



РЕСПУБЛИКА КАЗАХСТАН

(19) KZ (13) U (11) 13191
(51) G07C 13/00 (2006.01)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ К ПАТЕНТУ

(21) 2026/1224.2

(22) 29.05.2026

(45) 23.10.2026, бюл. №42

(72) Киреева Анель Ахметовна; Урдабаев Марат Тагайбекович; Дигель Иван Евгеньевич

(73) Товарищество с ограниченной ответственностью «Университет Международного Бизнеса имени Кенжегали Сагадиева»

(74) Жангабылов Абай Токтарбекович

(56) US 2010017274 A1, 21.01.2010

(54) **БИОМЕТРИЧЕСКИЙ ТЕРМИНАЛ ДЛЯ ТАЙНОГО ГОЛОСОВАНИЯ ЧЛЕНОВ ДИССЕРТАЦИОННОГО СОВЕТА С ВЕРИФИЦИРУЕМЫМ БУМАЖНЫМ АУДИТОРСКИМ СЛЕДОМ**

(57) Полезная модель относится к области информационно-коммуникационных технологий, электронных систем голосования, точного приборостроения и средств автоматизации коллегальных процедур принятия решений, и предназначена для проведения процедуры тайного голосования в малых экспертных группах, преимущественно в диссертационных советах высших учебных заведений и научно-исследовательских организаций. Полезная модель объединяет технологии мультиспектральной биометрической идентификации, криптографические протоколы обеспечения анонимности на основе слепой подписи (Blind Signature), средства формирования верифицируемого бумажного аудиторского следа (Voter-Verified Paper Audit Trail, VVPAT), а также механизмы физической рандомизации бумажных носителей.

Задача полезной модели заключается в создании специализированного биометрического терминала для тайного голосования, обеспечивающего защиту анонимности участников в малых экспертных группах путем предотвращения подлога личности участника, исключения возможности сопоставления личности участника с бумажным носителем результатов голосования, обеспечения криптографического разрыва связи между

пользователем и сформированным бюллетенем, а также исключения внешнего сетевого воздействия на систему голосования.

Технический результат полезной модели заключается в обеспечении анонимности волеизъявления участников при одновременной биометрической верификации права голоса и формировании верифицируемого бумажного аудиторского следа за счет исключения возможности хронологического и пространственного сопоставления участников голосования и бумажных носителей результатов голосования при их хранении и ручном пересчете.

Предложен биометрический терминал для тайного голосования членов диссертационного совета с верифицируемым бумажным аудиторским следом, выполненный в виде переносного аппаратно-программного моноблока, содержащий корпус, внутри которого размещены блок управления, сенсорный экран, биометрический сканер, модуль печати бумажных носителей, автоматический резчик и накопитель для бумажных носителей, при этом внутри корпуса под выходным трактом автоматического резчика установлен пассивный накопитель-рандомизатор, содержащий канал сброса с размещенным в нем клиновидным рассекателем, выполненным с возможностью хаотичного отклонения падающих бумажных носителей для их пространственного перемешивания внутри накопителя, причем блок управления выполнен с возможностью реализации криптографического протокола слепой подписи для обеспечения разрыва связи между личностью пользователя и сформированным бюллетенем, биометрический сканер выполнен в виде мультиспектрального оптического датчика, снабженного функцией определения живой ткани, а блок управления выполнен на базе вычислительного модуля, физически лишенного интерфейсов беспроводной передачи данных для обеспечения работы терминала в режиме изолированной среды.

(19) KZ (13) U (11) 13191

Полезная модель относится к области информационно-коммуникационных технологий, электронных систем голосования, точного приборостроения и средств автоматизации коллегиальных процедур принятия решений, и предназначена для проведения процедуры тайного голосования в малых экспертных группах, преимущественно в диссертационных советах высших учебных заведений и научно-исследовательских организаций. Полезная модель объединяет технологии мультиспектральной биометрической идентификации, криптографические протоколы обеспечения анонимности на основе слепой подписи (Blind Signature), средства формирования верифицируемого бумажного аудиторского следа (Voter-Verified Paper Audit Trail, VVPAT), а также механизмы физической рандомизации бумажных носителей.

Известна система и метод голосования с возможностью проверки избирателями журнала аудита в режиме реального времени. Система голосования включает в себя как минимум один терминал для голосования, способный регистрировать большинство действий сотрудников избирательного участка и большинство действий избирателей, совершенных на этом терминале. Система голосования также включает в себя как минимум один принтер, подключенный к избирательному терминалу, который может печатать информацию о действиях сотрудников избирательного участка и действиях избирателей на непрерывном рулоне бумаги, чтобы в режиме реального времени создавать печатный журнал аудита по мере выполнения действий сотрудниками избирательного участка и действиями избирателей на избирательном терминале (US2006266829A1, 30.11.2006г.).

Недостатком системы является сохранение хронологической последовательности бумажных записей в накопителе, выполненном в виде непрерывного рулона или упорядоченного массива носителей. В условиях малых экспертных групп это позволяет сопоставить порядок подхода участников к терминалу с последовательностью размещения бумажных носителей, что создает риск деанонимизации результатов голосования и нарушения тайны волеизъявления.

Известен также электронный терминал для голосования, который использует биометрическое устройство ввода для проверки личности избирателя, использует устройство ввода данных для приема бюллетеня от избирателя и использует средство связи для передачи бюллетеня. Система голосования также включает в себя централизованный компьютер и базу данных регистрации избирателей (US2010017274A1, 21.01.2010г.).

Недостатком указанного устройства-прототипа является отсутствие средств формирования и хранения бумажных носителей результатов голосования, пригодных для независимого аудита, что не обеспечивает необходимый уровень

верифицируемости и доверия к результатам голосования в малых экспертных группах.

В условиях диссертационных советов, где порядок участия членов совета в процедуре голосования фактически может быть установлен или наблюдаем, сохранение последовательности размещения бумажных носителей позволяет сопоставить порядок голосования с конкретными участниками, что создает риск деанонимизации результатов голосования и нарушения принципа тайны волеизъявления.

В связи с этим существует техническая потребность в создании устройства, обеспечивающего не только верификацию результатов голосования посредством бумажного аудиторского следа, но и физическое исключение возможности установления связи между временем голосования участника и порядком хранения бумажных носителей.

Задача полезной модели заключается в создании специализированного биометрического терминала для тайного голосования, обеспечивающего защиту анонимности участников в малых экспертных группах путем предотвращения подлога личности участника, исключения возможности сопоставления личности участника с бумажным носителем результатов голосования, обеспечения криптографического разрыва связи между пользователем и сформированным бюллетенем, а также исключения внешнего сетевого воздействия на систему голосования.

Технический результат полезной модели заключается в обеспечении анонимности волеизъявления участников при одновременной биометрической верификации права голоса и формировании верифицируемого бумажного аудиторского следа за счет исключения возможности хронологического и пространственного сопоставления участников голосования и бумажных носителей результатов голосования при их хранении и ручном пересчете.

Указанный технический результат достигается тем, что предложен биометрический терминал для тайного голосования членов диссертационного совета с верифицируемым бумажным аудиторским следом, выполненный в виде переносного аппаратно-программного моноблока, содержащий корпус, внутри которого размещены блок управления, сенсорный экран, биометрический сканер, модуль печати бумажных носителей, автоматический резчик и накопитель для бумажных носителей, при этом внутри корпуса под выходным трактом автоматического резчика установлен пассивный накопитель-рандомизатор, содержащий канал сброса с размещенным в нем клиновидным рассекателем, выполненным с возможностью хаотичного отклонения падающих бумажных носителей для их пространственного перемешивания внутри накопителя, причем блок управления выполнен с возможностью реализации криптографического протокола слепой подписи для обеспечения разрыва связи между личностью пользователя и сформированным бюллетенем,

биометрический сканер выполнен в виде мультиспектрального оптического датчика, снабженного функцией определения живой ткани, а блок управления выполнен на базе вычислительного модуля, физически лишенного интерфейсов беспроводной передачи данных для обеспечения работы терминала в режиме изолированной среды.

В одном из вариантов выполнения корпус выполнен из ударопрочного непрозрачного материала, например ABS-пластика или алюминийевого композита, обеспечивающего электромагнитное экранирование.

В одном из вариантов выполнения корпус выполнен неразборным для пользователя и снабжен датчиками вскрытия, выполненными с возможностью инициирования стирания криптографических ключей при попытке физического взлома.

В одном из вариантов выполнения сенсорный экран снабжен фильтром конфиденциальности, выполненным на основе микро-жалюзийной структуры и ограничивающим угол визуального обзора экрана диапазоном не более 30 градусов от нормали к поверхности экрана.

В одном из вариантов выполнения терминал снабжен защищенным физическим интерфейсом ввода-вывода, выполненным с возможностью инициализации сессии голосования при наличии внешнего аппаратного ключа авторизации.

В одном из вариантов выполнения блок управления соединен с модулем энергонезависимой памяти, сконфигурированным в режиме однократной записи для ведения неизменяемого аудиторского журнала событий.

Сущность технического решения поясняется следующими графическими материалами.

На фигуре 1 показан общий вид терминала для тайного голосования.

На фигуре 2 показан схематичный разрез устройства в профиль (вид сбоку).

На фигуре 3 показана структурная схема блока управления.

Предлагаемая полезная модель не ограничивается приведенным вариантом исполнения, и конкретная реализация может изменяться в зависимости от конструктивных особенностей терминала, типа применяемого вычислительного модуля, средств биометрической идентификации и конфигурации механизма рандомизации бумажных носителей.

Далее полезная модель будет подробно раскрыта со ссылками на прилагаемые фигуры.

На прилагаемых фигурах приведены следующие обозначения: (101) – корпус; (102) – сенсорный экран; (103) – фильтр конфиденциальности; (104) – биометрический сканер; (105) – защищенный физический интерфейс ввода-вывода; (201) – модуль печати бумажных носителей; (202) – смотровое окно; (203) – автоматический резчик; (204) – канал сброса; (205) – клиновидный рассекатель; (206) – накопитель-рандомизатор; (301) – блок управления; (302) – защищенный криптографический элемент; (303) – аккумулятор; (304) – подсистема хранения данных.

Подробное описание работы и использования терминала.

Предлагаемая полезная модель представляет собой биометрический терминал для тайного голосования членов диссертационного совета с верифицируемым бумажным аудиторским следом, выполненный в виде переносного аппаратно-программного моноблока, обеспечивающего проведение процедуры голосования в изолированной среде с одновременным обеспечением биометрической идентификации участников, криптографической анонимизации бюллетеней и возможности последующего независимого аудита результатов голосования.

Функционирование терминала осуществляется в полуавтоматическом режиме с участием технического секретаря диссертационного совета и членов совета, принимающих участие в голосовании.

Как показано на фиг.1, терминал содержит корпус (101), внутри которого размещены сенсорный экран (102), фильтр конфиденциальности (103), биометрический сканер (104), защищенный физический интерфейс ввода-вывода (105), модуль печати бумажных носителей (201), смотровое окно (202), автоматический резчик (203) и накопитель-рандомизатор (206). На фиг.2 показана конструкция механизма хаотичного сброса бумажных носителей, включающая канал сброса (204), клиновидный рассекатель (205) и накопитель-рандомизатор (206).

Как показано на фиг.3, управление работой терминала осуществляется блоком управления (301), выполненным на базе вычислительного модуля. Для обеспечения математического разрыва связи «личность–голос» блок управления (301) снабжен выделенным защищенным криптографическим элементом (302), выполненным с возможностью реализации криптографического протокола слепой подписи, аккумулятором (303) и подсистемой хранения данных (304).

Перед началом процедуры голосования технический секретарь диссертационного совета формирует конфигурационный файл голосования на отдельной изолированной рабочей станции, не подключенной к сети Интернет. Указанный файл содержит сведения о составе членов совета, параметрах голосования, вопросах повестки дня и иных необходимых данных. Для обеспечения конфиденциальности биометрических данных участников конфигурационный файл содержит не графические изображения отпечатков пальцев, а необратимые криптографические представления биометрических шаблонов, например хеш-образы, сформированные с использованием алгоритма SHA-256.

Автономная работа терминала обеспечивается аккумулятором (303), выполненным, например, в виде литий-полимерного аккумулятора, обеспечивающего проведение продолжительной сессии голосования без подключения к внешней электросети. В одном из вариантов выполнения подсистема питания снабжена контроллером аварийного завершения работы, обеспечивающим

корректное завершение записи данных в подсистему хранения данных (304) при критическом снижении заряда аккумулятора либо при попытке физического отключения питания.

После формирования конфигурационного файла он записывается на защищенный внешний носитель данных, например USB-носитель, который подключается к защищенному физическому интерфейсу ввода-вывода (105) терминала. Для активации терминала технический секретарь использует внешний аппаратный ключ авторизации. После подключения ключа блок управления (301) выполняет проверку цифровой подписи конфигурационного файла, осуществляет загрузку

параметров голосования и переводит устройство в режим ожидания голосования.

Для исключения возможности удаленного вмешательства блок управления терминала выполнен на базе вычислительного модуля, физически лишенного интерфейсов беспроводной передачи данных, включая Wi-Fi, Bluetooth и GSM-модули. Обмен информацией с внешними устройствами осуществляется исключительно через физический интерфейс ввода-вывода (105), что обеспечивает работу терминала в режиме изолированной среды (Air-gapped) и исключает возможность сетевых атак. В таблице 1 указана рекомендуемая спецификация компонентов.

Таблица 1

Узел	Тип компонента / характеристики	Функциональное назначение
Вычислительное ядро	SoC (System on Chip), архитектура ARMv8 или выше, отсутствие Wi-Fi/Bluetooth модулей	Обработка логики голосования и выполнение криптографических операций
Биометрический модуль	Мультиспектральный сенсор (Multispectral Imaging), USB-интерфейс	Идентификация по отпечатку пальца с защитой от использования муляжей
Экран	Сенсорная панель 7–10 дюймов с фильтром конфиденциальности (Privacy Filter)	Ввод данных и ограничение обзора интерфейса для посторонних лиц
Модуль печати	Термопринтер с шириной ленты 58–80 мм и автоматическим резчиком (Auto-cutter)	Печать бумажного аудиторского следа (VVPAT)
Подсистема хранения данных	SD/eMMC в режиме WORM (Write Once Read Many)	Неизменяемое хранение журналов событий и результатов голосования
Подсистема питания	Li-Po аккумулятор емкостью не менее 10000 mAh	Обеспечение автономной работы терминала

Корпус (101) терминала выполнен из ударопрочного непрозрачного материала, например ABS-пластика или алюминиевого композита, обеспечивающего электромагнитное экранирование внутренних электронных компонентов. В одном из вариантов выполнения корпус выполнен неразборным для пользователя и снабжен датчиками вскрытия, выполненными с возможностью инициирования удаления криптографических ключей при попытке физического несанкционированного доступа к внутренним компонентам устройства.

Для защиты визуальной информации сенсорный экран (102) снабжен фильтром конфиденциальности (103), выполненным на основе микро-жалюзийной структуры. Конструкция фильтра обеспечивает ограничение угла визуального обзора экрана диапазоном не более 30 градусов от нормали к поверхности экрана, вследствие чего информация на дисплее остается видимой только непосредственно пользователю, осуществляющему голосование.

После перехода терминала в рабочий режим член диссертационного совета подходит к устройству и проходит процедуру биометрической

аутентификации посредством биометрического сканера (104). В одном из вариантов выполнения биометрический сканер представляет собой мультиспектральный оптический датчик, обеспечивающий получение изображения как поверхности кожи, так и подповерхностных структур, включая капиллярный рисунок, что позволяет реализовать функцию определения живой ткани и исключить возможность использования муляжей или поддельных отпечатков.

После успешного подтверждения права голоса блок управления (301) формирует анонимизированный бюллетень с использованием криптографического протокола слепой подписи (Blind Signature). На первом этапе формируется электронный бюллетень В. Далее бюллетень подвергается криптографической анонимизации посредством случайного множителя R. После этого система выполняет проверку права голоса участника и подписывает анонимизированный бюллетень без раскрытия его содержимого внутри системных журналов. В результате формируется валидный бюллетень, не содержащий криптографически

устанавливаемой связи с идентификатором пользователя.

Программная архитектура блока управления (301) реализует принцип изолированной программной среды, при котором процессы обработки биометрических данных и процессы формирования бюллетеня разделены друг от друга на уровне ядра операционной системы. Передача информации между указанными процессами осуществляется через однонаправленный буфер обмена без сохранения метаданных. После подтверждения права голоса оперативная память, содержащая биометрические данные пользователя, подвергается принудительной очистке до момента отображения интерфейса голосования следующему участнику.

После завершения биометрической аутентификации участнику отображается интерфейс голосования на сенсорном экране (102), посредством которого пользователь осуществляет выбор варианта голосования. После подтверждения выбора блок управления (301) передает данные в модуль печати бумажных носителей (201), который формирует бумажный аудиторский след (VVPAT).

Как показано на фиг.2, бумажный носитель после печати перемещается через автоматический резчик (203) в канал сброса (204). Участник голосования может визуально проверить корректность напечатанного результата через смотровое окно (202), расположенное на передней части терминала.

После подтверждения пользователем правильности отображенного результата автоматический резчик (203) отделяет бумажный носитель, который под действием силы тяжести поступает в канал сброса (204) и взаимодействует с клиновидным рассекателем (205). Рассекатель (205) расположен непосредственно под выходным трактом автоматического резчика и выполнен с возможностью хаотичного отклонения падающих бумажных носителей от вертикальной оси падения.

За счет взаимодействия бумажного носителя с поверхностями клиновидного рассекателя (205) каждый бумажный носитель получает случайное направление движения и падает в различные области накопителя-рандомизатора (206). Дополнительно хаотичность распределения обеспечивается соотношением размеров накопителя и бумажных носителей, при котором площадь горизонтального сечения накопителя превышает площадь единичного бумажного носителя не менее чем в 2,5 раза.

Вследствие указанной конструкции внутри накопителя-рандомизатора (206) формируется пространственно перемешанный массив бумажных носителей, не сохраняющий последовательность голосования участников. Это исключает возможность установления соответствия между временем голосования конкретного участника и положением соответствующего бумажного носителя внутри накопителя даже при последующем ручном пересчете.

После подтверждения пользователем результата голосования цифровой голос сохраняется в подсистеме хранения данных (304), соединенной с

блоком управления (301). Для обеспечения юридической значимости результатов голосования и соответствия требованиям аудита подсистема хранения данных (304) выполнена в режиме «Однократная запись – многократное чтение» (Write Once Read Many – WORM), исключающем возможность изменения ранее записанных данных.

В одном из вариантов выполнения подсистема хранения данных (304), выполненная в режиме WORM, реализуется посредством использования промышленных SD/microSD-карт с физически заблокированной возможностью перезаписи ранее записанных секторов памяти. В другом варианте выполнения файловая система раздела, содержащего журнал голосования, автоматически переводится в режим read-only после записи очередного блока данных.

Дополнительно каждая новая запись журнала содержит криптографический хеш предыдущей записи, формируя цепочку взаимосвязанных блоков данных. Благодаря этому любое несанкционированное изменение или удаление информации приводит к нарушению математической целостности цепочки и может быть выявлено при проверке цифровой подписи итогового протокола.

По завершении процедуры голосования технический секретарь повторно использует аппаратный ключ авторизации для закрытия сессии голосования. После завершения голосования блок управления (301) осуществляет финализацию цепочки блоков данных, формирует итоговый протокол голосования, подписывает его закрытым криптографическим ключом устройства и записывает зашифрованный файл результатов на внешний носитель данных.

Передача результатов голосования осуществляется путем физического переноса носителя данных на отдельный мастер-компьютер, предназначенный для расшифровки и подсчета итогов голосования. Отсутствие сетевого взаимодействия между терминалом и внешними вычислительными устройствами обеспечивает физический разрыв возможных каналов удаленного сетевого воздействия.

В случае возникновения сомнений в достоверности цифровых результатов производится вскрытие накопителя-рандомизатора (206) и извлечение бумажных носителей для ручного пересчета. Благодаря хаотичному пространственному перемешиванию бумажных носителей внутри накопителя отсутствует возможность сопоставления порядка извлечения бумажных носителей с последовательностью голосования участников, вследствие чего сохраняется анонимность волеизъявления членов диссертационного совета даже при проведении физического аудита результатов голосования.

Таким образом, предлагаемая полезная модель обеспечивает проведение процедуры тайного голосования с одновременным обеспечением биометрической идентификации участников, криптографической анонимизации бюллетеней,

защиты от внешнего вмешательства и формирования верифицируемого бумажного аудиторского следа, при этом конструкция накопителя-рандомизатора исключает возможность установления связи между личностью участника и соответствующим бумажным носителем даже при последующем ручном пересчете результатов голосования.

ФОРМУЛА ПОЛЕЗНОЙ МОДЕЛИ

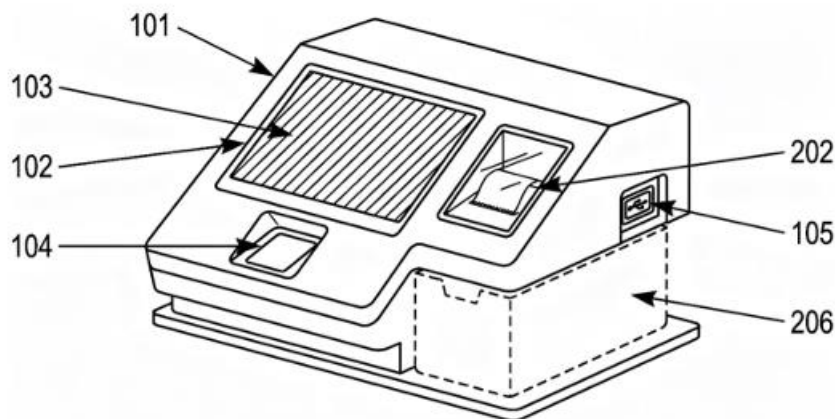
1. Биометрический терминал для тайного голосования членов диссертационного совета с верифицируемым бумажным аудиторским следом, включающий корпус, сенсорный экран, биометрический сканер и блок управления, **отличающийся** тем, что терминал выполнен в виде переносного аппаратно-программного моноблока, внутри корпуса которого размещены модуль печати бумажных носителей, смотровое окно, автоматический резчик и накопитель для бумажных носителей, при этом внутри корпуса под выходным трактом автоматического резчика установлен пассивный накопитель-рандомизатор, содержащий канал сброса с размещенным в нем клиновидным рассекателем, выполненным с возможностью хаотичного отклонения падающих бумажных носителей для их пространственного перемешивания внутри накопителя, причем блок управления снабжен защищенным криптографическим элементом, выполненным с возможностью реализации криптографического протокола слепой подписи, аккумулятором и подсистемой хранения данных, биометрический

сканер выполнен в виде мультиспектрального оптического датчика, снабженного функцией определения живой ткани, а блок управления выполнен на базе вычислительного модуля, физически лишенного интерфейсов беспроводной передачи данных, при этом блок управления соединен с модулем энергонезависимой памяти, сконфигурированным в режиме однократной записи для ведения неизменяемого аудиторского журнала событий, а сенсорный экран снабжен фильтром конфиденциальности, выполненным на основе микро-жалюзийной структуры и ограничивающим угол визуального обзора экрана диапазоном не более 30 градусов от нормали к поверхности экрана.

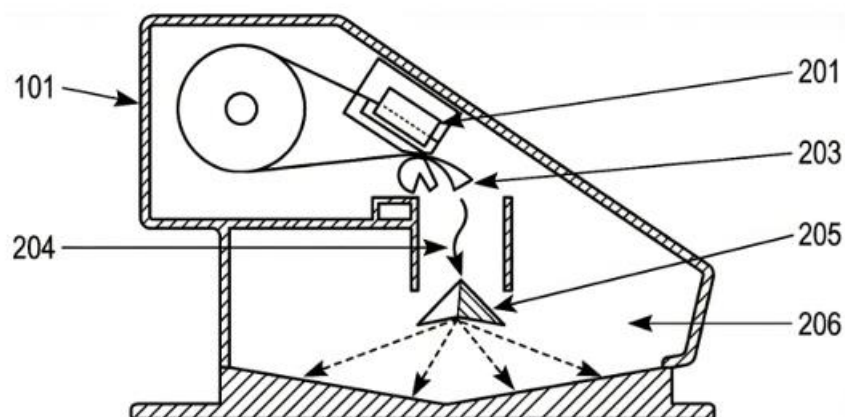
2. Биометрический терминал по п.1, **отличающийся** тем, что корпус выполнен из ударопрочного непрозрачного материала, например ABS-пластика или алюминиевого композита, обеспечивающего электромагнитное экранирование.

3. Биометрический терминал по п.1, **отличающийся** тем, что корпус выполнен неразборным для пользователя и снабжен датчиками вскрытия, выполненными с возможностью инициирования стирания криптографических ключей при попытке физического взлома.

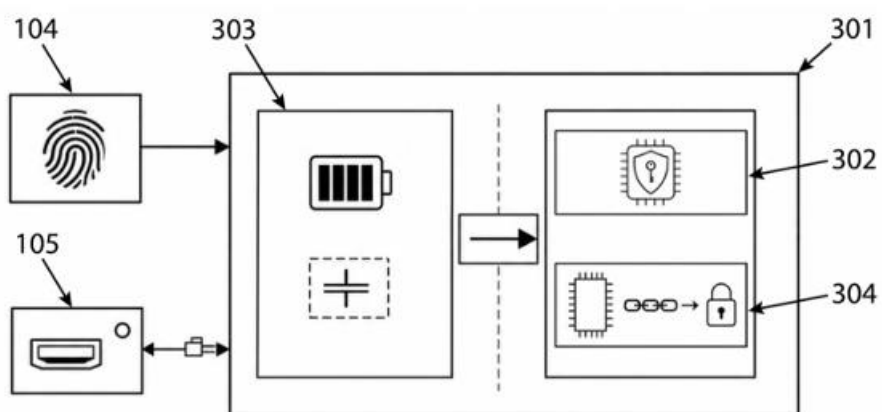
4. Биометрический терминал по п.1, **отличающийся** тем, что терминал снабжен защищенным физическим интерфейсом ввода-вывода, выполненным с возможностью инициализации сессии голосования при наличии внешнего аппаратного ключа авторизации.



ФИГУРА 1



ФИГУРА 2



ФИГУРА 3