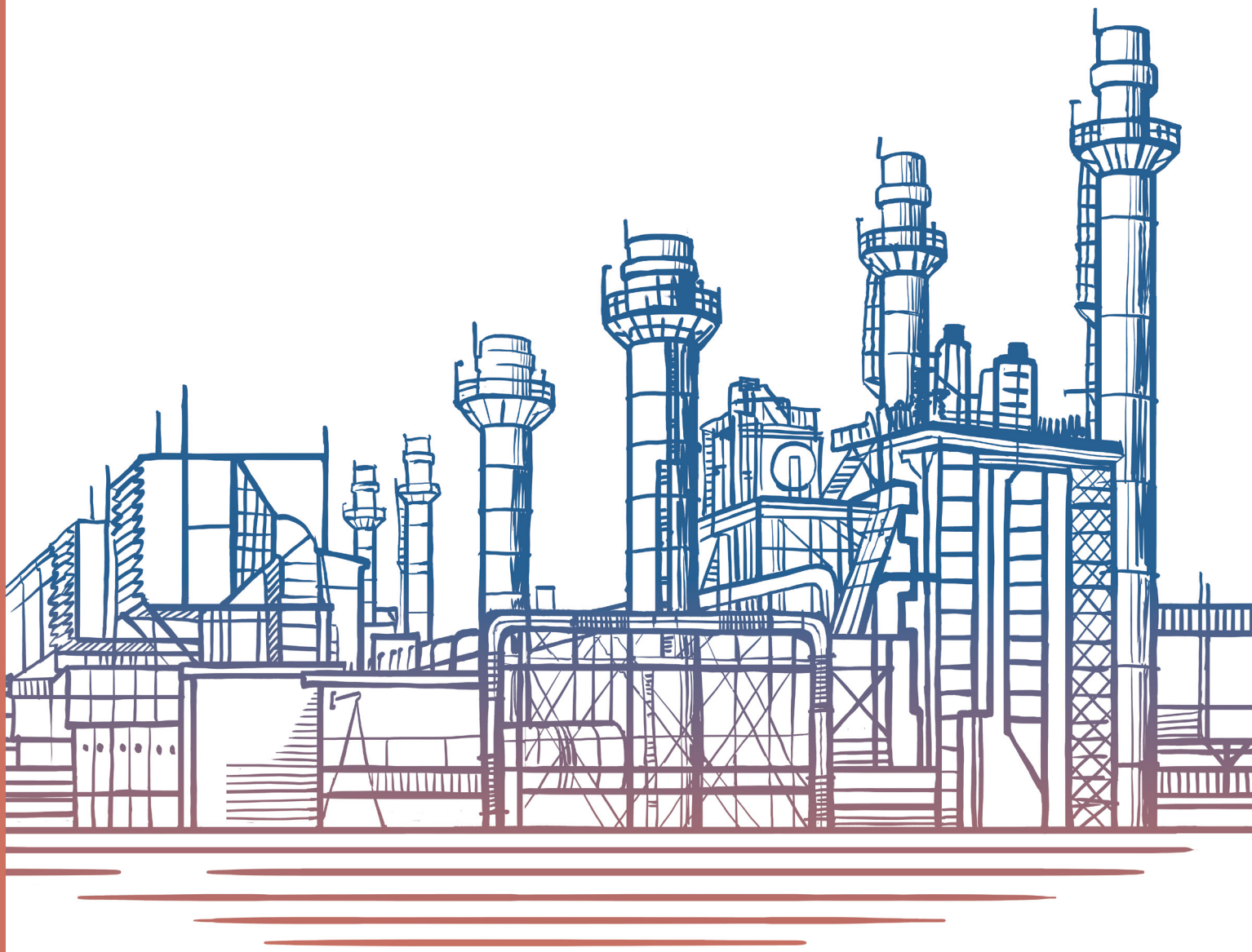
infotecs

ViPNet Industrial Security

Решения для защиты информации АСУ ТП



Информационная безопасность промышленных предприятий

В современном мире ввиду продолжающейся цифровизации целевые атаки на промышленные системы превратились из виртуальных рисков в повседневную рутину, с которой ежедневно сталкиваются специалисты по информационной безопасности и службы эксплуатации. При этом атаки год от года становятся более сложными, а инструменты воздействия – более продвинутыми.

Уход зарубежных вендоров с российского рынка АСУ ТП потянул за собой остановку технической поддержки систем и привел к постепенному ослабеванию уровня защищенности для промышленных предприятий в силу отсутствия своевременных патчей (обновлений) информационной безопасности от разработчиков. Несмотря на требования регуляторов по переходу на российские ПО и ПАК для многих отраслей промышленности, компании не могут одномоментно поменять дорогостоящее оборудование и продолжают эксплуатировать западные системы. Использование устаревшего уязвимого ПО повышает риски ИБ и упрощают работу хакеров, компетенция которых продолжает расти.

С другой стороны, компетенции в сфере информационной безопасности российских разработчиков SCADA-систем и устройств автоматизации очень низки. Ранее российские вендоры не сталкивались с большим количеством атак на свое оборудование в виду небольшого процента распространения и не занимались задачами защиты информации. Сегодня же в условиях массового перехода на российские решения в очень сжатые сроки системы оказываются под воздействием непрекращающихся целевых атак и достаточно легко становятся жертвами хакеров.

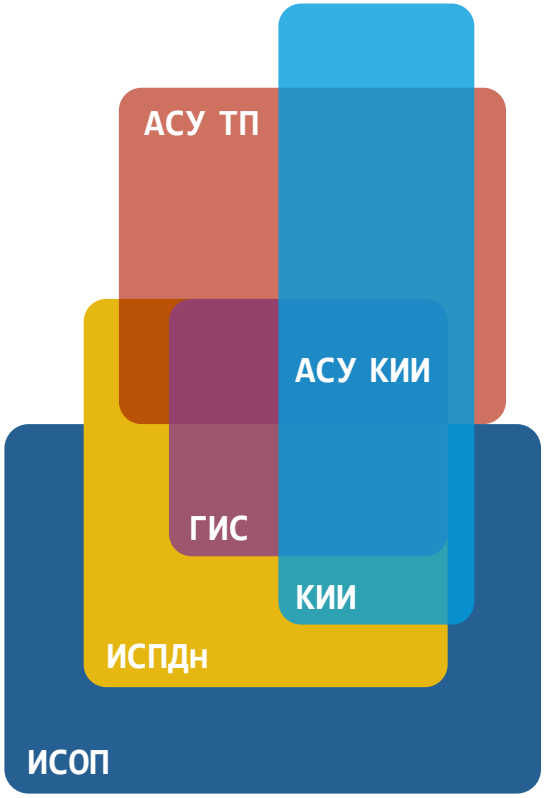
Последствия же кибератак на промышленные предприятия становятся причиной не только утечек данных и перебоя в работе IT-систем, но и прямой причиной внеплановых простоев, приводящих к прямым убыткам.

Устойчивая работа промышленных предприятий и объектов критической инфраструктуры напрямую зависит от предпринимаемых мер по защите важных активов. Продукты ИнфоТеКС для защиты промышленных систем помогут построить подсистему информационной безопасности и решить важные задачи – защитить периметр, предотвратить несанкционированный доступ, построить защищенные каналы, организовать доверенный удаленный доступ.

НОРМАТИВНО-ПРАВОВАЯ БАЗА

Законодательное регулирование для промышленных предприятий в сфере информационной безопасности зависит от типа информационных систем, которыми владеет предприятие:

1. объекты критической информационной инфраструктуры (КИИ)
2. государственные информационные системы (ГИС)
3. информационные системы персональных данных (ИСПДн)
4. информационные системы общего пользования (ИСОП)
5. автоматизированные системы управления технологическим процессом (АСУ ТП)



Требования по защите технологической части предприятия – автоматизированных систем управления (АСУ) – содержатся в нормативно-правовых документах по обеспечению безопасности КИИ РФ и АСУ ТП. Безопасность КИИ РФ регулируется Федеральным законом № 187-ФЗ «О безопасности Критической информационной инфраструктуры Российской Федерации» и его подзаконными актами. К объектам КИИ относятся АСУ, а также информационные системы и информационно-телекоммуникационные сети предприятий следующих сфер экономики: здравоохранение, наука, транспорт, связь, энергетика, банки и иные организации финансового рынка, топливно-энергетический комплекс, атомная энергия, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленности. Большая часть из этих предприятий является промышленными предприятиями с большим числом АСУ. Для построения подсистемы информационной безопасности объектов АСУ КИИ на промышленных предприятиях необходимо руководствоваться следующими нормативно-правовыми документами:

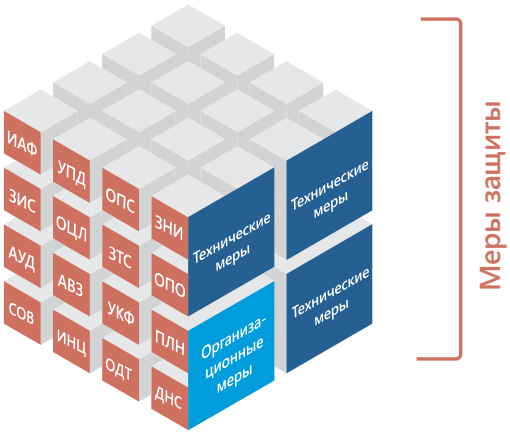
- Приказ ФСТЭК России № 235 от 21.12.2017 г. «Требования к созданию систем безопасности объектов КИИ»
- Приказ ФСТЭК России № 239 от 25.12.2017 г. «Требования по обеспечению безопасности объектов КИИ»
- Приказ № 336 ФСБ России от 24.07.2018 г. «О Национальном координационном центре по компьютерным инцидентам»
- Приказ ФСБ России от 06.05.2019 г. № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»
- Приказ ФСБ России от 19.06.2019 г. № 281 «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»

Защита АСУ ТП должна осуществляться на основе Приказа ФСТЭК России № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» или Приказа ФСТЭК России № 31 от 14.03.2014 г. «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Выбор технических средств защиты информации как для объектов КИИ, так и для АСУ ТП зависит от категории значимости объекта/класса защищенности и мер защиты, которые должны быть реализованы согласно модели угроз и нарушителя. Объектами защиты в индустриальных системах являются информация о параметрах или состоянии управляемого объекта или процесса, а также все сопутствующие технические средства (рабочие станции, серверы, каналы связи, контроллеры), ПО и средства защиты.

ФЗ №187-ФЗ «О безопасностии КИИ РФ»

Субъекты КИИ

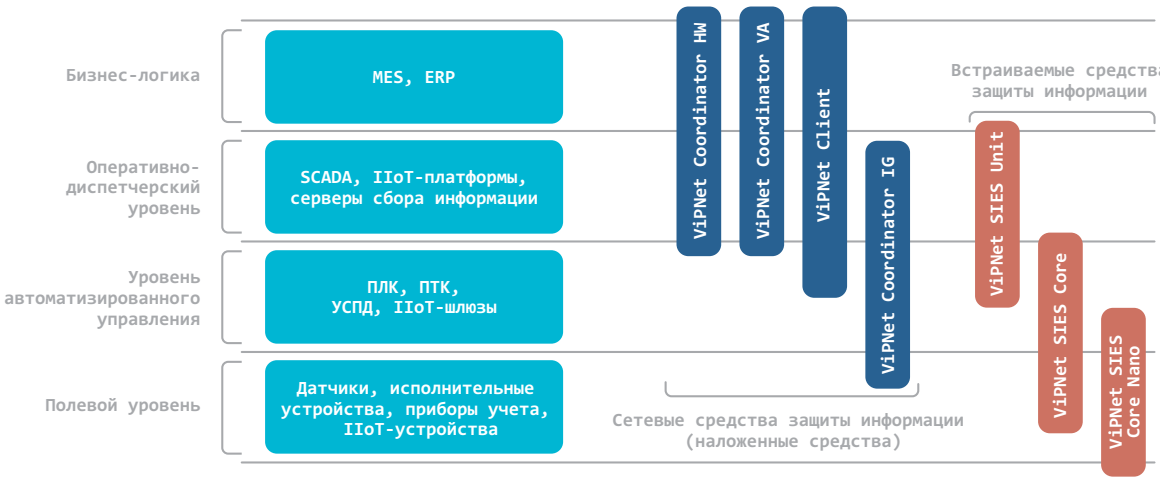


Меры Приказа № 239 ФСТЭК России

Объекты защиты АСУ

- Информация о параметрах и объектах процесса АСУ
- Программно-аппаратные средства АСУ
- Средства защиты информации
- Программные средства АСУ
- Архитектура и конфигурация АСУ

Продукты ИнфоТеКС для обеспечения информационной безопасности АСУ КИИ и АСУ ТП



Комплексный подход ИнфоТеКС по обеспечению информационной безопасности АСУ КИИ и АСУ ТП

Традиционно структуру промышленного предприятия представляют в виде многоуровневой модели: полевого уровня, уровня автоматизированного управления и оперативно-диспетчерского уровня, где эксплуатируются SCADA-системы. Каждый из этих уровней имеет свои особенности, влияющие на выбор средств защиты информации (СЗИ). Если для оперативно-диспетчерского уровня, например, не требуются изделия, работающие в тяжелых условиях эксплуатации, то для уровня автоматизированного управления и полевого уровня, как правило, есть требования работы в условиях низких и высоких температур, часто требуется электромагнитная совместимость, пыле- и влагозащищенность, вибростойкость. Применяемые технологии на каждом из уровней также влияют на выбор СЗИ. Для SCADA-систем на оперативно-диспетчерском уровне применяются обычные TCP/IP-сети, на остальных уровнях много последовательных каналов связи, LPWAN-сетей и non-IP-сетей. Способы защиты информации и допустимые значения по задержкам для таких сетей будут разные. Несмотря на отличия в предъявляемых требованиях, СЗИ на промышленных предприятиях должны обеспечивать сквозную безопасность и функционировать в единой инфраструктуре.

Компания «ИнфоТеКС» предлагает продукты двух направлений для защиты промышленных предприятий:

1. сетевые средства защиты информации ViPNet Channel Protection
2. встраиваемые средства ViPNet SIES

Каждое из направлений имеет полный набор продуктов для построения сквозной безопасности для всех уровней объекта. Сетевые средства защиты для промышленных объектов используют общую с СЗИ для корпоративных систем (MES, ERP) технологию ViPNet VPN и полностью совместимы друг с другом.

Сетевые средства защиты

Направление сетевых средств защиты информации включает в себя индустриальные шлюзы безопасности ViPNet Coordinator IG и адаптированные для применения в АСУ продукты ViPNet Channel Protection – шлюзы безопасности ViPNet Coordinator HW, ViPNet Coordinator VA и программные комплексы ViPNet Client

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:

01. Для защиты информации на всех уровнях значимых и незначимых объектов АСУ КИИ
02. Для защиты информации на всех уровнях АСУ ТП
03. 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

СЦЕНАРИИ

> Сегментирование сети и разграничение доступа к ее сегментам

> Защита проводных и беспроводных каналов связи сети

> Организация защищенных каналов связи между сегментами сети

> Организация защищенного удаленного доступа для мобильных пользователей

> Организация ДМЗ

> Организация защищенного удаленного мониторинга

> Организация защищенного удаленного сервисного обслуживания

> Организация защищенного подключения оборудования по последовательным интерфейсам

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

ВОЗМОЖНОСТИ

VPN

> ViPNet VPN-шлюз сетевого уровня (L3 VPN)
> ViPNet VPN-шлюз канального уровня (L2OverIP VPN)
> Скрытие структуры трафика за счет инкапсуляции в UDP, TCP

Межсетевой экран

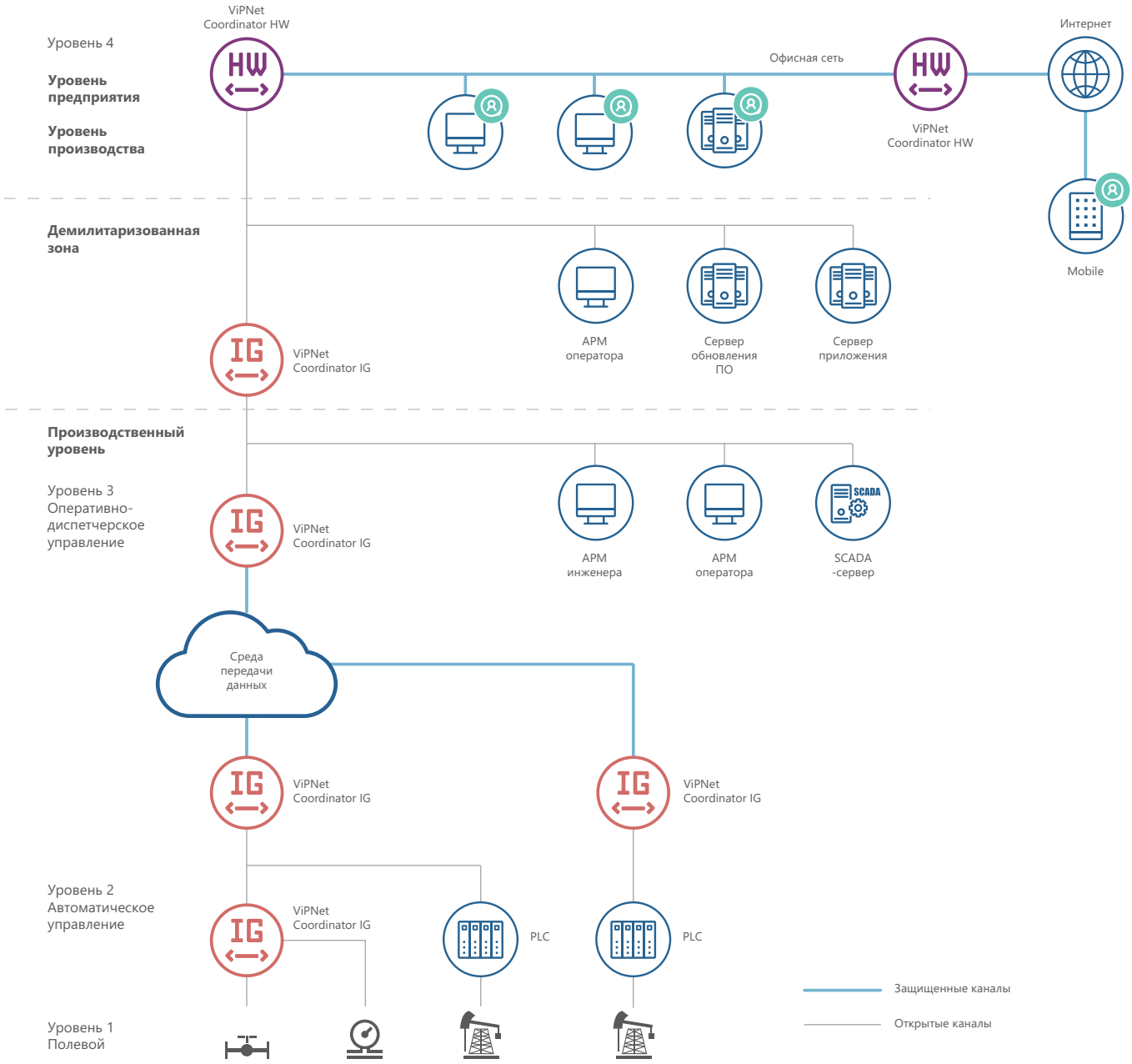
> Межсетевой экран с контролем состояния сессий
> Раздельная настройка правил фильтрации для открытого и шифруемого IP-трафика
> Раздельная настройка правил фильтрации для режимов работы промышленного МЭ: штатный режим, регламентное обслуживание, специальный режим
> NAT/PAT
> Фильтрация промышленных протоколов Modbus, Profinet, МЭК 60870-5-104, Ethernet/IP, OPC UA, MMS, DNP3
> Глубокая фильтрация протокола Modbus, МЭК-60870-5-104
> Антиспуфинг
> Прокси-сервер

Сервисные функции

> DNS-сервер
> NTP-сервер
> DHCP-сервер и DHCP-relay
> Кластер горячего резервирования
> Dead Gateway Detection (DGD) и MultiWAN
> Резервирование каналов

Сетевые функции

> Статическая маршрутизация
> Динамическая маршрутизация
> Поддержка VLAN (dot1q)
> Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)
> Агрегирование интерфейсов (EtherChannel (LACP))
> Преобразователь протоколов Modbus TCP/RTU



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 020/2011на ЭМС по промышленным стандартам

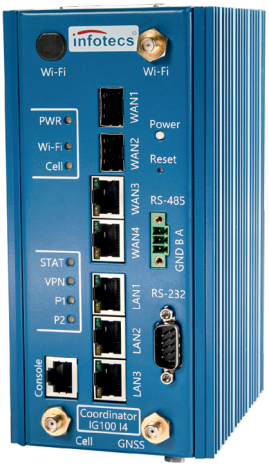
МОДЕЛЬНЫЙ РЯД

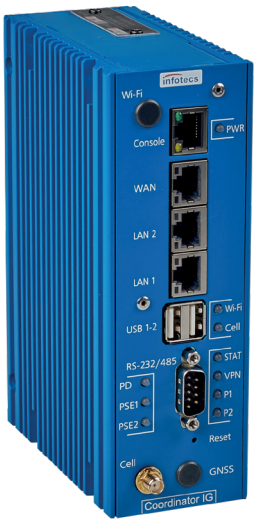
IG10 I1, IG100 I1

Порты USB	2 x USB 2.0	**RS-232/RS-485**	+ (совмещенный)
GPIO	1 x In, 1 x Out	**Разъем для SIM-карты**	1
Порты Ethernet	WAN: 1 x 10/100Base-T LAN: 2 x 10/100Base-T	**Беспроводные интерфейсы**	Wi-Fi, 3G, 4G с выносной антенной (опционально)

IG100 I4

Порты USB	2 x USB 2.0	**RS-232/ RS-485**	+
GPIO	1 x In, 1 x Out	**Разъем для SIM-карты**	2
Порты Ethernet	WAN: 2 x 10/100/1000Base-T или 2 x 10/100/1000Base-X SFP LAN: 3 x 10/100/1000Base-T	**Беспроводные интерфейсы**	Wi-Fi, 3G, 4G с выносной антенной (опционально)





IG100 I5

Порты USB	2 x USB 2.0	**RS-232/ RS-485**	+ (совмещенный)
GPIO	1 x In, 1 x Out	**Разъем для SIM-карты**	1
Порты Ethernet	WAN: 1 x 10/100BASE-T с возможностью получать питание по стандартам IEEE 802.3af и IEEE 802.3at (PoE) LAN: 2 x 10/100BASE-T с возможностью питать PoE-устройства по стандартам IEEE 802.3af и IEEE 802.3at	**Беспроводные интерфейсы**	Wi-Fi, 3G, 4G с выносной антенной (опционально)

Аппаратные характеристики	ViPNet Coordinator IG10		ViPNet Coordinator IG100		
Аппаратная платформа	IG10 I1	IG10 I2	IG100 I1	IG100 I4	IG100 I5
Форм-фактор	Блок с креплением на DIN-рейку				
Размеры (Ш × В × Г), мм	52 x 132 x 120	69 x 157 x 122	52 x 132 x 120	100 x 172 x 120	55 x 169 x 126
Вес, кг	Не более 0,65	Не более 1,5	Не более 0,65	Не более 1,8	Не более 1
Питание	12 - 24 В DC	12 - 24 В DC 2 порта	12 - 24 В DC	12 - 24 В DC 2 порта	Через порт питания – постоянный ток с напряжением от 12 до 24 В (при подключении PoE-устройств – 24 В) Через порт WAN по технологии PoE
Потребляемая мощность, Вт	Не более 10	Не более 15	Не более 10	Не более 30	С беспроводными модулями, но без подключенных USB-устройств: > не более 15 – без PoE-устройств > не более 30 – с PoE-устройствами и питанием по PoE (4 класс мощности) > не более 95 – с PoE-устройствами и питанием от блока питания
Питание от PoE	-	-	-	-	+
Рабочая температура	–40° до +60° С[1]	–40° до +60° С[1]	–20° до +60° С[1]	–40° до +60° С[1]	–20° до +60°С[1]
Электромагнитная совместимость (EMI)	ГОСТ Р51318-22 (СИСПР 22), ГОСТ CISPR 24 2013 (СИСПР 24)	ГОСТ 30805.22-2013 (CISPR.22:2006), ГОСТ 30804.6.2-2013 (IEC 61000-6-2:2005), ГОСТ CISPR 24 2013 (СИСПР 24), ГОСТ Р 51317.6.5-2006 (МЭК 61000-6-5:2001)	ГОСТ Р51318-22 (СИСПР 22), ГОСТ CISPR 24 2013 (СИСПР 24)	ГОСТ Р51318-22 (СИСПР 22), ГОСТ CISPR 24 2013 (СИСПР 24)	ГОСТ 30804.6.4 – 2013 ГОСТ 30805.22-2013 (CISPR 22:2006) для устройств класса А ГОСТ CISPR 24-2013 ГОСТ 30804.6.2-2013 (IEC 61000-6-2:2005)
Класс защиты IP	IP30				

[1] Исполнение с беспроводными модулями от -20° до +60°С

Межсетевой экран (МЭ)

Производительность МЭ, Мбит/с	10	10	60	160	60
Максимальное количество одновременных сессий	до 1000	до 1000	до 15000	до 100000	до 15000
Межсетевой экран глубокой фильтрации (DPI)	Modbus TCP, МЭК-60870-5-104				

VPN

Пропускная производительность VPN L3 и L2 на проводном канале[1], Мбит/с	10	10	60	160	60
Максимальное количество узлов, туннелируемое координатором	Не ограничено				
Рекомендуемое число зарегистрированных VPN-клиентов[2]	Недоступно	Недоступно	до 10[3]	до 10[3]	до 10[3]

Порты ввода-вывода	ViPNet Coordinator IG10		ViPNet Coordinator IG100		
Аппаратная платформа	IG10 I1	IG10 I2	IG100 I1	IG100 I4	IG100 I5
Порты Ethernet	WAN: 1 x 10/100Base-T LAN: 1 x 10/100Base-T	WAN: 2 x 10/100Base-T LAN: 3 x 10/100Base-T	WAN: 1 x 10/100Base-T LAN: 2 x 10/100Base-T	WAN: 2 x 10/100/1000Base-T или 2 x 10/100/1000Base-X SFP LAN: 3 x 10/100/1000Base-T	WAN: 1 x 10/100BASE-T с возможностью получать питание по стандартам IEEE 802.3af и IEEE 802.3at (PoE) LAN: 2 x 10/100BASE-T с возможностью питать PoE-устройства по стандартам IEEE 802.3af и IEEE 802.3at
Порты USB	2 x USB 2.0				
GSM-интерфейсы	3G или 4G с выносной антенной (опционально)				
Разъем для SIM-карты	1	2	1	2	1

[1]Указана максимальная пропускная производительность. Реальная производительность зависит от среды передачи данных и технической реализации
[2]Только для узлов со следующими версиями ПО: ViPNet Client for Windows 4.3.2, 4.5.1, ViPNet Client for Linux 4.6.0 и выше, ViPNet Client for Android 2.12, ViPNet Client for iOS 2.16 и выше; ViPNet Client 4U
[3]Не поддерживает «Деловую почту» и «Фаловый обмен» для ViPNet Client for Windows, а также ViPNet Connect

Wi-Fi в режиме клиента/ Wi-Fi в режиме точки доступа	Wi-Fi-модуль стандарта IEEE 802.11 b/g/n 2,4 ГГц с выносной антенной (опционально)				
RS-232/ RS-485	+ (совмещенный)	+	+ (совмещенный)	+	+ (совмещенный)
GPIO	1 x In, 1 x Out				

Интегрированные сервисы

DNS, NTP, DHCP-сервер	+	Прокси-сервер	+
DHCP-relay	+	Шлюз Modbus TCP/RTU и Modbus RTU/TCP	+
MultiWan	+		

Управление

Локальное управление	Консоль RS-232 (RJ45), веб-интерфейс
Удаленное управление	ViPNet Administrator, ViPNet Prime, веб-интерфейс, системная консоль
Удаленное обновление	ViPNet Administrator, ViPNet Prime
Управление политиками безопасности	ViPNet PolicyManager, ViPNet Prime

Доступность и надежность

Кластер горячего резервирования	+
Работа в необслуживаемом режиме 24x7	+
Время наработки на отказ (MTBF)	350 000 часов

ViPNet Coordinator HW4

Криптографический шлюз безопасности
для защиты каналов связи

Благодаря функциям криптографической защиты, межсетевого экранирования, а также наличию встроенных сетевых сервисов ПАК ViPNet Coordinator HW 4 является оптимальным средством защиты компьютерных сетей организации от несанкционированного доступа к ее ресурсам при передаче информации по открытым каналам связи.

В зависимости от модификации, ПАК ViPNet Coordinator HW 4 позволяет организовать защищенный доступ как в ЦОДы, так и в корпоративную облачную инфраструктуру, может быть использован для защиты филиалов компаний, небольших удаленных офисов, удаленных рабочих мест, а также терминалов и устройств, в том числе обеспечивая безопасное подключение к корпоративной защищенной сети по беспроводным каналам связи.

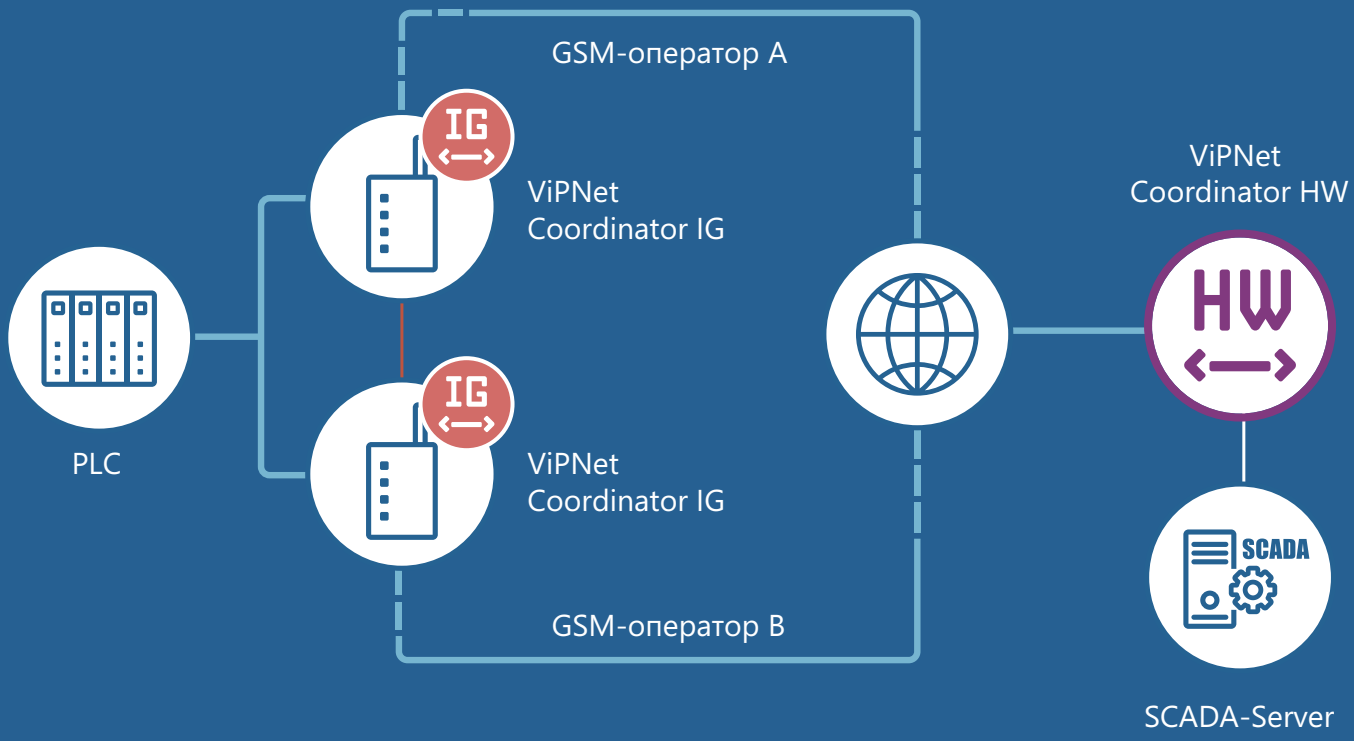
ЧТО НОВОГО

- > Поддержка новых аппаратных платформ HW100 Q1/Q2
- > Работа координаторов через TCP-туннель
- > Управление видимостью узлов ViPNet, расположенных на мобильных устройствах
- > Мониторинг внешних адресов доступа к клиентам сети ViPNet по протоколу SNMP
- > Автоматическое определение провайдера
- > Настройка прямого подключения между клиентами для протоколов SIP и H.323 через веб-интерфейс
- > Настройка маршрутизации транспортных конвертов MFTP между клиентами доверенных сетей
- > Поддержка порта 9443 в прозрачном и непрозрачном режиме работы прокси-сервера на ViPNet Coordinator HW
- > Учет расхода мобильного трафика и настройка SMTP-оповещений

ПРЕИМУЩЕСТВА

01. Организация VPN на сетевом (L3) и канальном уровне (L2)* в одном устройстве
02. Отказоустойчивый кластер (High-Availability cluster) с синхронизацией сессий позволяет минимизировать время переключения между элементами кластера до 1 секунды
03. Работа в необслуживаемом режиме
04. Централизованное и удаленное управление (SSH, WebUI)
05. Поддержка работы в современных мультисервисных сетях связи без ограничений по совместимости:
    - > со службами DHCP, WINS, DNS
    - > с динамическим преобразованием адресов (NAT, PAT)
    - > с использованием мультимедийных протоколов (SIP, H323, SCCP и др.)

*Кроме исполнения HW50



СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

01. Построение защищенных каналов связи между объектами организации (Site-to-Site и Multi Site-to-Site)
02. Защита магистральных каналов
03. Защита беспроводных сетей связи 3G и Wi-Fi
04. Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь)
05. Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение ДМЗ)
06. Защищенный доступ удаленных и мобильных пользователей
07. Взаимодействие с сетями ViPNet других организаций

СЕРТИФИКАЦИЯ

ФСБ России
> СКЗИ класса КС3
> МЭ 4 класса защищенности

ФСТЭК России
> МЭ типа А 4 класса (ИТ.МЭ.А4.ПЗ)
> МЭ типа Б 4 класса (ИТ.МЭ.Б4.ПЗ)
> 4 уровень доверия средств защиты информации

Свидетельства
> В реестре российского ПО
> В реестре Минпромторга

ВОЗМОЖНОСТИ

VPN

> VPN-шлюз сетевого уровня (L3 VPN)
> VPN-шлюз канального уровня (L2OverIP VPN)*
> Сервер IP-адресов*
> Маршрутизатор VPN-пакетов
> Маскирование структуры трафика за счет инкапсуляции в UDP, TCP

Межсетевой экран

> Межсетевой экран с контролем состояния сессий
> Раздельная настройка фильтрации для открытого и шифруемого IP-трафика
> NAT/PAT
> Антиспуфинг

Прокси-сервер

> Поддержка протокола HTTP
> Работа в «прозрачном» режиме
> Кэширование данных
> Проверка и фильтрация трафика по разным типам содержимого, передаваемого в протоколе HTTP
> Проверка трафика сторонним антивирусом по протоколу ICAP

Отказоустойчивость и резервирование

> Отказоустойчивый кластер высокой доступности по схеме «активный/пассивный» с минимальным временем переключения между элементами кластера (до 1 секунды)
> Поддержка синхронизации таблицы соединений между элементами кластера
> Отказоустойчивый кластер горячего резервирования
> Резервирование каналов связи
> Резервирование сетевых интерфейсов
> Поддержка ИБП (UPS)

Сетевые функции

> Резервирование и балансировка каналов связи: WAN (балансировка и резервирование), VPN (резервирование)
> Маршрутизация сетевого трафика на основе:
  - статической маршрутизации
  - динамической маршрутизации (OSPFv2)*
  - политик маршрутизации (Policy based routing)
> Поддержка виртуальных локальных сетей (VLAN IEEE 802.1Q)
> Агрегирование сетевых интерфейсов (bonding, EtherChannel, LACP)
> Поддержка Jumbo-кадров и технологии Path MTU Discovery
> Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)
> Реализация функций клиента и точки доступа Wi-Fi (для платформ HW50 N2 и HW100 N2)

Сервисные функции

> DHCP-сервер
> DHCP-relay
> DNS-сервер
> NTP-сервер

Управление и мониторинг

> Централизованное управление с помощью ViPNet Administrator и ViPNet Policy Manager
> Удаленное управление с помощью SSH-консоли и веб-интерфейса (HTTP/HTTPS)
> Мониторинг по протоколу SNMP v1, v2c, v3
> Экспорт системного журнала по протоколу Syslog
> Экспорт журнала IP-пакетов в формате CEF

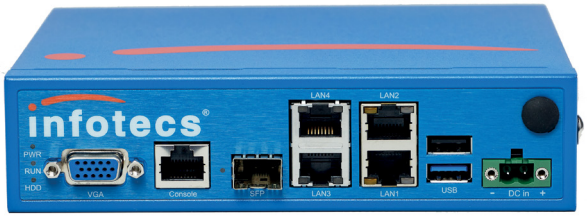
*Кроме исполнения HW50

МОДЕЛЬНЫЙ РЯД

HW50
N1-N3

VPN, Мбит/с	75	**Количество соединений**	150 000
МЭ, Мбит/с	320	**Сетевые интерфейсы**	3 x 1G RJ-45 Wi-Fi (только для N2) 3G (только для N3)

HW100
N1-N3



VPN, Мбит/с	175	**Количество соединений**	150 000
МЭ, Мбит/с	930	**Сетевые интерфейсы**	4 x 1G RJ-45 1 x 1G SFP Wi-Fi (только для N2) 3G (только для N3)

HW100
Q1-Q2

VPN, Мбит/с	400	**Количество соединений**	150 000
МЭ, Мбит/с	1400	**Сетевые интерфейсы**	4 x 1G RJ-45 2 x 1G SFP

HW1000
Q7-Q9

VPN, Мбит/с	Q7 – 915 Q8 – 2 500 Q9 – 2 500	**Количество соединений**	1 000 000
МЭ, Мбит/с	Q7 – 2 500 Q8 – 2 800 Q9 – 2 800	**Сетевые интерфейсы**	Q7 – 6 x 1G RJ-45 Q8 – 8 x 1G RJ-45 Q9 – 8 x 1G RJ-45 4 x 1G SFP

HW2000
Q5

VPN, Мбит/с	L3 – 6 600 L2 – 6 000	**Количество соединений**	3 000 000
МЭ, Мбит/с	9 200	**Сетевые интерфейсы**	4 x 1G RJ-45 4 x 1G SFP 4 x 10G SFP+

HW5000
Q2

VPN, Мбит/с	10 000	**Количество соединений**	6 500 000
МЭ, Мбит/с	13 000	**Сетевые интерфейсы**	4 x 1G RJ-45 8 x 10G SFP+

ViPNet Coordinator VA

Виртуализированный криптографический шлюз безопасности

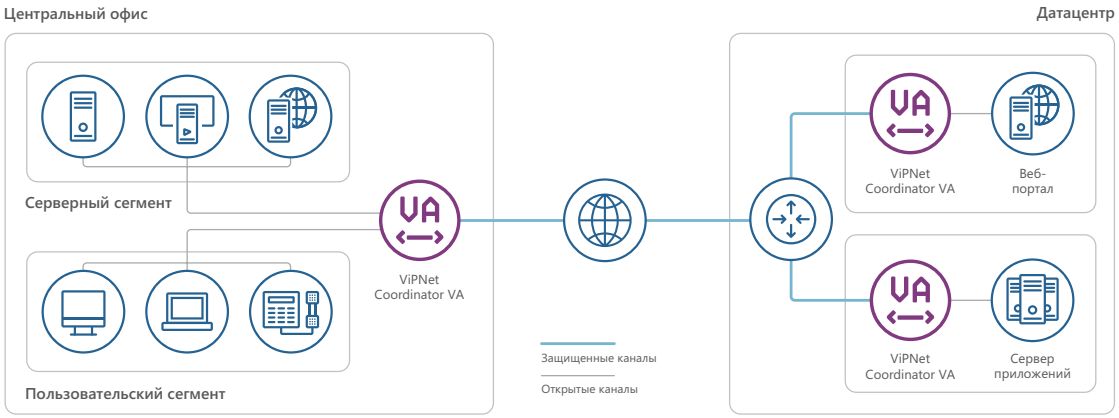
Виртуальный шлюз легко интегрируется в существующую сетевую инфраструктуру и отвечает самым высоким требованиям с точки зрения функциональности, удобства для пользователя, надежности и отказоустойчивости.

ViPNet Coordinator VA обеспечивает безопасность передаваемых данных и многоуровневую защиту виртуальной и облачной инфраструктуры как для частных, так и для публичных облаков, не меняя привычного способа доступа пользователей к бизнес-данным.

ViPNet Coordinator VA представляет собой виртуализированное программное обеспечение, которое предназначенно для развертывания на популярных платформах виртуализации (KVM, VMware ESXi, Microsoft Hyper-V, Oracle VM).

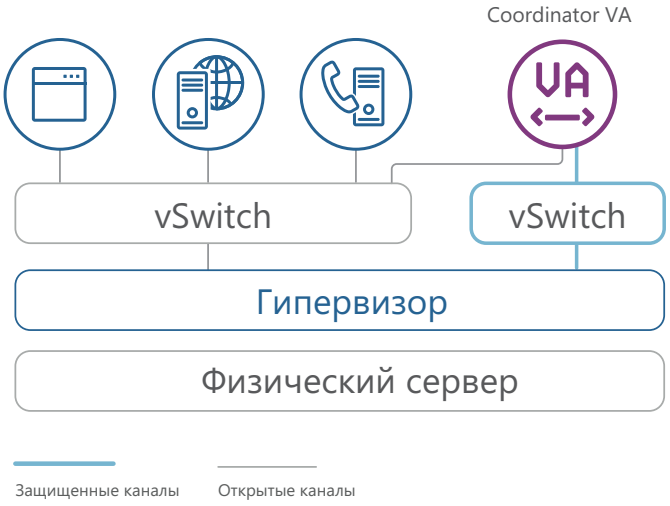
ПРЕИМУЩЕСТВА

- > Удобство управления и скорость развертывания
- > Функциональность, соответствующая аппаратным шлюзам ViPNet Coordinator HW
- > Отсутствие дополнительных затрат на размещение и обслуживание оборудования
- > Единая система управления для виртуальных и аппаратных шлюзов безопасности
- > Отказоустойчивый кластер (High-Availability cluster) с синхронизацией сессий позволяет минимизировать время переключения между элементами кластера до 1 секунды
- > Поддержка распространенных систем виртуализации
- > Гибкое лицензирование и быстрое масштабирование
- > Организация VPN на сетевом (L3) и канальном уровне (L2) в одном виртуальном устройстве



СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

01. Построение защищенных каналов связи между объектами организации (Site-to-Site и Multi Site-to-Site)
02. Защита магистральных каналов связи
03. Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение ДМЗ)
04. Защита данных внутри виртуальной и облачной инфраструктуры
05. Взаимодействие с сетями ViPNet других организаций
06. Защищенный доступ удаленных и мобильных пользователей
07. Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь)



ВОЗМОЖНОСТИ

VPN

> VPN-шлюз сетевого уровня (L3 VPN)
> VPN-шлюз канального уровня (L2OverIP VPN)
> Сервер IP-адресов
> Маршрутизатор VPN-пакетов
> Маскирование структуры трафика за счет инкапсуляции в UDP, TCP

Сетевые функции

> Резервирование и балансировка каналов связи: WAN (балансировка и резервирование), VPN (резервирование)
> Маршрутизация сетевого трафика на основе:
  - статической маршрутизации
  - динамической маршрутизации (OSPFv2)
  - политик маршрутизации (Policy based routing)
> Поддержка виртуальных локальных сетей (VLAN IEEE 802.1Q)
> Агрегирование сетевых интерфейсов (bonding, EtherChannel, LACP)
> Поддержка Jumbo-кадров и технологии Path MTU Discovery
> Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)

Межсетевой экран

> Межсетевой экран с контролем состояния сессий
> Раздельная настройка фильтрации для открытого и шифруемого IP-трафика
> NAT/PAT
> Антиспуфинг

Прокси-сервер

> Поддержка протокола HTTP
> Работа в «прозрачном» режиме
> Кэширование данных
> Проверка и фильтрация трафика по разным типам содержимого, передаваемого в протоколе HTTP
> Проверка трафика сторонним антивирусом по протоколу ICAP

Сервисные функции

> DHCP-сервер
> DHCP-relay
> DNS-сервер
> NTP-сервер

Отказоустойчивость и резервирование

> Отказоустойчивый кластер высокой доступности по схеме «активный/пассивный» с минимальным временем переключения между элементами кластера (до 1 секунды)
> Поддержка синхронизации таблицы соединений между элементами кластера
> Резервирование сетевых интерфейсов как на уровне гипервизора, так и на уровне отдельных виртуальных машин
> Легкое восстановление конфигурации с помощью штатных средств гипервизора – резервных копий и снимков (снапшотов)

Управление и мониторинг

> Централизованное управление с помощью ViPNet Administrator и ViPNet Policy Manager
> Удаленное управление с помощью SSH-консоли и веб-интерфейса (HTTP/HTTPS)
> Мониторинг по протоколу SNMP v1, v2c, v3
> Экспорт системного журнала по протоколу Syslog
> Экспорт журнала IP-пакетов в формате CEF

Тип лицензии	VA100	VA500	VA1000	VA2000
Производительность[1]				
L3 VPN, Мбит/с	185	600	1 900	4 500
L2 VPN, Мбит/с	180	585	1 900	4 500
МЭ, Мбит/с	360	1 000	3 500	5 500
Количество обслуживаемых соединений	150 000	500 000	1 000 000	3 000 000
Рекомендуемое число зарегистрированных ViPNet-клиентов	100	500	1 000	2 000
Системные требования				
Количество ядер CPU, шт.	2	2	4	8
Оперативная память, Гб	2	2	4	8
Требования к дисковой подсистеме, Гб	80	80	80	80
Сетевые интерфейсы, Гбит/с	1	1	1/10	1/10
Поддерживаемые среды виртуализации[2]	> VMware ESXi 6.7/7.0 > VMware Workstation Pro 15.x / 16.x > Microsoft Hyper-V Server 2019 > KVM, например Qemu-KVM или Proxmox > Oracle VM VirtualBox 6.x > Oracle VM Server 3.4			

[1]Условия измерений: VMware ESX 6.7, CPU Xeon E-2278GE, сетевые адаптеры работают в режиме passthrough (DirectPath I/O). Производительность зависит от активированных функций, характеристик обрабатываемого сетевого трафика: протоколов, размера пакетов, количества сессий. Производительность может меняться вследствие изменений, вносимых в новые версии программного обеспечения.

[2]Работа на других платформах виртуализации возможна, но не гарантируется.

СЕРТИФИКАЦИЯ

ФСБ России
> СКЗИ класса КС1

ФСТЭК России
> МЭ типа Б 4 класса защищенности (ИТ.МЭ.Б4.ПЗ)
> 4 уровень доверия средств защиты информации

Свидетельства
> В реестре российского ПО

ViPNet Client

Программный комплекс для защиты информации при ее передаче по открытым каналам связи с мобильных и стационарных рабочих мест

ПРЕИМУЩЕСТВА

01. Высокая производительность шифрования и фильтрации трафика позволяет в реальном времени осуществлять защиту трафика
02. Защита канала не влияет на работу сторонних приложений на устройстве
03. Равный доступ к ресурсам корпоративных информационных систем независимо от места и способа подключения пользователя к телекоммуникационной сети
04. Ключи шифрования, политики безопасности и обновления ПО ViPNet доставляются через надежный защищенный канал

ВОЗМОЖНОСТИ

Защита устройства и трафика

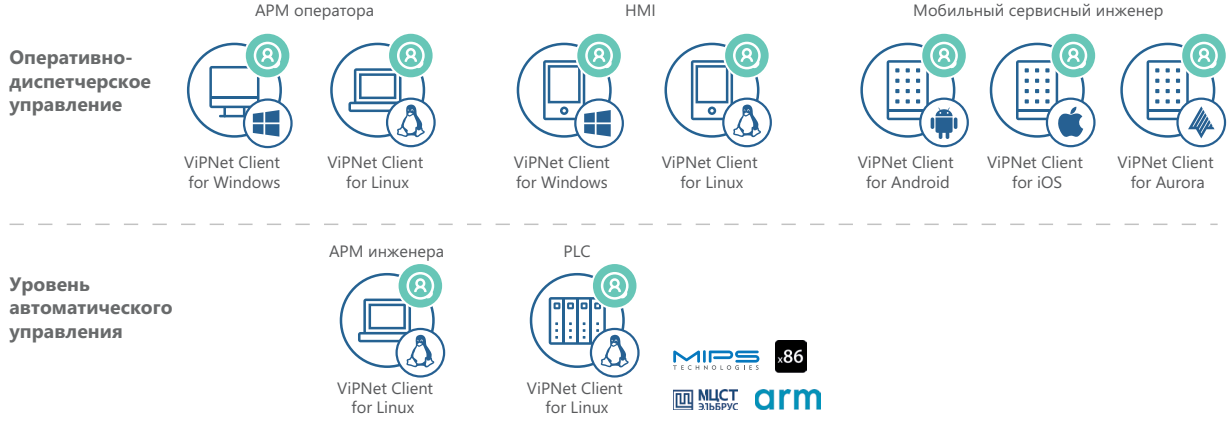
ViPNet Client защищает устройство пользователя, что позволяет безопасно работать с любыми внутренними ресурсами своей организации через интернет благодаря шифрованию трафика с использованием алгоритмов ГОСТ 28147-89, ГОСТ 34.12-2018, ГОСТ 34.13-2018 на ключах длиной 256 бит. Передаваемые данные недоступны для посторонних.

Работа в защищенной сети

ViPNet Client работает в составе сети ViPNet, совместимой со всеми продуктами линейки ViPNet Network Security, и поддерживает приложение ViPNet CSS Connect для защищенного общения пользователей (звонки, чат, файловый обмен).

Программный комплекс ViPNet Client благодаря возможности работы на разных операционных системах и архитектурах аппаратных платформ может быть установлен на объекты АСУ и АСУ ТП для защиты каналов связи этих объектов:

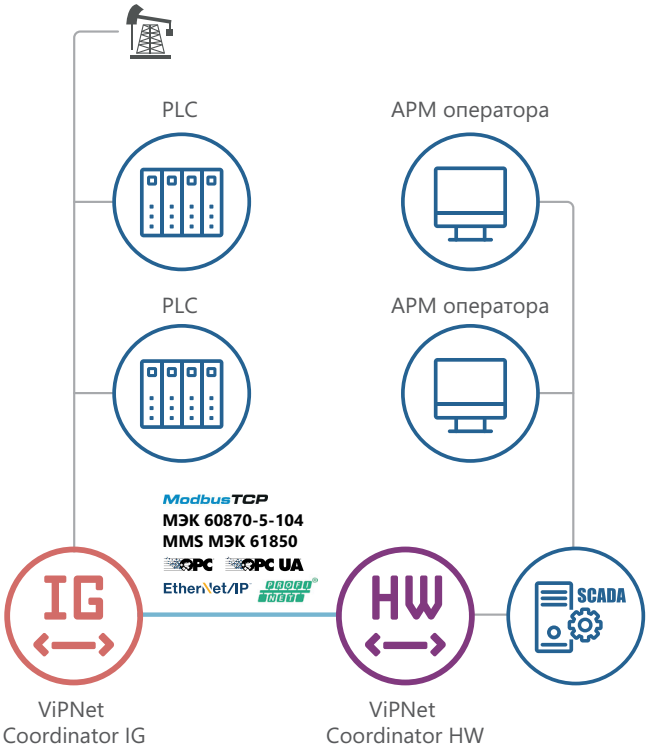
> стационарные АРМ операторов
> стационарные АРМ инженеров
> HMI-панели
> ноутбуки сервисного персонала
> мобильные устройства сервисного персонала
> программируемые логические контроллеры

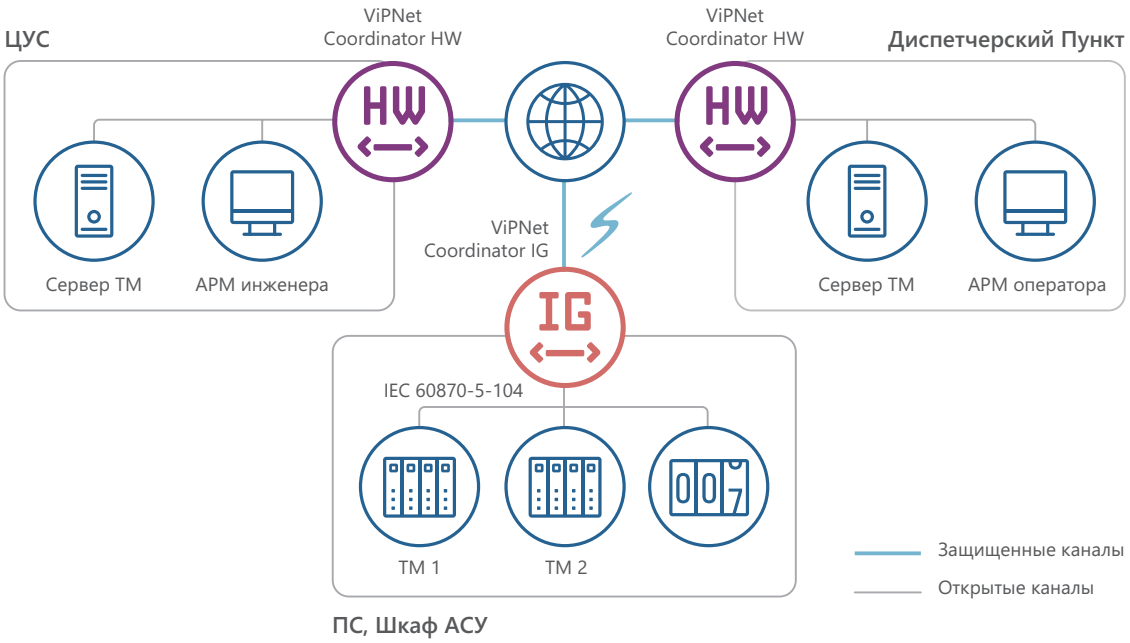


Сценарии эксплуатации сетевых средств защиты информации в АСУ и АСУ ТП

Защищенное удаленное управление

ПАК ViPNet Coordinator IG и ПАК ViPNet Coordinator HW могут использоваться для организации защищенного удаленного управления в АСУ и АСУ ТП за счет построения защищенного VPN-канала по технологии ViPNet между объектами систем. ПАК ViPNet Coordinator IG идеально подходит для решения задачи защиты передачи команд управления на уровне автоматического управления или полевом уровне систем, использующих проводные каналы связи. Продукт имеет 3 порта подключения к проводным сетям и может использоваться как в виде отдельной единицы, так и в виде кластера. Для организации канала связи на уровне оперативно-диспетчерского управления можно использовать как ПАК ViPNet Coordinator IG, так и ПАК ViPNet Coordinator HW соответствующей пропускной способности.

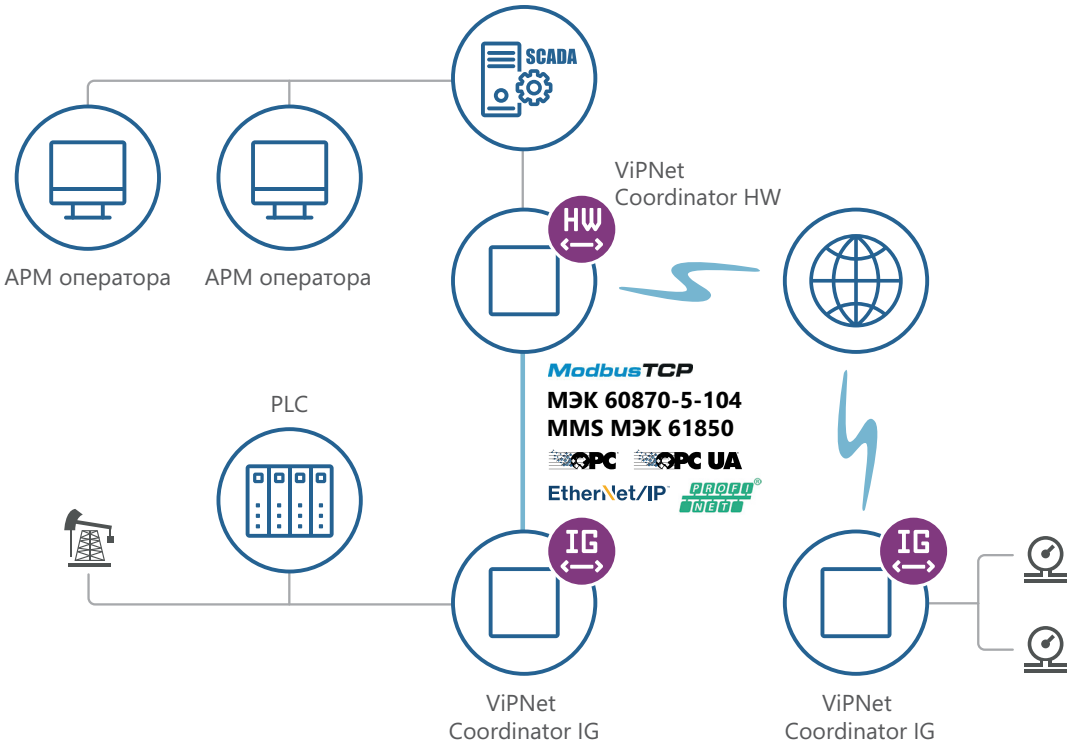




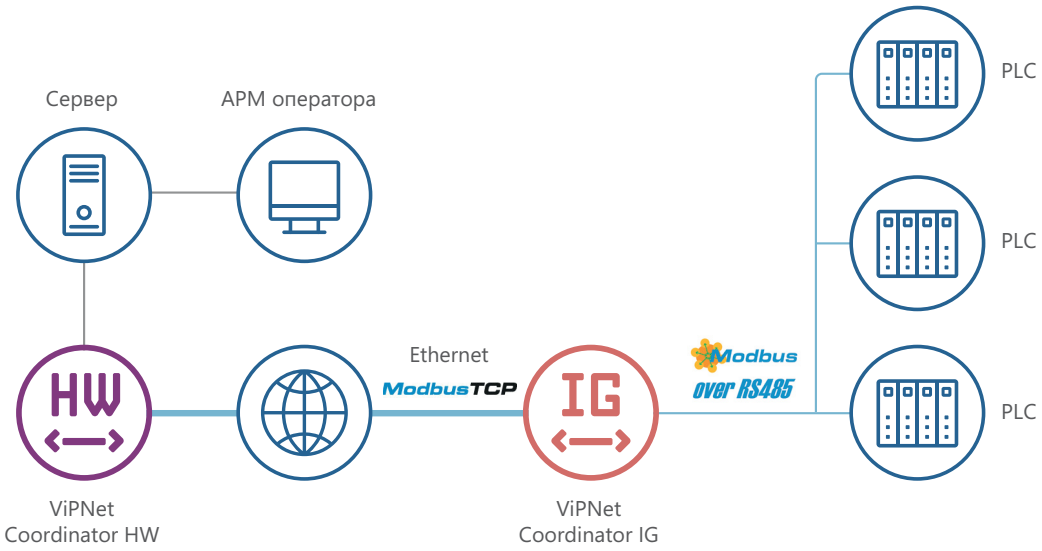
Для защищенного управления распределенными по территории объектами по беспроводному каналу Wi-Fi или по сотовым каналам передачи данных можно использовать ПАК ViPNet Coordinator IG с беспроводным модулем передачи данных. ПАК ViPNet Coordinator IG имеет возможность подключения внешней антенны, которая может быть вынесена за пределы места установки продукта. В качестве антенны можно использовать антенну из комплекта или подобрать необходимый по радиусу приема образец. ПАК ViPNet Coordinator IG может работать как в режиме точки доступа, так и в режиме беспроводного клиента.

Защищенный удаленный мониторинг

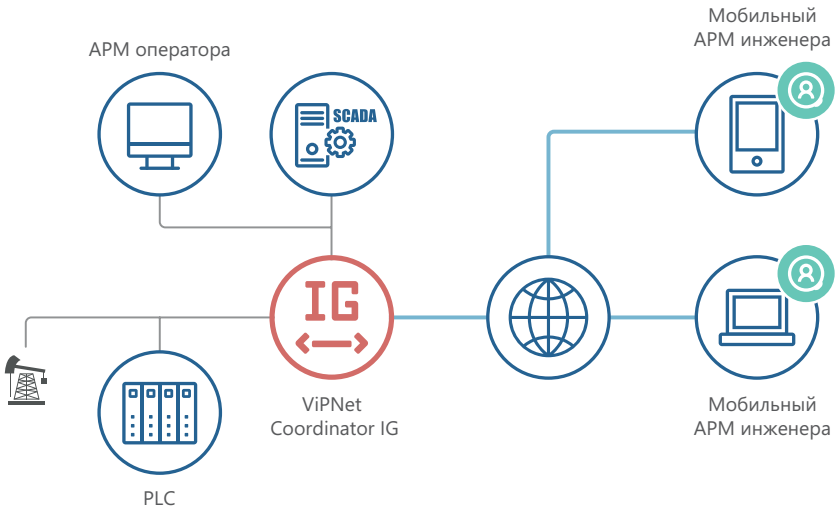
ПАК ViPNet Coordinator IG и ПАК ViPNet Coordinator HW могут использоваться для организации защищенного удаленного мониторинга в АСУ и АСУ ТП за счет построения защищенного VPN-канала по технологии ViPNet VPN между объектами систем. Для передачи данных мониторинга возможно использовать как проводные, так и беспроводные каналы связи.



С помощью ПАК ViPNet Coordinator IG можно подключить контроллеры и другое оборудование, работающее по последовательным интерфейсам, к системе сбора информации. Для данного функционала необходимо использовать встроенный в продукт конвертер протокола Modbus RTU/Modbus TCP.



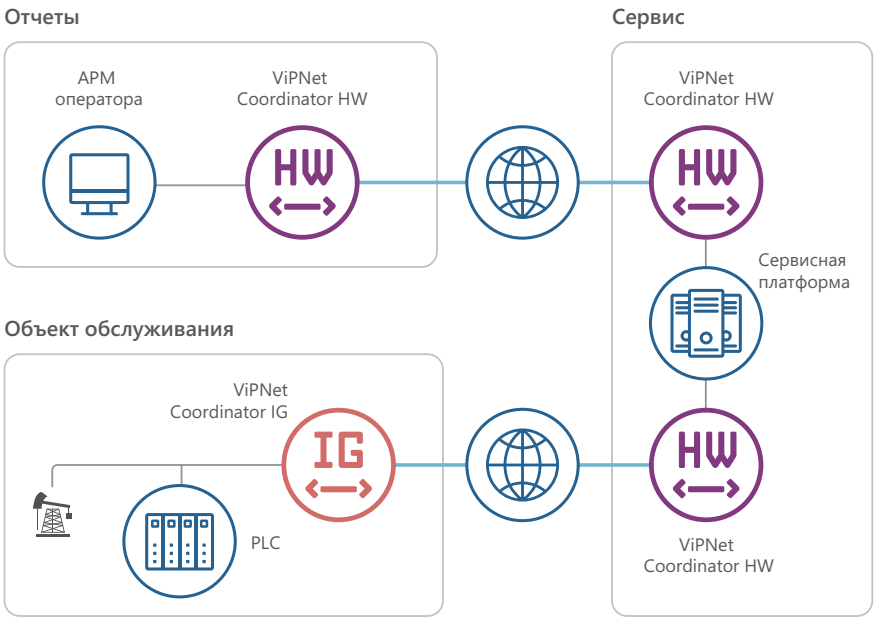
Защищенное удаленное обслуживание



ПАК ViPNet Coordinator IG позволяет подключить безопасно к объектам АСУ и АСУ ТП стационарные и мобильные рабочие места сервисных инженеров компании, на которых установлены ПК ViPNet Client или которые защищены ПАК ViPNet Coordinator HW.

В качестве рабочих мест могут использоваться стационарные компьютеры, ноутбуки и планшеты.

ПАК ViPNet Coordinator IG может использоваться для безопасного обслуживания объектов АСУ и АСУ ТП третьей стороной – сервисной компанией. Для такого сценария работы рекомендовано подключение через ДМЗ и эксплуатация ПАК ViPNet Coordinator IG как межсетевого экрана типа Д. Доступ сервисной компании необходимо ограничить получением информации мониторинга для штатного режима функционирования ПАК и разрешить режим управления и конфигурирования только для режима регламентного обслуживания.



Для выполнения операций по обслуживанию и конфигурированию объекта на ПАК ViPNet Coordinator IG должны быть высланы соответствующие политики безопасности, чтобы перевести его в режим регламентного обслуживания.

При таком сценарии воздействие на технологический процесс извне невозможно. ПАК ViPNet Coordinator IG также можно использовать для безопасного подключения оборудования объекта АСУ к сторонним сервисным платформам.

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

soft@infotecs.ru
hotline@infotecs.ru
www.infotecs.ru

IS24_00RU