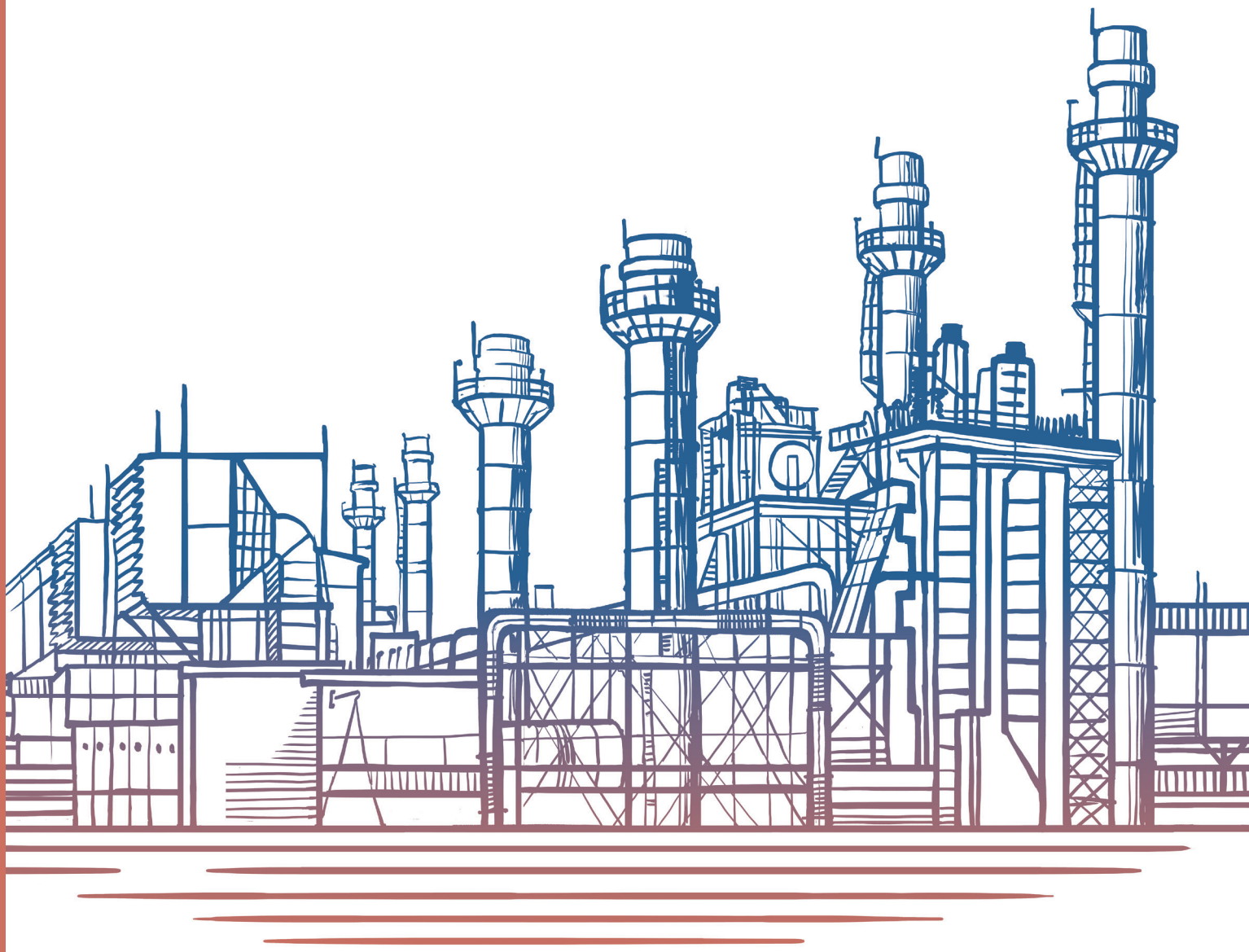
ИНФОТЕКС

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 недостаточны. Ранее российские вендоры не сталкивались с большим количеством атак на свое оборудование ввиду 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.

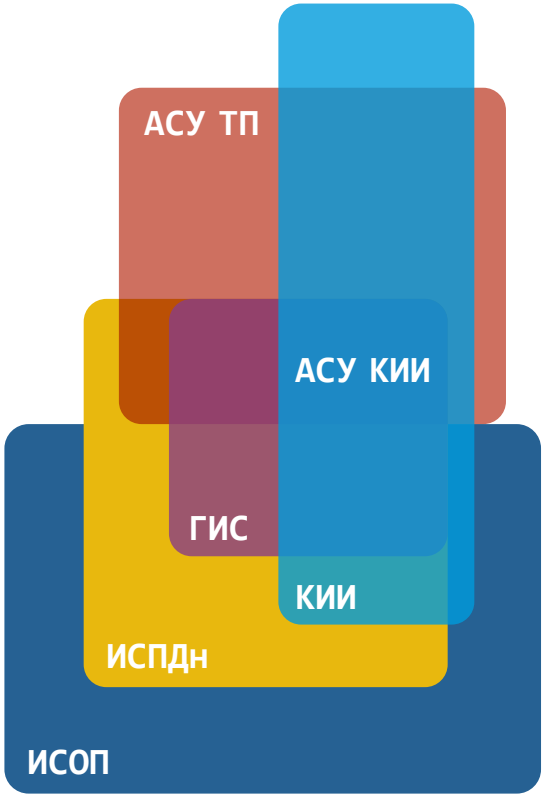
Последствия же кибератак на промышленные предприятия становятся причиной не только утечек данных и перебоя в работе IT-систем, но и прямой причиной внеплановых простоев, приводящих к прямым убыткам.

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:

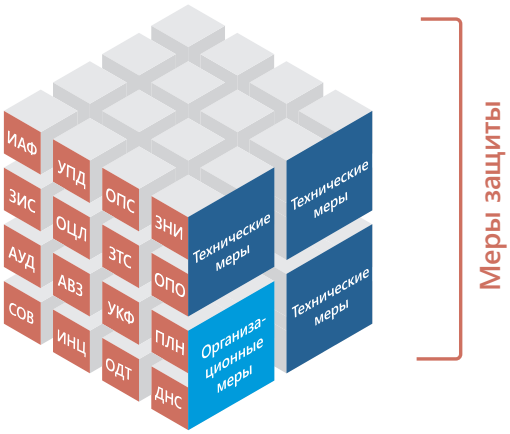
- Приказ ФСТЭК России № 235 от 21.12.2017 г. «Требования к созданию систем безопасности объектов КИИ»
- Приказ ФСТЭК России № 239 от 25.12.2017 г. «Требования по обеспечению безопасности объектов КИИ»
- Приказ № 336 ФСБ России от 24.07.2018 г. «О Национальном координационном центре по компьютерным инцидентам»
- 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

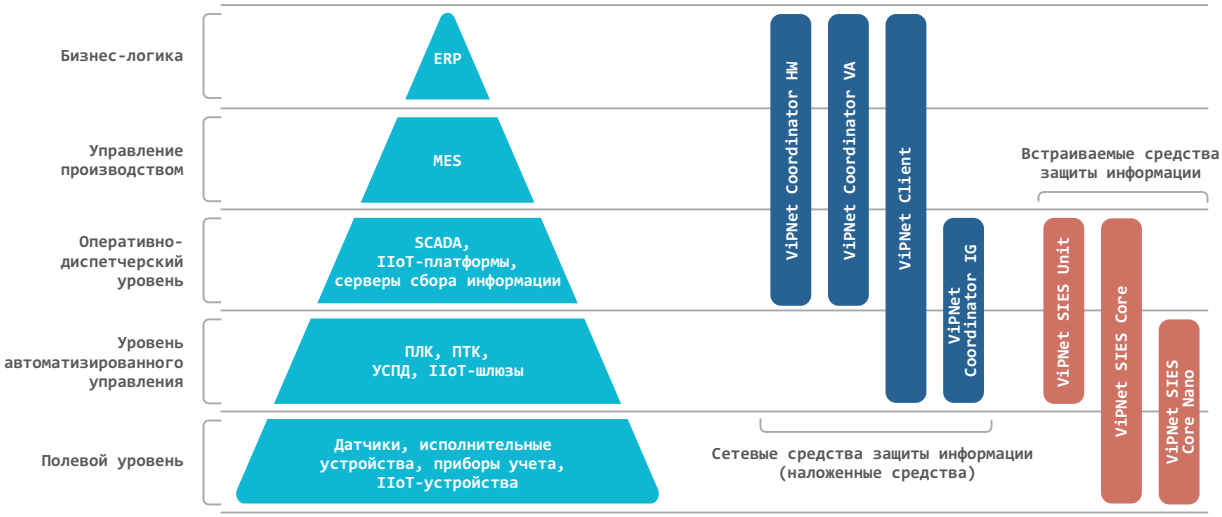


Меры Приказа № 239 ФСТЭК России

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 продукты ViPNet Channel Protection – шлюзы безопасности ViPNet Coordinator HW, ViPNet Coordinator VA и программные комплексы ViPNet Client

ViPNet Coordinator IG5

Программно-аппаратный комплекс (ПАК) ViPNet Coordinator IG5 – российский индустриальный шлюз безопасности, предназначенный для организации защищенных каналов связи, межсетевого экранирования и предотвращения несанкционированного доступа к объектам защиты

ПАК ViPNet Coordinator IG 5 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

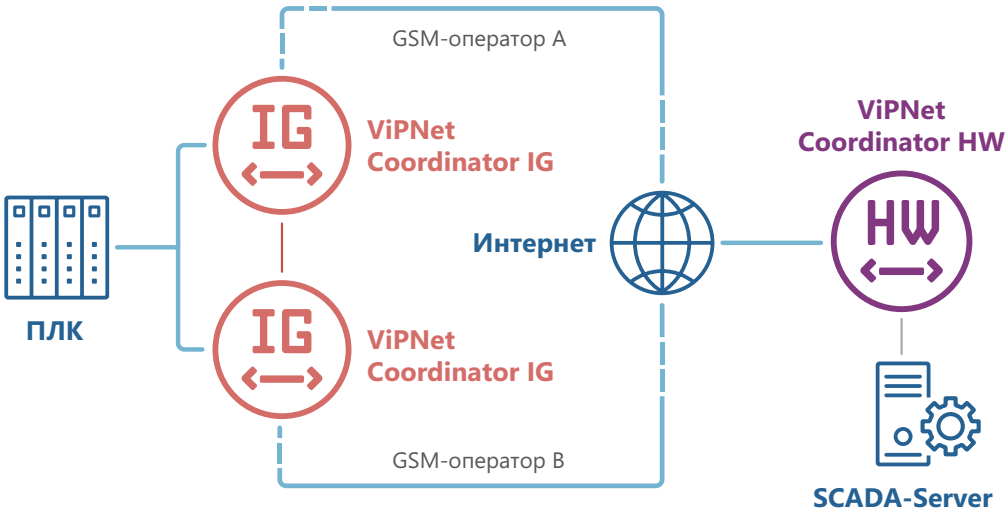
> Организация ДМЗ

> Организация защищенного удаленного мониторинга

> Организация защищенного удаленного сервисного обслуживания

> Организация защищенного подключения оборудования по последовательным интерфейсам

> Фильтрация промышленных протоколов на прикладном уровне



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

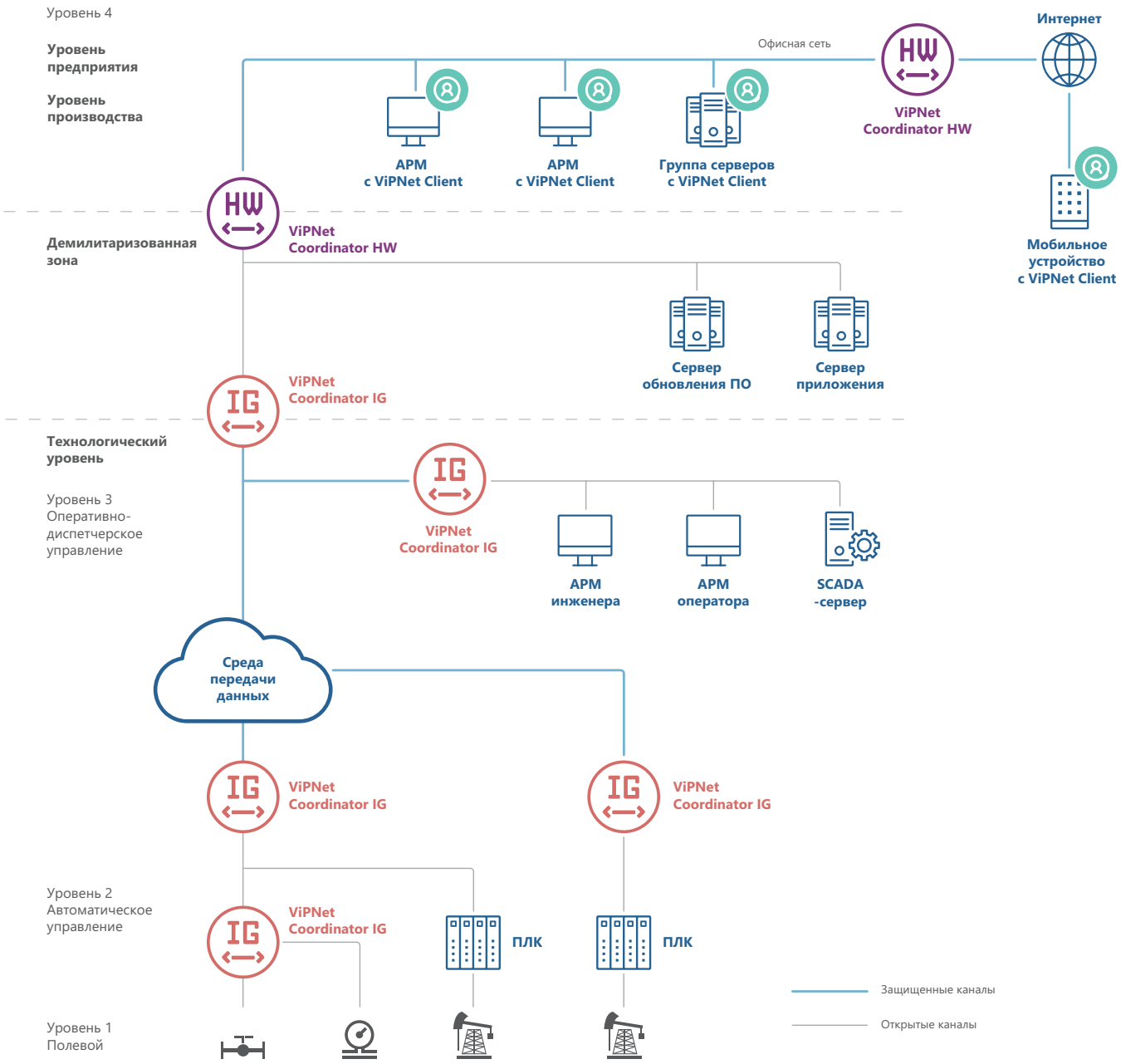
> Межсетевой экран с контролем состояния сессий
> Раздельная настройка правил фильтрации для открытого и шифруемого IP-трафика
> Раздельная настройка правил фильтрации для режимов работы промышленного МЭ: штатный режим, регламентное обслуживание, специальный режим
> NAT/PAT
> Глубокая фильтрация протокола Modbus, МЭК-60870-5-104
> Антиспуфинг
> Прокси-сервер с возможностью проверки трафика сторонним антивирусом

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

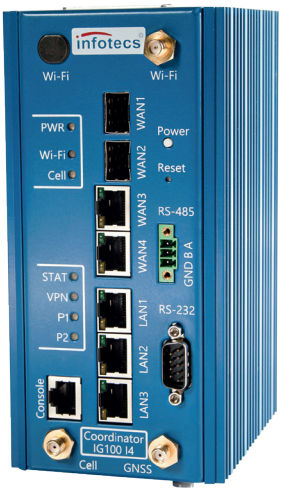
Декларация соответствия ТР/ТС 020/2011на ЭМС по промышленным стандартам

МОДЕЛЬНЫЙ РЯД

IG100 I1

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

IG100 I4



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

IG100 I5

Порты USB	2 x USB 2.0
GPIO	1 x In, 1 x Out
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
RS-232/ RS-485	+ (совмещенный)
Разъем для SIM-карты	1
Беспроводные интерфейсы	Wi-Fi, 3G, 4G с выносной антенной (опционально)

IG1000 Q1

VPN, Мбит/с	900	**Количество соединений**	1 000 000
МЭ, Мбит/с	900	**Сетевые интерфейсы**	4 x 1G RJ-45 4 x 1G SFP

Аппаратные характеристики	ViPNet Coordinator IG100			ViPNet Coordinator IG1000	ViPNet Coordinator IG VA*
Аппаратная платформа	**IG100 I1**	**IG100 I4**	**IG100 I5**	**IG1000 Q1**	**Виртуальная машина**
Форм-фактор	Блок с креплением на DIN-рейку			В стойку (19" Rack 1U)	В форматах OVA, Qcow2, RAW, VHD
Размеры (Ш × В × Г), мм	51 x 127 x 120	82 x 181 x 135	55 x 169 x 126	430 x 44 x 476	–
Версия ПО	5.1 и выше	5.1 и выше	5.2 и выше	5.2 и выше	5.2 и выше
Питание	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	220 В, 50 Гц, 2 резервированных блока пиания с «горячей» заменой	–
Потребляемая мощность, Вт	Не более 10	Не более 15	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	230 Вт	–
Питание от PoE	–	–	EEE 802.3at, power class 4 (до 25 Вт)	–	–
Рабочая температура	–40° до +60° С	–40° до +60° С	–40° до +60°С	+10° до +35° С	–

* ViPNet Coordinator IG VA поставляется только в ознакомительных целях. Не сертифицируется

Порты ввода-вывода

Аппаратная платформа	IG100 I1	IG100 I4	IG100 I5	IG1000 Q1	Виртуальная машина
Порты Ethernet	WAN: 1 x 10/100Base-T LAN: 2 x 10/100Base-T	WAN: 1 x 10/100 Base-T LAN: 2 x 10/100 Base-T	WAN: 1 x 10/100 Base-T PoE 802.3af&at LAN: 2 x 10/100 Base-T PoE 802.3af&at	4 x 10/100/1000 Base-T 4 x 1000 Base-X SFP	–
Порты USB	2 x USB 2.0	2 x USB 2.0	2 x USB 2.0	6 x USB 2.0	–
GSM-интерфейсы	3G или 4G с выносной антенной (опционально)	4G с выносной антенной (опционально)	4G с выносной антенной (опционально)	–	–
Разъем для SIM-карты	1 шт	2 шт	1 шт	–	–
Wi-Fi в режиме клиента	Wi-Fi-модуль стандарта IEEE 802.11 b/g/n 2,4 ГГц с выносной антенной (опционально)			–	–
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	+ (совмещен с RS-485)	+	+ (совмещен с RS-485)	–	–
RS-485	+ (совмещен с RS-232)	+	+ (совмещен с RS-232)	–	–
GPIO	1 x In, 1 x Out	2 x In, 2 x Out	1 x In, 1 x Out	16 x In, 8 x Out	–

VPN

Производительность VPN	55 Мбит/с	250 Мбит/с	55 Мбит/с	900 Мбит/с	900 Гбит/с
Производительность L2 VPN	55 Мбит/с	250 Мбит/с	55 Мбит/с	900 Мбит/с	900 Гбит/с
Рекомендуемое число зарегистрированных VPN-клиентов (сноска)	до 10	до 10	до 10	до 100	до 100

Межсетевой экран (МЭ)

Производительность МЭ	55 Мбит/с	250 Мбит/с	55 Мбит/с	900 Мбит/с	900 Гбит/с
Максимальное количество одновременных сессий	до 15 000	до 100 000	до 15 000	до 250 000	до 250 000
Межсетевой экран глубокой фильтрации (DPI)	Modbus TCP/RTU, МЭК 60870-5-104				

Интегрированные сервисы

Аппаратная платформа	IG100 I1	IG100 I4	IG100 I5	IG1000 Q1	Виртуальная машина
Прокси-сервер, подключение антивируса по ICAP	–	+	–	+	+
Шлюз Modbus TCP/RTU и Modbus RTU/TCP	1 шт	2 шт	1 шт	2 шт через внешний преобразователь USB/RS-485	–

Управление

Локальное управление	Консоль, веб-интерфейс
Удаленное управление	ViPNet Prime, веб-интерфейс, SSH
Удаленное обновление	ViPNet Prime
Управление политиками безопасности	ViPNet Prime

Доступность и надежность

Кластер горячего резервирования	+	+	+	+	–
Работа в необслуживаемом режиме 24x7	+	+	+	+	–
Время наработки на отказ (MTBF)	350 000 часов	350 000 часов	350 000 часов	50 000 часов	–

ViPNet Coordinator HW5

Криптографический шлюз безопасности,
реализующий концепцию NGFW
(Next-Generation Firewall –
межсетевой экран следующего поколения)

ViPNet Coordinator HW 5 – решение, реализующее в одном устройстве ряд функций безопасности, действующих совместно:

- криптографический шлюз, обеспечивающий построение VPN на сетевом (L3) и канальном (L2) уровнях модели OSI
- межсетевой экран SPI (Stateful Packet Inspection)
- прокси-сервер
- межсетевой экран уровня приложений DPI (Deep Packet Inspection)
- средство обнаружения и предотвращения вторжений (IDS/IPS)
- кластер высокой доступности (HA-cluster)

ViPNet Coordinator HW 5 реализуется в исполнении программно-аппаратного комплекса на доверенной аппаратной платформе, а также в виде виртуального устройства, которое может функционировать в виртуальной среде (KVM, VMware ESXi, Microsoft Hyper-V, Oracle XenServer).

Реализованные сетевые функции и сервисы безопасности активируются в соответствии с приобретенной лицензией (лицензируются отдельные модули).

ЧТО НОВОГО

01. Поддержка алгоритмов «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
02. Межсетевой экран уровня приложений (DPI)
03. Обнаружение и предотвращение вторжений (IDS/IPS)
04. Многопользовательский ролевой доступ
05. Подсистема идентификации пользователей (LDAP, Active Directory, Captive Portal)
06. Кластер высокой доступности (HA-cluster) с синхронизацией таблицы открытых соединений
07. Централизованное и удаленное резервное копирование конфигурации

СЕРТИФИКАЦИЯ

ФСБ России

- СКЗИ класса КС3

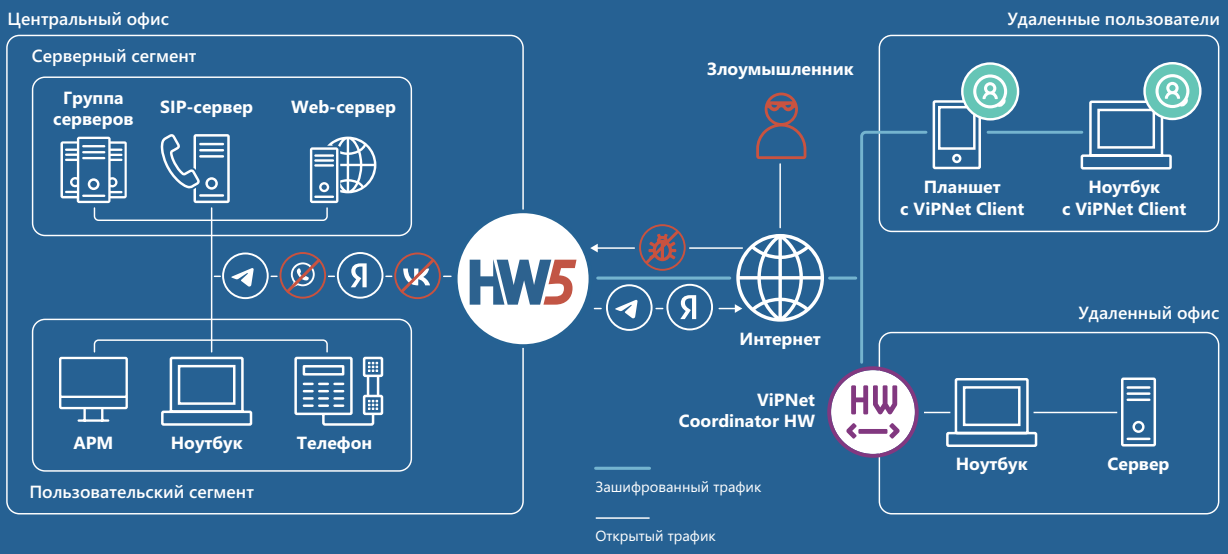
Свидетельства

- В реестре российского ПО
- В реестре Минпромторга

ФСТЭК России

- МЭ типа А 4 класса (ИТ.МЭ.А4.ПЗ)
- МЭ типа Б 4 класса (ИТ.МЭ.Б4.ПЗ)
- СОВ уровня сети 4 класса защиты (ИТ.СОВ.С4.ПЗ)
- 4 уровень доверия средств защиты информации

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ



- Построение защищенных каналов связи между объектами организации (Site-to-Site и Multi Site-to-Site)
- Защищенный доступ удаленных пользователей
- Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение ДМЗ)
- Обнаружение и нейтрализация сетевых вторжений
- Комплексная защита от сетевых угроз
- Защита магистральных каналов, соединяющих ЦОДы между собой
- Защита беспроводных сетей связи 3G/LTE и Wi-Fi
- Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь)
- Взаимодействие с сетями ViPNet других организаций

ВОЗМОЖНОСТИ

VPN

- VPN-шлюз сетевого уровня (L3 VPN)
- VPN-шлюз канального уровня (L2OverIP VPN)*
- Поддержка криптографических алгоритмов ГОСТ 34.12-2018 «Магма» и «Кузнечик», ГОСТ 28147-89
- Сервер IP-адресов и маршрутизатор VPN-пакетов*
- Маскирование структуры трафика за счет инкапсуляции в UDP, TCP

Идентификация пользователей

- Интеграция с Microsoft Active Directory
- Captive Portal и интеграция с LDAP-каталогом

Межсетевой экран (SPI)

- Фильтрация трафика на сетевом и транспортном уровнях модели OSI с контролем состояния сессий
- Раздельная настройка фильтрации для открытого и шифруемого IP-трафика
- NAT/PAT
- Антиспуфинг

Обнаружение и предотвращение вторжений (IPS)

> Анализ сетевого трафика для защиты от различного вида сетевых атак и вирусов, попыток эксплуатации уязвимостей и получения несанкционированного доступа
> Работа как в режиме предотвращения вторжений (IPS), так и обнаружения (IDS) с фиксацией событий
> Сигнатурный и эвристический методы анализа трафика
> Автоматизированное обновление баз правил с сервера обновлений
> База правил регулярно обновляется специалистами ГК «ИнфоТеКС» для поддержания в актуальном состоянии

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 каналов связи
> Резервирование сетевых интерфейсов
> Поддержка ИБП (UPS)

Управление и мониторинг

> Централизованное управление шлюзом
> Удаленное управление шлюзом с помощью SSH-консоли и веб-интерфейса (HTTPS)
> Ролевая модель доступа – разделение полномочий между несколькими администраторами, аудит действий администраторов
> Централизованное обновление ключевой информации и конфигурации
> Мониторинг по протоколам SNMP v1, v2c, v3
> Автоматическое резервное копирование конфигурации шлюза и экспорт в систему централизованного управления
> Экспорт системного журнала по протоколу Syslog
> Экспорт журнала IP-пакетов в формате CEF

* Кроме исполнения HW50

Межсетевой экран уровня приложений (DPI)

> Фильтрация трафика на прикладном уровне модели OSI с помощью технологии DPI с целью отслеживания активности приложений и прикладных протоколов
> Выявление и блокировка более 2000 прикладных протоколов и приложений
> Выявление приложений, трафик которых шифруется или маскируется
> Фильтрация трафика для заданного пользователя (AD, LDAP)

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 внешним антивирусом по протоколу ICAP

Сетевые функции

> Резервирование и балансировка каналов связи: WAN (балансировка и резервирование), VPN (резервирование)
> Маршрутизация сетевого трафика на основе:
  - статической маршрутизации
  - динамической маршрутизации (OSPFv2, BGP)*
  - политик маршрутизации (policy based routing)
> Поддержка виртуальных локальных сетей (VLAN 802.1Q)
> Агрегирование сетевых интерфейсов (802.3ad, 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

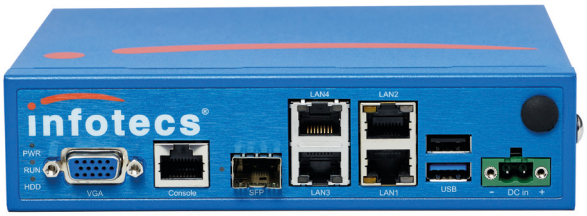
> DHCP-relay
> DHCP-сервер
> DNS-сервер
> NTP-сервер

МОДЕЛЬНЫЙ РЯД

HW50
N1-N3

МЭ UDP 1518 байт (Мбит/с)	450	**Application Control (МЭ+DPI) (Мбит/с)**	25	**Количество соединений**	150 000
МЭ TCP (Мбит/с)	320	**NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)**	-	**Сетевые интерфейсы**	3 x 1G RJ-45 Wi-Fi (только для N2) 3G (только для N3)
VPN, Мбит/с	70				

HW100
N1-N3



МЭ UDP 1518 байт (Мбит/с)	950	**Application Control (МЭ+DPI) (Мбит/с)**	85	**Количество соединений**	150 000
МЭ TCP (Мбит/с)	930	**NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)**	15	**Сетевые интерфейсы**	4 x 1G RJ-45 1 x 1G SFP Wi-Fi (только для N2) 3G (только для N3)
VPN, Мбит/с	160				

HW100
Q1-Q2

МЭ UDP 1518 байт (Мбит/с)	1500	**Application Control (МЭ+DPI) (Мбит/с)**	330	**Количество соединений**	1 500 000
МЭ TCP (Мбит/с)	1200	**NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)**	35	**Сетевые интерфейсы**	4 x 1G RJ-45 2 x 1G SFP
VPN, Мбит/с	320				

HW1000
Q7

МЭ UDP 1518 байт (Мбит/с)	1 900	**Application Control (МЭ+DPI) (Мбит/с)**	350	**Количество соединений**	1 000 000
МЭ TCP (Мбит/с)	1 800	**NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)**	80	**Сетевые интерфейсы**	6 x 1G RJ-45
VPN, Мбит/с	915				

HW1000
Q8–Q9

МЭ UDP 1518 байт (Мбит/с)	2 800	Application Control (МЭ+DPI) (Мбит/с)	1 000	Количество соединений	3 000 000
МЭ TCP (Мбит/с)	2 800	NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)	380	Сетевые интерфейсы	Q8 – 8 x 1G RJ-45 Q9 – 8 x 1G RJ-45 4 x 1G SFP
VPN, Мбит/с	2 500				

HW1000
Q10

VPN, Мбит/с	1000	Количество соединений	1 000 000
МЭ, Мбит/с	2500	Сетевые интерфейсы	Q10 – 4 x 1G RJ-45 2 x 1G SFP

HW2000
Q5

МЭ UDP 1518 байт (Мбит/с)	19 000	Application Control (МЭ+DPI) (Мбит/с)	2 600	Количество соединений	5 000 000
МЭ TCP (Мбит/с)	9 300	NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)	880	Сетевые интерфейсы	4 x 1G RJ-45 4 x 1G SFP 4 x 10G SFP+
VPN, Мбит/с	6 600				

HW5000
Q2

МЭ UDP 1518 байт (Мбит/с)	24 000	Application Control (МЭ+DPI) (Мбит/с)	3 300	Количество соединений	9 900 000
МЭ TCP (Мбит/с)	13 000	NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)	1 000	Сетевые интерфейсы	4 x 1G RJ-45 8 x 10G SFP+
VPN, Мбит/с	10 000				

ViPNet Coordinator VA5

Виртуализированный криптографический шлюз безопасности – межсетевой экран следующего поколения

ViPNet Coordinator VA 5 – шлюз безопасности в виртуальном исполнении, реализующий концепцию NGFW (Next-Generation Firewall – межсетевой экран следующего поколения), который объединяет в одном устройстве следующие функции безопасности, работающие совместно:

01. Криптографический шлюз, обеспечивающий построение VPN на сетевом (L3) и канальном (L2) уровнях модели OSI
02. Межсетевой экран SPI (Stateful Packet Inspection)
03. Прокси-сервер
04. Межсетевой экран уровня приложений DPI (Deep Packet Inspection)
05. Средство обнаружения и предотвращения вторжений (IDS/IPS)
06. Кластер высокой доступности (HA-cluster)

Реализованные сетевые функции и сервисы безопасности активируются в соответствии с приобретенной лицензией (лицензируются отдельные модули).

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 5 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 5 представляет собой виртуализированное программное обеспечение, предназначенное для развертывания на популярных платформах виртуализации (KVM, VMware ESXi, Microsoft Hyper-V, Oracle VM).

ЧТО НОВОГО

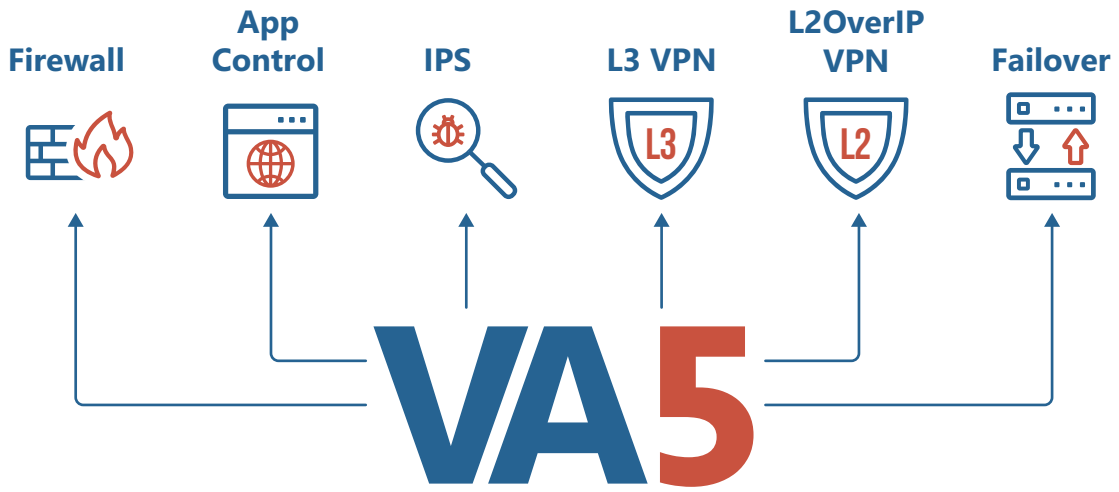
01. Поддержка алгоритмов «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
02. Межсетевой экран уровня приложений (DPI)
03. Многопользовательский ролевой доступ
04. Обнаружение и предотвращение вторжений (IDS/IPS)
05. Подсистема идентификации пользователей (LDAP, Active Directory, Captive Portal)
06. Кластер высокой доступности (HA-cluster) с синхронизацией таблицы открытых соединений
07. Централизованное и удаленное резервное копирование конфигурации

ПРЕИМУЩЕСТВА

> Удобство управления и скорость развертывания
> Функциональность, соответствующая аппаратным шлюзам ViPNet Coordinator HW
> Отсутствие дополнительных затрат на размещение и обслуживание оборудования
> Поддержка распространенных систем виртуализации
> Единая система управления для виртуальных и аппаратных шлюзов безопасности
> Объединение в одном виртуальном устройстве нескольких функций безопасности (FW, DPI, IPS, VPN, Proxy)
> Гибкая политика лицензирования позволяет приобрести только необходимые функции в зависимости от потребности
> Централизованное управление шлюзом безопасности с ролевой моделью доступа
> Гранулированные политики безопасности, которые строятся в терминах «Пользователь» - «Приложение» - «Действие»
> Обнаружение и нейтрализация сетевых вторжений с использованием встроенной системы предотвращения вторжений (IPS)
> Обеспечение безопасного использования персональных устройств в рабочих целях с полным соблюдением политик безопасности компании – BYOD (Bring Your Own Device)
> Отказоустойчивый кластер (High-Availability) с синхронизацией сессий позволяет минимизировать время переключения между элементами кластера до 1 секунды
> Выявление и блокировка более 2000 прикладных протоколов и приложений: игры, социальные сети, torrent и т.д

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

> Построение защищенных каналов связи между объектами организации (Site-to-Site и Multi Site-to-Site)
> Защита данных внутри виртуальной и облачной инфраструктуры
> Защищенный доступ удаленных пользователей
> Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение ДМЗ)
> Обнаружение и нейтрализация сетевых вторжений
> Комплексная защита от сетевых угроз
> Защита магистральных каналов, соединяющих ЦОД между собой
> Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь)
> Взаимодействие с сетями ViPNet других организаций



Тип лицензии	VA100	VA500	VA1000	VA2000	VA5000
Производительность[1]					
МЭ UDP 1518 байт, Мбит/с	380	1 500	2 500	5 000	9 500
МЭ UDP 64 байт, пакетов/с	450 000	900 000	1 750 000	2 100 000	3 200 000
МЭ TCP, Мбит/с	360	1 000	2 500	4 500	9 500
Application Control (МЭ+DPI)[2], Мбит/с	300	800	1 800	2 200	2 800
NGFW Throughput (МЭ + DPI + IPS)[3], Мбит/с	95	250	550	650	925
Количество обслуживаемых соединений	150 000	500 000	2 500 000	5 000 000	10 000 000
L3 VPN, Мбит/с	185	600	1 600	4 000	5 400
L2 VPN, Мбит/с	165	580	1 600	4 000	5 400
Рекомендуемое число связей с ViPNet-узлами	500	2 000	10 000	15 000	16 000
Рекомендуемое число зарегистрированных ViPNet-клиентов	100	500	1000	5000	6 000
Системные требования					
Количество ядер CPU, мин./рек., шт	2 / 4	4 / 4	6 / 8	8 / 12	12 / 16
Оперативная память, мин./рек., Гб	4 / 4	4 / 8	6 / 12	8 / 16	12 / 32
Требования к дисковой подсистеме, Гб	80	80	80	80	80
Сетевые интерфейсы, Гбит/с	1	1	1/10	1/10	1/10
Поддерживаемые среды виртуализации[4]	> KVM, QEMU-KVM и Libvirt > SharxBase 5.10.5 > Proxmox VE > VMware ESXi 6.7/7.0 > VMware Workstation Pro 15.x / 16.x			> Microsoft Hyper-V Server 2016/2019 > Oracle VM Server 3.4 > Oracle VM VirtualBox 6.x	

[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]Результаты получены для трафика EMIX, который представляет собой смесь трафиков различных прикладных протоколов: BitTorrent, HTTP, HTTPS, Oracle DB, SMTP, SSH и др.
[3]Результаты получены для активированных функций МЭ, DPI, IPS с использованием актуальной на момент теста базы правил IPS при анализе трафика EMIX, который представляет собой смесь трафиков различных прикладных протоколов: BitTorrent, HTTP, HTTPS, Oracle DB, SMTP, SSH и др.
[4]Работа на других платформах виртуализации возможна, но не гарантируется.

СЕРТИФИКАЦИЯ

ФСБ России
> СКЗИ класса КС1

Свидетельства
В реестре российского ПО

ФСТЭК России
> МЭ типа Б 4 класса (ИТ.МЭ.Б4.ПЗ)
> СОВ уровня сети 4 класса защиты (ИТ.СОВ.С4.ПЗ)
> 4 уровень доверия средств защиты информации

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

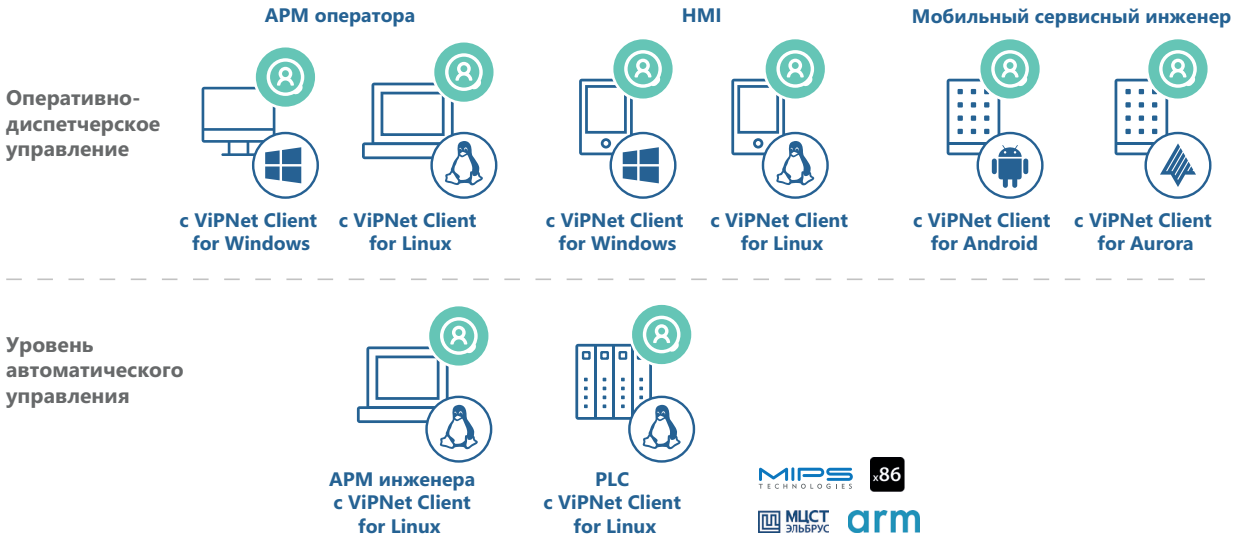
ViPNet Client защищает устройство пользователя, что позволяет безопасно работать с любыми внутренними ресурсами своей организации через интернет благодаря шифрованию трафика с использованием алгоритмов ГОСТ 28147-89, ГОСТ 34.12-2018, ГОСТ 34.13-2018 на ключах длиной 256 бит. Передаваемые данные недоступны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

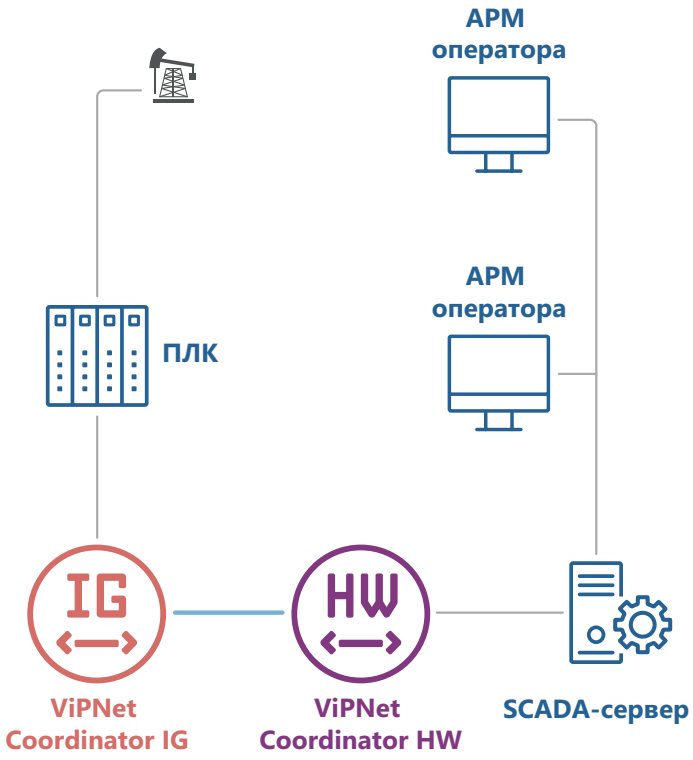
- стационарные АРМ операторов
- стационарные АРМ инженеров
- HMI-панели
- ноутбуки сервисного персонала
- мобильные устройства сервисного персонала
- программируемые логические контроллеры

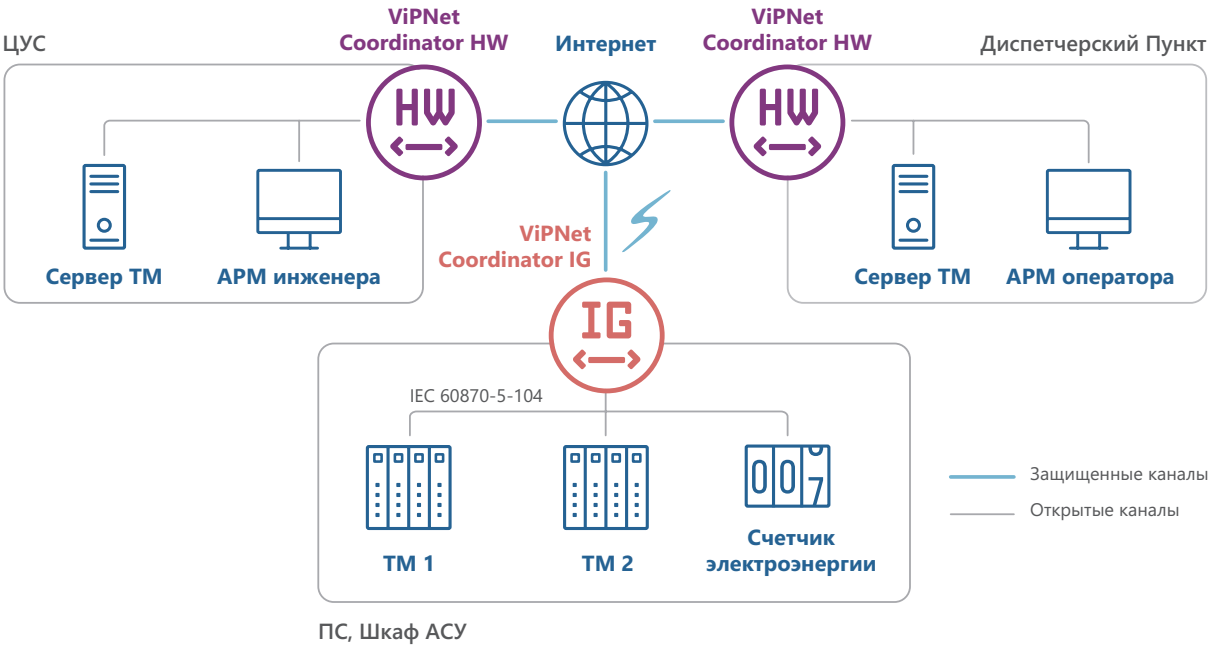


Сценарии эксплуатации сетевых средств защиты информации в АСУ и АСУ ТП

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.

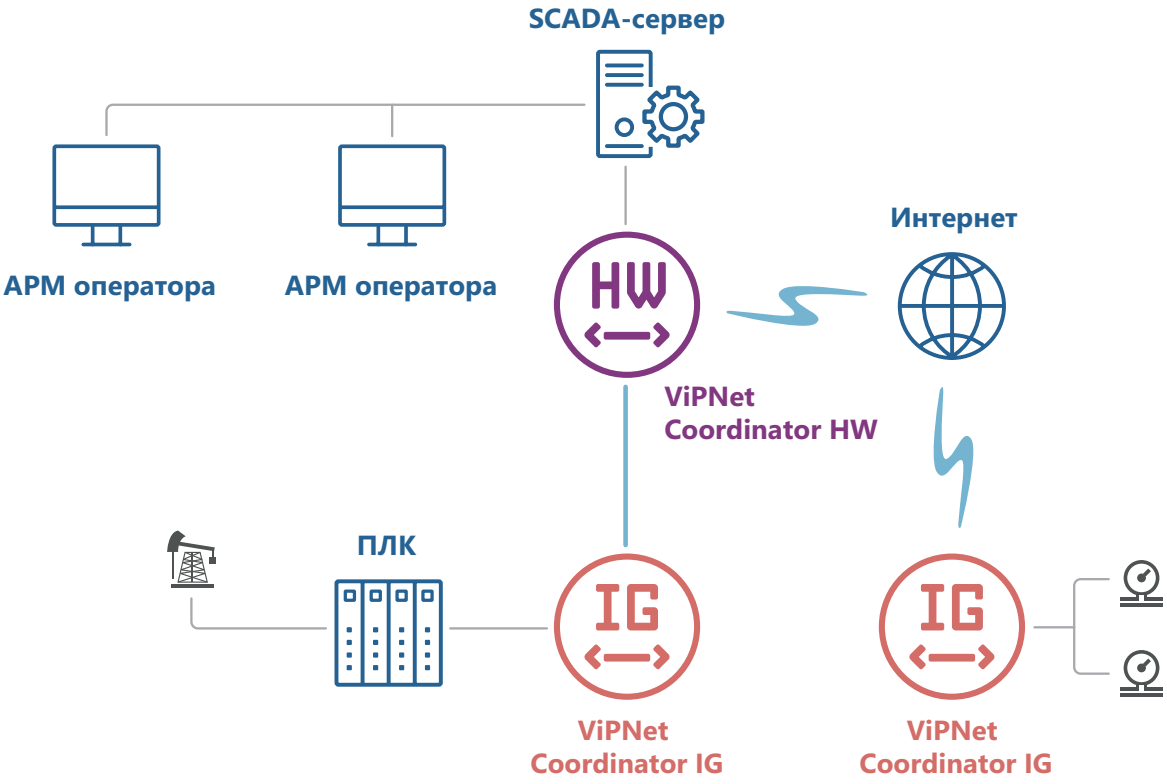




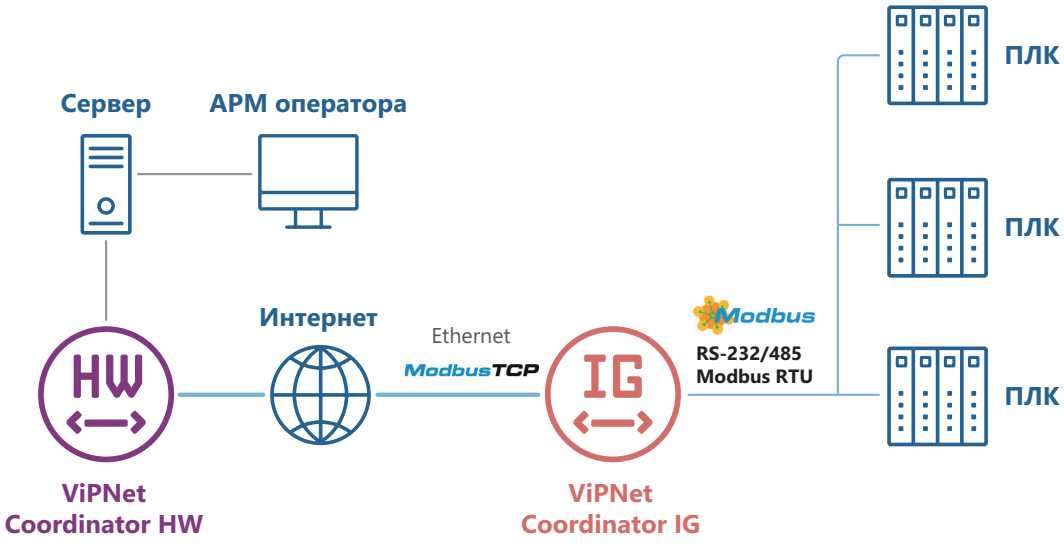
Для защищенного управления распределенными по территории объектами по беспроводному каналу Wi-Fi или по сотовым каналам передачи данных можно использовать ПАК ViPNet Coordinator IG с беспроводным модулем передачи данных. ПАК ViPNet Coordinator IG имеет возможность подключения внешней антенны, которая 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

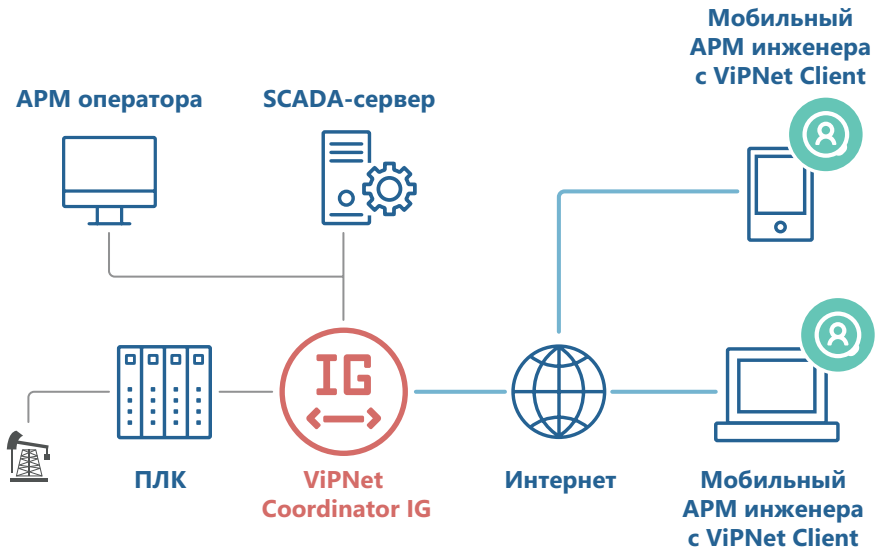
ПАК ViPNet Coordinator IG и ПАК ViPNet Coordinator HW могут использоваться для организации защищенного удаленного мониторинга в АСУ и АСУ ТП за счет построения защищенного VPN-канала по технологии ViPNet VPN между объектами систем. Для передачи данных мониторинга возможно использовать как проводные,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



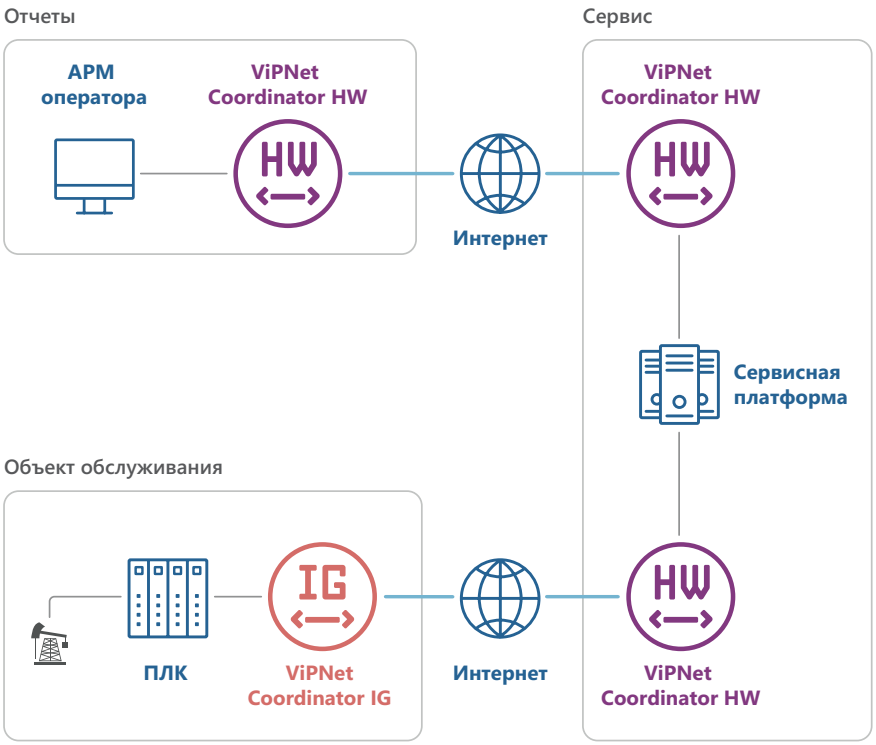
Защищенное удаленное обслуживание



ПАК ViPNet Coordinator IG позволяет безопасно подключить 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

IS26_00RU

Изобретения, примененные в представленных продуктах и решениях ИнфоТеКС, защищены следующими патентами РФ: 2517411, 2526282, 2507569, 2636403, 2635216, 2687217, 2530633