БУДНИ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

миниБИБ онлайн!

21 апреля, 10.00 мск

www.infosecuritydays.ru

infotecs

Решения ViPNet для объектов КИИ

Александр Шипков, CISM, CISSP



Федеральный закон №187-ФЗ «О безопасности КИИ РФ»

Субъекты и Объекты КИИ

- Государственные органы
- Государственные учреждения
- Российские юридические лица
- Индивидуальные предприниматели



которым на праве собственности, аренды или на ином законном основании принадлежат

Информационные системы (ИС)

Автоматизированные системы управления(АСУ)

Информационно-телекоммуникационные сети (ИТС)

Сферы деятельности

infotecs



Здравоохранение



Наука



Транспорт



Связь



Энергетика



Банковская сфера



ТЭК



Атомная энергетика



Оборонная промышленность



Ракетно-космическая промышленность



Горнодобывающая промышленность



Металлургическая промышленность



Химическая промышленность



Обеспечение взаимодействия ИС/ИТКС/АСУ

Основные мероприятия

В соответствии с ФЗ №187-ФЗ «О безопасности КИИ»

01

Категорирование объектов КИИ

Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»

02

Обеспечение безопасности объекта КИИ

- Приказ ФСТЭК №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ»
- Приказ ФСТЭК №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционированию»

03

Противодействие компьютерным атакам

Взаимосвязь с ГосСОПКА, размещение на территории объекта КИИ ТЗИ ГосСОПКА

Обеспечение безопасности объекта КИИ

Приказ ФСТЭК России №235

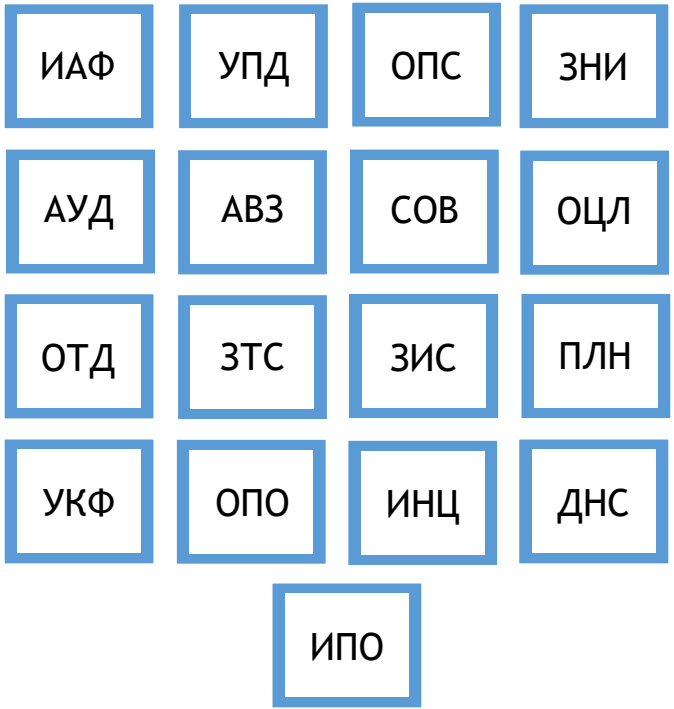
«Об утверждении требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»



Приказ ФСТЭК России №239

«Об утверждении требований по обеспечению безопасности значимых объектов КИИ РФ»

Состав мер по защите объектов КИИ согласно Приказу №239 ФСТЭК России



I. Идентификация и аутентификация (ИАФ)
II. Управление доступом (УПД)
III. Ограничение программной среды (ОПС)
IV. Защита машинных носителей информации (ЗНИ)
V. Аудит безопасности (АУД)
VI. Антивирусная защита (АВЗ)
VII. Предотвращение вторжений (компьютерных атак) (СОВ)
VIII. Обеспечение целостности (ОЦЛ)
IX. Обеспечение доступности (ОДТ)
X. Защита технических средств и систем (ЗТС)
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
XII. Планирование мероприятий по обеспечению безопасности (ПЛН)
XIII. Управление конфигурацией (УКФ)
XIV. Управление обновлениями программного обеспечения (ОПО)
XV. Реагирование на инциденты информационной безопасности (ИНЦ)
XVI. Обеспечение действий в нештатных ситуациях (ДНС)
XVII. Информирование и обучение персонала (ИПО)

всего 152 меры



Сетевая безопасность

Шлюзы безопасности ViPNet Coordinator



ViPNet Coordinator IG ViPNet Coordinator HW

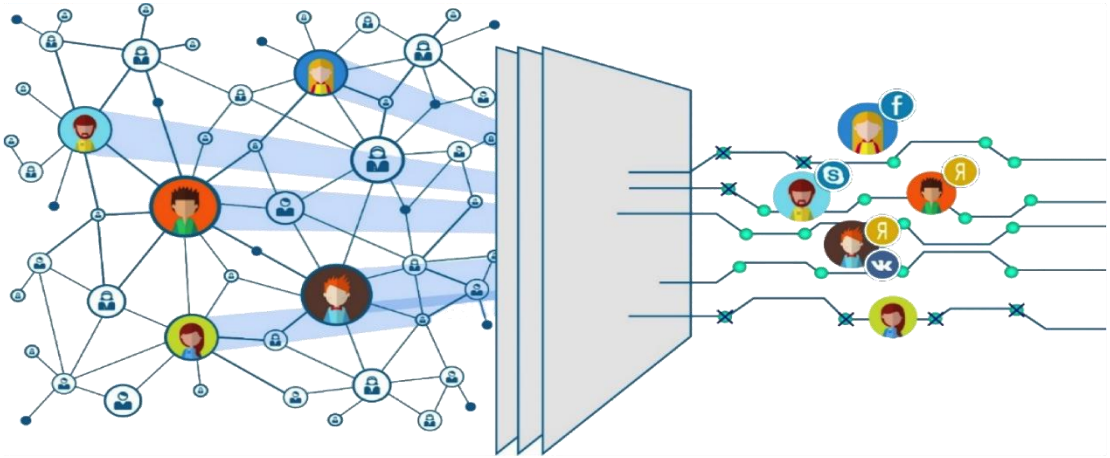
- ✓ Защита каналов передачи данных
- ✓ Межсетевое экранирование
- ✓ Сегментирование сети
- ✓ Соответствие требованиям регуляторов

ViPNet VPN-шлюз	МЭ
Сетевые функции	Локальное и дистанционное управление

ИАФ	АУД	ОДТ	ЗИС

ViPNet xFirewall

- Фильтрация трафика на сетевом и транспортном уровнях модели OSI с контролем состояния сессий
- Расширенная инспекция трафика (Deep Packet Inspection)

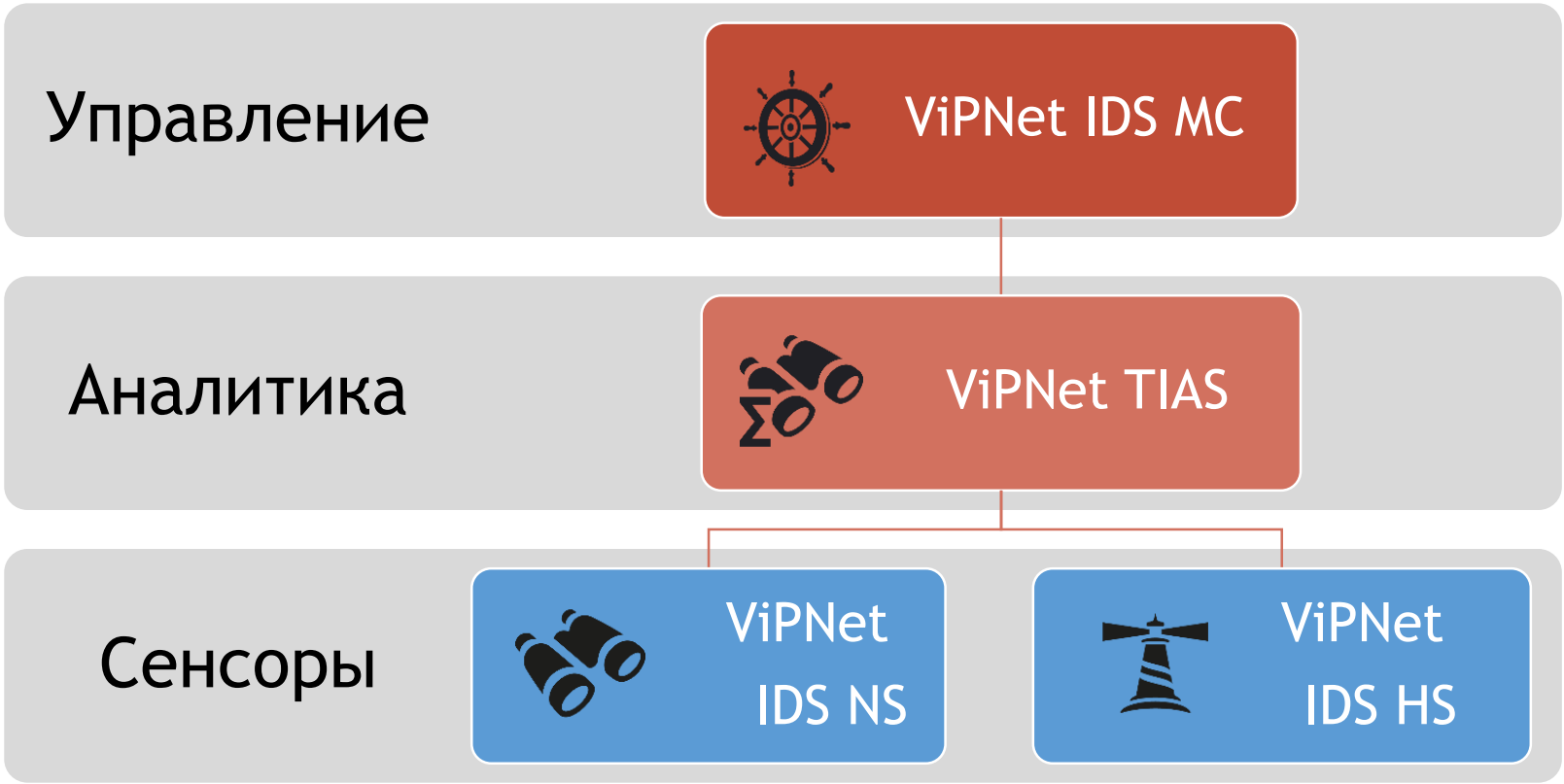


ИАФ АУД СОВ

ОДТ ЗИС

- Возможность определения политик безопасности на уровне пользователей и групп пользователей служб каталогов Active Directory или LDAP
- Фильтрация HTTP-трафика интегрированным прокси-сервером и его антивирусная проверка встроенным (KAV4Proxy) или внешним (по протоколу ICAP) антивирусом
- Анализ трафика системой предотвращения вторжений (Intrusion Prevention System)

Обнаружение сетевых атак



ViPNet IDS NS. СОВ уровня сети

ViPNet IDS NS – система обнаружения компьютерных атак (вторжений) на основе динамического анализа сетевого трафика



АУД СОВ

Возможности:

- Сигнатурный и эвристический метод выявления аномалий в сетевом трафике
- Регистрирует факт обнаружения атаки, идентифицирует событие (атаку), оповещает администратора о данном событии
- База сигнатур атак поставляется дочерней компанией «Перспективный мониторинг»

ViPNet TIAS

ViPNet TIAS – автоматическое выявление инцидентов информационной безопасности в ИС на основе анализа информации о событиях ИБ, поступающей от источников – сенсоров систем обнаружения атак (вторжений)



Возможности:

- Прием и обработка информации о событиях ИБ от сенсоров
- Обогащение, классификация, агрегация и корреляция обработанной информации о событиях
- Анализ обработанной информации о событиях сигнатурным и эвристическим методами
- Автоматическое выявление и регистрация инцидентов ИБ

АУД ИНЦ



infotecs

Защита рабочих станций и конечных устройств

ViPNet IDS HS. СОВ уровня узла

ViPNet IDS HS – мониторинг и обработка событий внутри хоста, с применением сигнатурного и эвристического метода анализа атак, используя отечественные правила и сигнатуры

Возможности:

- Анализ системных журналов ОС и приложений
- Мониторинг файловой активности и реестра
- Мониторинг результатов команд
- Анализ трафика, проходящего через хост
- Анализ событий и на хосте и на сервере



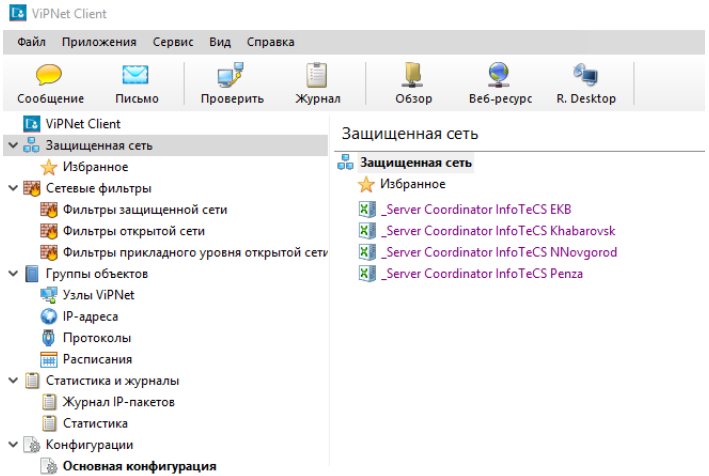
АУД СОВ

ViPNet Client

ViPNet Client – программный комплекс для защиты рабочих мест пользователей

Возможности:

- VPN-клиент (шифрование и имитозащита IP-пакетов)
- Персональный сетевой экран
- Контроль сетевой активности приложений и компонентов ОС
- Двухфакторная авторизация
- Поддержка ОС Windows, MacOS, Linux, iOS, Android, Sailfish

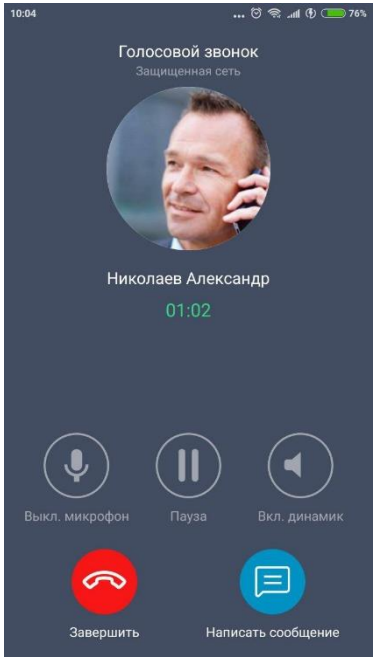


ИАФ АУД ЗИС

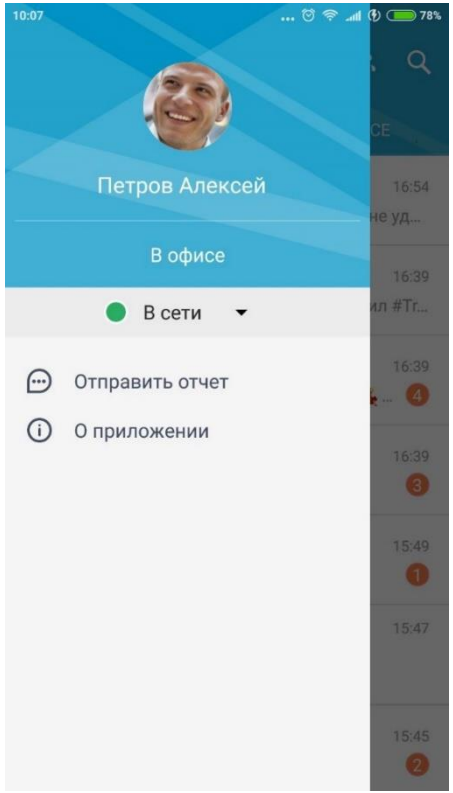
ViPNet Connect for Android/iOS

infotecs

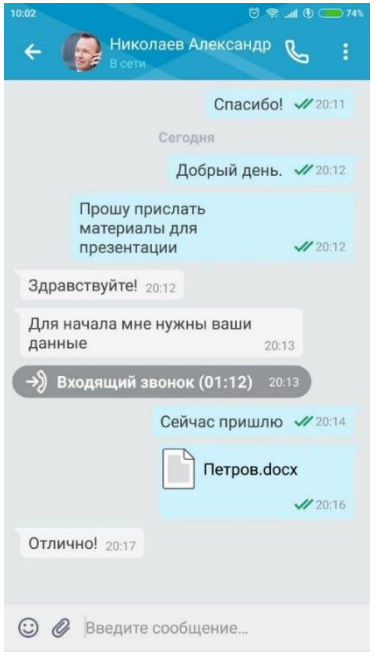
Голос



Передача файлов



Сообщения



Конференция

ViPNet SafeBoot

ViPNet SafeBoot – высокотехнологичный программный модуль доверенной загрузки, устанавливаемый в UEFI BIOS различных производителей. Предназначен для защиты компьютеров и серверов от современных угроз НСД и атак на сам BIOS

Возможности:

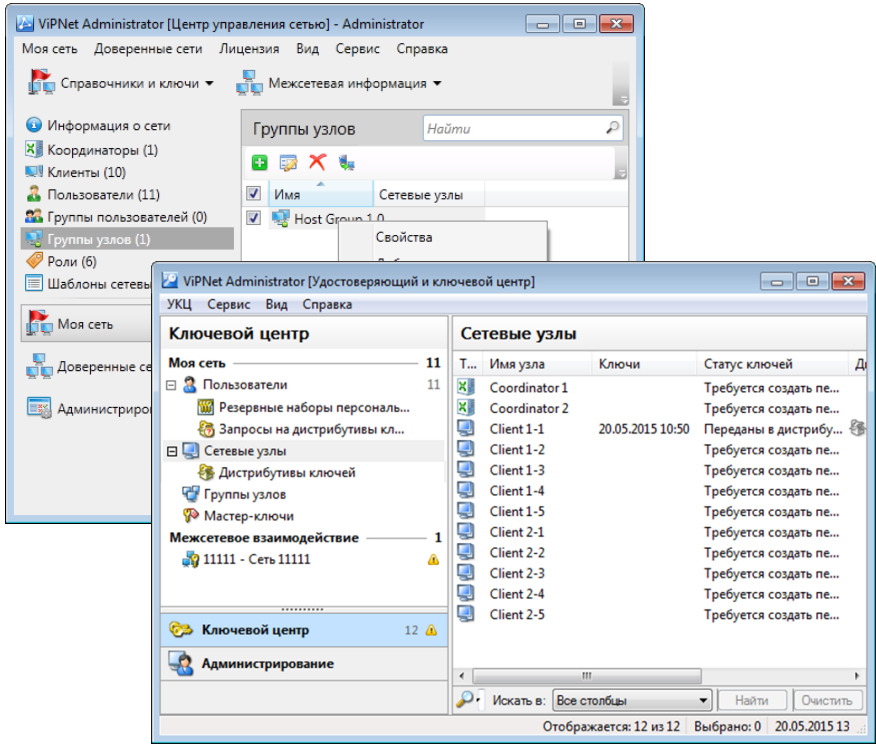
- Организация доверенной загрузки
- Авторизация на уровне BIOS до загрузки основных компонентов ОС
- Контроль целостности на уровне BIOS:
  - ✓ UEFI BIOS
  - ✓ MBR
  - ✓ Таблиц ACPI, SMBIOS
  - ✓ Файловых систем FAT32, NTFS, EXT2, EXT3, EXT4
  - ✓ Контроль завершенности транзакций - NTFS, EXT3, EXT4



ИАФ | УПД | АУД | ОЦЛ

ViPNet Administrator

ViPNet Administrator – программный комплекс, предназначенный для настройки и управления защищенной сетью



Центр управления сетью (ЦУС)

- Управление структурой сети
- Обновление ПО ViPNet
- Контроль лицензий ViPNet
- Аудит событий

Удостоверяющий и Ключевой центр (УКЦ)

- Первичная генерация ключей
- Плановая смена ключей
- Компрометация ключей

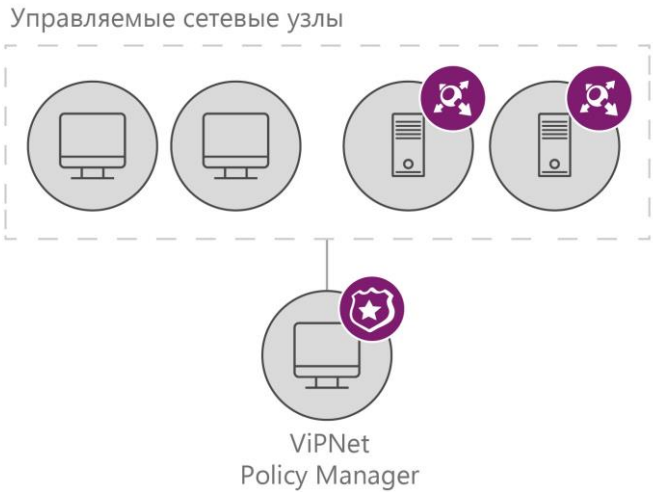
ИАФ УПД АУД

ViPNet Policy Manager

ViPNet Policy Manager – средство централизованного управления политиками безопасности узлов защищенной сети ViPNet

Основные возможности:

- Управление сетевыми фильтрами узлов сети ViPNet
- Управление настройками ViPNet Client
- Шаблоны и политики по расписанию
- Многопользовательский ролевой доступ
- Групповые операции с объектами



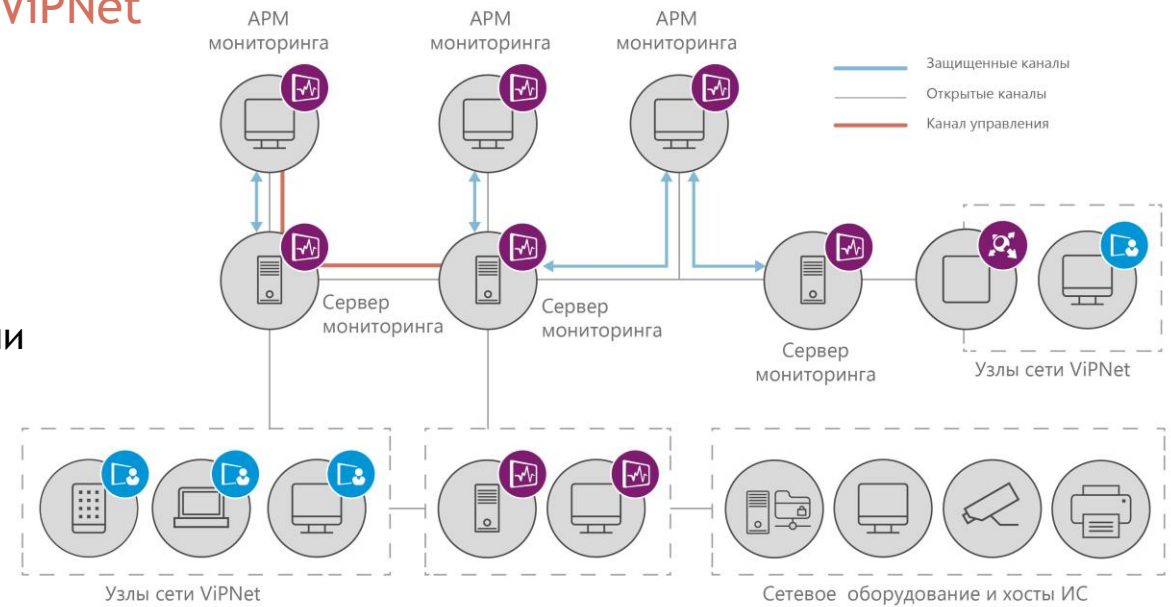


ViPNet StateWatcher

ViPNet StateWatcher – средство мониторинга узлов сети ViPNet

Возможности:

- Сбор параметров и статусов объектов мониторинга
- Выявление событий безопасности и эксплуатации
- Оповещение о событиях и состоянии объектов мониторинга
- Взаимодействие с корпоративными системами ИБ и управления



ViPNet SafePoint

ViPNet SafePoint – система защиты информации от несанкционированного доступа

Возможности:

- Двухфакторная аутентификация пользователей
- Контроль (разграничение) прав доступа пользователей
- Контроль целостности объектов файловой системы, реестра ОС и СЗИ ViPNet SafePoint
- Контроль устройств
- Гарантированное удаление и очистка памяти



ИАФ | УПД | ЗНИ

АУД | ОЦЛ

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Практические кейсы Центра мониторинга информационной безопасности

Сергей Нейгер

Менеджер по развитию бизнеса

«Перспективный мониторинг»

Повестка встречи

1. О Центре мониторинга
2. Как работает Центр мониторинга
3. Примеры взаимодействия

Мы вторые.

Это значит, что мы больше стараемся.

Сравнение услуг коммерческих SOC. Anti-malware.ru, конец 2019 года

Центр мониторинга

2014
год запуска

с 2017
Центр ГосСОПКА к. А

17
клиентов

30
операторов, исследователей, аналитиков и инженеров

Площадки:
Москва
Санкт-Петербург
Новосибирск

1,5 млрд
событий за 2019 г.

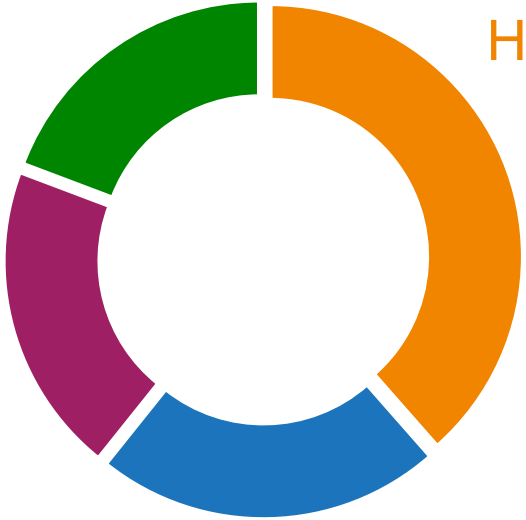
1 400
инцидентов за 2019 г.

13 000
собственных сигнатур атак для IDS

Ключевой угрозой кибербезопасности предприятий становится дефицит профессиональных навыков ИБ-департаментов*

Низкая мотивация к развитию в сфере ИБ

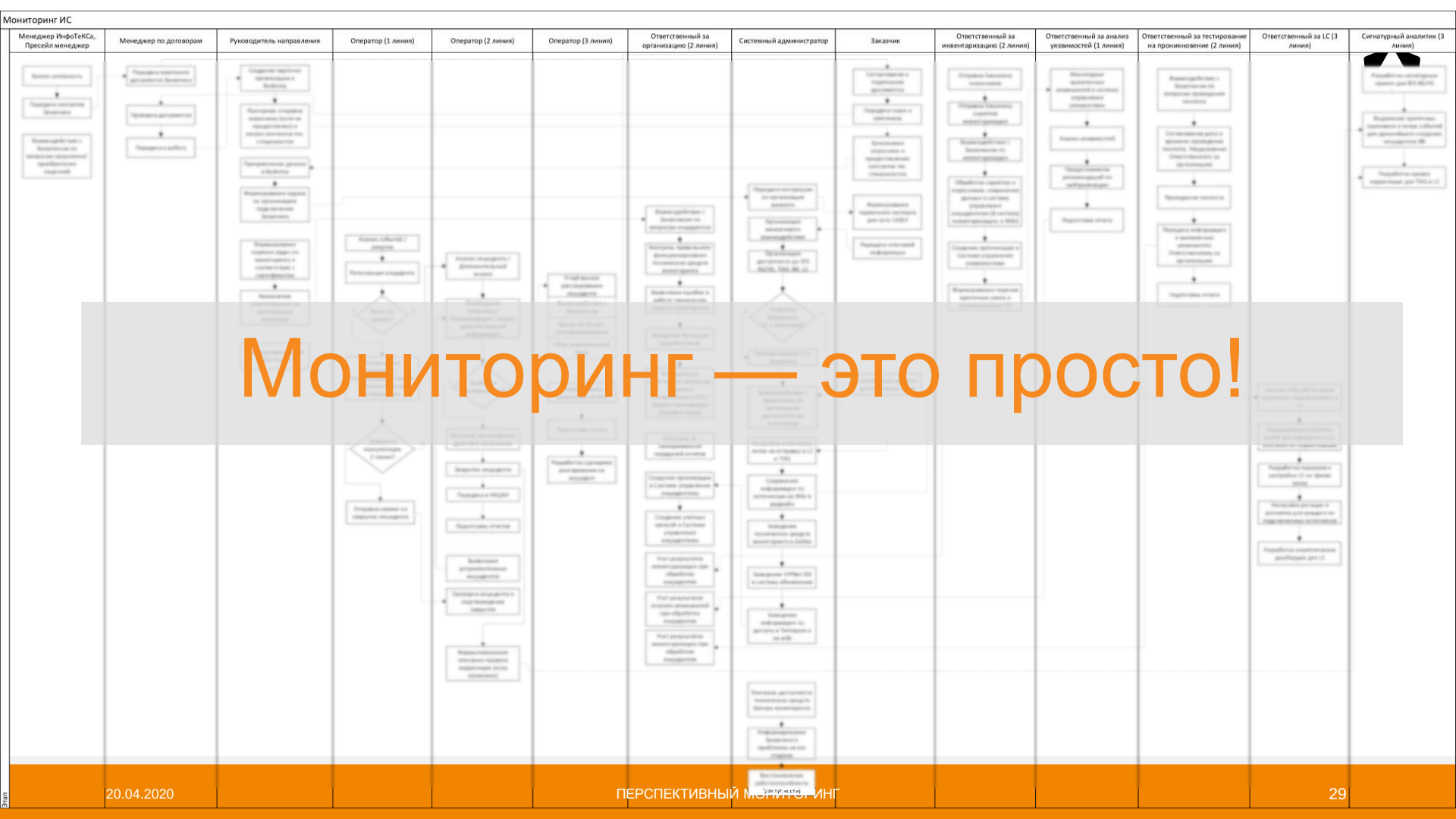
Нехватка кадров



Нехватка бюджетов

Нехватка навыков

* По результатам опроса, проведённого в социальных сетях накануне Infosecurity Europe 2019.



Мониторинг — это просто!

Но не стоит бояться становиться Центром

Функции	Центры ГосСОПКа		
	Класса А	Класса Б	Класс В
Взаимодействие с НКЦКИ при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и реагирования на компьютерные инциденты, в том числе в части информационно-аналитического и прогностического обеспечения функционирования ГосСОПКА, предоставление в НКЦКИ сведений о состоянии защищенности информационных ресурсов от компьютерных атак и информации о компьютерных инцидентах в соответствии с установленным порядком;	+	+	+
Разработка документов, регламентирующих процессы обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов и реагирования на компьютерные инциденты;	+	+	+
Эксплуатация средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, выявление ошибок в работе средств и направление производителю средств информации о выявленных ошибках, а также актуализация средств используемых для обеспечения защиты информационных ресурсов, направление в НКЦКИ предложений по совершенствованию средств;	+	+	+
Прием сообщений об инцидентах от персонала и пользователей информационных ресурсов;	+	+	+
Регистрация компьютерных атак и компьютерных инцидентов;	+	+	+
Анализ событий информационной безопасности;	+	+	+
Инвентаризация информационных ресурсов;	+	+	+
Анализ угроз информационной безопасности, прогнозирование их развития и направление в НКЦКИ результатов;	+	+	
Составление и актуализация перечня угроз информационной безопасности для информационных ресурсов;	+	+	
Выявление уязвимостей информационных ресурсов;	+	+	
Формирование предложений по повышению уровня защищенности информационных ресурсов;	+	+	
Составление перечня последствий компьютерных инцидентов;	+	+	
Ликвидация последствий компьютерных инцидентов;	+		
Анализ результатов ликвидации последствий инцидентов;	+		
Установление причин компьютерных инцидентов	+	+	

ИБшник перед стартом мониторинга

VS

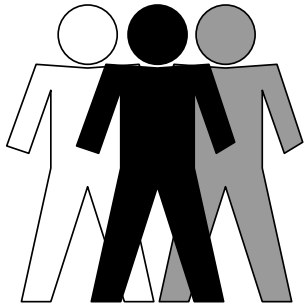
ИБшник после полугода работы с инцидентами





Необходимые ресурсы

Силы ГосСОПКА



Кадровое обеспечение

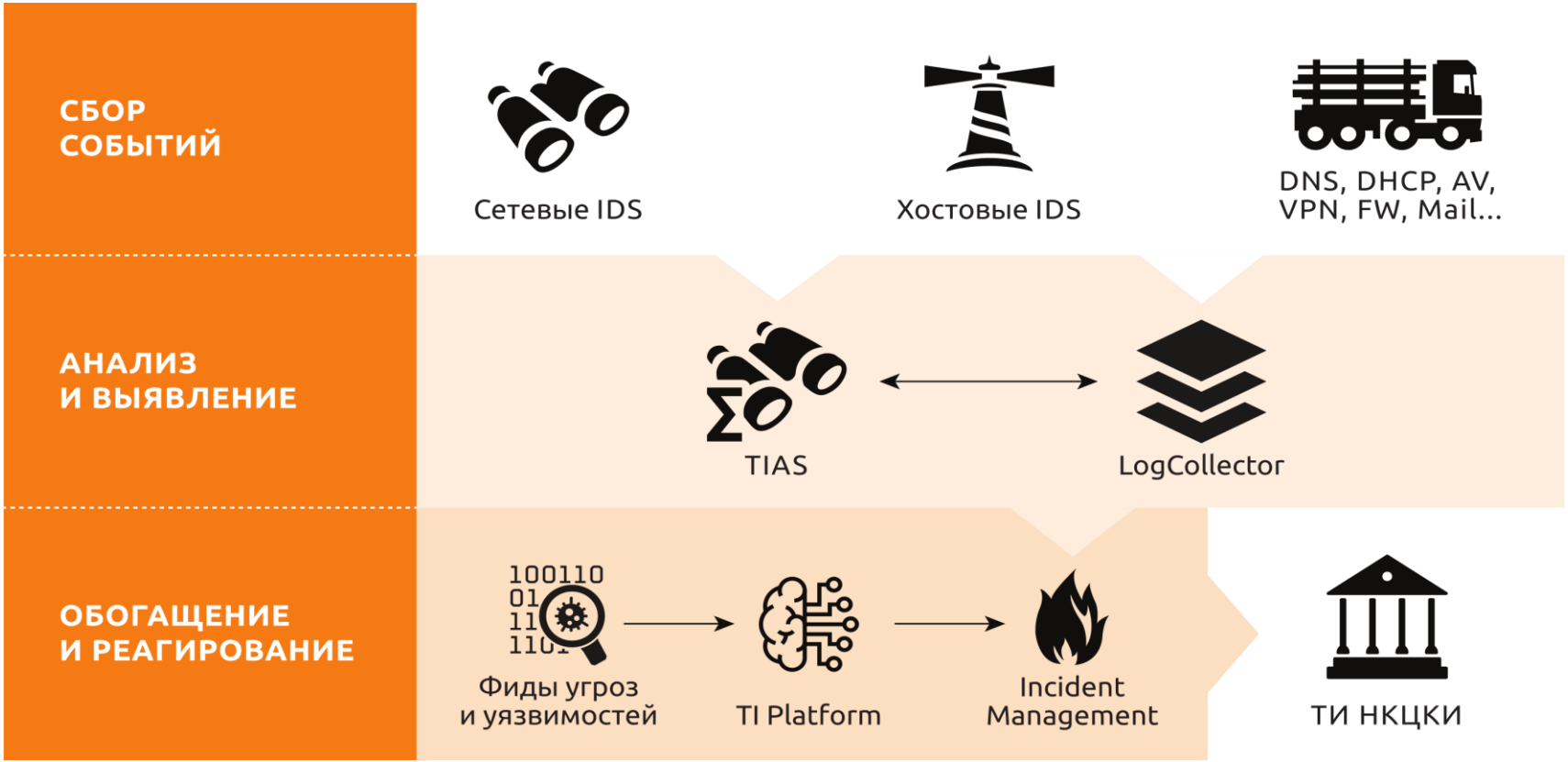
Средства ГосСОПКА



Персонал

Первая линия	Вторая линия	Третья линия
Взаимодействие с пользователями	Помощь в расследовании и установлении причин инцидентов	Подготовка и улучшение нормативной базы, описание сценариев выявленных инцидентов
Анализ событий и обнаружение компьютерных атак и инцидентов	Координация действий при реагировании на инциденты ИБ	Разработка сигнатурных правил и правил корреляции
Регистрация инцидентов ИБ и оповещение заинтересованных лиц	Анализ уязвимостей, анализ защищенности, тестирование на проникновение	Углубленный анализ Инцидентов ИБ, сбор доказательной базы

Схема подключения



Карточка инцидента

Расследование Организации

Инциденты / demo-28

Первое минуту назад
Последнее несколько секунд назад

Оповестить заказчика | Отправить в НКЦКИ | Редактировать

Создан 5 месяцев назад
Изменен 2 минуты назад

Потенциальная попытка проведения атаки SQL-injection на узел контролируемой инфраструктуры

Тип: Эксплуатация уязвимостей
Уровень: Высокий
Система: Demo DemoNetwork
Зафиксирован: 17.10.2018 09:41
Необходимо содействие НКЦКИ

Состояние: Неподтвержденный
Статус: Новый
Пользователь: TIAS
Наблюдатели: Администратор, TIAS

Описание:

Зафиксировано большое количество целенаправленных попыток проведения атаки типа SQL Injection

Рекомендации 4

Администратор	11.03.2019 16:50
Отключить пораженный актив от вычислительной сети	
Администратор	11.03.2019 16:50
Заблокировать на межсетевом экране IP-адрес атакующего	
Администратор	11.03.2019 16:50
Провериsти аудит атакуемого ресурса на наличие уязвимости к атакам типа SQL Injection и устранить при обнаружении	

Предпринятые действия 2

Администратор	11.03.2019 16:52
Отключен пораженный актив	
Администратор	11.03.2019 16:52
Заблокировн IP-адрес	

События 10 | История | Комментарии | Пораженные активы | Влияние | Файлы | Контакты

vipnet_ids_ns

Дата	Порт получателя	IP получателя	Порт отправителя	IP отправителя	Сенсор	Правило
17.10.2018 08:46	80	192.168.0.2	56735	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56736	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56737	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56738	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56739	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56740	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56741	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56742	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56743	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56744	91.59.66.41	10.0.24.201	ET WEB_S

Ресурсы | Сессии

```
GET /bWAPP/sqli_1.php?title=a%29%20UNION%20ALL%20SELECT%20NULL%23 HTTP/1.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Host: 10.10.10.241
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: sqlmap/1.0-dev (http://sqlmap.org)
Accept-Charset: ISO-8859-15,utf-8;q=0.7,*;q=0.7
Connection: close
Cookie: security_level=0; has_js=1; PHPSESSID=7a2cc3a82790b00f29ab627e0910cbe3
Pragma: no-cache
Cache-Control: no-cache,no-store
```

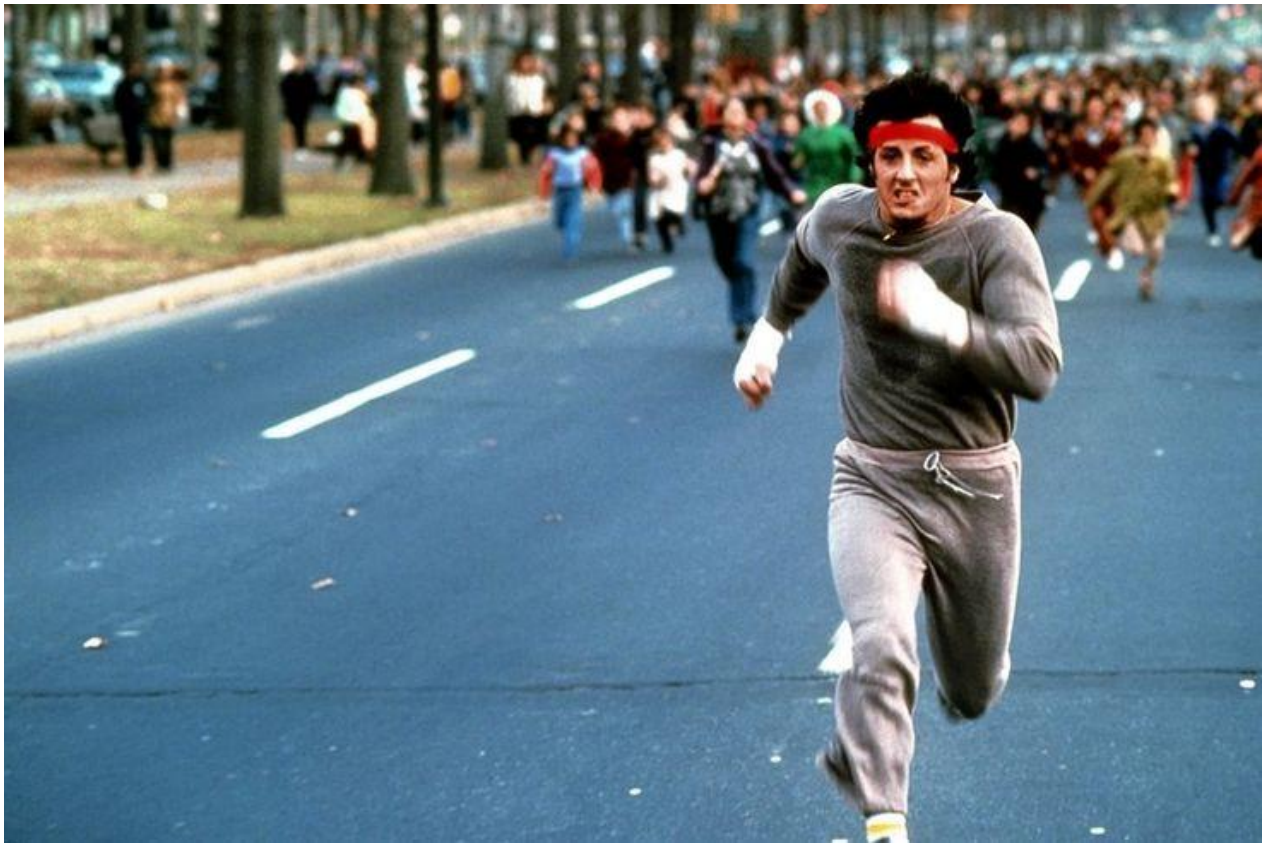


Примеры взаимодействия

Плохой пример реагирования



К успеху ведёт…



К успеху ведёт последовательность



Один раз — не танковый ас



Инцидент или не инцидент?



2 000
оповещений

1С·БИТРИКС

Проактивная
защита



cert@amonitoring.ru

Инцидент или не инцидент?



2 000
оповещений

1С·БИТРИКС

Проактивная
защита



Netsparker Web
Application
Security Scanner



2 дня работы



cert@amonitoring.ru

Помогаем не только клиентам



Сработала сигнатура на IDS



Майнер на сайте банка



Нашли безопасника



Отправили рекомендации



cert@amonitoring.ru

Спасибо за внимание!

Сергей Нейгер

Менеджер по развитию бизнеса

компании «Перспективный мониторинг»

Sergey.Neyger@amonitoring.ru

Практическое применение продуктов IG

Александр Шипков, CISM, CISSP

ViPNet Coordinator IG

Сценарии

- защита периметра сети
- сегментирования сети и разграничения доступа к ее сегментам
- защиты проводных и беспроводных каналов связи сети
- организация ДМЗ
- управление сетевыми потоками
- сокрытие реальных адресов и архитектуры сети
- организации удаленного доступа для стационарных и мобильных пользователей, в том числе с мобильных устройств



ViPNet Coordinator IG10



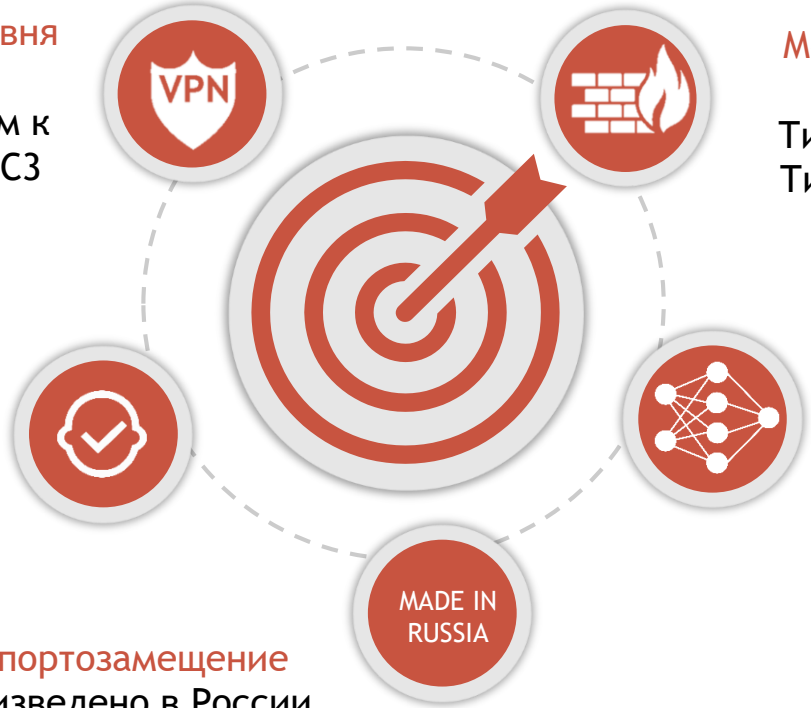
ViPNet Coordinator IG100

ViPNet Coordinator IG

infotecs

VPN – шлюз уровня L3, L2
По требованиям к СКЗИ класса КС3

Межсетевой экран SPI, DPI
Типа «Д» 4 класса
Типа «А» 4 класса



Доверенная платформа
Собственная схемотехника

Коммуникации
Проводные
3G, Wi-fi

Импортозамещение
Произведено в России

ViPNet Coordinator IG: характеристики

VPN

- ViPNet VPN-шлюз сетевого уровня L3
- ViPNet VPN-шлюз сетевого уровня L2 (L2OverIP)
- VPN-сервер
- 10 и 60 Мбит/с
- Аутентификация для каждого зашифрованного IP-пакета



ViPNet Coordinator IG: характеристики

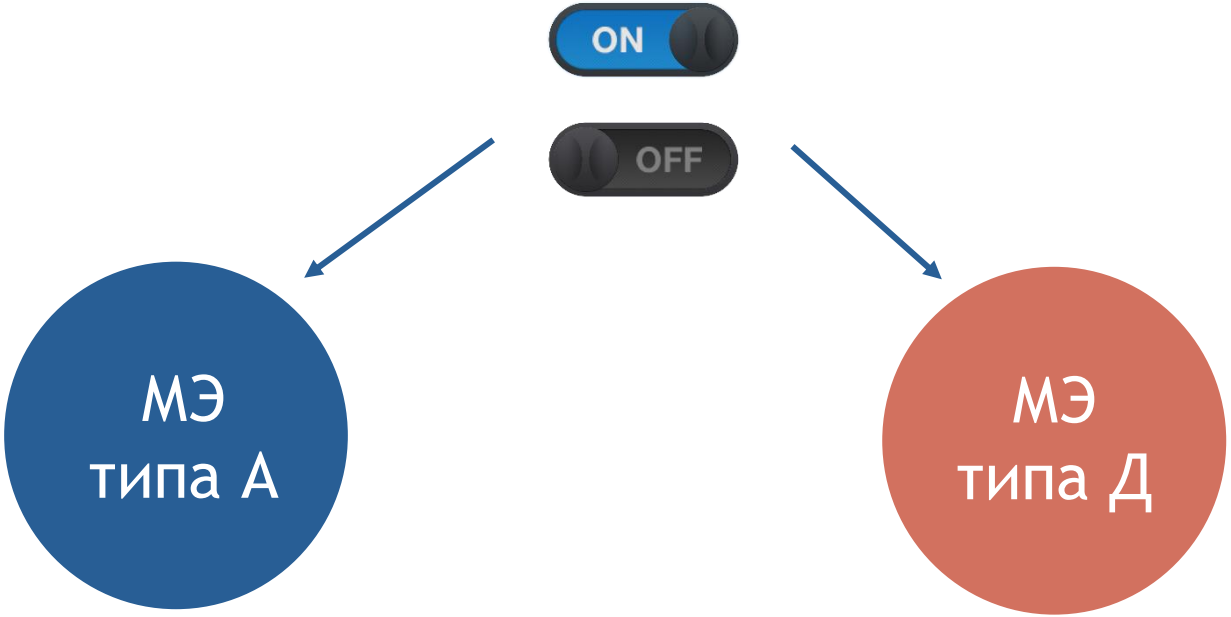
МЕЖСЕТЕВОЙ ЭКРАН

- NAT
- Антиспуффинг
- Фильтрация по IP источника и назначения, портам и типам протоколов
- Раздельная фильтрация для открытого IP-трафика и шифруемого IP-трафика
- Раздельные наборы фильтров для разных режимов работы
- Поддержка промышленных протоколов: EtherNet/IP, Modbus TCP, PROFINET, DNP, IEC 60870-104, MMS, OPC
- DPI для Modbus TCP/RTU

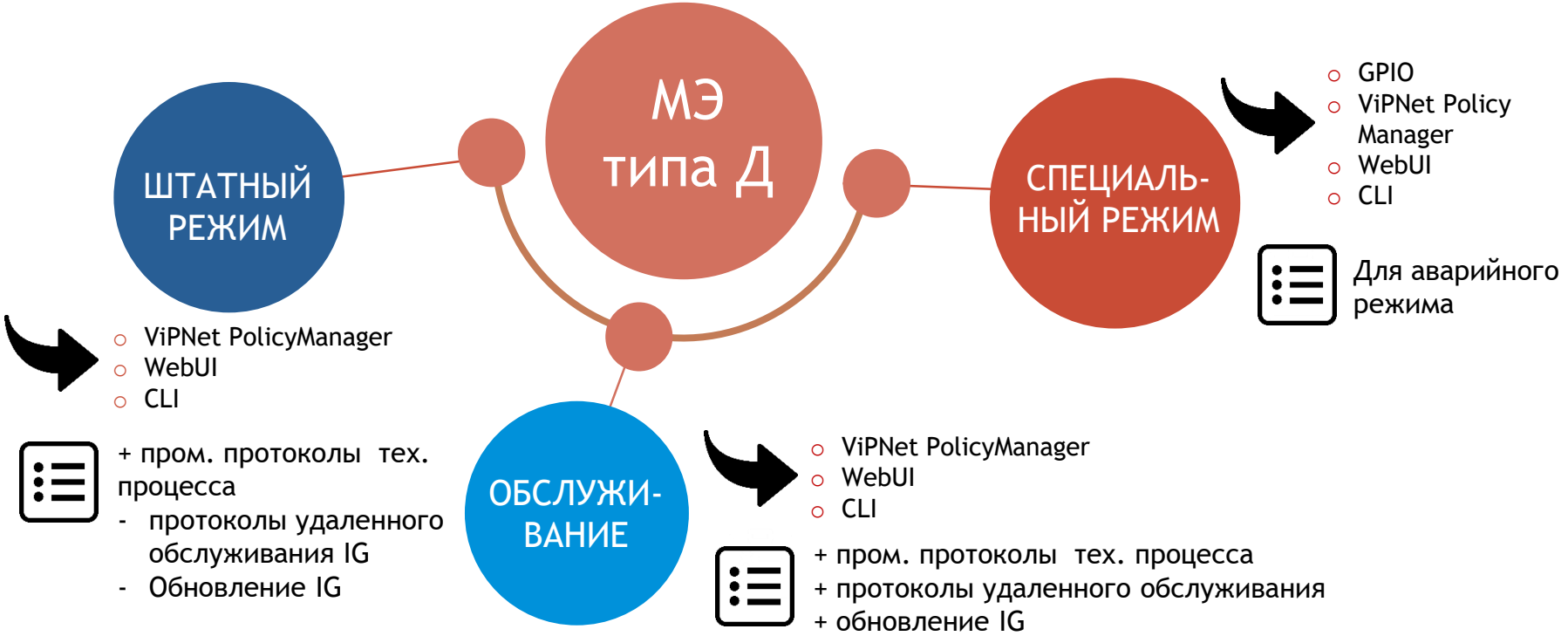


Межсетевой экран

ViPNet Administrator (ПЗ)



Правила МЭ для разных режимов работы ViPNet Coordinator IG



Фильтрация на прикладном уровне в ViPNet Coordinator IG



- Контроль пакетов на аномалии
- Возможность разрешения/запрета сообщений от конкретных адресов
- Возможность разрешения/запрета сообщений с конкретными командами

ViPNet Coordinator IG: характеристики

СЕТЕВЫЕ ФУНКЦИИ

- Статическая и динамическая маршрутизация
- DNS-сервер, DHCP-сервер, DHCP-relay
- VLAN, QoS, Etherchannel
- NTP-сервер
- WAN: 1xRJ45 10/100
- LAN: 2xRJ45 10/100
- Wi-Fi: IEEE 802.11 b/g,
- UMTS/HSPA, GSM/GPRS/EDGE
- Шлюза Modbus TCP/RTU
- GPIO



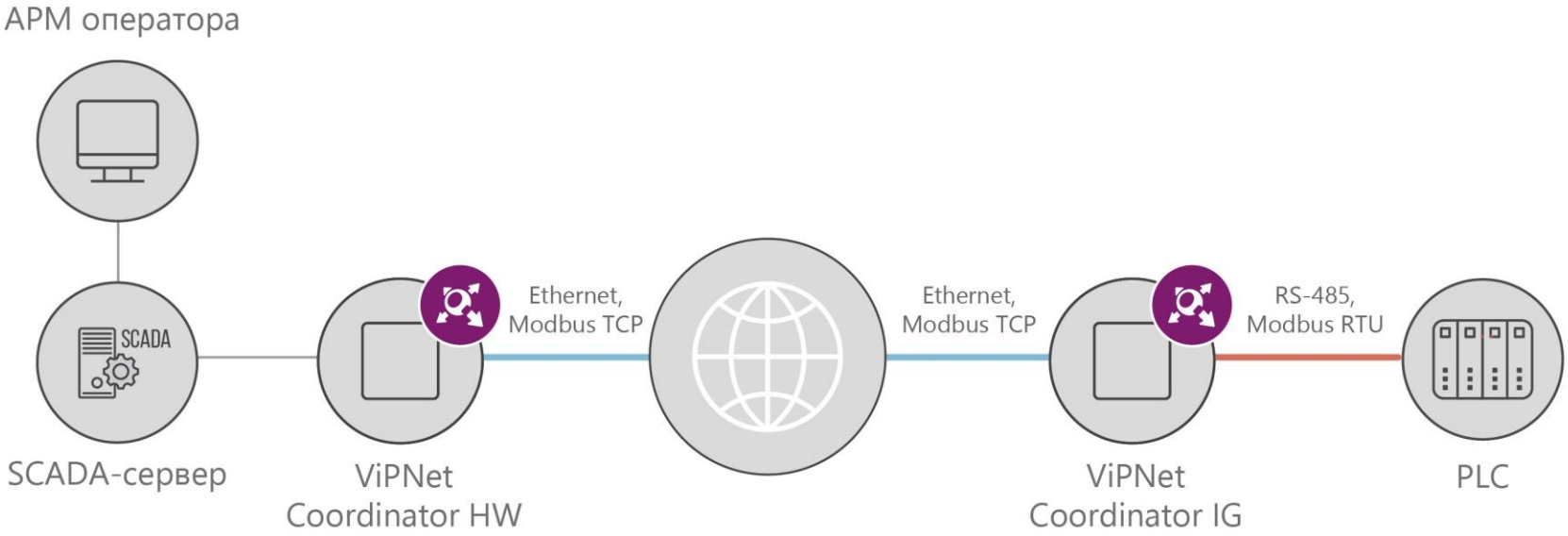
ViPNet Coordinator IG: характеристики

ФОРМ-ФАКТОР

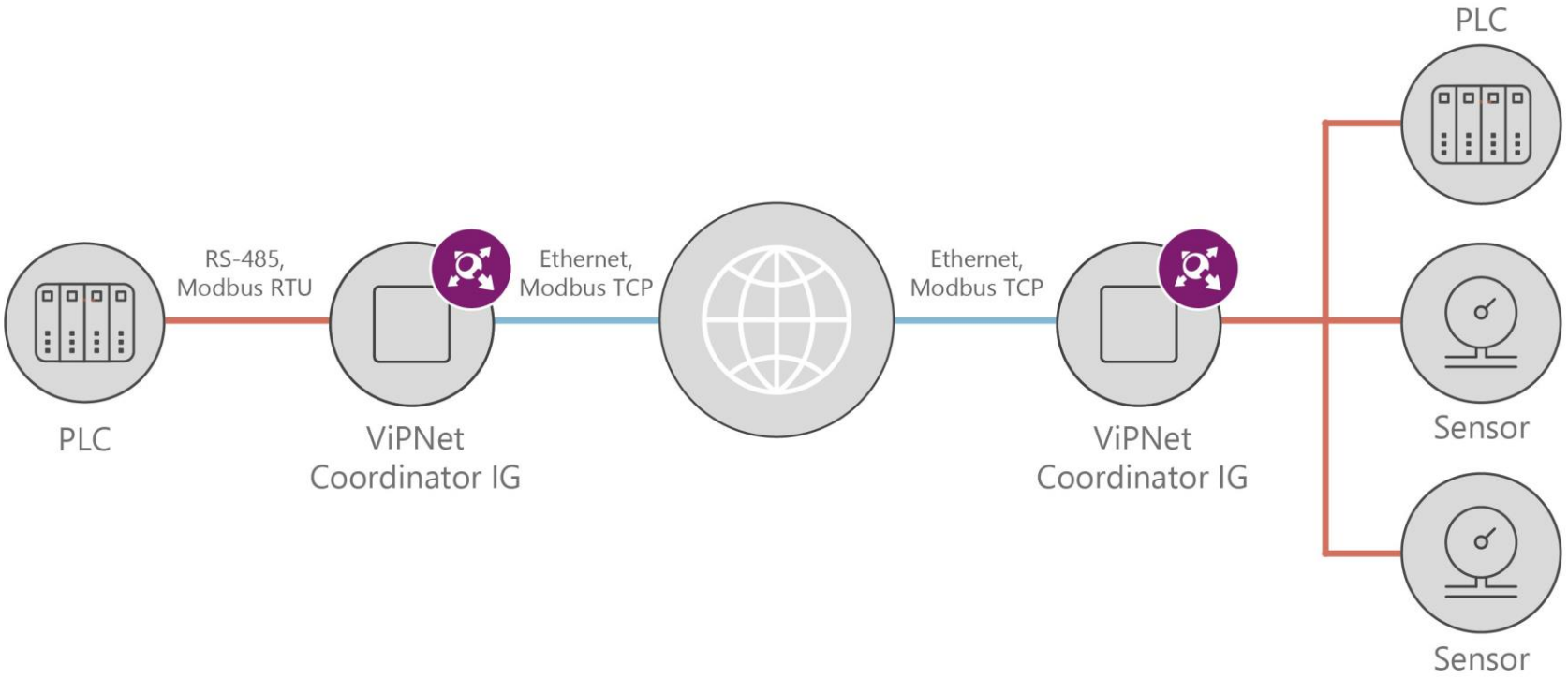
- ARM-платформа
- Безвентиляторный дизайн
- Рабочая температура: $20^0C(-40^0C)$ … $+60^0C$
- IP30 и бокс IP65 для кластера
- Напряжение питания: 12…24 В DC
- Крепление на din-рейку
- 50x120x120 мм, 0.6 кг
- ЭМС: ГОСТ 51318.22/CISPR22, ГОСТ CISPR 24



Шлюз Modbus TCP-RTU и RTU-TCP: пример №1



Шлюз Modbus TCP-RTU и RTU-TCP: пример №2



GPIO

Входной сигнал

- Датчик вскрытия внешнего шкафа
- Переключение режима работы МЭ типа Д 
- Сигнал с пользовательского устройства 

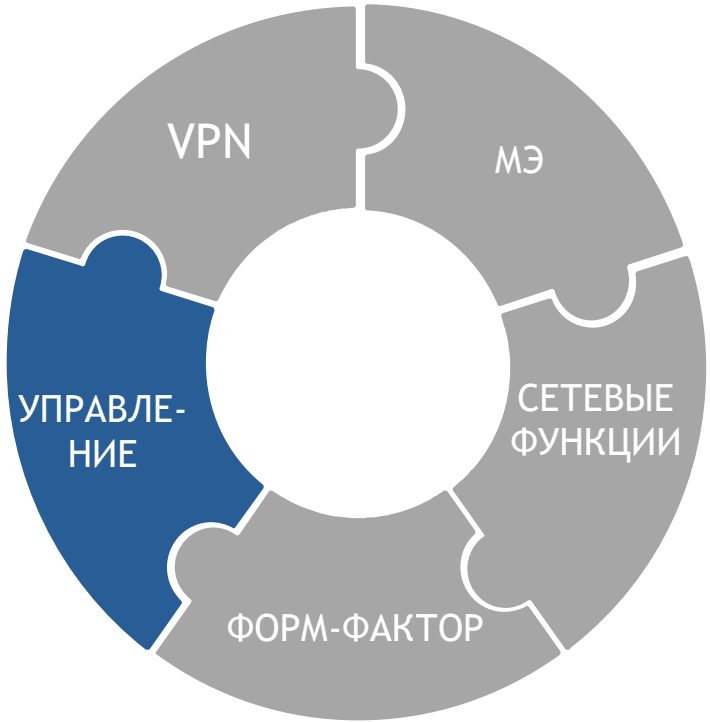
Выходной сигнал

- Кластер с шлюзом Modbus TCP-RTU
- Индикатор событий
  - Работа в регламентном обслуживании
  - Работа в штатном режиме
  - Работа в специальном режиме
  - Вскрыт шкаф
  - Сигнал с пользовательского устройства

ViPNet Coordinator IG: характеристики

УПРАВЛЕНИЕ

- Настройка: Web-интерфейс, консоль, SSH
- Обновления: локально, ViPNet Administrator
- Удаленное управление : ViPNet Administrator, ViPNet Policy Manager
- Удаленный мониторинг: ViPNet StateWatcher, SNMP, Syslog
- Event log: Firewall Event, System Security Event



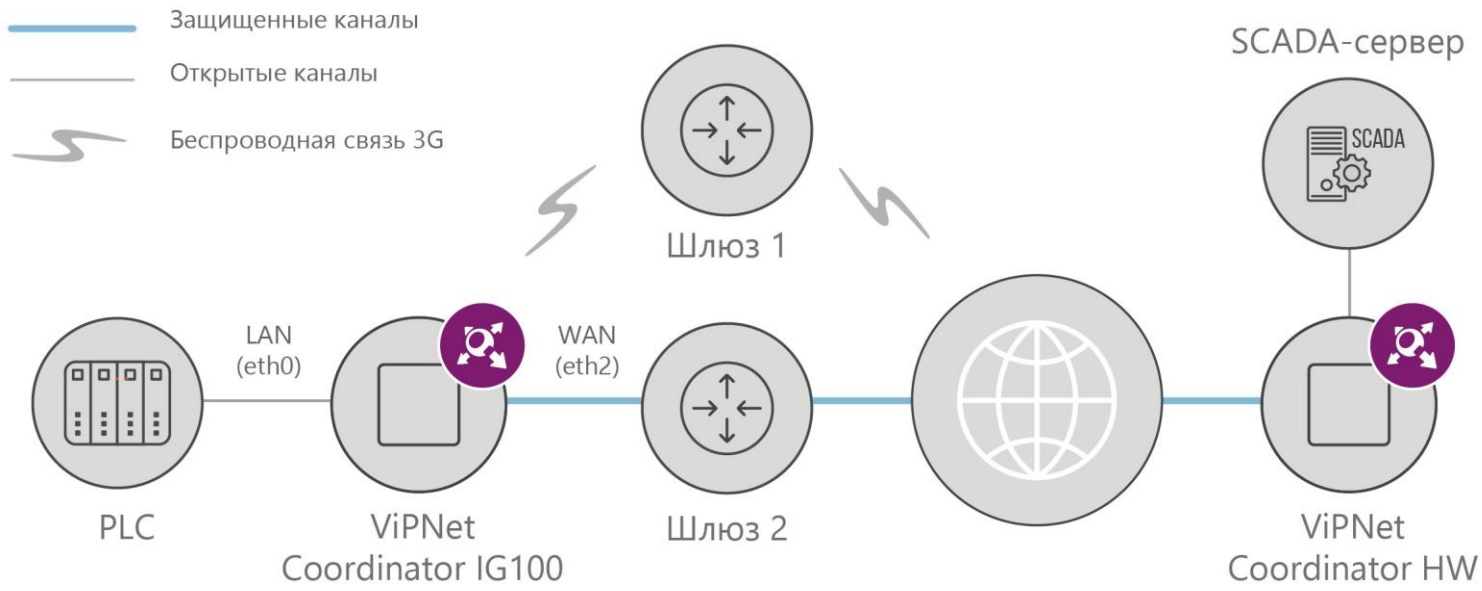
ViPNet Coordinator IG: характеристики

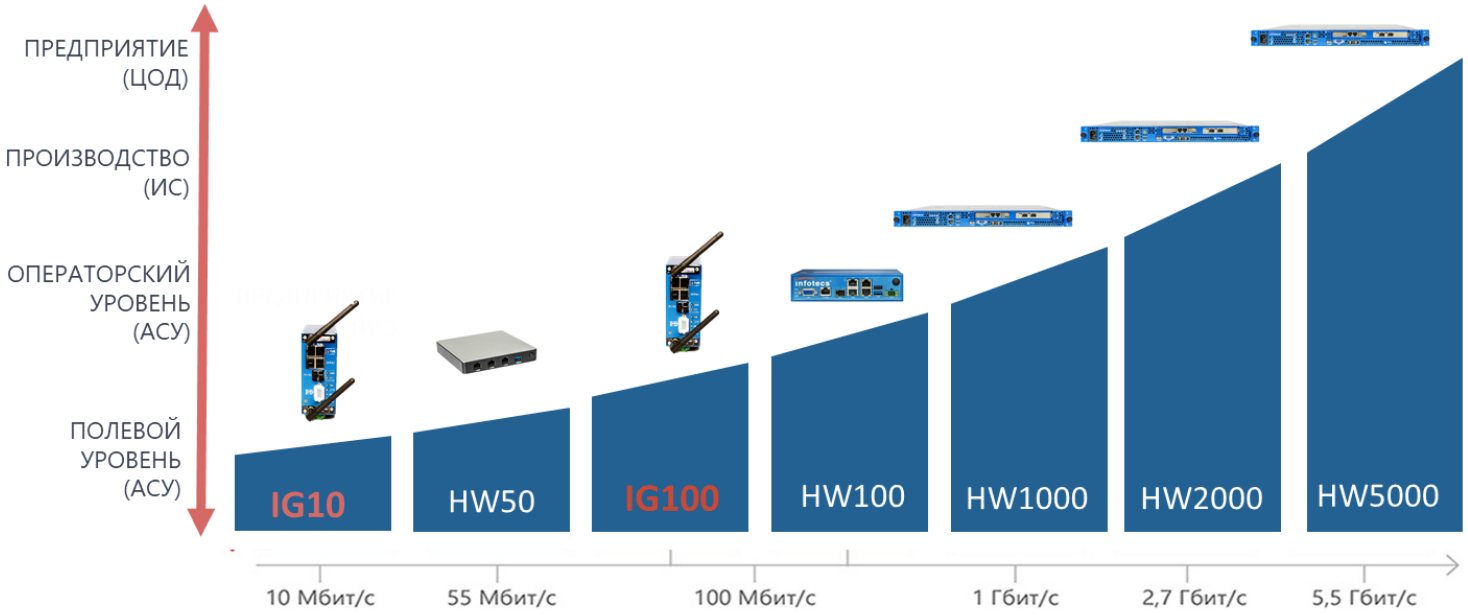
НАДЕЖНОСТЬ

- Кластер горячего резервирования (Failover)
- MultiWAN
- 24/7/235 режим работы
- 350 тыс. часов наработки на отказ



MultiWAN: резервирование каналов





Непрерывная безопасность от ЦОД до контроллера

- Встречная работа
- Единое управление

Сертификация

ViPNet Coordinator IG10

- Сертификат СКЗИ класса КС3
- Сертификат МЭ 4 класса защищенности

ViPNet Coordinator IG10 и ViPNet Coordinator IG100

- Отчетные материалы на СКЗИ класса КС3 и МЭ 4 класса защищенности отправлены регулятору
- Заключительная стадия подготовки отчетных материалов по МЭ типа А.4 и Д.4




infotecs
ViPNet SIES – решение для
защиты информации
промышленных систем

Что такое ViPNet SIES?

Встраиваемые криптографические средства защиты информации для интеграции в

- устройства автоматизации на всех уровнях АСУ
- устройства межмашинного взаимодействия M2M
- IoT/IIoT устройства
- встраиваемые системы



Состав решения ViPNet SIES

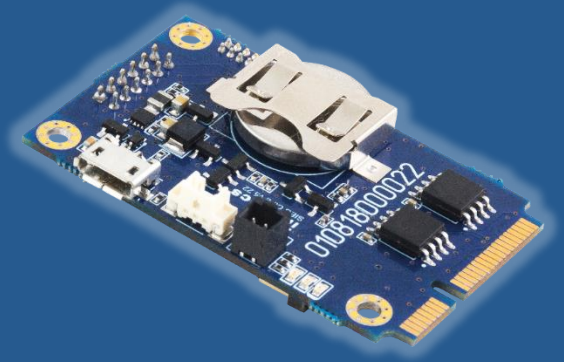


- Законченные СКЗИ класса КС1 и КС3, не требуют оценки влияния
- Возможность использования криптографии на разных по вычислительной мощности устройствах
- Нет зависимости от ОС и архитектуры устройств



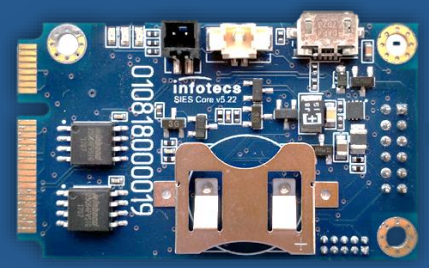
Компоненты для защиты устройств ViPNet SIES Core и ViPNet SIES Unit

Криптографический модуль ViPNet SIES Core

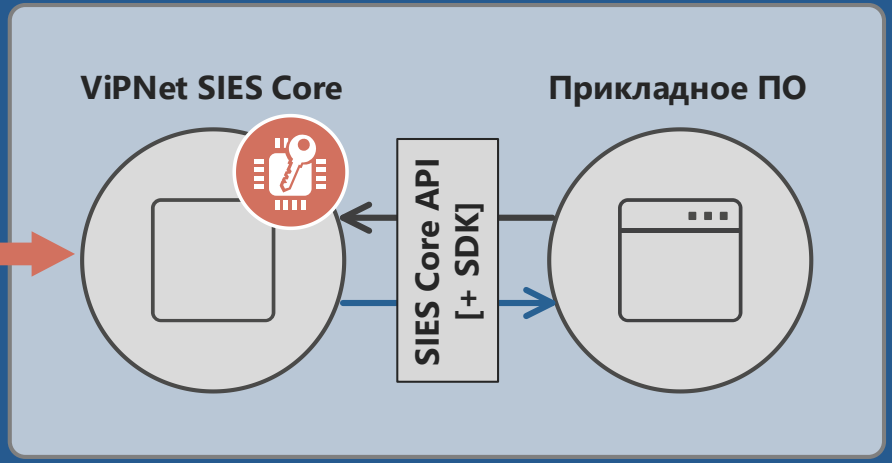


- Функционально законченное СКЗИ, соответствующее классам КС1, КС3
- Интеграция в защищаемое устройство при помощи интерфейсов UART, USB, SPI
- Доступ к криптографическим функциям через SIES Core API и SIES Core SDK
- Поддержка промышленных протоколов
- Пассивное устройство, выполняет функции защиты информации по вызову прикладного ПО
- Обеспечивает информационную безопасность на уровне данных
- Криптографические операции по алгоритмам ГОСТ (ГОСТ Р 34.12-2015+ГОСТ Р 34.13-2015, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ 28147-89)

Интеграция ViPNet SIES Core



UART / USB / SPI



ViPNet SIES Core

Защищаемое устройство

(ПЛК, УСО, датчик и т.п.)

Интеграция ViPNet SIES Unit

infotecs



Защищаемое устройство

Защищаемое устройство
(SCADA/OPC-сервер, рабочая станция и т. п.)

Операционная система

RESTful API

Прикладное ПО

ViPNet SIES Unit

Компоненты решения ViPNet SIES

infotecs

	ViPNet SIES Core	ViPNet SIES Unit
Защищаемые устройства	Контроллеры, УСПД, УСО, исполнительные устройства, датчики	Серверы и рабочие станции
Интерфейс интеграции	UART, USB, SPI	Инсталляция на ЗУ под управлением ОС Windows или Linux
API	SIES Core API [+ SDK]	RESTful API
Исполнение	SOM-модуль, PCI Express® Full-Mini Card, 4 -15 В DC, -40^0...+70^{0}C	Программное обеспечение
Криптография	ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015	

Функции защиты информации ViPNet SIES Core и ViPNet SIES Unit



Защита информации по протоколу CRISP

- зашифрование и расшифрование блока данных
- вычисление и проверка имитовставки для блока данных
- защита от навязывания повторных сообщений

Защита информации с помощью прикладной PKI

- зашифрование и расшифрование данных в CMS-контейнере
- создание и проверка усиленной неквалифицированной электронной подписи в CMS-контейнере

Другие функции защиты информации

- вычисление и проверка значения хэш-кода для блока данных

Криптографический протокол CRISP

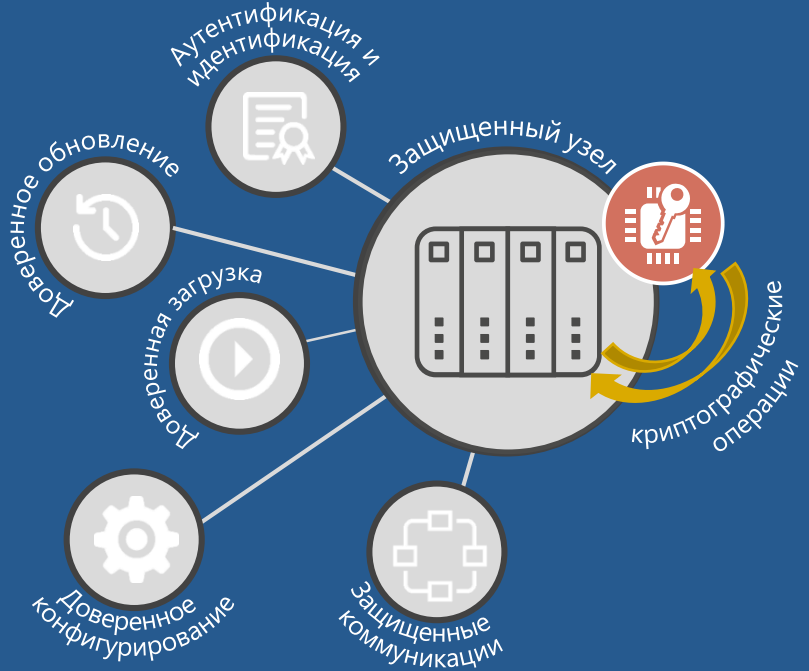
infotecs



CRISP (Cryptographic Industrial Security Protocol) – неинтерактивный протокол защищенной передачи данных для индустриальных систем

- Предраспределённые симметричные ключи
- Аутентификация источника сообщений (у абонентов общий секретный ключ)
- Поддержка адресных и широковещательных сообщений
- Обязательное обеспечение целостности при помощи имитовставки
- Обеспечение конфиденциальности при помощи блочного шифра
- Защита от навязывания повторных сообщений
- Малый размер вспомогательных данных

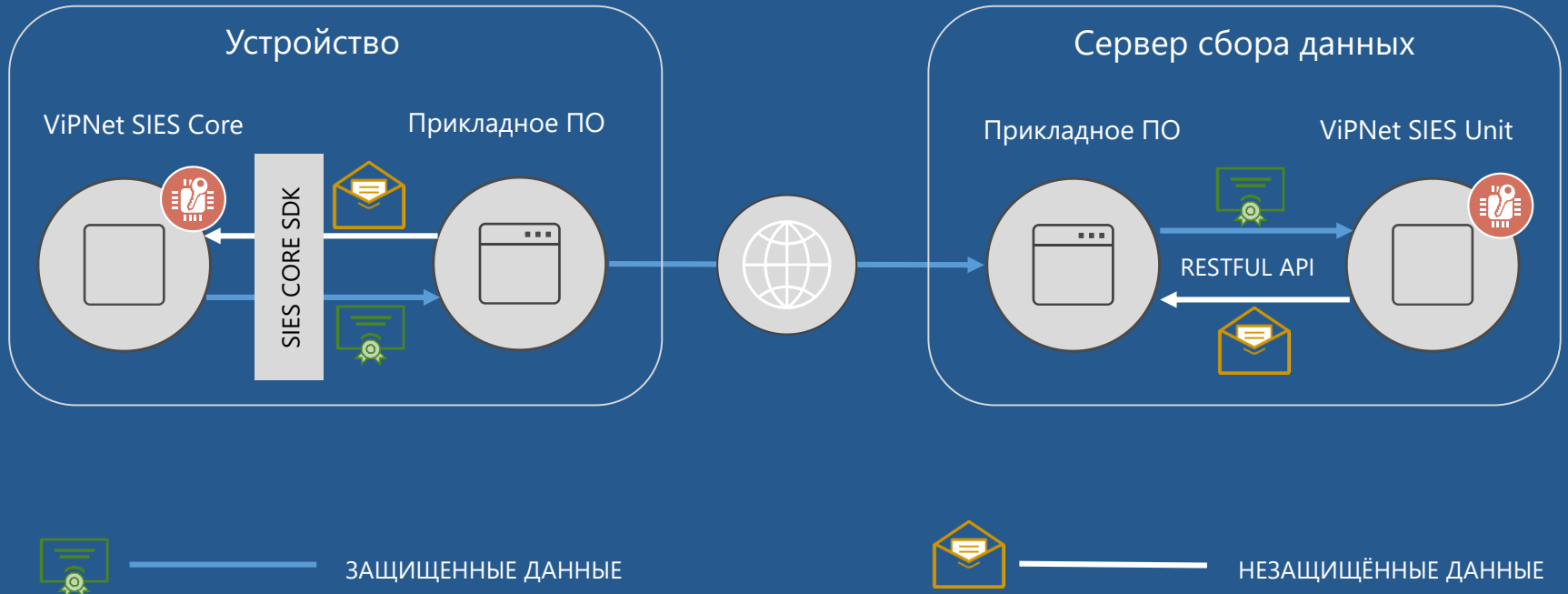
Криптографические сервисы для защищаемых устройств



Сценарии защиты информации:

- Обеспечение конфиденциальности передаваемых данных
- Обеспечение аутентичности и целостности передаваемых данных
- Доверенное локальное и удаленное обновление ПО устройства
- Доверенное локальное и удаленное конфигурирование устройства
- Доверенная загрузка устройства
- Двухфакторная аутентификация на устройстве

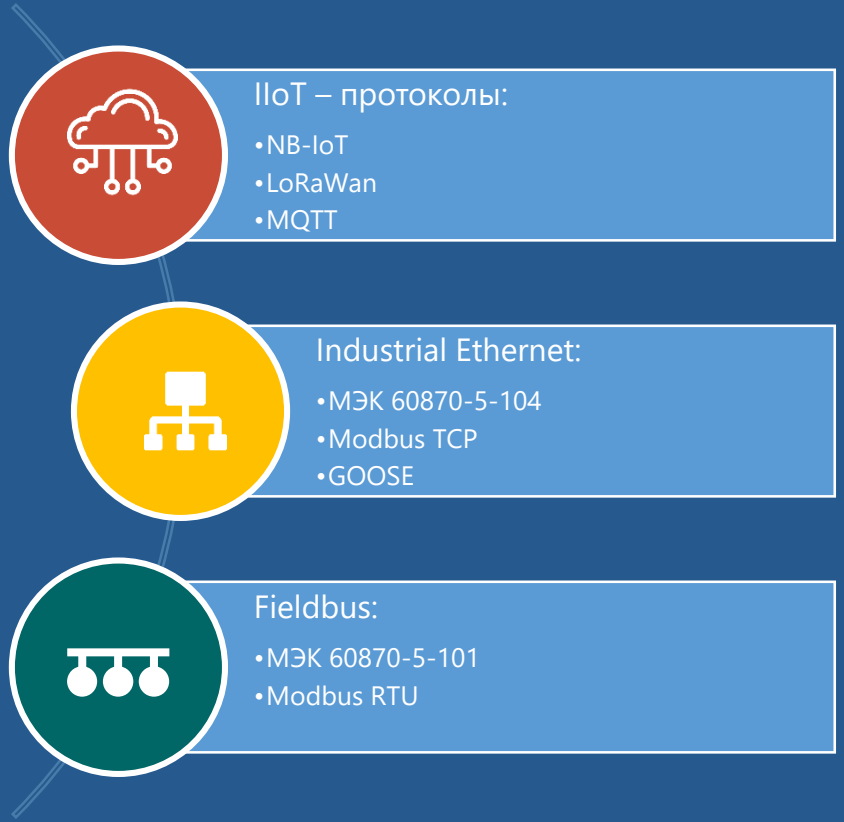
Защита коммуникаций с помощью ViPNet SIES



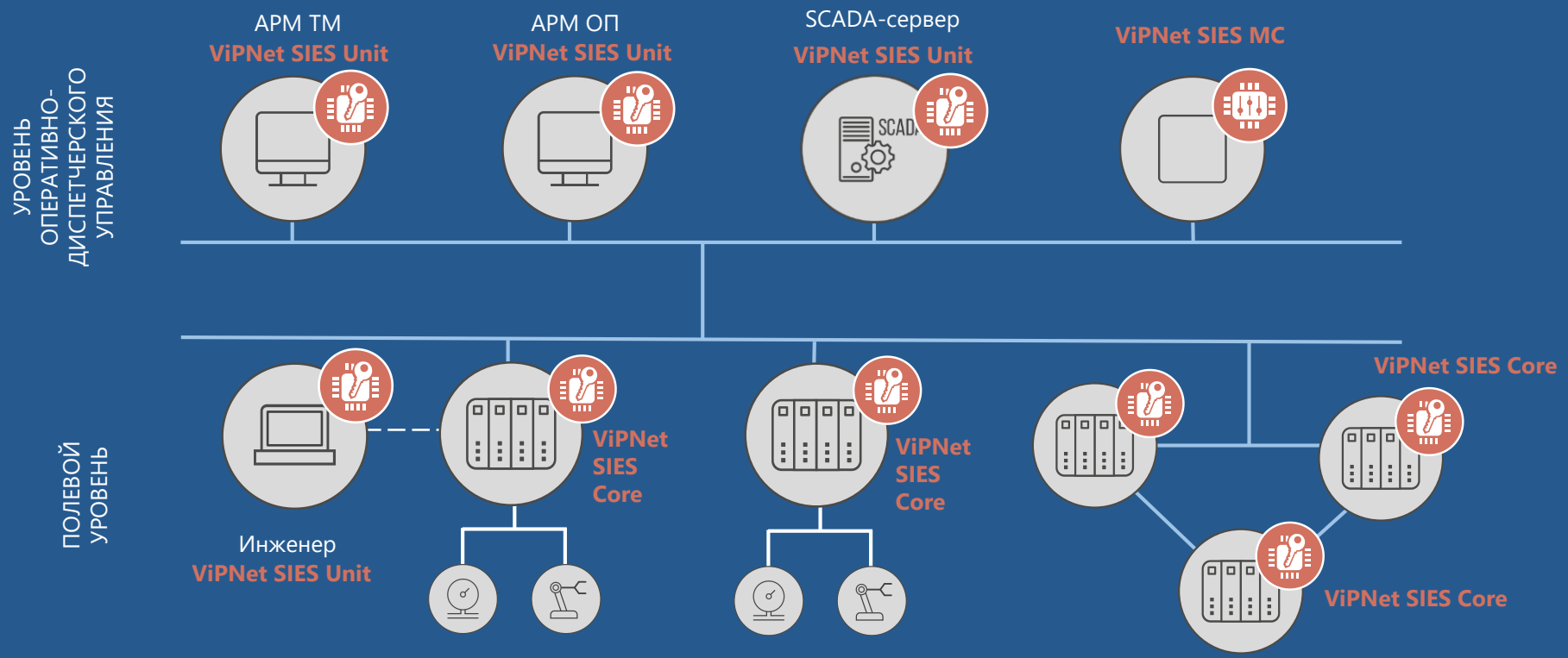
Какие промышленные протоколы можно защищать с помощью CRISP?

CRISP – рекомендация по стандартизации

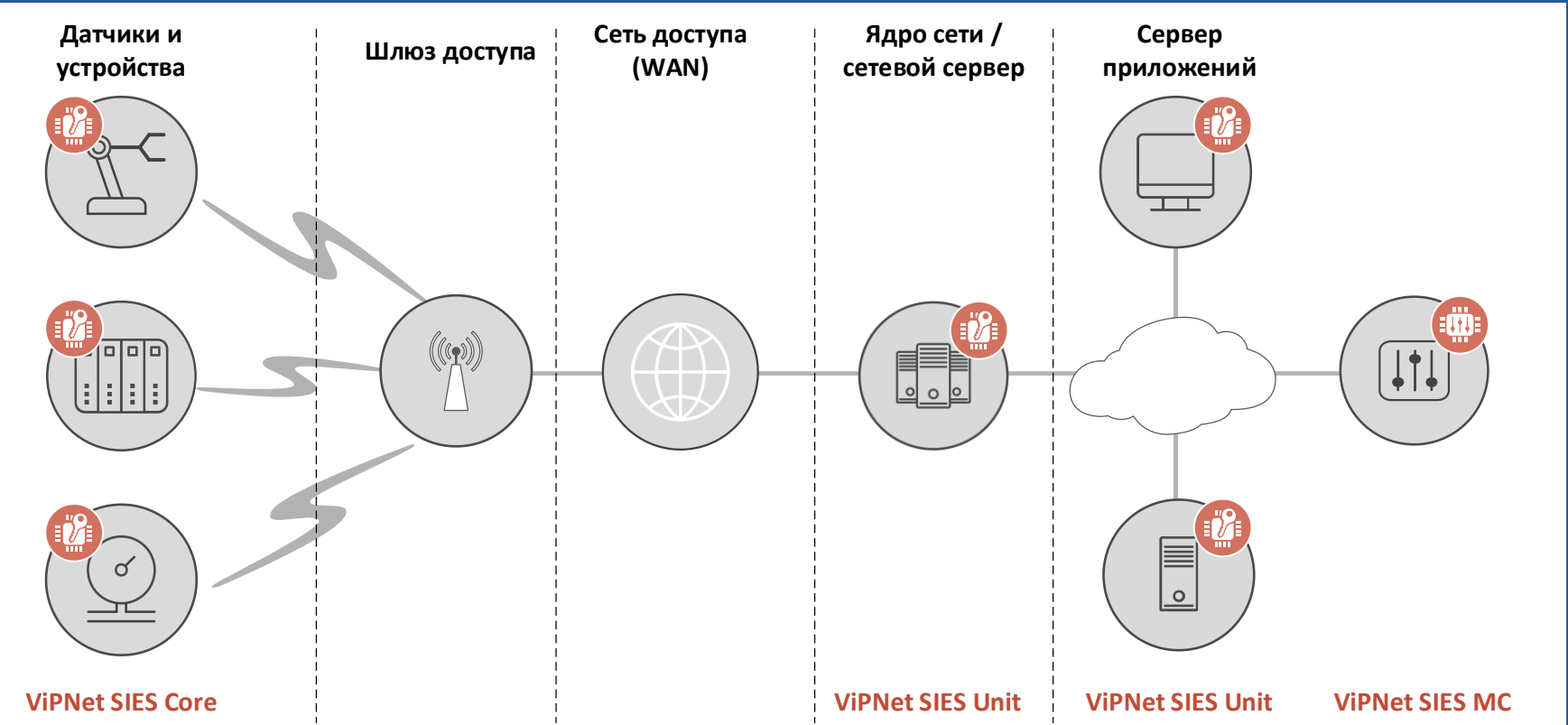
Технического комитета по стандартизации «Криптографическая защита информации» (ТК26)



Защищенная АСУ ТП



Защищенная IIoT-система





Управление решением ViPNet SIES

Центр управления ViPNet SIES MC







ViPNet SIES MC VA

- Max: 5000-узлов
- Max: 500 администраторов безопасности
- Планируется сертификация по требованиям ФСБ России к СКЗИ КС1

ViPNet SIES MC 3000

- Max: 3000-узлов
- Max: 300 администраторов безопасности
- Планируется сертификация по требованиям ФСБ России к СКЗИ КС3

ViPNet SIES MC 10000

- Max: 10000-узлов
- Max: 1000 администраторов безопасности
- Сертификация по требованиям ФСБ России к СКЗИ КС3

Основные задачи ViPNet SIES MC

infotecs



Управление ключами и сертифика-тами SIES-узлов



Защищенный обмен с SIES-узлами



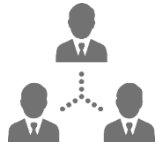
Управление SIES-узлами



Мониторинг состояния SIES-узлов



Настройка SIES MC



Разграничение прав доступа к решению SIES

Объекты управления SIES MC: SIES-узлы

infotecs



ПАК ViPNet SIES Core

ПО ViPNet SIES Unit

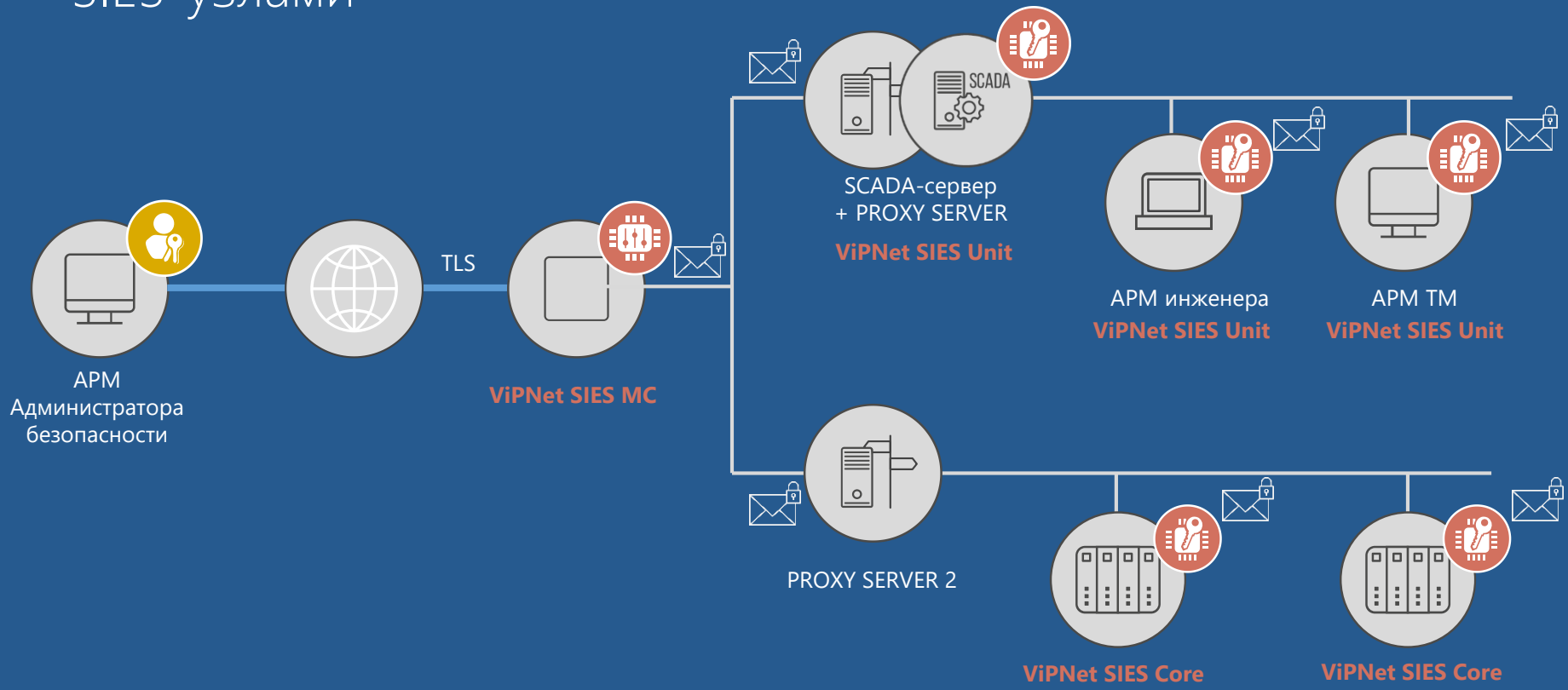
Пользователь АСУ

Сервисный инженер, Инженер КИП

Другой SIES-узел

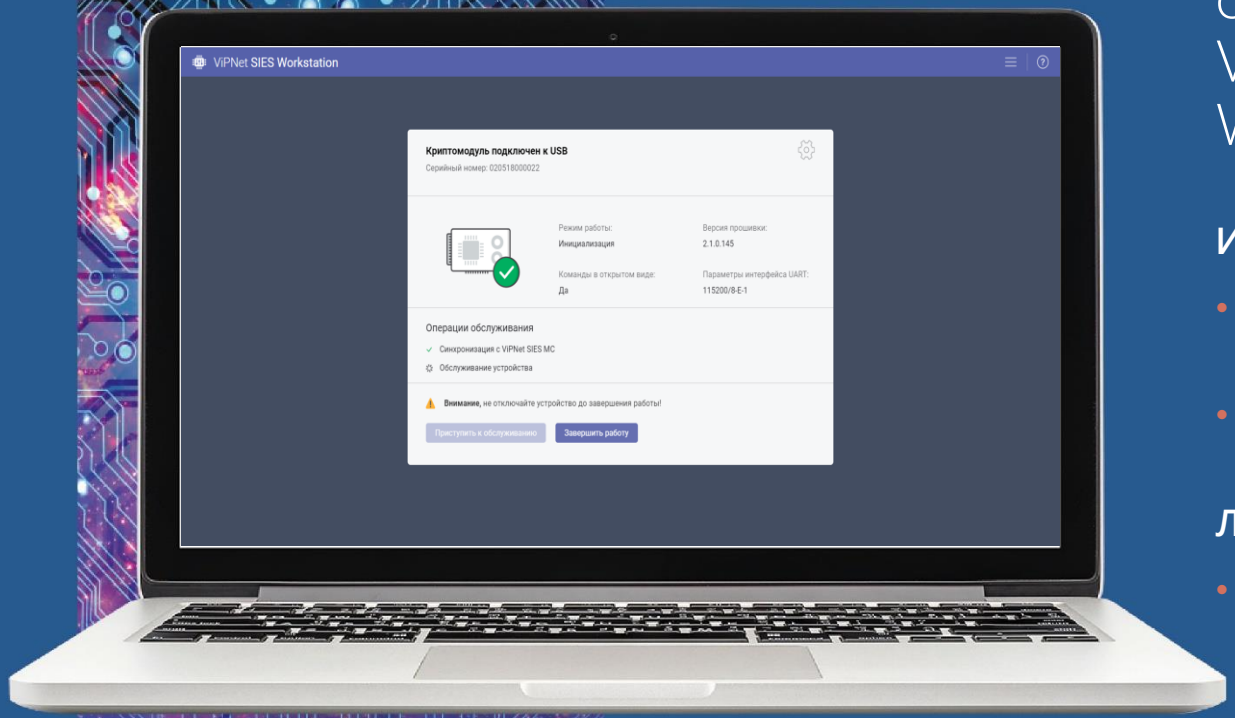
Криптопровайдеры и прочие PKI-продукты

Дистанционный защищенный обмен с SIES-узлами



infotecs

АРМ локального обслуживания ViPNet SIES Workstation



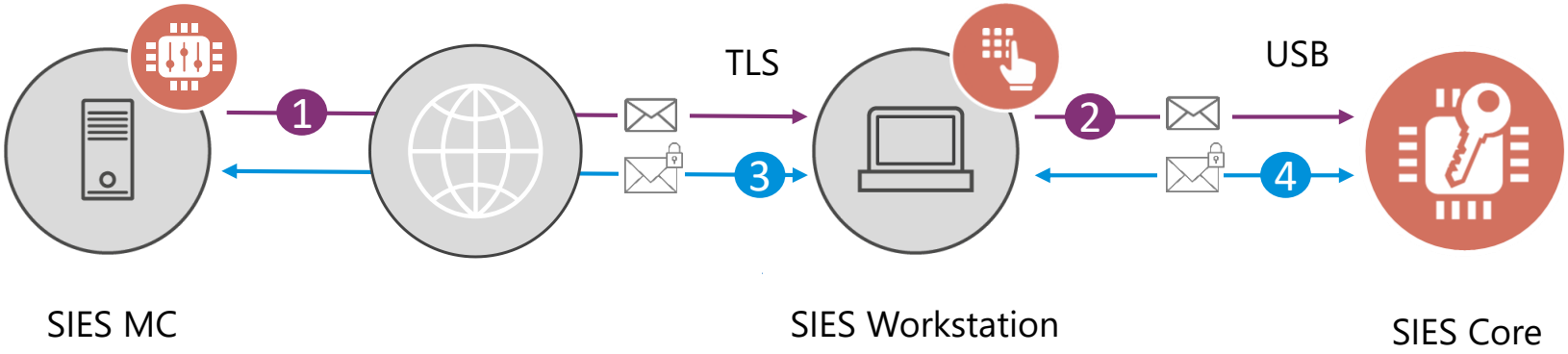
Инициализация

- Загрузка первичной ключевой информации
- Настройка служебной ключевой подсистемы

Локальное обслуживание

- Управление ViPNet SIES Core или SIES Unit в режимах штатный, конфигурирование, блокировка

ViPNet SIES Workstation



Инициализация

Локальное обслуживание

ViPNet SIES Development kit

infotecs



- **ViPNet SIES Core** – 2шт.
  SIES Core SDK, Тестовая утилита
- **ViPNet SIES Unit** – 1шт.
- **ViPNet SIES MC VA** – 1шт.
  Лицензия для администратора – 1шт.
- **ViPNet SIES Workstation** – 1шт.
- **ViPNet PKI Client с TLS Unit** – 2шт.
- **Документация:** описания протоколов, описание SDK, инструкция по разворачиванию, пользовательская документация

Спасибо за внимание!

БУДНИ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs

миниБИБ онлайн

www.infosecuritydays.ru

БУДНИ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs