

От 29.06.22 г. № 29/06-001

г. Москва

Академику РАЕН

Лисичкину В. А.

## ДОКЛАД

Лучшие и самые распространенные решения и продукты все появлялись на стыке самых передовых технологий и критически важных сфер жизни человека, чтобы обеспечить еще больший уровень комфорта и безопасности. В связи с этим на рассмотрение экспертного совета предлагаем уникальный продукт «ГазДома». Продукт «ГазДома» представляет собой симбиоз уникальных инновационных технологий в сфере информационных технологий, таких как децентрализованное хранение и распределенное принятие решения, уникальные криптографические алгоритмы и многослойные цифровые сети позволяют обеспечить наивысший уровень безопасности хранения и обработки информации. Также обеспечивают максимально возможный уровень защиты от умышленного повреждения и изменения данных на всех этапах работы с ними (формирование, отправка, получение, обработка и сохранение). Автономное устройство представляет собой совокупность газоанализатора, запорной арматуры, аналитического и криптографического модулей. Совместное использование которых позволяет обеспечить высочайший уровень безопасности формирования исходных данных, путем использования передовых криптографических алгоритмов; новейшие алгоритмы анализа позволяют обеспечивать достаточную скорость анализа данных по превышению ПДК (предельно допустимой концентрации) газа и оперативно, используя децентрализованную сеть хранилищ, принимать решение о последующих действиях; использование компонентной российской базы позволяет минимизировать риски с любыми ограничениями, накладываемыми третьими странами. Использование новейших технологий в обработке сигналов и использование российской компонентной базы позволили обеспечить оптимальное потребление электричества и таким образом обеспечить автономность работы устройства от 6 месяцев до года без необходимости подключения к сети 220В. Продукт «ГазДома» состоит из нескольких компонентов, способных работать в автономном режиме и объединенных единым децентрализованным хранилищем: 1. Рекурсивное децентрализованное хранилище с функционалом распределенного принятия решений, валидирования и верифицирования поступающей информации (минимизирует возможность подмены данных, их исправления и уничтожения) 2. Узел децентрализованной сети, объединение которых образует одноранговую сеть. Для увеличения скорости работы используется UDP протокол передачи данных, для исключения возможности потери пакетов данных используется запатентованный алгоритм UDP с подтверждением доставки (автор Бутяев Е. А.). Также каждый узел обеспечивает возможность получения внешних данных их первичной верификации. Так как все узлы представляют собой одноранговую сеть, то можно подключиться к любому узлу сети и отправить данные в сеть для их анализа

и сохранения, что обеспечивает высочайший уровень отказоустойчивости и минимизации аварийных сценариев отключения, что очень важно в критически важных сферах жизнедеятельности человека. 3. Платформа диспетчеризации, которая обеспечивает оперативное информирование контролирующих организаций о текущих показателях вверенных им устройств/адресов. 4. Пользовательское мобильное приложение, информирующее пользователя о текущем состоянии устройства, путем представления оперативных данных с него, также обеспечивает возможность интерактивного управления газозапорной арматурой. При необходимости платформа способна обрабатывать любые данные поступающие с устройств, интегрированных с решением. Общий принцип работы и используемые технологии: 1. Устройство, с интегрируемым SIM модулем устанавливается в помещении, где необходимо контролировать окружающую среду на ПДК газа. Использование SIM модуля позволяет обеспечить оперативность поступающих данных при минимизации проводов и расходов на их обслуживание. Так как объем данных, отправляемых за один запрос минимален ( от 56 до 87 байт) то для работы устройства подойдет любой стандарт сотовой сети от GPRS до современных 4G/LTE и даже 5G. 2. После установки и запуска устройства сбора показателя загазованности окружающей воздушной смеси в долях, датчик начинает с заданной периодичностью «нюхать» воздух и преобразовывать полученные значения в цифровые данные. 3. После формирования цифровых данных по концентрации в долях запускается модуль аналитики на устройстве. Данный модуль содержит алгоритм анализа и принятия локального решения. В случае если критический порог превышен - то отправляется электрический сигнал на газозапорную арматуру с целью перекрытия доступа газа, параллельно с этим процессом запускается процесс отправки данных в сеть с целью сохранения информации об инциденте (Alarm) в системе для последующего анализа в модуле диспетчеризации. В случае если превышения ПДК газа не обнаружено - в сеть сохраняются текущие показатели с целью сохранения исторических данных для последующего отображения и анализа в диспетчерском контроле. Запрос на сохранение данных использует протокол HTTPS и отправляется по TCP/IP. Запрос представляет собой набор данных, состоящий из данных по показателям концентрации CO<sub>2</sub>, CH<sub>4</sub> и показателям состояния аккумулятора (остаточный заряд), также содержит ЭЦП, сформированную на основе алгоритма ED25519 по результату работы характеристической функции Blake2b (получение хэша) на основе набора выше перечисленных данных. Алгоритм Blake2b обеспечивает высокую производительность при работе с большим набором данных, также он обеспечивает минимально возможный набор коллизий на схожем наборе данных. Алгоритм ED25519 позволяет сформировать уникальный набор ключей и обеспечить неподдельную ЭЦП при использовании эллиптических кривых в совокупности с алгоритмом SHA-512. 4. После поступления запроса на один из узлов сети начинается первичная валидация данных на их неизменность, путем проверки ЭЦП отправителя и хэша по предоставленным данным. В случае если проверка пройдена - данные помещаются для валидирования возможности сохранения и непосредственно записи в исторический массив данных. 5. В процессе принятия решения участвуют более 6-ти узлов сети, что позволяет избежать неправомерного сохранения данных, также минимизировать возможность атаки 51. Алгоритм совместного принятия решения соответствует “алгоритму византийских генералов”. 6. После подтверждения возможности сохранения данных, данные распределяются по всем узлам сети и обеспечивают полное и нативное сохранение данных с возможностью проверки и восстановления всего набора информации, размещенного в сети. 7. Модуль

диспетчеризации, используя интерактивные компоненты работы с пользовательскими интерфейсами (React/VUE), обеспечивает оперативное получение обновления данных из децентрализованного хранилища путем сбора данных по связанным с диспетчером устройствам и анализу сохраненных транзакций. Хранение транзакций в хранилище происходит в пределах хранилища Key=Value, где ключом является идентификатор рекурсивного блока информации, а в значение помещается информация о размещенной транзакции со всеми параметрами и данными. Данный подход позволяет обеспечить высокую скорость чтения (до 679349 транзакций в сек) и записи (до 790393 транзакций в сек) с одного узла. Сам модуль обеспечивает применимость высокоэффективной ролевой модели обеспечивающей разделение функциональных возможностей между ОКС (основной квартиросъемщик), управляющими компаниями (или другими обслуживающими организациями), контролирующими организациями (или аудиторами), а также администраторами системы. 8. Пользовательский модуль представляет собой пользовательский интерфейс (мобильное приложение), предоставляющее ОКС полную информацию о текущем состоянии устройства. Данные предоставляются оперативно (в случае если включено постоянно обновление данных), либо по требованию, в случае если необходимо минимизировать количество обращений к системе хранения информации. Приложение разрабатывается с использованием кроссплатформенных технологий (ReactNative). Данный набор технологий, алгоритмов и модулей в совокупности с приведенной выше последовательностью работы позволяет обеспечить уникальные показатели по безопасности и по оперативности представления и сохранения данных. Это полностью российская разработка, не имеющая аналогов в мире.

Авторами данной разработки являются (Грачев А. С., Шушунов А. А., Бутяев Е. А., Никулин К. М., Измайлов В. Ю.). Производство по изготовлению данного технологического оборудования расположено в Волгоградской области. На 01.07.2022 г. установлено 1000 штук приборов.

Предприятие технического обслуживания находится в г. Москва - ООО "КА" ЭкоУм", Генеральный директор А.С. Грачев.

С уважением,

Генеральный директор

ООО «КА «ЭкоУм»

Грачев А. С.

Исполнитель Быкова Я. О.

+79661718254

