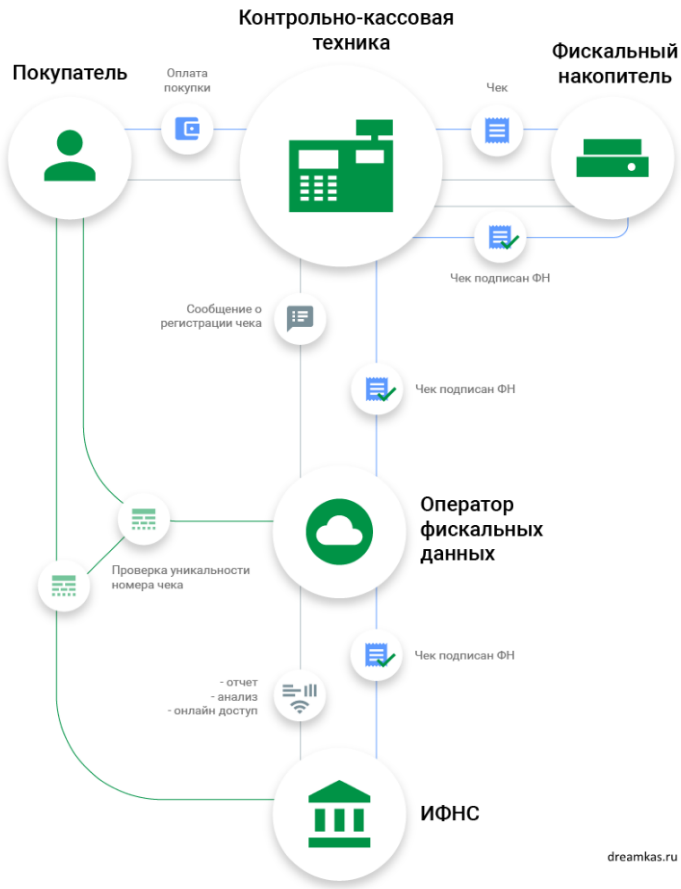
Проект по работе с фискальными данными

В современном мире постоянно оптимизируются средства связи хранения и обработки информации, что приводит к постоянному улучшению и упрощению систем учета и представления данных.

Современные системы и платформы научились быстро и красиво хранить данные, но это достигается компромиссом с безопасностью и доступностью этих самых данных и зачастую для достижения желаемого эффекта увеличивают количество используемых модулей, что приводит к снижению уровня отказоустойчивости. Это обусловлено тем, что при добавлении каждого модуля/компонента происходит постоянно чтение и запись в собственное хранилище, а также передача критически важной информации между модулями, что приводит к появлению уязвимых мест.

Цель и задача данного проекта - создать такое решение, которое бы позволило минимизировать кол-во используемых модулей/компонентов при выполнении того же функционала и при этом повысить отказоустойчивость и безопасность системы и данных в целом.



Общее представление системы выглядит так:

В текущей реализации данные хранятся в инфраструктуре ОФД (оператора фискальных данных), а вход (точка передачи) данных и запросов всегда один. Также в инфраструктуре ИФНС отсутствует дублирующее хранилище данных и поэтому при работе с данными пропускной канал и точка входа являются узким горлышком системы. Также в случае если злоумышленник захочет нанести вред противоправными действиями - то достаточно закупорить данное горлышко, как весь учет и фиксация перестанут работать. Для данной атаки достаточно использовать DDoS атаки на точку входа. Таким

образом мы имеем систему, которая при превышении критического числа запросов начнет захлебываться. Также существует риск перехвата всех входящих и исходящих запросов в точке входа путем прослушивания трафика. В случае если злоумышленник или не добросовестный администратор/пользователь ОФД/ИФНС попытается изменить и скомпрометировать данные - ему это удасться, также при должном уровне ИТ подготовки в сфере работы с БД и файловой системой можно скрыть свои следы присутствия.

Что предлагает проект:
Обеспечить хранение данных по средствам рекурсивно связанных блоков в пределах, которых размещается информация - данное решение обеспечивает неизменность данных, размещенных ранее и также валидация и верификация вновь размещаемых данных. Само хранилище представляет собой полностью распределенную инфраструктуру, состоящую из одноранговых узлов, в пределах каждого из которых происходит полное дублирование данных, сохраняемых в сети. Также каждый узел имеет свою собственную точку входа (API), что обеспечивает максимально широкий канал для передачи информации путем приема данных любым узлом сети и размещение этих данных в блоке принятия решения. Блок принятия решения представляет собой децентрализованную структуру, состоящую из тех же самых узлов сети. Принятие решения о подтверждении данных и сохранении их в хранилище происходит путем совместного голосования и подтверждения данных. Таким образом мы предлагаем разместить одноранговые узлы не только на ландшафте ОФД, но и на ландшафте ИФНС и аудиторов, что позволит минимизировать нагрузку на ресурсы и максимизировать распределение данных. Данных подход обеспечивает высокий уровень отказоустойчивости и минимизирует возможность остановки системы из-за блокирования одного из узлов сети. Также используя единую систему децентрализованных узлов можно обеспечить полностью распределенный доступ к наборам данных и в случае даже если злоумышленник получит доступ к одному узлу - то кто и где пользуется данными на других узлах он узнать не сможет. Сами узлы могут находится за фаерволами и работают они по конкретным открытым портами и каждый из полученных запросов и наборов данных тщательно проверяется и в случае если обнаружено даже малейшее отклонение от стандарта или попытка подделки данных - то запрос отклоняется. В случае если злоумышленник хочет провести DDoS атаку на ресурсы - ему необходимо атаковать сразу всю сеть а для этого необходимо пропорционально увеличить кол-во ресурсов, задействованных в атаке. Также данный подход обеспечивает простое восстановление данных в случае их аварийной потери/уничтожении. Минимизируется необходимость постоянного бэкапирования. А используя подход приватной сети с возможностью представления ограниченного набора данных в публичное представление мы минимизируем возможность получения данных сторонними пользователями. Многий функционал, используемый как отдельные модули системы (например проверка уникальности номера чека, регистрация чека, подписание чека…) - это уже встроенный механизм децентрализованной сети предлагаемой проектом.