Смена эпох и смена подходов к поставкам энергоресурсов

Сергей Головешко
к.т.н., заместитель начальника департамента разработок ГК «Астра Линукс»

Юрий Коровин
директор ООО «Рустехнология»

Сегодня, на заре эпохи всеобщей цифровизации, стали выявляться новые внешние риски, о которых еще вчера мы вряд ли задумывались: возникла необходимость смены подходов к технологии обслуживания абонентов — потребителей энергоресурсов и смены парадигмы организации средств сбора и хранения информации о потреблении ресурсов. Что же произошло?

Новые подходы к обслуживанию абонентов в цифровую эпоху

В цифровую эпоху автоматизация процессов достигает абонента на дому и в пути. «Умный» дом и «умный» смартфон делают контроль со стороны абонента тотальным, но и у поставщиков ресурсов и услуг появляется механизм контроля потребления. Потребление становится оптимальным, а расчет за потребленную услугу — обязательным. Но данную концепцию еще необходимо реализовать.

Ранее разработчики строили сервера сбора информации с приборов учета, используя понятие максимальной нагрузки. Тем самым система могла принимать только ограниченное количество запросов. Компания «Рустехнология» применила характерный для интернета подход, заявив механизмы балансировки нагрузки. То есть запрос на обработку сведений от прибора учета сначала попадает в балансировщик, а тот, зная загруженность компьютеров, участвующих в обработке, принимает решение кому перенаправить запрос.

Тем самым компания добилась отсутствия отказов от обслуживания. Так передаются сведения о потреблении ресурсов от индивидуального прибора учета в сервис приема сведений и взаимодействия с базой данных.

При этом прибор учета может только по шифрованному каналу, предоставленному провайдером, передавать показания, а не команды. Канал взаимодействия с базой данных извне не доступен.

Компания «Рустехнология» построила конфигурацию для СУБД такой системы. Она поддерживает отказоустойчивость, кластеризацию и автоматизированное построение резервных копий базы данных по расписанию. На рис. 1 изображена концепция сервиса сбора информации.

В рамках этого подхода реализован механизм «домашнего кабинета» для работы с абонентом через мобильное или web-приложение, находящиеся в отдельном промежуточном слое. Информация в «кабинете» отражается из той же базы данных.

Ресурсоснабжающие организации и «управляющие» компании имеют доступ и могут получить любой анализ, отчет и т.д. из среза той же базы данных.

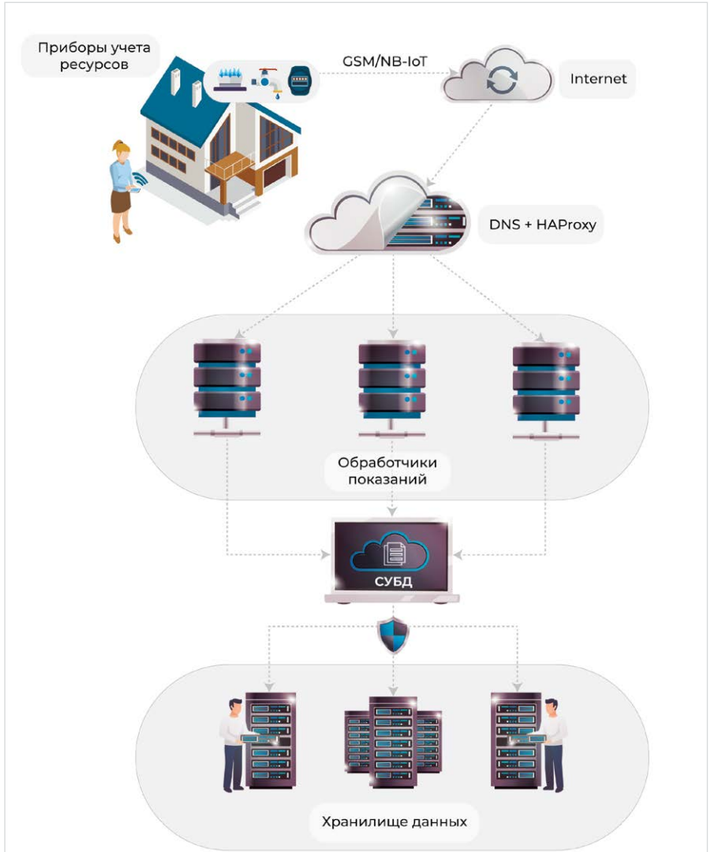

Рис.1 — концепция сервиса сбора информации.

Информационная война и методы защиты от ее влияния

США и Великобритания развязали информационную войну, связанную с недобросовестной конкуренцией, навязанной ими в поставках газа. Под угрозой оказываются не только оптовые поставки природного газа в Европу, но и все внутренние поставки, как фактор влияния. Сегодня, используя всевозможные закладки под угрозой находятся практически все технологические цепочки, при этом даже локализация ресурсов может не спасти от атак «партнеров».

Возникает риторический вопрос: «Что делать?». Наше правительство уже ответило на этот вопрос: «Панацея — импортозамещение!» Но среди специалистов по информационным технологиям все равно слышен ропот. Он связан с применением в технологических цепочках системного программного обеспечения, разработанного в США и других странах «партнерах». Да, прикладное ПО — родное, но управляется оно чужой операционной системой (ОС), чужой системой управления базами данных (СУБД) и другими базовыми продуктами «опасного» происхождения. Уйти от этого можно только одним путем — перейти на сертифицированную как средство технической защиты информации операционную систему и связанную с нею продукцию (к примеру, СУБД). Возможно, этот переход сузит возможности прикладных систем, а в определенных вопросах — расширит. Применение средств криптозащиты информации в сочетании с технической защитой серверов и созданием доверенных защищенных зон передачи информации позволяет надеяться на бесперебойность работы сервисов.

Чем из арсенала современных технологических подходов можно подкрепить надежду на победу в развязанном противостоянии?

Ключ к успеху — применение технологии мандатного и дискреционного разграничений доступа и применение контроля целостности. Но изюминка решения данной проблемы в том, что эти технологии реализуются кодом, разработанным в АНБ США. Тем самым мы опять попадаем в зависимость и уязвимы?

Компания «Рустехнология» провела исследование отечественного рынка программного обеспечения и выявила, что данная проблема решена в продуктах ГК «Астра Линукс». Проведена беспрецедентная работа по реализации и сертификации продуктов с реализацией упомянутых технологий для систем, удовлетворяющих требованиям по обработке государственной тайны. Применение данной линейки продуктов с успехом защитит системы от различных происков.

Компания «Рустехнология» приобрела компетенции в применении упомянутых технологий и реализовала систему сбора основываясь на них.

Безопасная архитектура системы сбора информации о потреблении ресурсов

Более конкретное описание для специалистов-компьютерщиков выглядит примерно так. Как мы уже отмечали, реализация сервисов сбора информации осуществляется, базируясь на отечественной операционной системе Astra Linux Special Edition, задействуя настройки DNS и HAProxy. В балансировку включаются сервера с Astra Linux Special Edition (ALSE) и установленное средство семантического разбора сообщений от приборов учета. Данное средство реализовано на C и содержит обращения через отдельный сетевой интерфейс к СУБД Postgres Pro Enterprise, входящей в поставку ALSE. Postgres Pro Enterprise конфигурируется как кластерная система, обладающая отказоустойчивостью и поддерживаемая средствами резервного копирования.

В качестве средств ведения «кабинета» абонента построено промежуточное ПО для взаимодействия мобильного приложения и СУБД. Подобным образом организован web-интерфейс поставщика ресурсов и услуг.

Данная схема выглядит достаточно громоздко и нуждается в средствах оптимизации инфраструктуры, администрирования и управления. За решение задач безопасности, оптимизации и управляемости отвечает программный комплекс средств виртуализации ПКСВ «Брест» (ALSE), который дает возможность развернуть систему сбора информации о потреблении ресурсов с приборов индивидуального учета потребления по каналам связи с замечательной масштабируемостью. Управление инфраструктурой осуществляется средствами OpenNebula, при этом настраивается отказоустойчивость, балансировка нагрузки, масштабируемость, высокая доступность.

Как ни странно, многие из поставщиков ресурсов до настоящего времени используют решения в основе которых лежат «опасные» операционные системы, управляемые из Вашингтона или Сан-Франциско. В них, к примеру, задействуются многие непромышленные решения (к примеру, СУБД FireBird). Производители утверждают, что все, что сделано, полностью подконтрольно. Но системные компоненты данных решений подлежат импортозамещению, а значит, сами решения остаются в неработоспособном состоянии и не поддаются сертификации безопасности промышленных систем.

Решения, реализованные компанией «Рустехнология», могут быть развернуты как на вычислительных ресурсах заказчиков, так и поставляться на серверных ресурсах разработчика, и являются на 100% отечественной разработкой. ООО «РусТехнология» имеет все предпосылки для внедрения технологической линейки в ЦОДы предприятий осуществляющих поставки ресурсов потребителям. Решение успешно интегрировано в линейку продуктов ГК «Астра Линукс».

Решения «Рустехнология»	Другие системы
1. Разработка системы	
технологически сложная разработка	быстрая разработка с использованием широкого спектра компонентов и модулей
2. Внедрение системы	
быстрое внедрение	быстрое внедрение
3. Наращивание	
наращивание системы сбора происходит без затрат на программирование, увеличение количества приборов учета не приводит к реинжинирингу всей системы	сложное наращивание, увеличение количества приборов учета приводит к сбоям и потере информации
4. Сертификация по безопасности промышленных систем	
быстрая сертификация (СУБД и ОС уже сертифицированы)	невозможность сертификации
5. Криптозащита	
поддерживается	поддерживается
6. Защита персональных данных	
поддерживается защита персональных данных	не поддерживается защита персональных данных
7. Масштабирование	
реализовано в рамках города-региона-страны-мира	невозможно
8. Импортозамещение	
100% импортозамещение	частично, только прикладное ПО
9. Модификация системы под новые требования и задачи, согласно п.1 – п.8	
возможна разработка дополнительных модулей	невозможна, требуется выбор новой платформы и новая разработка

Таб.1 — Основные этапы разработки и внедрения системы сбора информации о расходе энергоресурсов.