КСБ-СОФТ

Мониторинг в АСУ ТП – не попробуешь, не узнаешь

Спикер:

Шипицын Михаил

заместитель генерального директора, КСБ-СОФТ

«КСБ-СОФТ»

- Лицензиат ФСТЭК России
- Лицензиат ФСБ России

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

80+
регионов внедрения

4000+
реализованных проектов

ПОРТФОЛИО В ЧАСТИ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ ЗА 2023 Г.

Сфера: энергетика.
Конечный Заказчик: ПАО «Россети» и его филиалы.
Объекты защиты: АСУ ТП электрических подстанций 500 кВ, 330 кВ, 220 кВ
Работы: проектирование СИБ, пусконаладочные работы СИБ

Сфера: топливно-энергетический комплекс.
Конечный Заказчик: ООО «Арктик СПГ 2», АО «Верхнечонскнефтегаз» (ПАО «НК «Роснефть»)
Объекты защиты: АСУ по управлению электроснабжением, пожарной сигнализации и управления пожаротушением
Работы: проектирование СИБ, пусконаладочные работы СИБ

Сфера: транспорт.
Конечный Заказчик: ФГБУ «Канал имени Москвы»
Объекты защиты: АСУ телемеханики, контроля шлюзования, судопропуска и т.д.
Работы: проектирование СИБ

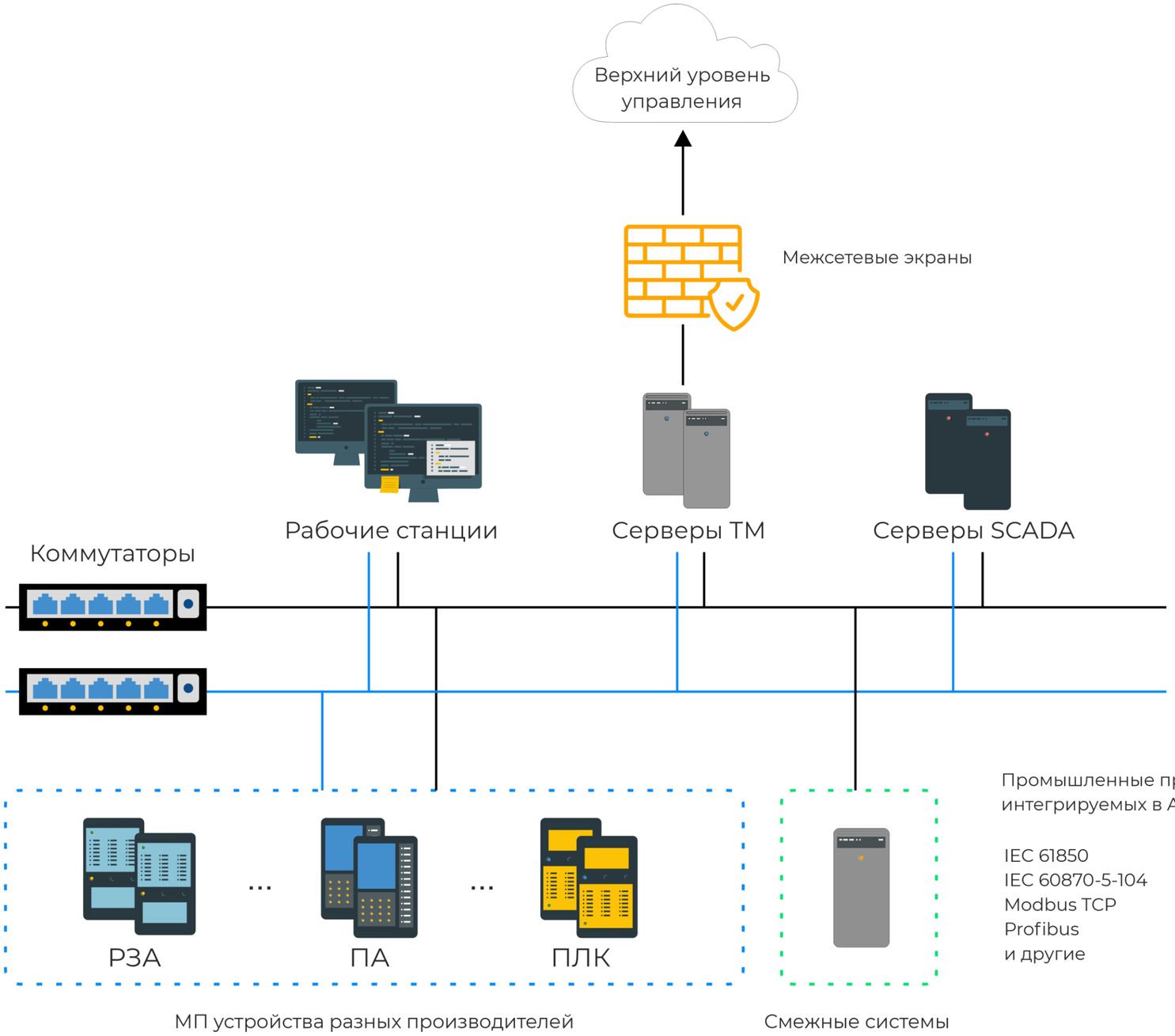
Мониторинг в АСУ ТП – тот, кого нельзя называть

Предприятие, внедрившее мониторинг в АСУ ТП – то, которое выжило

Основные вызовы для предприятия при организации мониторинга

1	Риск нарушения технологического процесса
2	Специфика АСУ ТП (промышленные протоколы, зоопарк оборудования, изолированность)
3	Недостаток экспертизы в части обеспечения ИБ в АСУ ТП
4	Страх ответственности, взаимодействие с ГоССОПКА

Специфика АСУ ТП



Промышленные протоколы МП устройств, интегрируемых в АСУ ТП:

IEC 61850
IEC 60870-5-104
Modbus TCP
Profibus
и другие

Подход КСБ-СОФТ

Возможные причины нарушения технологического процесса:

- Компьютерные атаки
- Воздействие СЗИ
- Действия персонала (внутреннего нарушителя)
- Действия подрядчиков
- Отсутствие организованного взаимодействия технологической службы, ИТ подразделения информатизации и службы ИБ

Наш подход:

- Предпроектное обследование профильными специалистами с опытом работы в АСУ ТП
- Моделирование угроз и проектирование системы защиты с учетом специфики АСУ ТП
- Пилотирование СЗИ на стенде
- Внедрение СЗИ и приемочные испытания
- Организация мониторинга безопасности
- Подключение к ГоССОПКА
- Обучение персонала

КЛЮЧЕВЫЕ ПРИНЦИПЫ ИБ В АСУ ТП

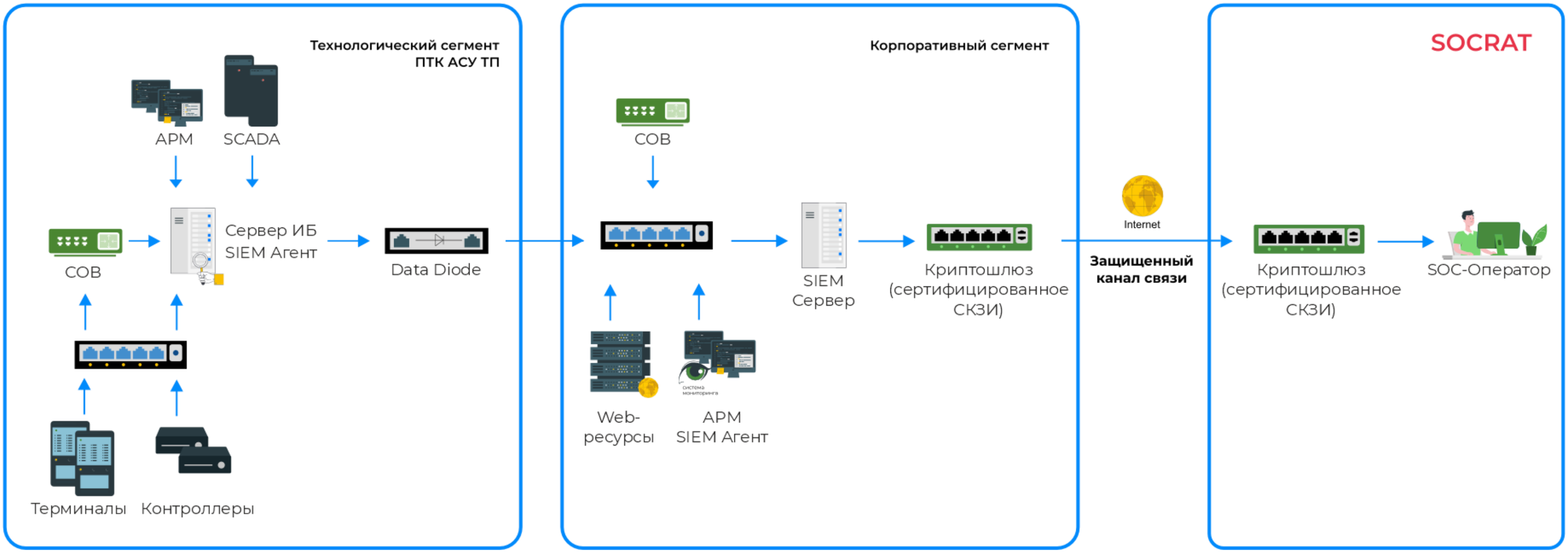
Экспертиза в АСУ ТП –
нельзя защищать то,
в чем не разбираешься

Пилотирование решений
перед внедрением

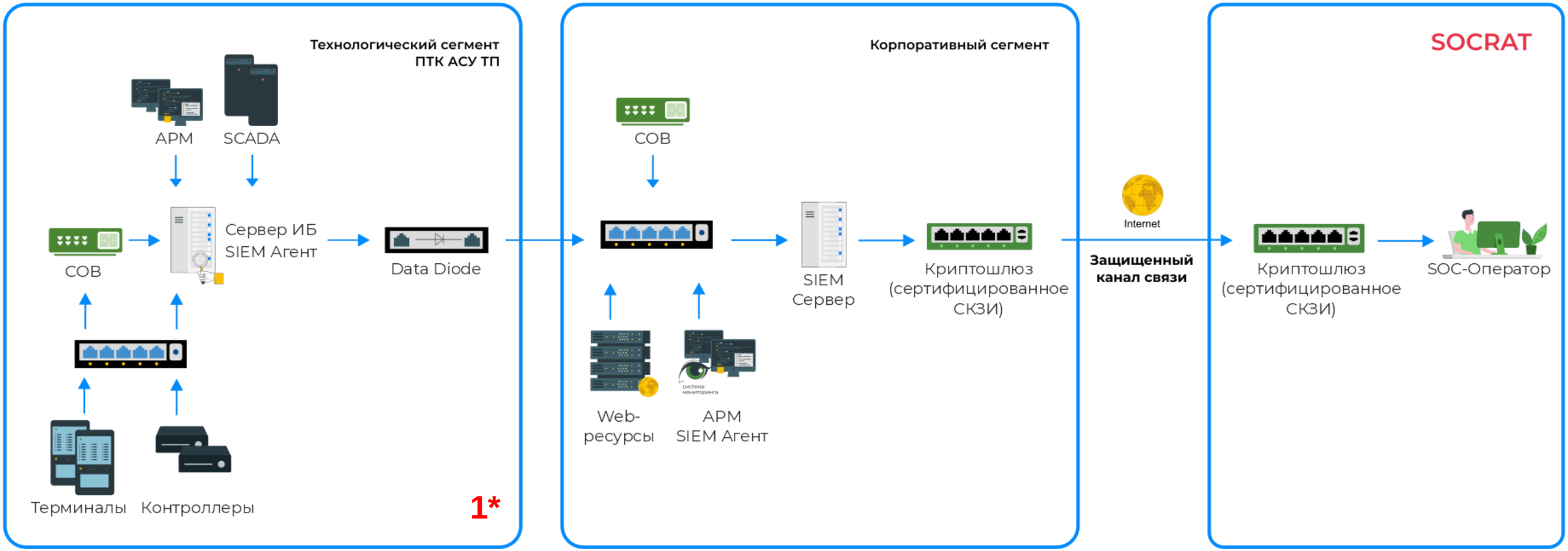
Исключение управляющих
воздействий на АСУ ТП

Исключение влияния системы
ИБ на технологический процесс

Мониторинг в АСУ ТП с помощью SOCRAT

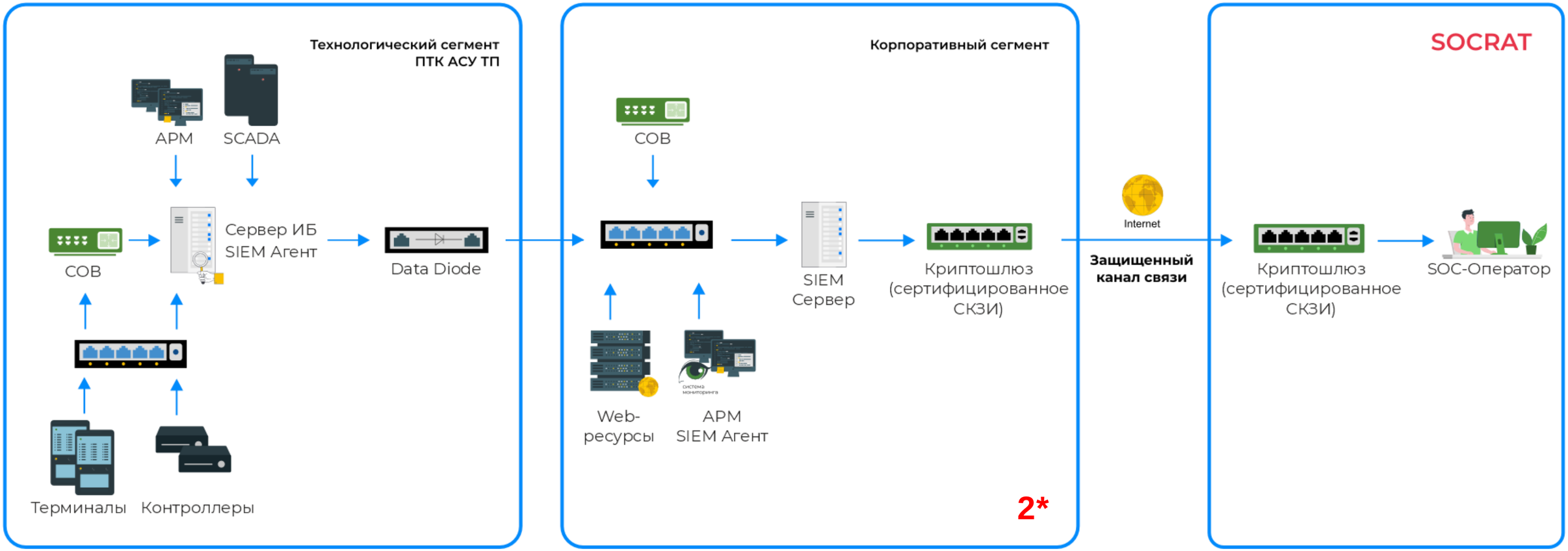


Мониторинг в АСУ ТП с помощью SOCRAT



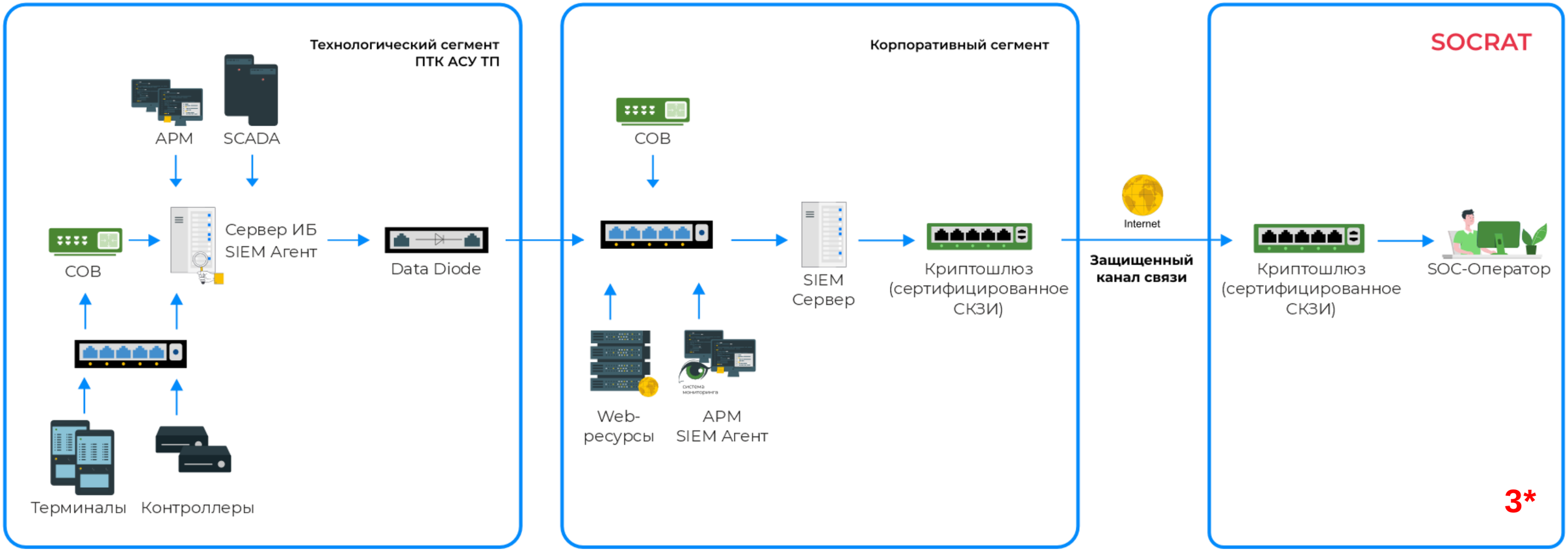
* 1– передача событий технологической сети в SIEM, развернутую в корпоративном сегменте, осуществляется через устройство однонаправленной передачи данных, что позволяет обеспечить изоляцию АСУ ТП

Мониторинг в АСУ ТП с помощью SOCRAT



* 2 – осуществляем защиту и мониторинг ВСЕЙ инфраструктуры предприятия – и технологической и корпоративной

Мониторинг в АСУ ТП с помощью SOCRAT



* 3 – аналитики SOCRAT с богатой экспертизой в АСУ ТП

Интеграция с ГосСОПКА

Взаимодействие с ГосСОПКА Через SOCRAT

Взаимодействие с ГосСОПКА напрямую

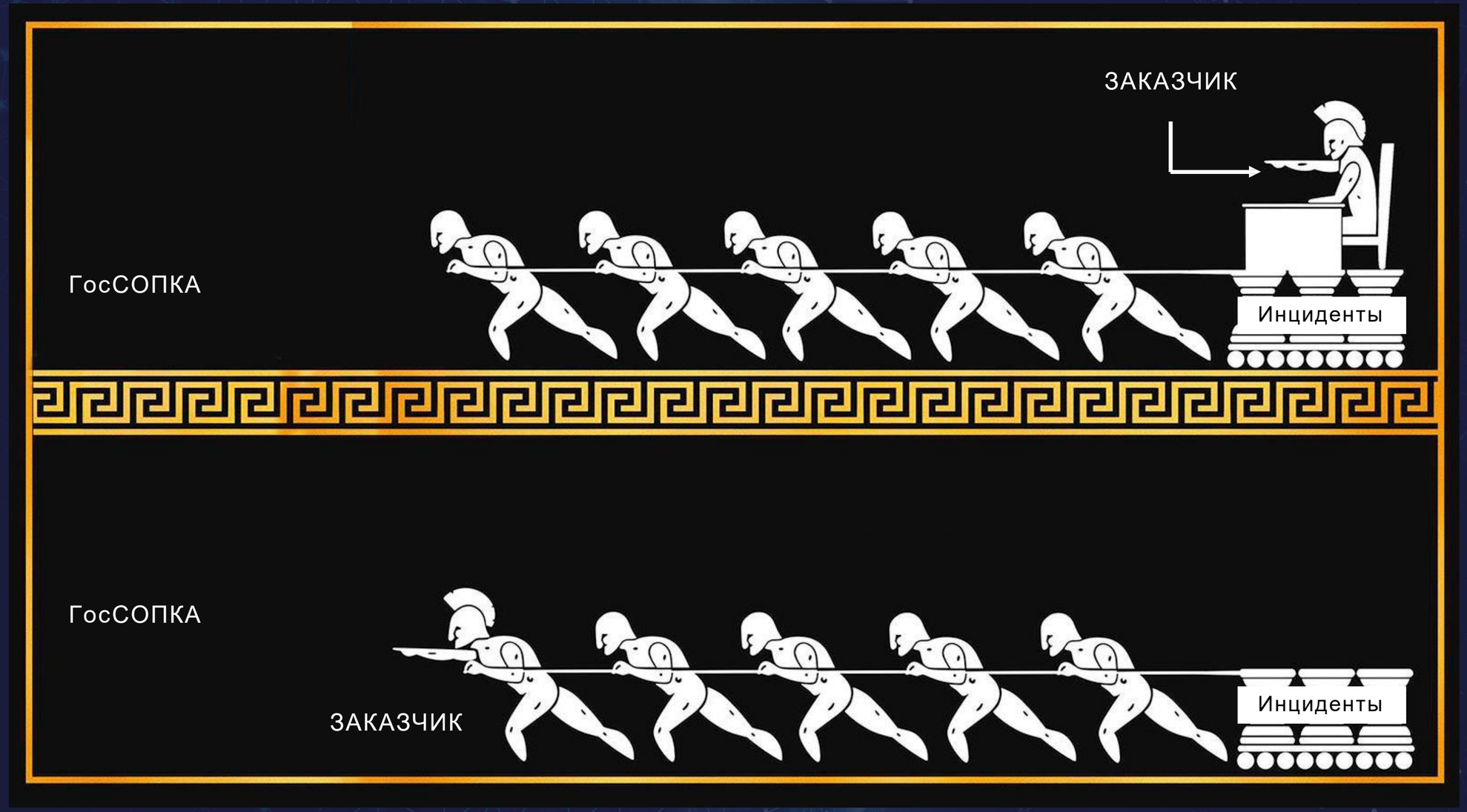
Преимущества взаимодействия с ГосСОПКА через корпоративный центр

1. Команда SOCRAT отслеживает не только инциденты информационной безопасности (в соответствии с классификацией НКЦКИ), но также реагирует на компьютерные атаки и уязвимости, тем самым **предотвращая появление инцидентов**

2. Реагирование на инциденты **происходит оперативно и своевременно**, так как команда SOCRAT следит за состоянием защищенности контролируемых объектов **в режиме 24x7**

3. Центр мониторинга SOCRAT является корпоративным центром ГосСОПКА и способен **самостоятельно направлять информацию об инцидентах в НКЦКИ, а также, получать рекомендации и сопровождать инцидент до полной ликвидации**

Интеграция с ГосСОПКА



Ценность мониторинга

Подключение к SOCRAT – это возможность

- Выполнять требования законодательства
- Обеспечивать процесс выявления событий и инцидентов
- Выявлять инциденты, ошибки конфигурации, уязвимости ПО, следы вредоносных программ
- Предотвращать инциденты, их влияние на инфраструктуру
- Осуществлять взаимодействие с ГосСОПКА
- Повышать уровень защищенности инфраструктуры

SOCRAT

Технические системы

передают аналитикам сообщения от средств защиты и компонентов информационных систем

Эксперты

отличают ложное срабатывание от «боевого»

оценивают, являются ли цепочки штатных событий началом зарождающейся атаки

прогнозируют вероятность совершения атаки

помогают клиентам отработать и расследовать инциденты

КСБ-СОФТ

8 800 3333-872

+7 (8352) 322-322

info@ksb-soft.ru

КАНАЛ
«МНЕНИЕ ИНТЕГРАТОРА»

ПОДКАСТ
«SOCRAT ЗА СТЕКЛОМ»

САЙТ
КОМПАНИИ