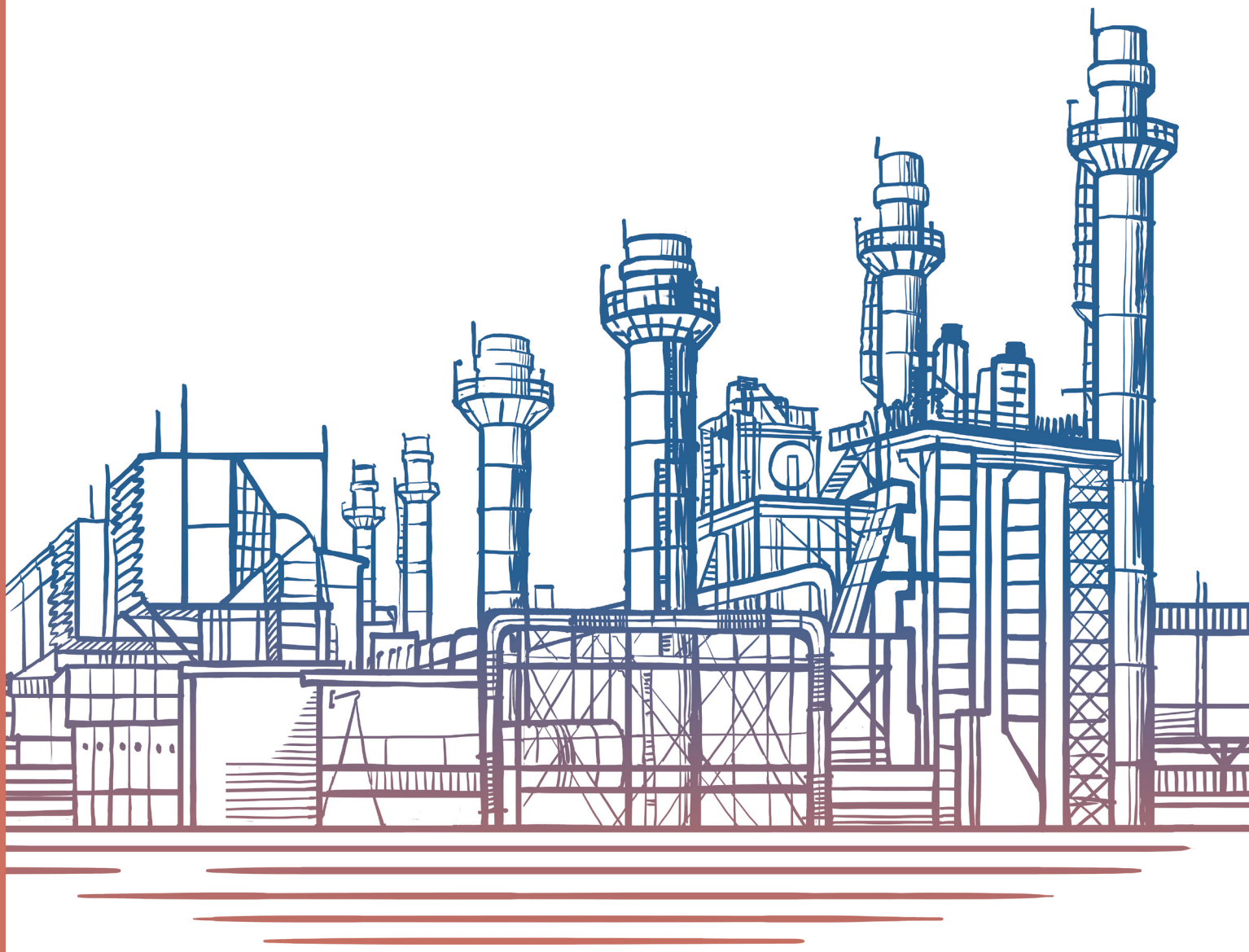
infotecs

# Защита распределенных систем нефтегазовых предприятий



Снижение издержек на разведку, добычу, транспортировку, переработку сырья и готовой продукции и общее повышение эффективности производственных процессов, доступные в рамках интенсивной цифровизации топливно-энергетического комплекса, в частности предприятий нефтегазовой отрасли, рождает новые вызовы со стороны информационной безопасности эксплуатируемых систем. Применение распределенных систем управления, активное внедрение большого количества IoT-устройств, увеличение объемов передаваемых данных приводит к необходимости интеграции новых ИТ-решений с АСУ ТП, что может приводить к пересечениям корпоративных и промышленных сетей и открывать возможность киберпреступникам проведения атак на промышленную инфраструктуру.

Еще одним вызовом для предприятий нефтегазовой сферы из мира информационной безопасности, стал уход с российского рынка зарубежных производителей средств защиты информации. Отсутствие технической поддержки и своевременных обновлений уже внедренных систем обеспечения информационной безопасности (ИБ) со стороны зарубежных компаний привело и будет приводить к постепенной деградации уровня защищенности.

В ответ на эти вызовы государство предпринимает попытки урегулировать ситуацию путем введения нормативных мер, предписывающих осуществить переход на промышленные информационные системы отечественного производства, однако реальный сектор не может одномоментно поменять дорогостоящее иностранное оборудование и программное обеспечение, и продолжает эксплуатировать существующие системы.

Использование устаревшего уязвимого программного обеспечения повышает риски ИБ и упрощает работу злоумышленников, компетенции и мотивация которых продолжают расти. Кибератаки на промышленные компании могут привести к утечке конфиденциальной информации, парализовать бизнес-процессы вплоть до остановки производства и повреждения оборудования. Последствия таких атак могут носить опасный техногенный характер.

Устойчивая работа предприятий газовой и нефтяной промышленности напрямую связана с национальной безопасностью, именно поэтому вопросы кибербезопасности в этой сфере регулируются государством. Требования по защите технологической части предприятия содержатся в нормативно-правовых документах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и регулируются Федеральным законом № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и его подзаконными актами.

Требования законодательства, регулирующего сферу информационной безопасности, зависят от типов информационных систем, эксплуатируемых промышленными предприятиями:

- объекты критической информационной инфраструктуры (КИИ)
- государственные информационные системы (ГИС)
- информационные системы персональных данных (ИСПДн)
- информационные системы общего пользования (ИСОП)
- автоматизированные системы управления технологическим процессом (АСУ ТП)

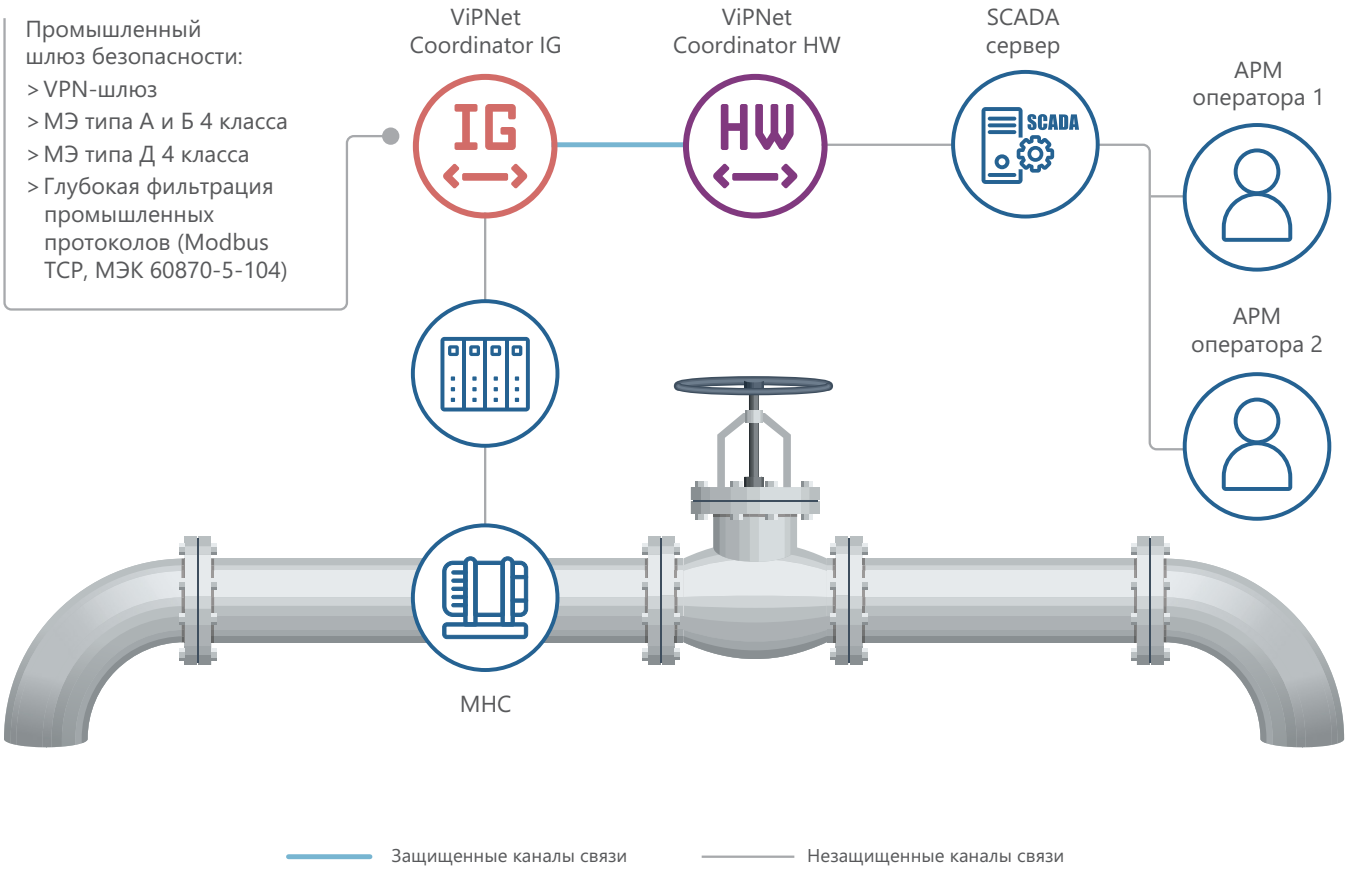
Компания «ИнфоТеКС» предлагает продукты двух направлений для обеспечения информационной безопасности промышленных предприятий:

- сетевые средства защиты информации ViPNet Channel Protection
- встраиваемые средства криптографической защиты информации (СКЗИ) ViPNet SIES

Каждое из направлений имеет полный набор продуктов для реализации сквозных сценариев защиты информации промышленных информационных систем от полевого уровня АСУ ТП до систем управления производственными и бизнес-процессами. Сетевые средства защиты для промышленных объектов используют общую с СЗИ для корпоративных систем (MES, ERP) технологию ViPNet VPN. Встраиваемые СКЗИ ViPNet SIES реализуют стандартизованные протоколы и алгоритмы защиты информации и имеют открытые API-интерфейсы для интеграции с продуктами сторонних производителей.

# Сценарии использования

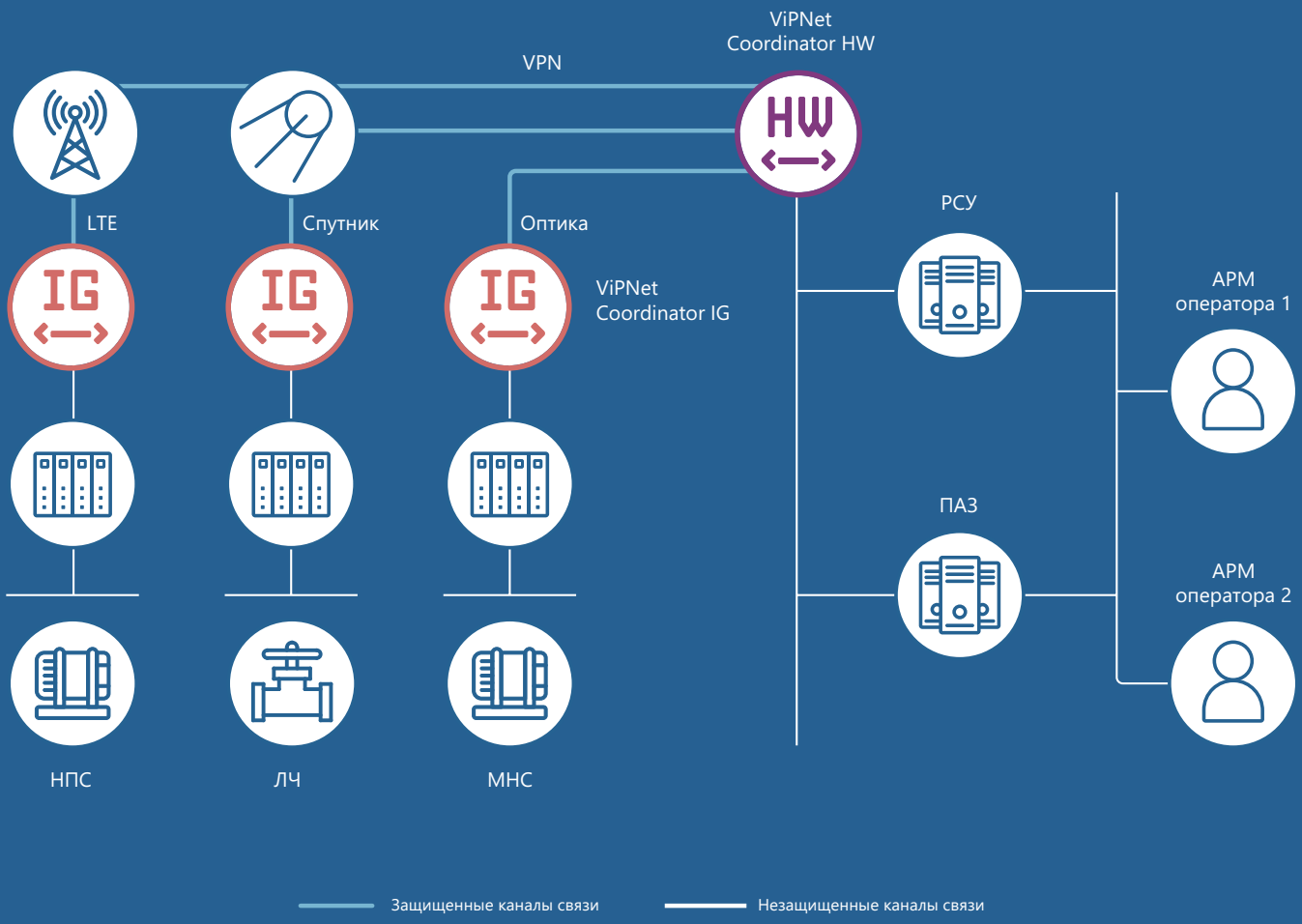
## Защита канала связи с удаленным объектом распределенной системы




В распределенных системах для диспетчеризации и управления удаленными объектами необходимо передавать информацию по защищенным каналам связи. Защита канала связи с удаленными объектами осуществляется с помощью VPN-соединения по технологии ViPNet VPN. Для организации VPN-соединения используются шлюзы безопасности ПАК ViPNet Coordinator IG и ПАК ViPNet Coordinator HW. ПАК ViPNet Coordinator IG идеально подходит для решения задачи защиты передаваемых данных на уровне автоматического управления или полевом уровне распределенных систем. Для защиты канала связи на уровне оперативно-диспетчерского управления можно использовать как ПАК ViPNet Coordinator IG, так и ПАК ViPNet Coordinator HW соответствующей пропускной способности.

## VPN для распределенных систем

В распределенных системах связь с удаленными объектами может осуществляться не только по проводным, но и по оптическим и беспроводным каналам передачи данных. Технология ViPNet VPN одинаково надежно работает на любых каналах связи, независимо от их типа: витая пара, ВОЛС, спутниковая или сотовая сеть. ПАК ViPNet Coordinator IG может комплектоваться оптическими и беспроводными модулями связи для подключения к каналам передачи данных от удаленных объектов. Защищенное ViPNet VPN-соединение устанавливается от ПАК ViPNet Coordinator IG на полевом уровне до уровня оперативно-диспетчерского управления, где может использоваться ПАК ViPNet Coordinator IG или ПАК ViPNet Coordinator HW.



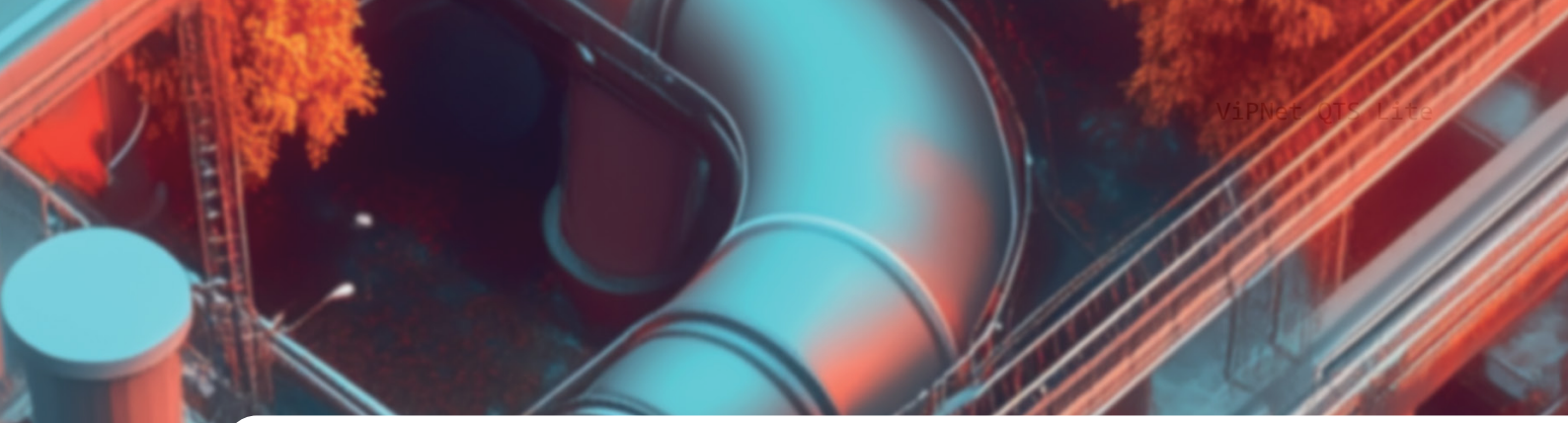
# Используемые продукты

## ViPNet Coordinator IG

**Программно-аппаратный комплекс (ПАК) ViPNet Coordinator IG является российским индустриальным шлюзом безопасности, предназначенным для организации защищенных каналов связи и предотвращения несанкционированного доступа к объектам защиты.**

**ПАК ViPNet Coordinator IG может быть использован:**

1. Для защиты информации на всех уровнях значимых и незначимых объектов АСУ КИИ
2. Для защиты информации на всех уровнях АСУ ТП
3. Для защиты данных информационных систем и информационно-телекоммуникационных сетей, в том числе значимых и незначимых объектов КИИ, где необходима работа СЗИ при высоких и низких температурах или есть расширенные требования к условиям эксплуатации



## ПРЕИМУЩЕСТВА

> Защита проводных и беспроводных каналов связи

> Ограничение трафика на уровне разрешения определенных промышленных протоколов

> Возможность запрета использования сервисных функций для определенных режимов функционирования объекта

> Сужение векторов атак за счет глубокой фильтрации промышленных протоколов

> Возможность использования «старых» устройств в системе за счет организации защиты информации при подключении по интерфейсам RS-232 и RS-485

> Дистанционное конфигурирование и управление политиками безопасности

> Работа в режиме горячего резервирования и возможность организации резервирования каналов связи

> Индустриальный дизайн и возможность использования в жестких условиях эксплуатации

> Возможность построения сквозной безопасности предприятия от ERP-уровня до нижнего уровня АСУ и АСУ ТП на основе единой технологии ViPNet VPN с помощью линейки продуктов ViPNet Channel Protection

> Защита объекта при подключении к сетям связи общего пользования одним устройством

> Произведено в России

## СЕРТИФИКАЦИЯ

**ФСБ России**

> СКЗИ класса КС3
> МЭ 4 класса защищенности

**ФСТЭК России**

> МЭ типов А, Б, Д 4 класса защиты
> 4 уровень доверия средств защиты информации

**МИНЦИФРЫ**

> Включен в реестр Российского ПО

**МИНПРОМТОРГ России**

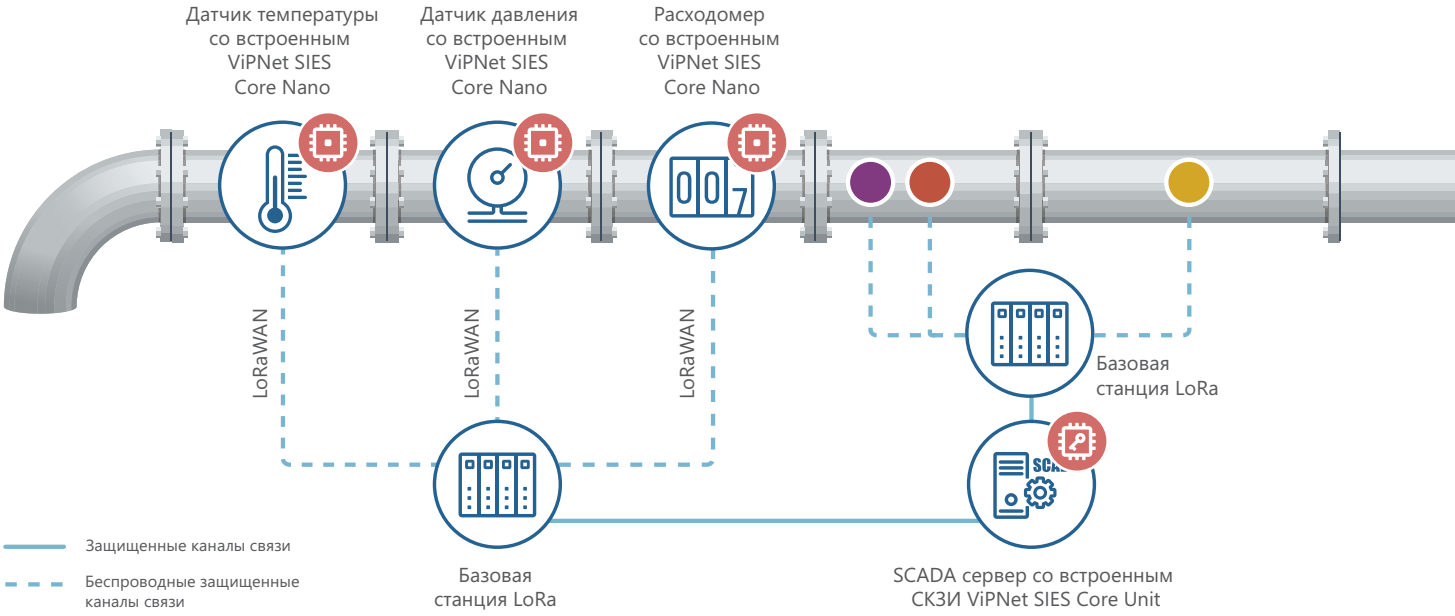
> Включен в единый реестр РЭП

**РОСАККРЕДИТАЦИЯ**

> Декларация соответствия ТР/ТС 020/2011 на ЭМС по промышленным стандартам

# Сценарии использования

## Автоматизированная система сбора данных с трубопровода




Задача состоит в защите данных, собираемых с множества датчиков, устанавливаемых на инфраструктурных объектах, например, на трубопроводных системах. Информация с таких датчиков, как правило, передается по энергоэффективным каналам с низкой пропускной способностью, такими как LoRaWAN или NB-IoT. При передаче информации по подобным каналам связи необходимо использовать защиту на уровне передаваемых блоков данных, для этого применяются встраиваемые СКЗИ из состава решения ViPNet SIES. В устанавливаемые на трубопроводе датчики встраиваются крипточипы ПАК ViPNet SIES Core Nano, которые могут эксплуатироваться вне контролируемой зоны и не требуют смены ключей защиты и какого-либо обслуживания в течение всего срока службы (16 лет). На верхнем уровне для обработки защищенных данных используется программный комплекс СКЗИ ViPNet SIES Unit, интегрируемый, например, со SCADA-сервером. При необходимости криптографической обработки данных на среднем уровне в базовую станцию может быть встроено СКЗИ ПАК ViPNet SIES Core.

Передаваемые данные защищаются с помощью криптографического протокола CRISP (ГОСТ Р 71252-2024)

### Защита данных с помощью CRISP

- Целостность
- Конфиденциальность (опционально)
- Защита от навязывания повторных сообщений
- Аутентификация источника сообщений

Протокол CRISP (ГОСТ Р 71252-2024) рекомендован Минцифрой для применения в ИСУЭ и IIoT

→ Защита адресных и групповых сообщений

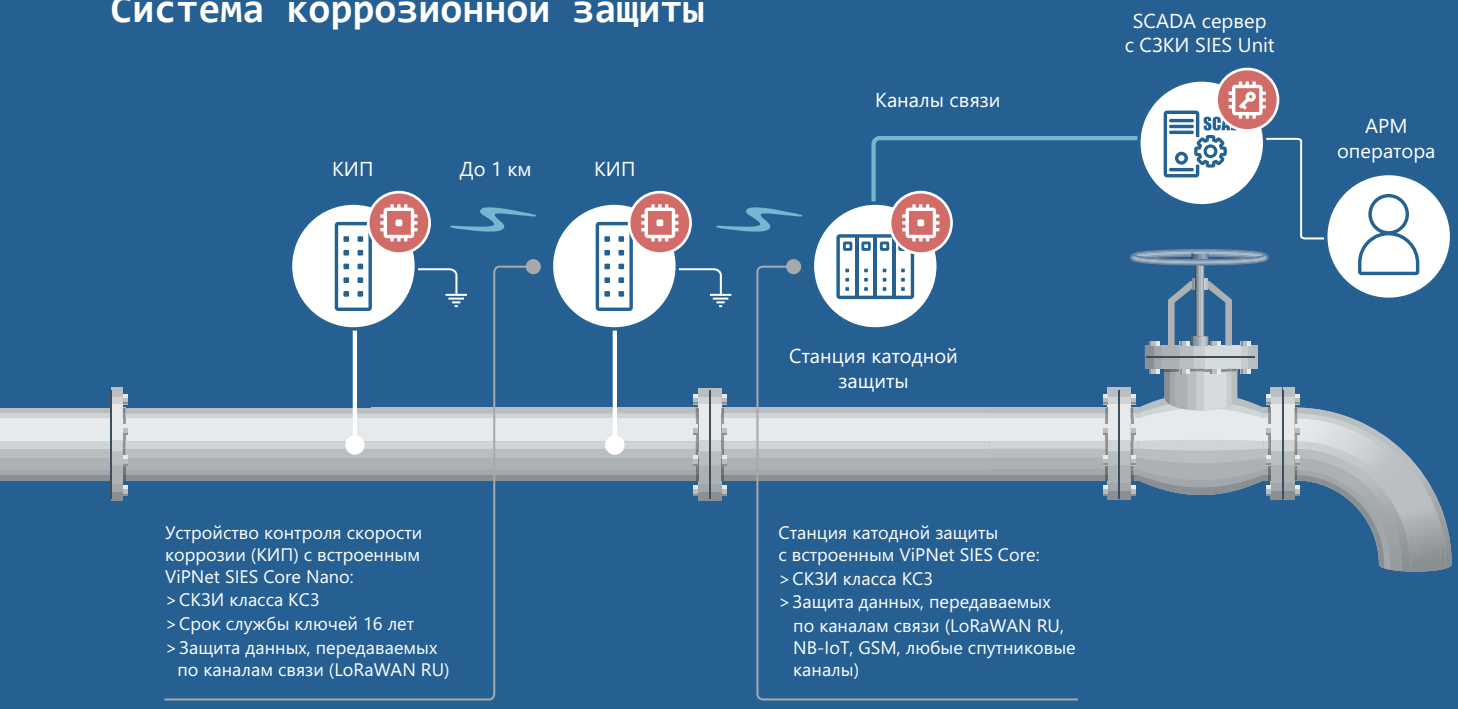
→ Бессессионный криптографический протокол

→ Минимальные накладные расходы (overhead) и минимальная нагрузка на сеть

→ Универсальный стандартизированный протокол защиты любых протоколов IIoT

RS-485 GSM PLC Ethernet KNX zigbee LoRaWAN RF NB-IoT

## Система коррозионной защиты




Система коррозионного мониторинга и коррозионной защиты трубопроводов является одной из разновидностей систем промышленного интернета вещей (IIoT). Данные от контрольно-измерительных пунктов (КИП) передаются на станцию катодной защиты по беспроводным каналам связи (LoRaWAN RU). Для их защиты в КИП встраивается крипточип ПАК ViPNet SIES Core Nano, в станцию катодной защиты – криптомодуль ПАК ViPNet SIES Core из состава решения ViPNet SIES. На уровне сервера для защиты данных используется программный комплекс СКЗИ ViPNet SIES Unit. Передаваемые между объектами системы данные защищаются при помощи криптографического протокола CRISP (ГОСТ Р 71252–2024).

## Система телеметрического контроля и телемеханизации

Это распределенная система, состоящая из OPC UA-серверов, серверов ввода-вывода и крановых узлов, устанавливаемых на трубопроводе и являющихся удаленными объектами телеуправления и мониторинга. Особенностью такой системы является необходимость защиты данных, передаваемых с использованием дорогостоящих спутниковых и GSM-каналов, а также использование автономного аккумуляторного питания крановых узлов.
На крановых узлах для защиты передаваемых данных применяются встраиваемые СКЗИ ПАК ViPNet SIES Core с низким энергопотреблением, позволяющие обеспечить необходимую энергоэффективность и продлить срок службы аккумуляторного источника питания. Криптографический протокол CRISP (ГОСТ Р 71252–2024) позволяет сократить объем передаваемой служебной информации, а, следовательно, снизить стоимость и повысить энергоэффективность при передаче данных. Для обработки защищенных данных на верхнем уровне в OPC UA-сервер встраивается программный комплекс СКЗИ ViPNet SIES Unit, входящий в решение ViPNet SIES.

# Используемые продукты

## ViPNet SIES Core

**Программно-аппаратный комплекс (ПАК) ViPNet SIES Core предназначен для интеграции с такими защищаемыми устройствами, как программируемые логические контроллеры (PLC), промышленные контроллеры автоматизации (PAC), терминалы (RTU), интеллектуальные устройства (IED), IIoT-устройства, устройства сбора и передачи данных (УСПД), оконечное оборудование (датчики и исполнительные устройства).**

### ПРИНЦИП РАБОТЫ

ПАК ViPNet SIES Core интегрируется с защищаемыми устройствами через межплатные интерфейсы и в пассивном режиме выполняет запросы на криптографические операции с данными. Защищаемое устройство обращается к ПАК ViPNet SIES Core через API-интерфейс напрямую или с использованием SIES Core SDK. Структуру и состав данных (команды управления, телеметрическую информацию, сервисные команды) определяет разработчик АСУ ТП или M2M. ViPNet SIES Core выполняет запрошенную операцию и возвращает результат в виде криптографического преобразования обработанных данных или их анализа.

В зависимости от запрошенной криптографической операции защищаемое устройство может использовать результат обработки блока данных для принятия решения о достоверности данных либо его обмене с другими защищаемыми устройствами.

### СЕРТИФИКАЦИЯ

**ФСБ России**
> СКЗИ класса КС3

**Свидетельства**
> В реестре российского ПО
> В реестре Минпромторга


## ПРЕИМУЩЕСТВА

> ПАК ViPNet SIES Core является функционально законченным средством криптографической защиты информации (СКЗИ) и может эксплуатироваться вне контролируемой зоны

> Все криптографические вычисления и хранение дополнительной информации осуществляются внутри ПАК ViPNet SIES Core, что позволяет не расходовать вычислительные ресурсы защищаемого им устройства на выполнение криптографических преобразований информации

> ПАК ViPNet SIES Core является пассивным устройством и работает в режиме ответа на запросы защищаемого им устройства. При этом объем и тип защищаемых данных самостоятельно определяется разработчиком АСУ, M2M или IIoT

> Для реализации сценариев защиты информации защищаемое устройство вызывает требуемые криптографические функции при помощи API-интерфейса

> Поддерживает работу с промышленными протоколами. Для защиты передаваемых данных используется промышленный криптографический протокол с малым объемом вспомогательных данных

> Обеспечивает информационную безопасность на уровне данных, не требуя внесения изменений на канальном уровне коммуникаций информационной системы

> ПАК ViPNet SIES Core не зависит от архитектуры и операционной системы защищаемого устройства. ViPNet SIES Core можно интегрировать в защищаемые устройства без операционной системы (bare metal)

# ViPNet SIES Core Nano

**Криптографический чип для защиты информации устройств автоматизации, IoT и приборов учета, реализованный в виде миниатюрного чипа российского производства.**

## ПРИНЦИП РАБОТЫ

ViPNet SIES Core Nano реализован в виде системы на кристалле (System-on-a-Chip, SoC), монтируемой на печатную плату защищаемого устройства. Для интеграции крипточипа с защищаемым устройством используется интерфейс SPI.

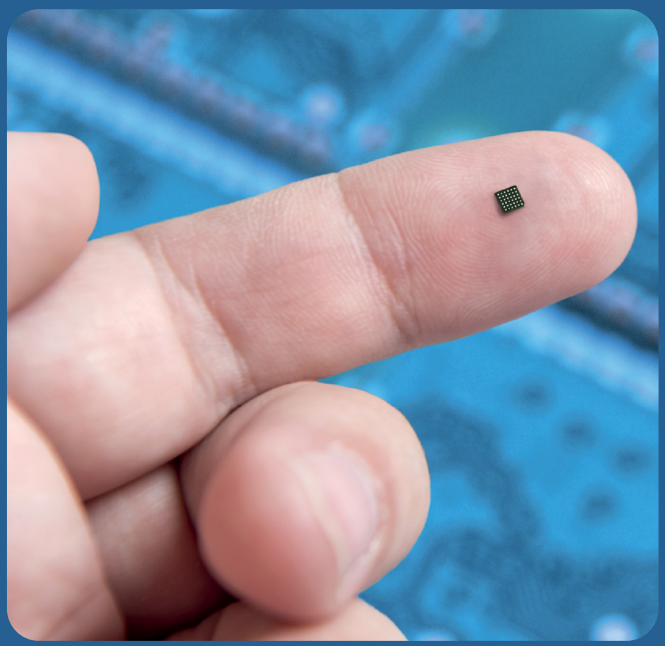
ViPNet SIES Core Nano работает в пассивном режиме, выполняя криптографическую обработку данных по команде защищаемого устройства. Защищаемое устройство через API-интерфейс отправляет крипточипу блок данных и код команды, определяющий требуемую обработку блока данных. ViPNet SIES Core Nano выполняет запрошенную криптографическую операцию над переданным блоком данных и возвращает защищаемому устройству ответ в виде преобразованного блока данных или результата его обработки.

Структуру и состав данных для защиты (команды управления, телеметрическую информацию, сервисные команды) задает разработчик защищаемого устройства. Он же определяет алгоритмы обработки результата запрошенной криптографической операции прикладным ПО защищаемого устройства.

Ключи в ViPNet SIES Core Nano хранятся в специальной защищенной области памяти в неизменяемом и неизвлекаемом виде. Благодаря высокой степени защиты от атак инженерного проникновения в соответствии с требованиями к СКЗИ-НР крипточип может эксплуатироваться вне контролируемой зоны, а срок хранения и использования ключевой информации может достигать 16 лет.

## ПРЕИМУЩЕСТВА

- > Низкое энергопотребление
- > Не требует обслуживания
- > Высокий класс защиты
- > Эксплуатация вне контролируемой зоны
- > Не требует смены ключей в течение всего срока службы изделия
- > Протокол CRISP, подходящий для защиты данных в большинстве известных IoT- протоколов
- > Централизованное управление из ViPNet SIES MC
- > Полностью российская разработка
- > Срок хранения и использования ключевой информации до 16 лет



# ViPNet SIES Unit

**ViPNet SIES Unit предназначен для защиты устройств уровня оперативно-диспетчерского управления АСУ ТП (SCADA-серверы, OPC-серверы, серверные системы сбора и мониторинга данных, рабочие станции и др.), информационно-вычислительного комплекса ИСУЭ или серверов приложений IIoT.**

## ПРИНЦИП РАБОТЫ

ViPNet SIES Unit работает под управлением операционных систем Windows и Linux. ViPNet SIES Unit устанавливается на выделенный сервер или непосредственно на защищаемые устройства – серверы и рабочие станции уровня оперативно-диспетчерского управления АСУ ТП, например, SCADA-сервер, OPC-сервер, АРМ оператора, АРМ инженера и др. Защищаемое устройство взаимодействует с ViPNet SIES Unit на уровне прикладного ПО посредством программного интерфейса приложения API. ViPNet SIES Unit работает в пассивном режиме, выполняя криптографические операции с данными по запросу прикладного ПО защищаемого устройства.

Структуру и состав данных (команды управления, телеметрическая информация, сервисные команды и др.), а также метод защиты определяет разработчик АСУ ТП, M2M или IIoT. ПК ViPNet SIES Unit выполняет запрошенную операцию и возвращает результат в виде криптографического преобразования обработанных данных или их анализа. В зависимости от запрошенной криптографической операции защищаемое устройство может использовать результат обработки блока данных для принятия решения о достоверности данных либо использовать полученный результат в защищенном обмене с другими защищаемыми устройствами.

## ПРЕИМУЩЕСТВА

> Функционально законченное средство криптографической защиты информации (СКЗИ)

> Работает как программный сервис, в пассивном режиме отвечая на запросы прикладного ПО защищаемого им устройства. При этом объем и тип защищаемых данных самостоятельно определяется разработчиком АСУ ТП, M2M или IIoT

> Для реализации сценариев защиты информации защищаемое устройство вызывает требуемые криптографические функции при помощи API-интерфейса

> Поддерживает работу с промышленными протоколами. Для защиты передаваемых данных используется промышленный криптографический протокол CRISP с малым объемом вспомогательных данных

> Обеспечивает информационную безопасность на уровне данных, не требуя внесения изменений на канальном уровне коммуникаций информационной системы

## СЕРТИФИКАЦИЯ

**ФСБ России**
> СКЗИ классов КС1 и КС3

**Свидетельства**
> В реестре российского ПО

# ViPNet SIES MC

**ViPNet SIES MC позволяет управлять жизненным циклом продуктов ViPNet SIES и СКЗИ сторонних разработчиков как единой платформой: разворачивает решение ViPNet SIES и СКЗИ других производителей доверенным образом, обеспечивает ввод в эксплуатацию компонентов решения ViPNet SIES и СКЗИ сторонних производителей и позволяет обновлять как сами компоненты решения, так и их ключевую информацию. ViPNet SIES MC отвечает за управление компонентами решения на всех стадиях их жизненного цикла от ввода в эксплуатацию до вывода из обращения.**

## ОСНОВНЫЕ ФУНКЦИИ

- Инициализация ViPNet SIES Core, ViPNet SIES Unit
- Ввод в эксплуатацию компонентов решения ViPNet SIES
- Мониторинг компонентов решения ViPNet SIES
- Управление ключевой информацией и сертификатами компонентов решения ViPNet SIES
- Вывод из эксплуатации компонентов решения ViPNet SIES
- Обновление программного обеспечения компонентов решения ViPNet SIES
- Организация защищенного взаимодействия между защищаемыми устройствами с помощью компонентов решения ViPNet SIES
- Проведение мероприятий при компрометации компонентов решения ViPNet SIES

## ПРЕИМУЩЕСТВА

> Быстрый ввод в эксплуатацию защищенной системы с СКЗИ

> Снижение затрат на обслуживание СКЗИ за счет автоматизации, смены ключевой информации и периодического контроля

> Повышение прозрачности в управлении СКЗИ за счет наличия функционала инвентаризации

> Возможность интеграции в защищенную систему СКЗИ сторонних производителей для управления ими

> Нет необходимости установки дополнительного ПО на рабочие места администратора системы безопасности. Для подключения администраторов можно использовать любой браузер

> Подходит для работы в компаниях как с территориально распределенными системами, так и для сервис-провайдеров

## СЕРТИФИКАЦИЯ

**ФСБ России**

> СКЗИ класса КС1 и КС3

**Свидетельства**

> В реестре российского ПО

> В реестре Минпромторга

+7 495 737-61-92
8 800 250-0-260 (бесплатный звонок по России)

soft@infotecs.ru
hotline@infotecs.ru

www.infotecs.ru

IS24_OG_00RU



Изобретения, примененные в представленных продуктах и решениях ИнфоТеКС, защищены следующими патентами РФ: 2517411, 2526282, 2507569, 2636403, 2635216, 2687217, 2706176