Вадим Дрошнев — заместитель главного инженера по автоматизации и метрологическому обеспечению ООО «Газпром добыча Оренбург»

Игорь Кириллов — начальник производственного отдела автоматизации ООО «Газпром добыча Оренбург»

Владислав Фарафонтов — заместитель начальника производственного отдела автоматизации ООО «Газпром добыча Оренбург»

Антон Пальгов — начальник отдела перспективных разработок Управления комплексных проектов ПАО «Газпром автоматизация»

Алексей Власенко — ведущий менеджер продуктов ИнфоТеКС

Защищенный IoT на труднодоступных активах

как встраиваемая криптография и LoRa меняют подход к мониторингу скважин на примере Оренбургского нефтегазоконденсатного месторождения

В нефтегазовой отрасли России остро стоит вопрос мониторинга фонда скважин с длительной историей разработки. Объекты, введенные в эксплуатацию десятилетия назад, часто не имеют ни систем автоматизации, ни линий электропередачи. Классические решения телеметрии из-за отсутствия ЛЭП неприменимы, в результате контроль за работой удаленных объектов ведётся выездными бригадами. Это в свою очередь влечёт высокие эксплуатационные расходы, задержки в поиске нарушений и потенциальные потери добычи.

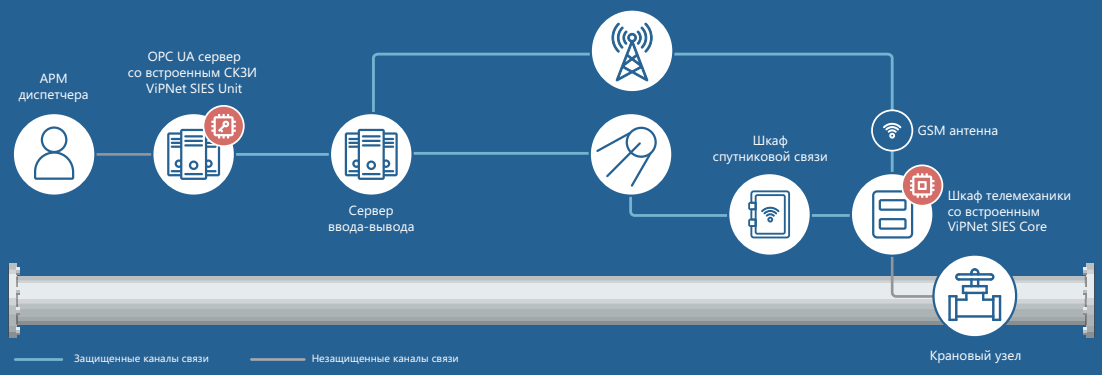
Перед отраслью встала задача: как организовать надежный контроль технологических параметров работы оборудования (давление, температура, загазованность и др.) на удаленных точках при минимальном энергопотреблении и при этом гарантировать безопасность передаваемых данных? Решение, успешно апробированное на объекте с длительной историей разработки, предложили специалисты ГК «ИнфоТеКС» совместно с партнерами из дочерних обществ ПАО «Газпром». В основе подхода — использование локальных энергонезависимых систем телеметрии и передовых встраиваемых средств криптографической защиты информации (СКЗИ).

ПРОБЛЕМЫ АВТОМАТИЗАЦИИ НА ЗРЕЛЫХ МЕСТОРОЖДЕНИЯХ

Эксплуатация месторождений с многолетней историей, к числу которых относится, к примеру, Оренбургское нефтегазоконденсатное месторождение (ОНГКМ), сопровождается серьезными вызовами в области контроля технологических процессов. Значительная часть российского скважинного фонда изначально не была оснащена современными системами автоматизации. Усугубляет ситуацию и отсутствие линий электропередачи на удаленных объектах, что делает невозможным применение стандартных проводных систем телеметрии. Как следствие, обслуживание таких скважин требует регулярных объездов, что влечет за собой высокие трудозатраты и увеличивает время реагирования на инциденты.

По результатам анализа ситуации специалисты ПАО «Газпром» определили: эффективным направлением решения данных сложностей является внедрение энергонезависимого комплекса телеметрии. Для передачи данных на расстояния, превышающие 10 километров, хорошо подходит технология дальней радиосвязи LoRa, которая сочетает низкое энергопотребление с высокой помехоустойчивостью. Однако передача критически важной информации о параметрах работы скважин по открытым беспроводным каналам требует строгого соблюдения требований конфиденциальности и целостности данных, установленных как государственными регуляторами, так и отраслевыми стандартами. Традиционные наложенные средства криптографической защиты информации (СКЗИ) в данном случае неприменимы из-за отсутствия совместимости с технологией LoRa, крупных габаритов и высокого уровня энергопотребления, не соответствующих концепции автономного устройства.

В связи с этим целью исследования стала разработка и апробация подхода к обеспечению информационной безопасности в энергонезависимых системах телеметрии на базе LoRa с использованием специализированных встраиваемых СКЗИ.

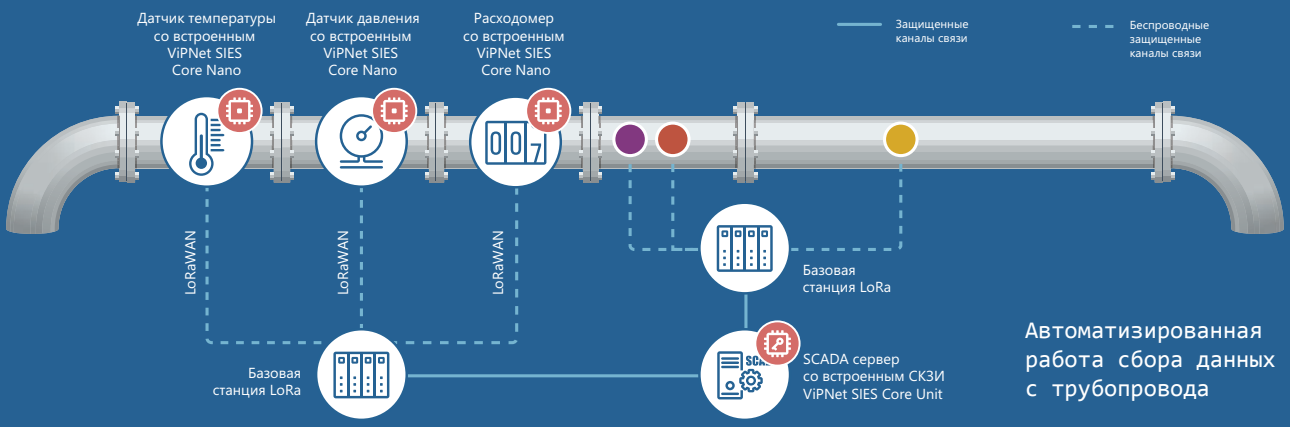


Система телеметрического контроля и телемеханизации

АРХИТЕКТУРА АВТОНОМНОЙ СИСТЕМЫ МОНИТОРИНГА

Предлагаемое решение включает в себя сеть телеметрических устройств, устанавливаемых непосредственно на скважинах. Каждое устройство включает в себя несколько ключевых компонентов. В его состав входят датчики для контроля технологических показателей (температуры, давления, уровня загазованности), микроконтроллер, отвечающий за сбор и первичную обработку данных, а также модуль связи LoRa, обеспечивающий передачу информации на базовую станцию.

Автономность обеспечивается батарейными элементами, рассчитанными на продолжительный срок службы. Критически важным элементом архитектуры является выбор технологии передачи данных: LoRa выбрана не случайно. Она обеспечивает устойчивую связь на расстоянии до 15–20 километров в условиях сельской местности, характеризуется высоким проникновением радиосигнала и низким энергопотреблением, что позволяет устройству работать длительное время от автономного источника питания.



Автоматизированная работа сбора данных с трубопровода

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ НА УРОВНЕ УСТРОЙСТВА: ПОДХОД К КРИПТОЗАЩИТЕ

В условиях, когда данные передаются по радиоканалу, выходящему за пределы контролируемой зоны, требования к защите информации становятся критически важными. Требования нормативно-правовой базы РФ и нормативные документы, такие как СТО Газпром 4.2-2-002-2009 «Система обеспечения информационной безопасности ОАО "Газпром". Требования к АСУ ТП», предписывают обязательную криптографическую защиту данных, передаваемых по незащищенным каналам, а также устойчивость системы к подмене датчиков и случайному или преднамеренному искажению данных. Кроме того, используемые алгоритмы шифрования должны соответствовать требованиям ГОСТ и быть сертифицированы ФСБ России.

В рамках исследования в качестве основного метода защиты было предложено применение встраиваемых СКЗИ. В отличие от наложенных средств, которые устанавливаются поверх операционной системы или прикладного ПО, встраиваемые решения выполнены в виде компактных чипов или модулей, интегрируемых непосредственно в плату телеметрического устройства. Это позволяет осуществлять защиту информации на самом источнике ее генерации – до того, как данные попадут в открытый радиоканал LoRa.

Для защиты сетей интернета вещей (IIoT) и протокола LoRa компания «ИнфоТеКС» предлагает программно-аппаратные комплексы (ПАК) ViPNet SIES Core и ViPNet SIES Core Nano. Это встраиваемые СКЗИ, обеспечивающие решение полного спектра задач по защите данных – от уровня устройств IIoT до рабочих станций диспетчерских пунктов. В состав комплекса продуктов ViPNet SIES также входит центр управления встраиваемыми СКЗИ и их ключевой информацией.

В основе выбранного подхода к защите данных лежит использование отечественных стандартов шифрования, в том числе ГОСТ 34.12–2018, а также криптографического протокола CRISP (ГОСТ Р 71252-2024). В рамках данного проекта рассматривались оба продукта ИнфоТеКС:

01. **ViPNet SIES Core**: криптомодуль, представляющий собой законченное устройство в виде платы, подключаемое к микроконтроллеру по стандартному интерфейсу.

02. **ViPNet SIES Core Nano:** крипточип в корпусном исполнении для впаивания на печатную плату. Обладает минимальными размерами и энергопотреблением.

Продукты реализуют необходимые криптографические алгоритмы шифрования и имитозащиты в соответствии с требованиями регуляторов и СТО Газпром 4.2-2-002-2009.

КРИПТОЧИП VIPNET SIES CORE NANO: МИНИАТЮРНОЕ РЕШЕНИЕ ДЛЯ ДАТЧИКОВ

Для защиты оконечных устройств – сенсоров, датчиков, счетчиков – оптимальным выбором является крипточип ViPNet SIES Core Nano.

ViPNet SIES Core Nano

- Микросхема в корпусе BGA36 с габаритами всего 3×3 мм и высотой 0,4 мм.
- Чип легко размещается на плате самого компактного датчика

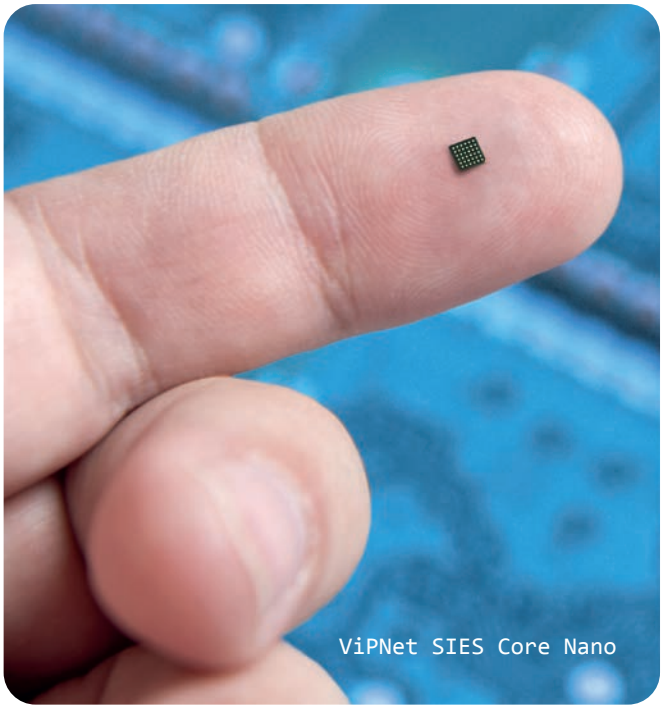
Устройство со встроенным в него ViPNet SIES Core Nano может эксплуатироваться вне контролируемой зоны без дополнительных мер защиты от доступа к нему потенциального нарушителя. Это возможно благодаря встроенным в крипточип на уровне кристалла инженерным мерам защиты, обеспечивающим невозможность извлечения или искажения ключевой информации или встроенного программного обеспечения.

ViPNet SIES Core Nano обладает всеми преимуществами, необходимыми для защиты телеметрических устройств на удаленных объектах:

- низкое энергопотребление
- не требует обслуживания
- высокий класс защиты
- не требует смены ключей в течение всего срока службы изделия
- протокол CRISP – национальный стандарт (ГОСТ Р 71252–2024), утвержденный Росстандартом для защиты промышленных сетей. Подходит для защиты данных в большинстве известных IoT-протоколов, отличается минимальным объемом служебных накладных расходов и не требует установления сессии между устройствами

Взаимодействие основного микроконтроллера с крипточипом осуществляется по интерфейсу SPI. Для управления крипточипом из системы централизованного управления ViPNet SIES MC используется тот же интерфейс SPI через защищаемое устройство. При этом само защищаемое устройство работает с чипом на уровне команд: зашифровать или расшифровать блок данных, вычислить или проверить имитовставку.

Все криптографические операции и хранение ключевой информации выполняются внутри чипа. Ключи хранятся в защищенной области памяти в неизвлекаемом виде в течение всего срока службы – до 16 лет. Крипточип ViPNet SIES Core Nano имеет сертификат ФСБ России о соответствии требованиям к СКЗИ класса КС3.



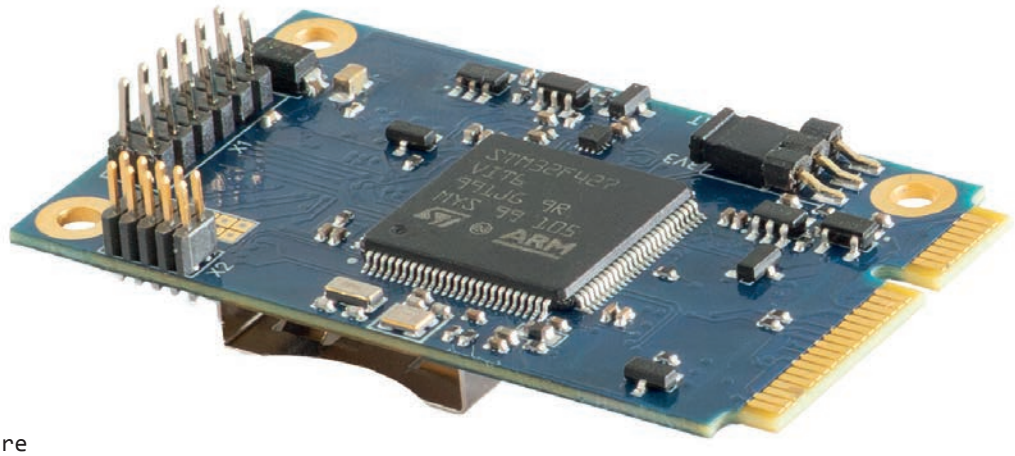
КРИПТОМОДУЛЬ VIPNET SIES CORE: ПРОИЗВОДИТЕЛЬНОСТЬ ДЛЯ КОНТРОЛЛЕРОВ

Когда требуется защита таких устройств, как программируемые логические контроллеры (PLC), устройства сбора и передачи данных (RTU) или промышленные контроллеры автоматизации (PAC), целесообразно применение криптомодуля ViPNet SIES Core.

ViPNet SIES Core

- Устройство с габаритами 51×30×11,2 мм
- Продукт поддерживает несколько интерфейсов интеграции: UART, USB 2.0 Full-speed и SPI, что обеспечивает высокую гибкость при проектировании системы
- Питание модуля организовано с возможностью резервирования: основной источник рассчитан на 4–15 В постоянного тока, резервный – на 3–5 В.
- Потребляемый ток в активном режиме не превышает 80 мА, а в режиме энергосбережения снижается до 60 мкА, что позволяет использовать модуль в энергоэффективных системах
- Важной особенностью криптомодуля является наличие встроенной памяти объемом 16 Мбайт и возможность хранения до 150 прикладных связей
- Диапазон рабочих температур составляет от –40 до +70 °C
- Допустимая влажность воздуха – до 98 % при 25 °C
- ViPNet SIES Core имеет класс СКЗИ КС3 по требованиям ФСБ России
- Хранение ключевой информации и криптографические операции выполняются внутри модуля, а взаимодействие с защищаемым устройством строится на уровне прикладных команд (шифрование блока данных, вычисление имитовставки, и т.д.)

ViPNet SIES Core выполняет запрошенную операцию и возвращает результат криптографического преобразования, либо результат анализа данных. В зависимости от запрошенной криптографической операции защищаемое устройство может использовать результат обработки блока данных для принятия решения о достоверности данных, либо использовать результат обработки блока данных в защищенном обмене информацией с другими защищаемыми устройствами.



ViPNet SIES Core

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ И ПРАКТИЧЕСКИЕ РЕЗУЛЬТАТЫ

Применение встраиваемых СКЗИ ИнфоТеКС в составе систем телеметрии позволило в полной мере выполнить ключевые требования к защите информации:

01. Конфиденциальность
Все данные телеметрии шифруются непосредственно на устройстве перед отправкой в эфир, что исключает их перехват третьими лицами

02. Энергоэффективность
Энергопотребление крипточипов ViPNet SIES Core Nano сопоставимо с потреблением остальных компонентов системы, что не снижает расчетный срок автономной работы, определяемый емкостью батарейных элементов

03. Целостность
Обеспечивается имитозащита, предотвращающая несанкционированное изменение показаний

04. Соответствие стандартам
Используемые алгоритмы и протоколы соответствуют требованиям ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015, а также отраслевым нормативам нефтегазовой отрасли

ViPNet SIES Core и ViPNet SIES Core Nano прошли успешные испытания в ПАО «Газпром автоматизация», по итогам которых комиссией было принято положительное решение о возможности их применения.

В рамках первого этапа проекта в ООО «Газпром добыча Оренбург» была развернута опытная зона системы мониторинга с использованием решения ViPNet SIES. Практическое внедрение подтвердило полную работоспособность предложенной архитектуры: связка «телеметрическое устройство – встраиваемое СКЗИ – модуль LoRa» функционирует корректно. Передача данных осуществляется стабильно, а энергопотребление системы остается в расчетных пределах, что подтверждает пригодность решения для длительной автономной работы.

ЗАКЛЮЧЕНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Проведенные работы наглядно продемонстрировали, что задача организации безопасной передачи данных в условиях отсутствия инфраструктуры и централизованного электроснабжения имеет эффективное решение. Сочетание энергоэффективной технологии связи LoRa и встраиваемых СКЗИ создает стабильную основу для автоматизации скважин старого фонда.

Предложенный подход позволяет:

- организовать централизованный контроль параметров работы скважин, ранее не охваченных автоматизацией
- снизить эксплуатационные расходы благодаря оперативному выявлению и реагированию на нарушения режимов работы
- обеспечить полное соответствие передаваемых данных требованиям информационной безопасности, включая требования СТО Газпром

Первые результаты внедрения подтверждают высокую практическую ценность и эффективность описанного подхода. В качестве дальнейших направлений работ рассматривается масштабирование системы на весь фонд скважин.

У вас похожая задача? Интересует совместный проект?
По всем вопросам вас проконсультируют эксперты ИнфоТеКС: soft@infotecs.ru