тогда как настоящее изобретение эффективно задействует отдельных избирателей в процессе наблюдения за системой, система Scytl содержит роковую ошибку в том, что она не имеет возможности или способности обеспечивать электорат полномочием непрерывно отслеживать и наблюдать за своими собственными голосами.

Проект Accountable Democracy является на порядок более прозрачным в том, что 1) избиратель никогда не теряет непосредственный доступ к своему бюллетеню и 2) настоящая система использует другой криптографический способ, чтобы защищать бюллетени, предоставляя возможность им оставаться незашифрованными и считываемыми посредством объектов-сущностей для подсчета голосов. Файл бюллетеней может быть сделан публичным после дня выборов, и фактические голоса легко считываются и подсчитываются любым компетентным компьютерным специалистом. Этот публичный учет происходит в дополнение к индивидуальной верификации бюллетеней гражданами и служит в качестве дополнительного уровня подотчетности, прозрачности и верификации целостности в системе. Вкратце, настоящая система и

изобретение предоставляют возможность для безопасности (1) от избирателя в восходящем направлении (посредством привязки бюллетеня 1:1 и неразрывной связи избиратель/бюллетень) и (2) сверху вниз (система подведения итогов) посредством доступности открытого исходного кода с прозрачным непрерывным наблюдением за выборами.

Кроме того, в описываемой в настоящий момент системе, избиратели имеют возможность осуществлять доступ к своим бюллетеням для исправления, в то же время оставаясь анонимными для системы в целом. Программное обеспечение может быть направлено на экспертную оценку, и программы 'в использовании' могут публично контролироваться и наблюдаться на протяжении всего процесса голосования посредством использования специальной технологии шифрования в дополнение к публичному и конфиденциальному доступу к ключам шифрования.

Очевидно, существует множество факторов, затрагиваемым при использовании систем онлайн-голосования. Одним ресурсом, который всесторонне описывает такие факторы, является The Electoral Knowledge Network. Этот ресурс обсуждает несколько типов вопросов безопасности и многие, если не все, вопросы, которые относятся к предоставлению гражданам возможности голосования и наблюдения в режиме онлайн. Однако, многие из проблемных ситуаций, рассматриваемых этим обсуждением, просто не существуют в системе Accountable Democracy. Например, не существуют подсчеты голосов, сохраненные где угодно в системе, таким образом, не существуют подсчеты для манипуляций или подделки. И, поскольку связь бюллетеня с фактическими избирателями и регистрациями избирателей поддерживается, добавление поддельных бюллетеней или какое-либо удаление бюллетеней легко наблюдается, проверяется и является обнаруживаемым. Что еще важно отметить, в настоящей системе, процесс голосования является развернутым и имеет место в поддающемся учету более размеренном темпе заблаговременно перед днем выборов, который распределяет данные в более пригодных к потреблению количествах для наблюдения и безопасности. Это благоприятствует участию избирателя и предоставляет возможность обнаружения и корректировки каких-либо аномалий своевременным, неспешным образом, порождая целостность в системе, доверие к системе голосования и, более важно, повышенное удовлетворение избирателя/потребителя - все превращается в большее участие избирателей и точное представление всего населения.

Последнее, но не менее важное, Microsoft® создал комплект компьютерных программ с открытым исходным кодом, которые реализуют множество особенностей в системе Scytl. Это предоставляет всеобъемлющий подход к использованию электронных бюллетеней вместе с бумажными бюллетенями, что составляет монументальный шаг вперед в технологии подсчета голосов. К несчастью, множество существующих моментов уязвимости голосования сохраняется. Эти моменты рассматриваются в данном документе.

Дополнительно, Election Guard® использует усложненный способ шифрования бюллетеней, который предоставляет возможность их подсчета, в то время как они

остаются в зашифрованной форме. К несчастью, опять, это является существенным шагом назад, когда это касается доверия избирателей. Создание бюллетеней нечитаемыми за исключением нескольких избранных является именно той областью, в которой люди не доверяют какой-либо форме электронной обработки голосов, и является готовым для манипулирования и фальсификации.

В отличие от способа Accountable Democracy, в Election Guard®:

1. Если хакер задействует исполнение программного обеспечения, которое действует подобно немодифицированной версии, но изменяет бюллетени выборочно во время процесса регистрации, это действие будет происходить необнаруженным. По сути, оно будет действовать как самозванец. Кроме того, поскольку Election Guard® имеет открытый исходный код, будет относительно легко создать такую программу. Не существует способа, в Election Guard®, непрерывно гарантировать, что программное обеспечение фактически используется немодифицированным.

2. Избиратель не имеет способа позволить системе впоследствии информировать избирателя о том, за кого он или она проголосовал(а). Таким образом, снова, аналогично шифрованию (выше), технология говорит "просто доверься мне".

3. Поскольку (1) бюллетени не отслеживаются непрерывно по отношению к регистрационным данным избирателей, (2) множество зарегистрированных избирателей не голосуют, и (3) все бюллетени шифруются, не будет трудным для злоумышленника добавить бюллетени в смесь законного пула голосования без обнаружения или возможности проверки, когда система будет "видеть" эти бюллетени как просто дополнительные поданные голоса.

4. Самой важной уязвимостью Election Guard® является то, что она предназначена, чтобы поддерживать бумажные бюллетени, очевидно, чтобы заверять избирателей, что пересчеты являются возможными. Но в действительности это открывает дверь к нескольким уязвимостям безопасности. Посредством географической децентрализации голосования с помощью бумажных бюллетеней, которое происходит все в один день (т.е., способ, которым голосование проводится в наши дни), невозможно предотвращать значительную мошенническую деятельность в многочисленных местоположениях или нарушения в конкретных пунктах подсчета голосов (или даже кабинках для голосования в пунктах).

Проект Accountable Democracy устраняет множество существующих моментов уязвимости вместо попытки контролировать их, регулировать их или улучшать или нейтрализовать их исполнение.

К слову, если избирательный орган хочет напечатать твердую копию (бумажный бюллетень), резервную по отношению к электронной системе, в день выборов, эта возможность может также быть предоставлена изначально, чтобы укреплять доверие к системе и комфорт для тех, кто полностью не доверяет компьютерной технологии. Эта возможность может оставаться в качестве унаследованной функции или быть устранена совсем.

По сути, Accountable Democracy является *системой серверного уровня*, которая фундаментально изменяет способ, которым записи голосования вводятся, принимаются, управляются, наблюдаются, защищаются, хранятся, подсчитываются и верифицируются. Она строго обеспечивает анонимность и безопасность, в то же время предоставляя избирателям доступ к их собственным бюллетеням в целях безопасности и верификации, также как в целях внесения правок.

Существующие приложения для голосования помогают с регистрацией голосов, при этом бюллетени отделяются от избирателей (через внесения бумажных бюллетеней), оставляя дверь открытой для необнаруженного изменения голосов и подделки, также как вычитаний и добавлений голосов. Дополнительно, существует возможность ошибок подсчета, как намеренных, так и непреднамеренных, в результате чего, аномалии и несогласованности могут возникать в результате использования бумажных бюллетеней, посредством человеческой ошибки или намерения. Сотни, а в некоторых случаях тысячи, отдельных подсчетов используются традиционными системами голосования. Машины для голосования, центры голосования, округа, регионы и федеральные органы проведения голосования, все накапливают и подсчитывают голоса (например, результаты голосования). Система Accountable Democracy устраняет мошенничество и злоупотребление посредством того, что НЕ зависит от способа, которым голоса подсчитываются, ни от самих результатов голосования. Она фокусируется на целостности *файла бюллетеней* и *используемом* программном обеспечении для голосования, и кое-чем еще.

Предыдущие патенты и электронные системы голосования, как иностранные, так и отечественные, фокусируются на устаревших системах, выбирающих некие исторически определенные признаки (например, непрослеживаемость бумажных бюллетеней или их цифровых представлений) на протяжении транзакций с электронными данными, которые показывают удобство, предоставляют аутентификацию избирателя, безопасность волеизъявления и анонимность избирателя, защищенную посредством современных использований сбора данных, обработки данных, хранения данных, защищенных каналов связи и криптографической технологии. В то время как изобретатель признает пользу таких приложений, эти устаревшие системы страдают от многочисленных недостатков, фундаментально характеризуемых машинами для обработки бюллетеней, отделяющими бюллетени (т.е., данные) от их создателей - избирателей, и зависимостью от результатов голосования, собранных и подсчитанных во множестве рассредоточенных мест. Очевидно, они прилагают усилия, чтобы обеспечивать анонимность избирателя, но ценой потери прозрачности, продолжающейся слабостью в аутентификации, безопасности и целостности - все краеугольные камни здоровой демократии. Предшествующий уровень техники до сих пор явно не фокусируется на:

1. Прозрачности исходного кода программного обеспечения *верифицируемым образом* перед, *во время* и после процесса выборов.

2. Непрерывном контроле бюллетеней и верифицируемости, не обеспечивая

избирателей возможностью "просматривать" или изменять свои бюллетени со временем.

3. Уведомлении избирателя, не уведомляя независимо избирателей, что они проголосовали. Это предоставляет возможность для других людей посягать на право голоса избирателя.

4. *Способах обнаружения и восстановления* после отказа среды или намеренного изменения или подделки бюллетеня.

5. Верифицируемости процесса подведения итогов голосования, в результате чего, текущая система не разрешает публичную инспекцию конечного файла бюллетеня.

Как показано выше, предшествующие изобретатели фокусируются больше на одноразовой аутентификации, которая, в то время как является оправданной и легитимной, служит только для дополнения новых особенностей настоящего изобретения. Остается фактом, что аутентификация *избирателя* и верификация должны решительно поддерживаться как естественное следствие для первоначальных верификаций, которые имеют место во время регистрации избирателя, в результате чего, после того как голосование происходит, доступ остается открытым для каждого избирателя.

В настоящее время, избирателям не предоставляется извещение, подтверждающее голоса, и бюллетени больше не являются доступными для избирателей. В результате, избиратель должен быть верифицирован в момент, когда избиратель осуществляет доступ к бюллетеню, и непосредственно перед подачей голоса или голосов, а не в другое время в текущем процессе. В резком контрасте, настоящее изобретение предоставляет возможность для аутентификации и верификации на протяжении всего процесса голосования, а вернее значительно позже того, как голос подается.

Фокус настоящего изобретения, в частности, находится на том, что происходит с бюллетенем, после того как избиратель выразил свои предпочтения (проголосовал), и с этого времени вперед до времени значительно позже выборов. Текущее изобретение позволяет избирателям не только аутентифицировать свою личность и право голосовать (посредством верификации своей регистрации), но также верифицировать то, что их голос был принят и записан корректно (например, не пропущен, изменен, сфабрикован или продублирован), все с возможностью изменять свое мнение и повторно отдавать голос, который может отличаться от их предыдущего голоса или голосов. Настоящая система также устраняет возможность изменения *результатов голосования*, поскольку результаты не хранятся в настоящей системе кроме как временно и на мгновение. И вычисленные результаты голосования могут быть верифицированы внешне посредством выгрузки файла бюллетеней для общего пользования. Таким образом, настоящее изобретение обеспечивает анонимность избирателя от общественного контроля, в то же время одновременно предоставляя непрерывную видимость бюллетеня и доступность индивидуальным избирателям.

Однако, более подробное понимание изобретения будет получено из последующего описания, подлежащего рассмотрению вместе с сопровождающими таблицами на всем протяжении данного документа. Кроме того, эти варианты осуществления не следует

истолковывать как ограничения рамок какого-либо варианта осуществления, но, более того, как примеры различных вариантов его осуществления. Само изобретение является конфигурируемым и модифицируемым во множество других разновидностей, возможных в этом варианте применения и предоставленных посредством учений различных вариантов осуществления, которые будут очевидны специалистам в области техники. Таким образом, рамки следует определять посредством прилагаемой формулы изобретения и ее эквивалентов, которые интерпретируются в свете настоящего описания, а не просто посредством приведенных примеров.

Подробное описание изобретения

Для более полного понимания настоящего раскрытия, ссылка выполняется на последующее подробное описание. Хотя настоящее раскрытие описывается подробно с помощью примерных вариантов осуществления, настоящее раскрытие не подразумевает ограничения конкретными вариантами осуществления, изложенными в данном документе. Понятно, что различные опущения и замены эквивалентов рассматриваются изобретателем, как обстоятельства могут подсказывать или представлять целесообразным, но эти модификации, исправления и вариации предназначаются, чтобы охватывать вариант применения или его реализацию без отступления от духа или рамок настоящего раскрытия.

Дополнительно, следует понимать, что ограничение в рамках раскрытия при этом не подразумевается, поскольку такие изменения и дополнительные модификации существуют в таблицах, и такие дополнительные варианты применения принципов раскрытия, как иллюстрировано в данном документе, как предполагается, придут на ум специалисту в области техники, к которой раскрытие относится. Также, должно быть понятно, что фразеология и терминология, применяемая здесь, используются с целью описания и не должна быть расценена как ограничение. Кроме того, появления таких фраз и терминов, в различных местах, предусмотренных в данном документе, необязательно все ссылаются на один и тот же вариант осуществления. Указание термина в единственном числе в данном документе не означает ограничение количества, а скорее означает наличие по меньшей мере одного из упомянутых элементов. Наконец, оптимальный режим или режимы реализации и применения на практике настоящего изобретения раскрываются при этом, и такие подробности, необходимые для осуществления работы представленной системы голосования, предоставляются, которые позволят специалисту в области техники создавать и осуществлять их на практике.

Настоящее раскрытие предоставляет средство и способ проведения процесса голосования, предоставляющие устойчивость к условиям использования, надежность и верифицируемость упомянутой системе, в результате чего, избиратели могут взаимодействовать с системой голосования и избирательным органом, и аудиторы могут взаимодействовать с системой голосования и избирательным органом, чтобы одновременно обеспечивать прозрачность и безопасность. Кроме того, настоящая система обеспечивает легкость идентификации избирателя, идентификации голоса, также как

подачи голоса в эффективном и модифицируемом конструктиве голосования, который остается изменяемым избирателем (в течение назначенного периода перед подачей голоса) и верифицируемым посредством верифицирующего объекта-сущности (в течение определяемых периодов после подачи голоса или дня выборов). Наконец, настоящая система предоставляет уникальное средство обеспечения целостности системы для системы посредством поддержки раздельных механизмов и серверов для "дублируемых" операций в целях проверки и наблюдения. Как предусмотрено ниже, этот процесс начинается с самой процедуры выборов.

Процедура выборов

Существующие процедуры выборов требуют от избирателей зарегистрироваться в системе регистрации избирателей государства, региона, района, княжества, участка (или другого избирательного органа). Это будет оставаться обязательным требованием.

Каждому избирателю назначается (1) публичный номер избирателя (PVN) и (2) секретный номер избирателя (SVN). Секретные номера избирателей не раскрываются или не публикуются для кого-либо. SVN также являются неизвестными для их назначенных (избирателей), а PVN являются открыто доступными и используются для устранения двусмысленностей и потенциальных расхождений между и среди имен. Эта идея доказывается и объясняется более подробно ниже (см., в частности, раздел “Неизвестность секретного номера”).

В целях настоящего изобретения, голосование имеет место *перед* "днем выборов". День выборов определяется как день, когда все бюллетени голосов требуется принять и собрать избирательным органом. Подсчет может быть проведен, и результаты делаются доступными либо в день выборов, либо в последующий день. Избирательный орган, согласованно с законами государства и местными законами и должностными лицами, определяет, когда выборы начнутся, и когда бюллетени будут подсчитаны. Типично, отведенное время равно шести неделям, но может быть меньше или больше в зависимости от законов каждого государства и от типа выборов (например, предварительные, второй тур и т.п.).

Когда операция голосования отдельного лица выполняется, избиратель информируется о том, что квитанция, цифровая или бумажная, сделана доступной для каждого избирателя. Если избиратель предпочитает получить квитанцию, цифровая или печатная квитанция выдается электронным образом или в бумажной форме, подтверждающая, за кого проголосовал избиратель, также как индивидуальный публичный номер избирателя (PVN). Кроме того, каждая квитанция не содержит идентификационную информацию избирателя (например, имя, адрес и т.д.) или дату, в которую бюллетень был подан. Только PVN избирателя подтверждается, чтобы предотвращать ненадлежащее использование информации об избирателе или использование содержимого заполненного бюллетеня. В настоящем примере, голосование осуществляется в предоставленном органами власти центре голосования или, альтернативно, через Интернет. Печатные квитанции также идентифицируют механизм

взаимодействия избирателя (например, через центр голосования, через телефонное приложение или на компьютере), использованный для регистрации голоса.

Когда голос или голоса обрабатываются избирательным органом, каждый голос или голоса (единственного избирателя) создают "запись бюллетеня" в ядре Accountable Democracy (ADE) с той же информацией, которая представлена на квитанции, за исключением того, что вместо публичного номера избирателя (PVN) она содержит зашифрованный секретный номер избирателя (SVN) (см. также “Неизвестность секретного номера” ниже).

Ядро Accountable Democracy будет предоставлять прикладной программный интерфейс (API) для приложений голосования в режиме онлайн и машин для голосования избирательного органа, используемых для авторизации и регистрации голосов. ADE-авторизация избирателя будет использовать систему избирательного органа, чтобы получать зарегистрированные удостоверения личности (водительские права или государственный ID, и т.д.) и коды авторизации, и будет передавать их третьесторонним приложениям для голосования конечного пользователя для верификации личности избирателя. ADE будет запоминать и хранить конфиденциальные (зашифрованные) секретные номера избирателей, в то время как оно авторизует процесс голосования для публичного номера избирателя. Ядро будет также включать в себя API для использования правительствами регионального и федерального уровня для запроса.

Программное обеспечение пользовательского интерфейса (клиента), которое обеспечивает фактический процесс голосования (и необязательно предоставляет квитанцию), может быть или может не быть соединено с Интернетом во время, когда голос подается. Авторизация голосования может быть получена в режиме офлайн посредством сохранения локальной копии публичного файла регистрации избирателей (исключающего секретные номера избирателей). Временный бюллетень может тогда быть создан в режиме офлайн и позже предоставлен на рассмотрение приложением в ядро Accountable Democracy (ADE). Если избиратель еще не проголосовал, когда бюллетень позже предоставляется на рассмотрение в ядро, он проходит через тот же процесс верификации избирательным органом и уведомления избирательного органа, который имел бы место в случае голосования пользователя в режиме онлайн. Если избиратель ранее проголосовал, и кто-то пытается зарегистрировать голос или голоса в ADE, голос блокируется, и фактический авторизованный пользователь уведомляется о том, что неудачная попытка проголосовать была выполнена с помощью его учетных данных. Время и место или механизм неавторизованной попытки будут предоставлены.

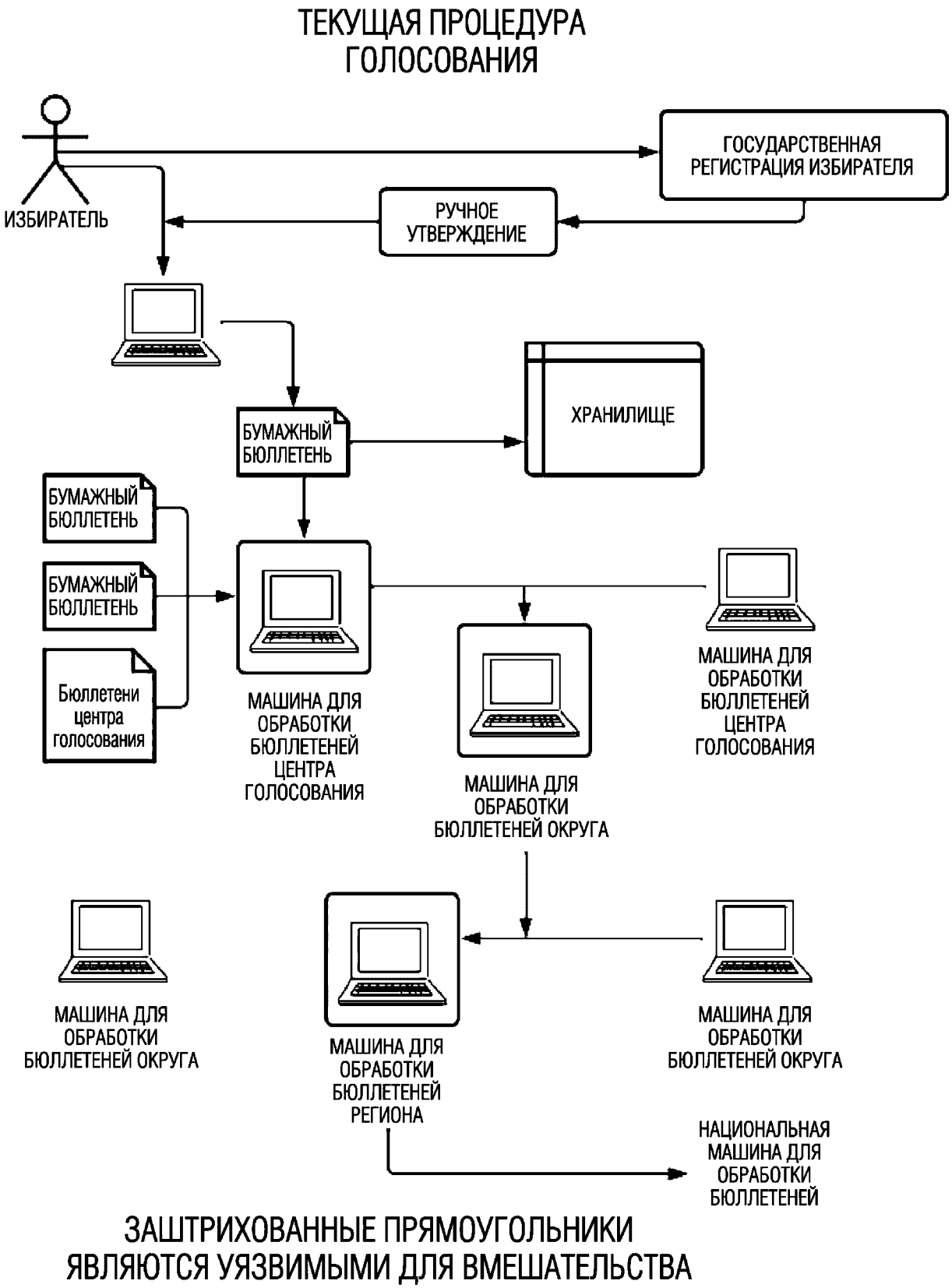
Когда ядро Accountable Democracy обрабатывает бюллетень, оно создает *запись бюллетеня* внутри, и избиратель уведомляется о том, что он проголосовал (посредством текста, электронной почты, записанного телефонного сообщения и/или почтовым отправлением). В это время, запись о регистрации избирателя в избирательном органе обновляется, чтобы показывать дату, время и центр для голосования, использованный для регистрации голоса. Ядро, конечно, знает, проголосовал ли избиратель, поскольку

упомянутое ядро имеет доступ ко всем бюллетеням.

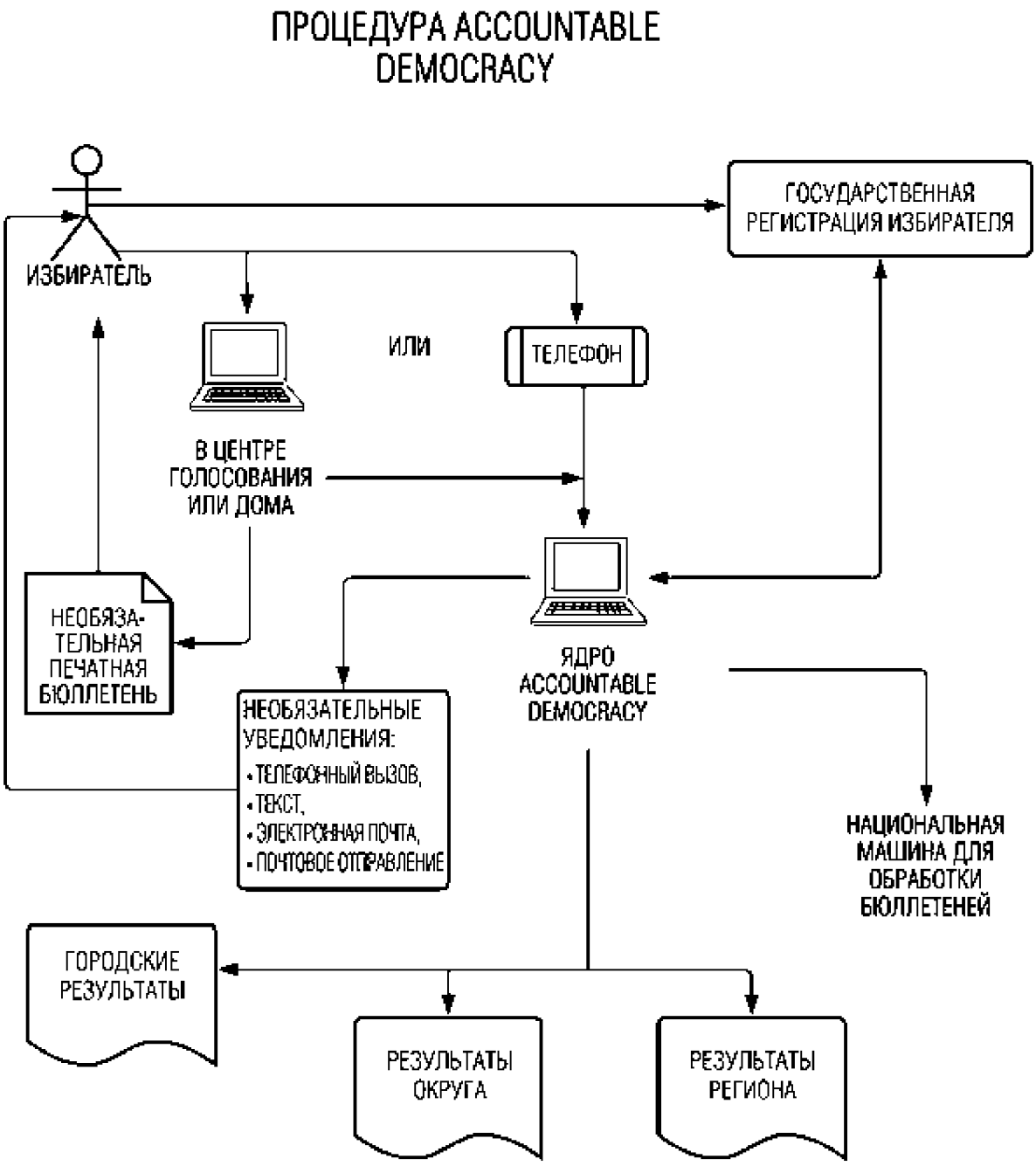
После того как запись бюллетеня создана, избиратель волен контролировать и запрашивать свою собственную запись бюллетеня в режиме онлайн (служба, предлагаемая избирательным органом с помощью API ADE), чтобы удостовериться, что каждый голос или голоса были правильно зарегистрированы. Если существует расхождение с поданными голосом или голосами и/или первоначальной печатной квитанцией, он или она может размещать возражение с помощью избирательного органа. В любой момент после этого, во время и после выборов, и пока избирательный орган считает это надлежащим, или в периоде времени, допустимом по закону, избиратель может напечатать другую квитанцию бюллетеня с полной информацией бюллетеня, но не датой или деталями механизма, использованного для голосования.

После того как голос подан, и запись бюллетеня создана, избиратель имеет заданное время (определенное избирательным органом - типично не менее 72 часов), чтобы аннулировать свой голос, если он так пожелает. В каждом голосовании будет существовать предельный срок (типично 24 часа перед днем выборов), после которого аннулирования не допускаются. Если избиратель аннулирует свой голос или голоса, он волен проголосовать снова. Ограничение может быть помещено на количество допустимых повторных голосований.

Таблица ниже показывает обзор текущего процесса, посредством которого выборы проводятся в настоящий момент, и избранных потенциальных слабых мест безопасности в потоке данных. За упомянутой таблицей непосредственно следует схема, показывающая поток данных, использующий эту новую процедуру голосования.



Заштрихованные области идентифицируют слабости в безопасности в настоящих системах выборов.



Накопление записей бюллетеней

Записям бюллетеней назначается порядковый номер как часть их структуры, который может быть использован для последующего доступа к ним. Записи бюллетеней замораживаются спустя 72 часа (или другой точно указываемый период, как определено выше) с момента их создания. По мере накопления замороженных бюллетеней, они собираются в пачки. Списки номеров бюллетеней (пачки) хранятся в файле пачек (таблице), при этом размер пачки может быть установлен во время настройки системы, и каждой пачке выпускается 256-байтное SHA хэш-значение и номер пачки. Хэш-значение принадлежит всем данным бюллетеней в пачке, в том числе зашифрованным SVN.

Содержимое записи пачки:

- бюллетень номер A
- бюллетень номер B
- бюллетень номер C
- бюллетень номер $[(N)_n]$
- хэш-значение данных бюллетеней
- номер пачки

Сами данные бюллетеней (отличные от множества SVN) хранятся в незашифрованном состоянии. Голоса за конкурирующих кандидатов выражаются посредством двоичной системы нумерации кандидатов. Например, если четыре человека баллотируются на конкретную должность, они будут пронумерованы внутренним образом как 1, 2, 4 и 8. Вместо наличия специально выделенной графы для галочки внутренним образом, они будут иметь один номер кандидата на каждую открытую должность. Это гарантирует, что, если какие-либо бюллетени изменяются, резкое изменение произойдет в SHA хэш-значении пачки. Возможными альтернативами этому являются 1) выражение номеров кандидатов на место с помощью алфавитных значений или 2) номера выражаются с помощью алфавитных знаков.

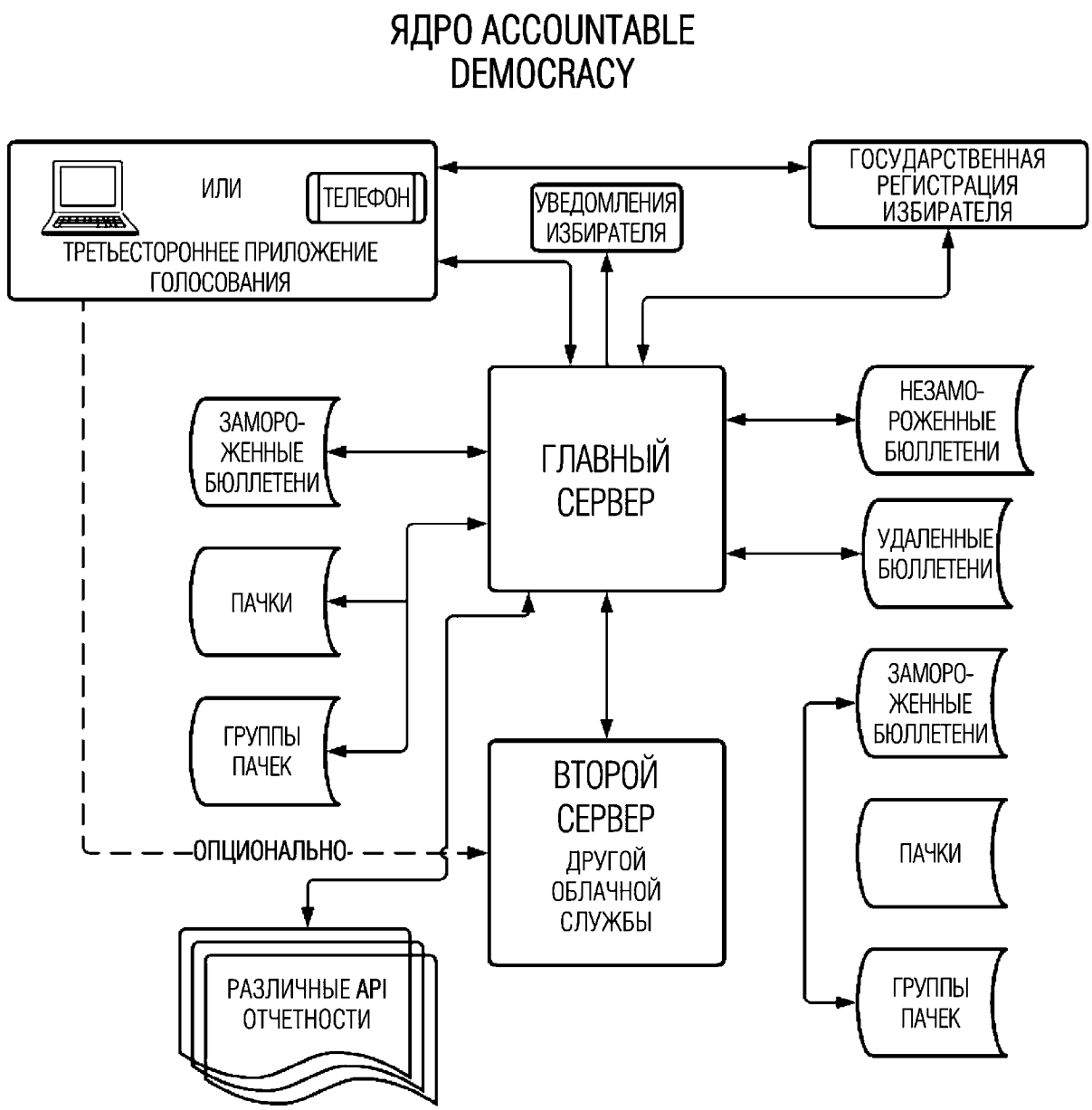
Сами пачки группируются (перечисляются) в записях группы пачек, которые хранятся в файле группы пачек, и каждой группе пачек выпускается порядковый номер и хэш-значение, которое принадлежит всем записям пачек в группе. Существуют два типа записей группы: 1) записи, которые принадлежат пачкам, и 2) записи, которые принадлежат группам. Записям групп пачек назначаются номера уровней таким образом, чтобы группы могли "образовываться" (т.е., компоноваться) иерархически. Первый уровень является уровнем 1, который перечисляет записи пачек. Уровень 2 и выше записывает список (и хэш) записей групп на уровне, непосредственно ниже их.

Бюллетени, хранящиеся в файле незамороженных бюллетеней, защищаются посредством индивидуальных хэш-значений бюллетеней, сохраненных в отдельном файле незамороженных хэш-значений.

В общих словах, существует управляемый избирательным органом файл регистрации избирателей, файл незамороженных бюллетеней, файл замороженных бюллетеней, файл пачки, файл группы пачек и файл удаленных бюллетеней. Программное обеспечение работает на двух серверах в тандеме со вторым программным обеспечением, по сути, верифицирующим первое программное обеспечение для избыточности и помощи в наблюдении и верификации.

Дополнительно изобретателем рассматривается то, что третий ADE-сервер, работающий совместно, может быть системой, управляемой объектом-сущностью, отличной от управляемого на региональном или федеральном уровне объекта-сущности (например, частным образом управляемой, публично управляемой или иным не спонсируемым государством предприятием), или через партнерство между системой, управляемой на региональном / федеральном уровне, и частным предприятием, при этом система проверок и противовесов создается, чтобы добавлять надзор, наблюдение и/или

легитимность к настоящей системе. Стандартная ADE-система дополнительно показывается и иллюстрируется посредством следующей (упрощенной) таблицы:



Безопасность и прозрачность

Определение терминов:

- Хэш-значение - Значение, которое является накоплением битов из потока данных способом, который использует математический алгоритм, такой как SHA-256. Оно также называется "контрольной суммой" или просто "хэшем".

- Ассиметричное шифрование - Тип шифрования, который использует два различных ключа. Каждый ключ может дешифровать то, что другой шифрует. Часто они называются открытым и закрытым ключами.

Намерением изобретателя является создание исходного кода главного сервера для ядра Accountable Democracy (ADE), в том включающего в себя операционную систему,

доступного для общественного контроля и лицензирования упомянутой системы для использования при проведении выборов. Здесь описывается то, как общественности гарантируется, что используемое программное обеспечение является точным программным обеспечением, которое выпущено для общественности.

Прозрачность

ADE проектируется для работы одновременно на двух до множества выделенных серверах (типично предоставляемых конкурирующими облачными службами), и ядро включает в себя свою собственную операционную систему (OS). Первоначально это уменьшенный по масштабу Linux или ОС типа BSD. Во время начальной загрузки текущая программа устанавливает всю неиспользуемую память в ноль, а по завершении начальной загрузки она устанавливает хэш-значение для ОС и другое хэш-значение для исполняемых модулей приложения.

Со случайными интервалами настоящая система повторно вычисляет и сравнивает эти программные хэш-значения с хэш-значениями, установленными при начальной загрузке, чтобы гарантировать, что программы не изменились. Она также периодически повторно подтверждает (проверяет) хэш-значения всех файлов (таблиц), чтобы гарантировать целостность системы. Программы выделения памяти, используемые программным обеспечением, обнуляют память при ее освобождении.

Программное обеспечение, также по запросу или инструкции, повторно вычисляет хэш-значение всех исполняемых модулей, которые обрабатывают записи бюллетеней, пачек и групп, и предоставляет их клиентским и правительственным приложениям через API. Весь исходный код в главном ADE-сервере является публично доступным для независимой проверки и компиляции в целях верификации хэша (таким образом, обеспечивая управление на уровне государства и общественный надзор). Это включает в себя исходный и объектный код для вычисления хэш-значений. Это предоставит повышенную проверку правильности результатов выборов посредством открытой проверки способов и процессов, но не раскроет идентификацию избирателя или фактические результаты бюллетеней.

Ожидается, что во время выборов 8 символов низшего порядка этих критических хэш-значений будут опубликованы в СМИ и/или сделаны доступными на публично доступном веб-сайте, и эти значения будут динамически получаться от ядра и отображаться на клиентских пользовательских интерфейсах при голосовании.

Функциональность второго сервера

Второй сервер работает в "подчиненном" режиме и, по сути, дублирует все процессы учета бюллетеней, выполняемые главным сервером. Главный сервер пересылает копию всего входящего трафика данных второму серверу. Второй сервер может также принимать входные данные непосредственно от клиентских приложений в целях верификации. Периодически, верхние хэш-значения групп, созданные двумя серверами, сравниваются, чтобы гарантировать, что оба функционируют аналогично. Необязательный третий сервер, или множество серверов, могут быть присоединены к конфигурации, для большей

безопасности и для идентификации корректной информации бюллетеня в случае расхождения между главным и вторым серверами, или каким-либо назначенным первичным и вторичным сервером или набором серверов. И третий сервер может быть где-угодно в Интернете, как, например, в аудиторском центре.

В случае, когда главный сервер компрометируется или отключается, изменение ролей может иметь место посредством 1) помещения главного сервера в двухсторонний только пересылающий режим или перемаршрутизации сетевого трафика к и от второго сервера, и 2) переключения второго сервера в автономный режим. После того как главный сервер либо защищен, либо восстановлен, этот сервер может использоваться в качестве вторичного сервера или быть переклассифицирован в качестве первичного сервера, как диктуют условия, действующего в качестве зеркального сервера или сервера подтверждения.

Несколько вспомогательных функций главного сервера не предоставляются в автономном режиме, но он включает в себя всю обработку бюллетеней и обработку записей групп, уведомление избирателей и поддержку запросов избирателей. Файлы, созданные и сохраненные вторым сервером в автономном режиме, являются идентичными файлам на главном сервере и служат в качестве функции зеркалирования.

Поскольку бюллетени группируются иерархически, все уровни могут сравниваться между серверами посредством сравнения единственного хэш-значения на верхнем уровне каждого файла группы. Если расхождение происходит, программное обеспечение может быстро идентифицировать группы бюллетеней и фактические бюллетени, которые различаются между двумя серверами или множеством серверов, изучая хэши групп вниз до самого нижнего расхождения хэшей, и затем сравнивая записи фактических бюллетеней в каждой группе, чьи ключи не совпадают, тем самым, обеспечивая одновременную функцию наблюдения и проверки для того, чтобы обнаруживать и точно указывать расхождения, существующие в хэшах групп, вниз до уровня индивидуальной пачки. После того как ошибочная пачка идентифицирована, другое средство используется для идентификации расхождений в пачке (например, сравнение с резервными копиями и зеркальными данными).

Программное обеспечение, следовательно, может быстро идентифицировать любые ошибочно записанные бюллетени (т.е., бюллетени, которые различаются между дублирующими наборами данных бюллетеней) и сообщать конкретные расхождения в таких бюллетенях. Посредством создания прогрессивных наборов резервных копий в третьем местоположении совершенно легко увидеть, какие оригинальные значения были в таких бюллетенях. Конечно, с величиной защиты, которую эти бюллетени имеют, бюллетени будут очень редко изменяться, но ошибки среды не могут быть исключены, когда они случайно происходят.

Обработка исключения

С точно указанными или случайными интервалами программа-инспектор выгружается в настоящую систему с сервера Accountable Democracy (или аудитора

выборов), которая затем использует динамический алгоритм для модификации своего собственного хэша после запуска. Программа не знает, каким ее собственный хэш является или будет, но внешний сервер Accountable Democracy имеет доступ к этой информации. Программа-инспектор проверяет окружение и сообщает свое собственное хэш-значение вместе со своими обнаружениями со ссылкой на все хэш-значения исполняемого кода и карту динамически выделенной памяти.

По запросу от избирательного органа или другого наблюдающего учреждения, полный аудит файлов бюллетеней будет выполнен посредством отправки избирательным органом списка всех (зашифрованных) секретных номеров избирателей, *которые проголосовали*, в ADE. ADE затем найдет и отследит все бюллетени, ассоциированные с предоставленным списком. Какие-либо ненормальности, отсутствующие или лишние бюллетени, или их комбинация, будут затем сообщены в отчете.

Периодически система будет проверять файлы бюллетеней, пачек и групп, повторно вычисляя все хэш-значения в файлах пачек и групп и сопоставляя результаты с сохраненными значениями, выполняя проверку, чтобы быть уверенной, что каждый номер бюллетеня появляется в одной и только одной пачке, и выполняя проверку, чтобы быть уверенной, что дублирующие секретные номера избирателей в бюллетенях не существуют.

Перед публикацией окончательного файла бюллетеней секретные номера избирателей повторно шифруются с помощью новых ключей, на всякий случай, если внутренний ключ шифрования был злонамеренно получен. В это время все хэш-значения в порядке возрастания повторно вычисляются. Во время, когда окончательный файл бюллетеней выдается, соответствующий файл пачки будет сопровождать его.

Табличная электронная структура бюллетеней

Широкий диапазон возможных определений бюллетеней и способов голосования поддерживается, включающий в себя первичные выборы, выборы, предвыборную борьбу, замеры, референдумы, законопроекты и т.п. Более того, система проектируется как многоязыковая и приспособлена для поддержки множества визуальных подсказок и оптических вспомогательных средстве.

Информационная панель избирательного органа

ADE может сообщать избирательным органам географические статистические данные, касающиеся числа избирателей, которые проголосовали в каждой географической области. Эта информация будет также доступна избирательным органам через их собственные записи о том, кто проголосовал. Предположительно, информация бюллетеней не будет предоставлена избирательным органам перед выдачей окончательных результатов подсчета.

Неизвестность секретного номера (защита личности избирателя)

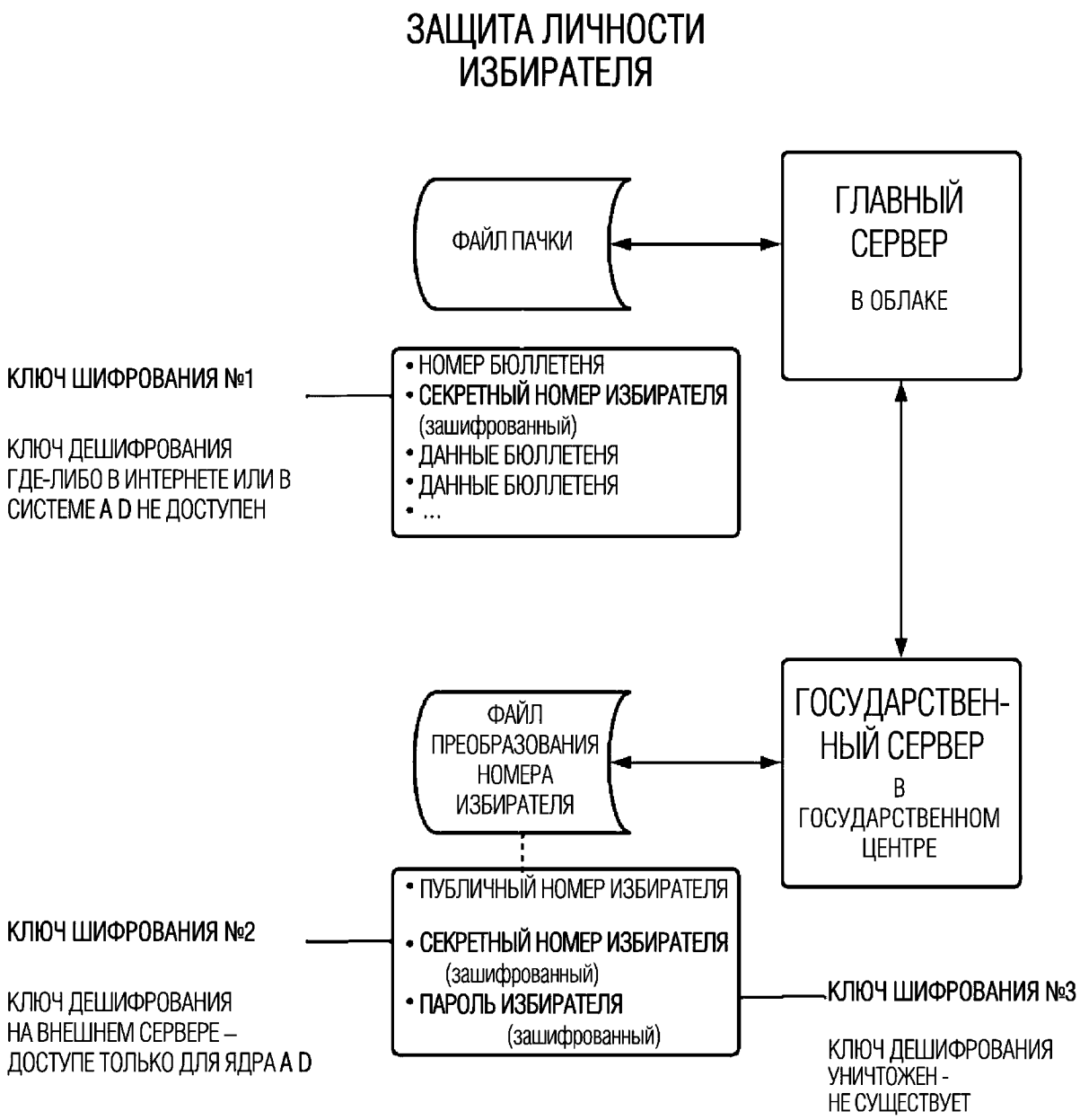
На государственных серверах (избирательного органа), когда избиратель регистрируется, ему или ей предоставляется учетная запись и назначается (1) публичный номер избирателя и (2) секретный номер избирателя. Секретный номер предоставляется

избирательному органу посредством обслуживающей программы ADE в ассиметрично зашифрованной форме, а первоначальный конкретный номер избирателя никому не раскрывается. Однозначно, избирательному органу не предоставляется ключ шифрования, либо ключ дешифрования. Секретный номер избирателя может содержать символы, отличные от цифр, включающие в себя, но не только: буквы верхнего и нижнего регистра и печатные специальные символы.

Когда ADE принимает зашифрованный секретный номер от сервера избирательного органа, ADE немедленно дешифрует этот номер и повторно шифрует его, с помощью другого ключа для хранения в бюллетене. ADE не имеет доступа к ключу дешифрования секретного номера бюллетеня. Ключ дешифрования для зашифрованных избирательным органом номеров хранится только на внешнем сервере Accountable Democracy (в зашифрованной форме) и в памяти ADE.

Резюмируя, избирательные органы не имеют доступа к ключам шифрования или дешифрования секретного номера, а ADE не имеет доступа к ключам дешифрования секретного номера бюллетеня, за исключением случая, когда они предоставляются из внешнего источника для повторного шифрования номера избирателя в бюллетене. Когда голосование происходит, публичные номера избирателей используются для координации между пользовательским приложением, ADE и серверами избирательного органа. Когда избиратель осуществляет доступ к своему бюллетеню, его зашифрованный секретный номер отправляется в ADE, которое преобразует его во вторую зашифрованную версию и отыскивает бюллетень.

Это представляется и осуществляется как в этой обзорной таблице:



Технические соображения

Сегодняшние компьютерные программные средства имеют очень широкую основу. Существует множество способов реализовать этот проект. С технической точки зрения ключевыми моментами, реализующими настоящую систему, являются:

1. Операционные системы с открытым исходным кодом;

2. Публично доступные компиляторы языков программирования и библиотеки исходного кода;

3. Публично доступные криптографические методы как для хэширования, так и для использования ассиметричных ключей;

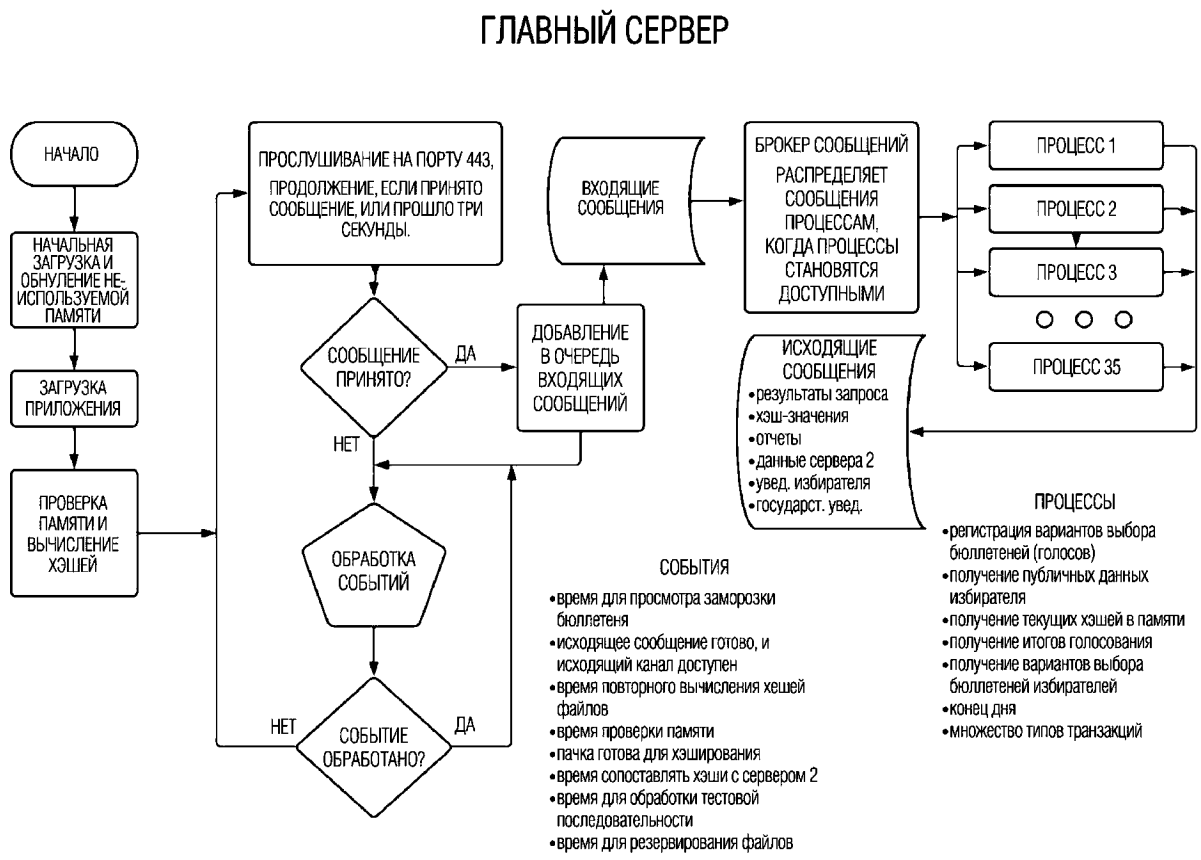
4. Способность программного обеспечения к самопроверке;

5. Способность программного обеспечения к экспертной оценке и наблюдению *во время выборов* посредством динамического вычисления программно-исполняемых хэш-

значений.

В случае тревожного оповещения, вследствие несоответствий между и среди сервером(ами), данных, или посредством выражения беспокойства избирателями, простым решением является выгрузка свежего программного обеспечения для проверки, которое подтвердит статус каждого сервера. Поскольку вся обработка бюллетеней является централизованной для каждого избирательного органа, существует только одна точка искажения данных или программы, за которой необходимо наблюдать, и которая может быть легко доступна.

Нижеследующая схема представляет одну возможную программную структуру для реализации этих способов. Представленный предпочтительный вариант осуществления служит в качестве примера, и со временем улучшения технологии станут доступными для более лучших реализаций. Значимые аспекты проекта перечислены в предыдущих разделах, и этот пример представляется, чтобы описать одну из множества возможных программных структур.



Блокчейн (цепочка блоков) - альтернативы

Цепочки блоков широко признаны как безопасные и неизменяемые. Следовательно, они создают хороший механизм хранения бюллетеней. Однако, настоящее изобретение не полагается или не становится обязательно зависимым от цепочки блоков и превосходит цепочку блоков в следующих отношениях:

1. Бюллетени являются в одно и то же время отслеживаемыми, анонимными, публично видимыми и неизменяемыми. В цепочке блоков бюллетени, по существу, не

видны для избирателей в форме, которую можно было бы осмыслить. Настоящее изобретение максимизирует прозрачность, которая является центральным аспектом достоверности. При использовании цепочки блоков, если ключи дешифрования намеренно или тайком выдаются общественности, тогда личности избирателей также становятся видимыми.

2. При использовании цепочки блоков усложненное программное обеспечение требуется для подсчета голосов, и это представляет точку уязвимости для вмешательства. Все, что не может быть осуществлено на виду, верифицируемым образом, подвергается вмешательству и сомнению. В настоящей системе, файл бюллетеней может быть выдан общественности для проверки, подтверждения целостности и для пересчетов.

3. Настоящее изобретение использует значительно более эффективный формат хранения по сравнению с цепочкой блоков. Только посредством шифрования секретных номеров избирателей оно минимизирует требования к хранению, и, посредством правильного использования криптографической технологии, настоящая система делает хранение несложным, эффективным и быстрым, чтобы идентифицировать и изолировать искажения данных, тогда как цепочка блоков должна использовать экстенсивную избыточность, сложные формы разрешения разногласий и существенную вычислительную мощность, и природные энергетические ресурсы.

4. Использование цепочек блоков является непригодным для избирателей, изменяющих свое мнение или аннулирующих голоса, которые являются спорными. После того как блок в цепочке сохраняется в цепочке, он является неудаляемым.

Ключевые операции

Ключами к успеху (с токи зрения конфиденциальности избирателя и управления) для этого типа подсчета и учета голосов являются:

1. Способность избирателей повторно рассматривать свои бюллетени, таким образом, предоставляя полномочие конечному пользователю гарантировать требуемую безопасность в том, что бюллетени не изменяются.

2. Способность программного обеспечения к самопроверке, в результате чего, программное обеспечение имеет контроль над всем своим операционным окружением (как ОС, так и приложениями) и может проверять и контролировать свое вычислительное окружение (также как и себя), и, с помощью методов хэширования, быстро определять какие-либо искажения или отклонения.

3. Способность быстро определять то, существует ли расхождение между копиями файлов бюллетеней, и быстро идентифицировать различия.

4. Посредством *не сохранения результатов подсчета и сохранения только бюллетеней* система использует наименьший объем данных, требующих защиты. Этот ключевой аспект, совместно с достаточными прогрессивными резервными копиями, максимизирует эффективность, в то же время минимизируя уязвимость.

5. Сокрытие секретных номеров избирателей предоставляет фундамент, на который опирается пункт 1 выше. Верифицируемость избирателем бюллетеней совместно с

анонимностью является фундаментальной по отношению к какому-либо процессу голосования, но не предоставляется посредством предыдущих методологий голосования. Настоящее средство защиты личности избирателя разрешает экспорт файла бюллетеней (например, для общественной проверки, резервирования и пересчетов) без компрометации идентичности и безопасности избирателей.

Ясно, что настоящая система отображает и является приспособленной для осуществления следующих способов и методов посредством некоторых предпочтительных вариантов осуществления: способность безопасно проводить выборы в течение увеличенного и продлеваемого периода времени, гораздо большего, чем единственный день (например, шесть недель), заканчивающегося перед днем выборов, способом, который обеспечивает быстрое, безопасное и прозрачное (публичное) подведение итогов в и после дня выборов, способность электронным образом соединять процесс авторизации голоса с базой данных регистрации избирателей избирательного органа, способность пересылать удостоверяющую информацию из базы данных избирательного органа приложениям голосования конечных пользователей (третьей стороны), способность немедленно уведомлять электронным образом сервер базы данных избирательного органа, когда избиратель проголосовал, способность избирателя просматривать свой бюллетень в режиме онлайн постоянно, пока избирательный орган позволяет, как во время, так и после выборов, способность предотвращать какое-либо обратное отслеживание от цифрового бюллетеня до избирателя, который создал его, *в то же время одновременно* предоставляя возможность избирателю наблюдать свой бюллетень, способность независимо уведомлять каждого избирателя о том, что голос был принят, через множество средств, таких как аудио, текст, электронная почта и почтовое отправление, и способность для избирателя аннулировать или изменять свой голос (которая восстанавливает его правомочность голосовать) в течение конкретного периода времени (предлагаются 72 часа), после того как он проголосовал, прежде чем его голос становится замороженным (неизменяемым). В то время как другие системы могут предоставлять печатную квитанцию во время голосования (которое эта система поощряет и продвигает), настоящее изобретение поддерживает способность для избирателя получать бумажную квитанцию (через систему избирательного органа) в любое время *после голосования*, как перед, так и после того как бюллетени подсчитываются, пока избирательный орган позволяет, показывающую, за кого или что он проголосовал. Эта квитанция должна быть без указания даты и показывать публичный номер избирателя, но не его имя.

Кроме того, настоящее изобретение и система продвигают способность НЕ шифровать цифровые бюллетени (за исключением ID-номеров избирателей), которые, в конечном счете, будут помещены в публичную область, и одновременно защищать бюллетени от изменения посредством хранения хэш-значений пачки в отдельном файле, способность поддерживать динамическое отображение всех или части хэш-значений программы операционной системы ядра для подсчета итогов на устройствах голосования

конечных пользователей, способность поддерживать динамическое отображение всех или части хэш-значений прикладной программы ядра для подсчета итогов на устройствах голосования конечных пользователей и способность повторно шифровать все секретные номера избирателей, сохраненные в бюллетенях, перед публикацией файла бюллетеней публично.

Кроме того, настоящее изобретение предоставляет возможность для ADE работать на множестве *скоординированных* серверов на одной и той же или отдельных облачных платформах, для этого же самого ADE использовать ключ дешифрования, сохраненный только внешне и в динамической памяти ADE с целью дешифрования секретных номеров избирателей, сохраненных на серверах избирательного органа, и для

1. ADE использовать ключ шифрования, сохраненный только внешне и в динамической памяти ADE, с целью шифрования секретных номеров избирателей, когда они хранятся в бюллетенях.

2. Настоящее изобретение также проявляет способность индивидуально хэшировать итоговые бюллетени, сохраненные в файле незамороженных бюллетеней, и сохранять такие хэш-значения в отдельном файле, способность иерархически группировать хэш-значения пачек бюллетеней, предоставляя суммарное хэш-значение верхнего уровня для всех бюллетеней, замороженных во время выборов, способность использовать множество ассиметричных ключей шифрования, чтобы скрывать личности избирателей таким образом, что зашифрованные номера избирателей, сохраненные на серверах избирательного органа, отличаются от зашифрованной формы тех же самых номеров, сохраненных в бюллетенях, способность периодически хэшировать все биты программы, из которых состоит операционная система ядра подведения итогов, способность для ADE обнулять всю неиспользуемую компьютерную память во время выборов, также как способность принимать данные от приложения пользовательского интерфейса избирателя независимо на более чем одном сервере и сравнивать такие квитанции в целях верификации.

3. Кроме того, система настоящего изобретения и способ использования обладают способностью управлять процессом подведения итогов голосования, при этом итоги голосования не хранятся в машине для обработки бюллетеней (табуляторе) кроме как во время процесса отчетности (в результате чего, голоса пересчитываются непосредственно из замороженных бюллетеней каждый раз, когда они сообщаются), способность отправки случайным образом программы-инспектора из внешнего центра для проверки содержимого памяти ADE-серверов, способность предоставлять информационную панель для избирательных органов, которая должна работать на серверах избирательных органов, чтобы сообщать, сколько избирателей проголосовало в каждой частичной области (например, округе), способность проверять файл бюллетеней посредством нахождения всех бюллетеней, ассоциированных с избирателями, которые проголосовали, согласно базе данных регистрации избирателей и сообщения о каких-либо отсутствующих или лишних бюллетенях.

4. Этот процесс использует два номера избирателя, один из них секретный, чтобы защищать личность избирателя, помечать голоса и привязывать их к избирателям, в то же время поддерживая анонимность избирателя.

5. Дополнительно, настоящее изобретение скрывает возможность устанавливать размер пачки бюллетеней и размер группы пачек для любых определенны выборов, периодически повторно вычислять все хэш-значения бюллетеней и пачек, чтобы подтверждать сохраненные хэш-значения, и способность быстро идентифицировать, какая пачка или пачки была/были модифицированы, посредством иерархического хэш-дерева в случае вмешательства или отказа среды.

В то время как вышеприведенное описание и чертежи представляют примеры и предпочтительные варианты осуществления настоящего изобретения, следует понимать, что различные добавления, компоновки, комбинации и/или замены, последовательно или параллельно, могут быть выполнены в данном документе без отступления от духа и рамок настоящего изобретения, которые определены в приложенной формуле изобретения. В частности, специалистам в области техники будет ясно, что настоящее изобретение может быть осуществлено в других конкретных конструкциях, конфигурациях, с помощью несходных структур, компоновок, пропорций, и с помощью других элементов, материалов и компонентов, без отступления от духа или его неотъемлемых характеристик. Специалист в области техники признает, что изобретение может быть использовано со многими модификациями в конструкции, компоновке, пропорциях, материалах и компонентах и иным образом использовано в практическом применении изобретения, которые, в частности, приспособлены к конкретным требованиям и операционным окружениям без отступления от принципов настоящего изобретения. Кроме того, признаки, описанные в данном документе, могут быть использованы в единственном числе или в сочетании с другими признаками. Раскрываемые в настоящий момент примеры, следовательно, должны рассматриваться во всех отношениях как иллюстративные, а не ограничивающие, рамки изобретения указываются посредством прилагаемой формулы изобретения и строго не ограничиваются вышеприведенным описанием.

Специалистам в области техники будет понятно, что изменения могут быть выполнены в примерах, предоставленных выше, без отступления от описанной широкой идеи изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ обеспечения безопасности для системы голосования, содержащий этапы, на которых:

i. реализуют центр для регистрации избирателя в избирательном органе и наблюдения;

ii. реализуют первичное ядро программного обеспечения для авторизации избирателя, регистрации голоса и подсчета голосов и отчетности;

iii. реализуют приложение избирателя для конечного пользователя;

iv. упомянутое ядро программного обеспечения предоставляет первый прикладной программный интерфейс (API), к которому должно осуществлять доступ упомянутое приложение конечного пользователя;

- a. упомянутый API используется в качестве ресурса и хранилища для авторизации и регистрации голосов;

- b. упомянутый API используется для получения идентификационной информации избирателя и документов, которые должны быть использованы для аутентификации избирателя;

- c. упомянутый API используется для получения текущих хэш-значений исполняемого кода программы и операционной системы для публичного отображения;

v. упомянутое ядро программного обеспечения предоставляет второй API, к которому должен осуществлять доступ упомянутый центр избирательного органа;

- a. упомянутый второй API используется упомянутым ядром для запроса и приема удостоверяющих данных избирателя, которые должны быть использованы для аутентификации избирателя;

- b. упомянутый второй API используется для предоставления неназначенных зашифрованных SVN упомянутого центра избирательного органа для назначения избирателям;

- c. упомянутый второй API используется для уведомления упомянутого центра избирательного органа о том, что избиратель проголосовал;

- d. упомянутый второй API используется, чтобы предоставлять возможность избирателю наблюдать и печатать содержимое своего бюллетеня;

- e. упомянутый второй API используется, чтобы предоставлять возможность избирателю аннулировать свой бюллетень, пока он не заморожен;

vi. предоставляют упомянутое первичное ядро, работающее на первом сервере, для приема, сбора, обработки и подсчета голосов;

vii. предоставляют вторичное ядро, работающее на втором сервере, в тандеме и независимо от упомянутого первого ядра, в то время как упомянутое первичное ядро не имеет зависимости от информации, поступающей от вторичного ядра;

viii. назначают каждому избирателю уникальный публичный номер избирателя (PVN) и (2) уникальный секретный номер избирателя (SVN);

- a. упомянутый публичной номер избирателя (PVN) является идентифицируемым индивидуальным избирателем;

- b. упомянутый секретный номер избирателя (SVN) является идентифицируемым упомянутым первым ядром;

- c. упомянутые SVN подвергаются шифрованию, составляющему две пары ассиметричных ключей шифрования, при этом SVN на серверах избирательного органа отличаются от зашифрованной формы тех же самых номеров, сохраненных в бюллетенях;

- d. сохраняют ключи шифрования и дешифрования внешне на отдельном сервере ключей и не предоставляют их избирательному органу или не сохраняют их в упомянутом ядре, но предоставляют возможность им временно находиться в памяти упомянутого ядра;

- e. упомянутое первичное ядро на первом сервере выполняет все шифрование и дешифрование SVN и предоставляет зашифрованные SVN упомянутому избирательному органу для последующего назначения избирателям;

ix. упомянутое вторичное ядро выполняет дублирующую обработку бюллетеней и хеша; принимает зашифрованные SVN от главного сервера вместе с соответствующими незашифрованными PVN и данными бюллетеней для независимого дублирующего хэширования, верификации и хранения;

x. предоставляют возможность упомянутым избирателям голосовать с интервалами и в моменты времени, предшествующие дням выборов;

xi. предоставляют из упомянутого приложения для голосования конечного пользователя запись бюллетеня для каждой индивидуальной совокупности голосов избирателя;

xii. снабжают упомянутую запись бюллетеня штампом времени, даты и индикатором центра;

xiii. уведомляют упомянутого избирателя непосредственно из упомянутого первичного ядра об упомянутой записи бюллетеня посредством аудио, текста, электронной почты и/или почтового отправления;

xiv. назначают статус незамороженных бюллетеней, которые являются модифицируемыми;

xv. предоставляют пользователю возможность проверки и запроса своего бюллетеня в любой момент во время и в течение периода после выборов, и аннулирования своего бюллетеня, прежде чем он будет заморожен;

xvi. после предварительно определенного периода (например, 72 часа) назначают статус замороженных бюллетеням, которые становятся немодифицируемыми; и

xvii. подсчитывают замороженные бюллетени.

2. Способ по п. 1, при этом множество ядер существуют на двух или более отдельных серверах, каждое работает в отдельных окружениях, работающих в тандеме, чтобы верифицировать взаимную функциональность.

3. Способ по п. 1, при этом упомянутый первый и второй API могут отображаться на персональных устройствах, включающих в себя планшеты, смартфоны и компьютеры, устройствах центра голосования или их комбинации;

4. Способ по п. 3, при этом упомянутые первые API могут быть использованы двухсторонне через упомянутое первичное ядро, чтобы передавать данные от избирателей в упомянутый избирательный орган и от упомянутого избирательного органа к упомянутым избирателям;

5. Способ по п. 4, при этом упомянутая принимаемая информация может состоять из идентифицирующей избирателя информации, идентифицирующей голос информации, голосов или их комбинации, и упомянутые передаваемые данные могут состоять из множества PVN, уведомления о принятых голосах, записанных голосов, удаленных голосов, отчетов, статистических данных и идентифицирующей голос информации.

6. Способ по п. 3, при этом третий API может быть использован проверяющим объектом-сущностью, чтобы запрашивать упомянутое первое, второе или множество ядер для определения расхождений между и среди ядер.

7. Способ по п. 1, при этом дополнительно содержит этапы, на которых:

a. назначают каждому бюллетеню уникальный номер, дополненный его зашифрованным SVN, хэшированный, подсчитанный и сохраненный в очереди, обозначенной как незамороженная;

b. помещают хэш-значения незамороженных бюллетеней в отдельный файл вместе с их номерами бюллетеней;

c. предоставляют возможность избирателям аннулировать (удалять) свои бюллетени из незамороженной очереди бюллетеней;

d. после предварительно указанного периода (например, 72 часа) перемещают незамороженные бюллетени в файл замороженных бюллетеней;

e. после того как бюллетени были добавлены в файл замороженных бюллетеней, создают запись пачки в отдельном файле пачки, состоящую из уникального номера пачки, списка всех номеров бюллетеней в пачке и хэш-значения всего перечисленного содержимого бюллетеней;

f. после того как записи пачки были добавлены в файл пачки, создают запись группы пачек, сохраняемую в отдельном файле группы пачек, состоящую из уникального номера группы пачек, номера уровня группы пачек, списка записей пачек в группе и хэш-значения всех перечисленных записей пачек;

g. после того как номера группы пачек были созданы, другая запись группы пачек создается, ссылающаяся на записи группы пачек (вместо записей пачек), и ей назначается номер уровня на один больше уровня перечисленных групп, в возрастающем иерархическом порядке;

h. непрерывно поддерживают хэш-значение верхнего уровня по мере накопления и группировки пачек;

i. специальным образом оставляют бюллетени незашифрованными за исключением

их SVN;

8. Способ по п. 6, при этом, после того как расхождение или расхождения идентифицированы, такие расхождения могут затем быть сообщены или запрошены избирательным органом, проверяющим органом, общественностью или их комбинацией.

9. Способ по п. 14, при этом с точно указанными или случайными интервалами программа-инспектор использует динамический алгоритм, чтобы модифицировать свои собственные хэш-значения после запуска, и сообщает внешнему серверу свои обнаружения и свое собственное повторно вычисленное хэш-значение.

10. Способ по п. 14, при этом каждое ядро на каждом сервере может предпринимать меры безопасности, содержащие:

периодическую выгрузку каждого файла бюллетеней в отдельное резервное хранилище, которое хранит все резервные копии до времени значительно позже выборов;

обнуление всей неиспользуемой памяти;

повторное вычисление хэш-значений операционной системы и исполняемого кода прикладной программы со случайными интервалами, чтобы верифицировать согласованность между серверами;

повторное вычисление, со случайными интервалами или заданными интервалами, всех хэш-значений бюллетеней; и

выгрузку программы проверки, размещаемой в упомянутом ядре, с удаленного сервера для проверки памяти ядра, динамической модификации упомянутой памяти программ, сообщения результатов аудита, повторного вычисления хэш-значений или их комбинации.

11. Способ по п. 14, при этом упомянутое ядро повторно шифрует все SVN и все хэш-значения бюллетеней и отправляет результирующий файл бюллетеней и файл итогов пачки списку независимых адресатов для верификации.