



Проблематика создания комплексных систем ИБ ОКИИ: взгляд со стороны интегратора



Спикер:

- **Татьяна Егорова** – заместитель руководителя департамента интеграционных решений по вопросам промышленной кибербезопасности, КСБ-СОФТ



Системный интегратор
в сфере информационной
безопасности и импортозамещения
информационных технологий



Входим в ГК «Кейсистемс»



Лицензиат ФСТЭК России

Лицензиат ФСБ России

Проекты компании курируют опытные
ИБ-специалисты, аккредитованные
по международным сертификациям
OSCP, CISM, CGEIT и CISA.

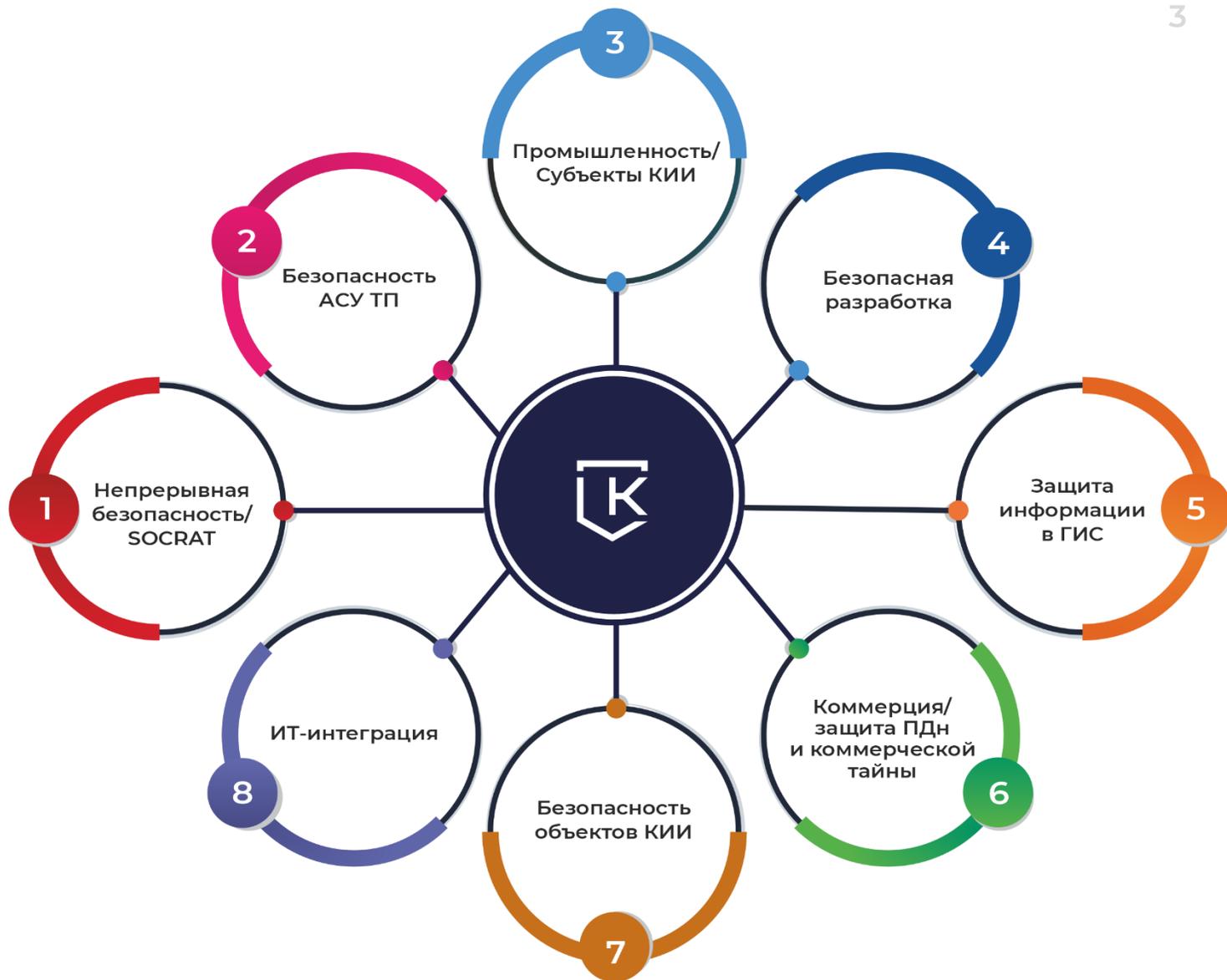
80+

регионов
внедрения

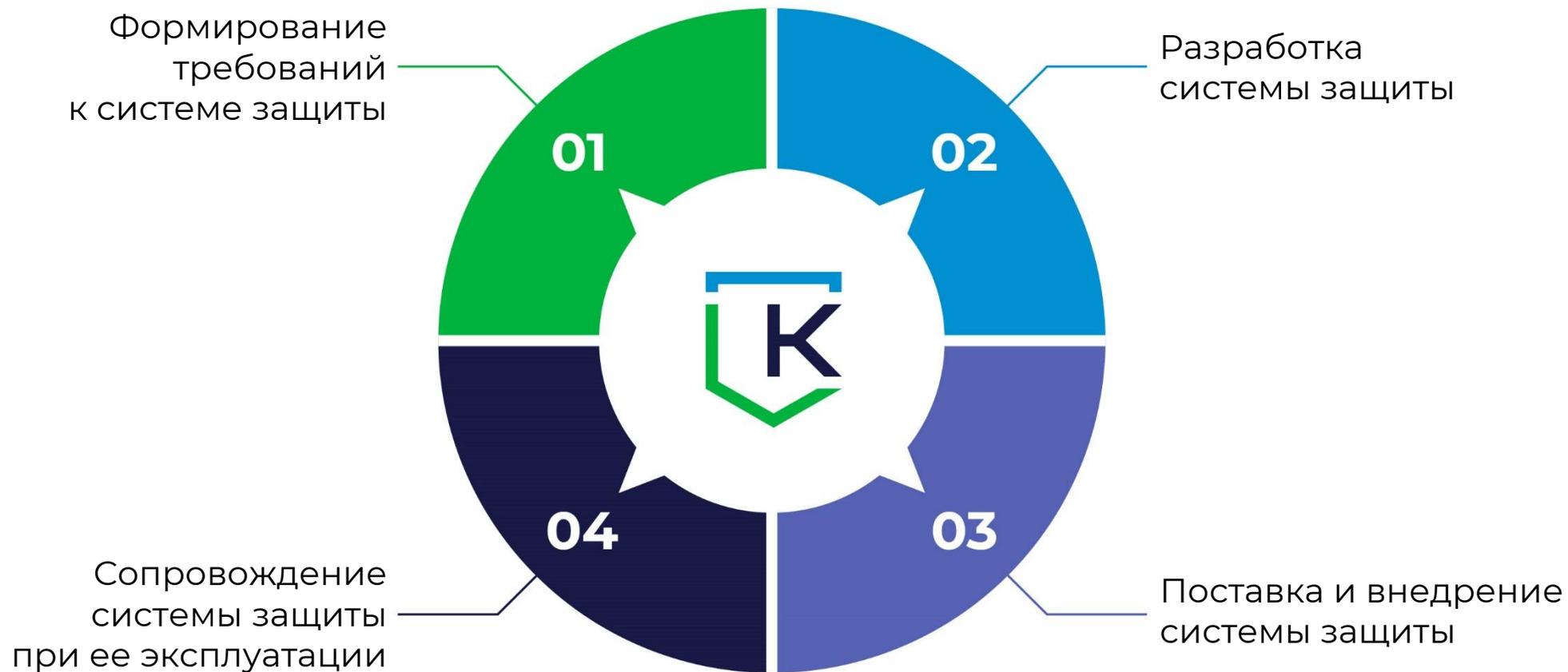
4000+

реализованных
проектов

НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ



ЭТАПЫ СОЗДАНИЯ СИСТЕМ ИБ АСУ ТП



УСПЕШНЫЙ ОПЫТ В РАЗЛИЧНЫХ ОТРАСЛЯХ

5



Сфера: энергетика

Конечный Заказчик: ПАО «Россети», ПАО «Интер РАО»

Объекты защиты: АСУ ТП ЭЭ объектов различного уровня и назначения

Работы: проектирование СИБ, пусконаладочные работы СИБ



Сфера: топливно-энергетический комплекс

Конечный Заказчик: ПАО «НК «Роснефть»

Объекты защиты: АСУ ТП по управлению электроснабжением, технологические АСУ ТП

Работы: проектирование СИБ, пусконаладочные работы СИБ



Сфера: химическая промышленность

Конечный Заказчик: ПАО «СИБУР Холдинг»

Объекты защиты: АСУ ТП по управлению электроснабжением, технологические АСУ ТП

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

ПАО «Россети»

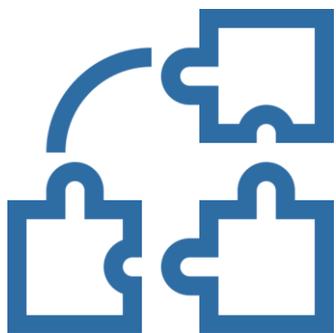
Наши проекты реализованы на ПС 220/330/500 кВ
всех филиалов МЭС ПАО «Россети»

Проекты по направлению электроэнергетики
можно разделить на 2 группы:

1. Проектирование комплексных систем защиты информации на всех стадиях (ОТР, ПД, РД)
2. Поставка комплексных систем информационной безопасности, включая пуско-наладочные работы, проведение испытаний и обучение конечного Заказчика

Проекты по построению систем информационной безопасности ПС для нашей команды на сегодня являются типовыми, так как в данном направлении накоплен колоссальный опыт





Лицензируемый вид деятельности:

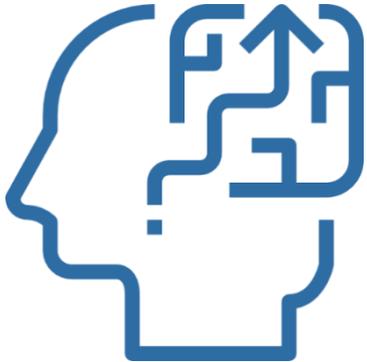
- ✓ Лицензия ФСТЭК
- ✓ Лицензия ФСБ

Допуски на предприятия:

- ✓ Электробезопасность
- ✓ Промышленная безопасность
- ✓ Охрана труда

Избыточные:

- ✗ СРО



Знание НТД

- ФЗ и подзаконные акты
- Актуальные требования регуляторов
- Актуальные отраслевые требования
- ГОСТ к системам автоматизации (ГОСТ 34)

Знание специфики АСУ ТП

Знание средств защиты информации

- Знание рынка СЗИ
- Практические навыки работы с СЗИ
- Совместимость СЗИ

ПРОБЛЕМАТИКА СОЗДАНИЯ КОМПЛЕКСНЫХ СИСТЕМ ИБ: ВЗГЛЯД СО СТОРОНЫ ИНТЕГРАТОРА

9



**ИБ
по «остаточному
принципу»**



**Отсутствие дорожной
карты СОИБ –
«Титульный хаос»**



**Отсутствие методик
определения сметной
стоимости ИБ**



Залог успеха - качественные исходные данные

- Техническое задание / задание на проектирование
- Исходные данные в части СОИБ
 - существующие
 - планируемые (проектируемые)
- Исходные данные в части защищаемых систем



Наблюдения:

- Минимальная проработка на этапе ТЗ
- Исходные данные не актуальны
- Не предоставляется информация о существующей или проектируемой комплексной системе СОИБ
- Не учитываются решения смежных титулов
- Сложности в коммуникациях
- Долгие цепочки запросов
- Отсутствие ответственных лиц
- Долгие сроки согласований



Последствия:

- Потеря времени
- Многократные итерации проектирования – увеличение трудозатрат
- Срыв сроков
- Ущерб качеству результатов проектирования – ущерб безопасности
- Финансовые ущербы
- «Проектирование в корзину»
- Теоретическое проектирование, не приводящее к реальной безопасности

Типичные примеры ТЗ:

Требования к обеспечению информационной безопасности	<ol style="list-style-type: none">1. Работы по созданию системы информационной безопасности определить и обосновать при проектировании с учетом действующей НТД;2. Средства и методы защиты информации, в том числе СЗИ встроенные в оборудование АСУ ТП и связи определить и обосновать при проектировании.
Требования к информационной безопасности	Перечень требований к обеспечению информационной безопасности на объекте формируется (уточняется) по результатам разработки проектной документации в отношении вновь устанавливаемого оборудования. Для ПС определение требований по обеспечению информационной безопасности производится в порядке, установленном для объектов КИИ 3-й категории значимости.



НТД в сфере ИБ актуализируются быстрее, чем формируются ТЗ.

Актуализация НТД – задача разработчика системы ИБ.

Актуализация исходных данных – задача всех участников процесса.

АУДИТ – решение для актуализации исходных данных



Задача аудита:

собрать полные и достоверные сведения по обработке конфиденциальной информации в организации

Результат проведения:

- ✓ Собраны все необходимые данные для формирования полного и корректного комплекта документов по защите информации
- ✓ Получена полная информация о текущем состоянии ИБ
- ✓ Проведена оценка достаточности действующих организационно-технических мер по защите информации
- ✓ Выдача рекомендации по устранению типовых нарушений, выявляемых регуляторами при проверках
- ✓ Составление планов по импортозамещению на основе проведенной инвентаризации

СИНХРОНИЗАЦИЯ ПРОЕКТОВ - «ТИТУЛЬНЫЙ ХАОС»

14



"У семи нянек дитя без глазу"

ДОРОЖНАЯ КАРТА СОЗДАНИЯ И РАЗВИТИЯ СИСТЕМ – залог успеха

15

- **СИНХРОНИЗАЦИИ ТИТУЛОВ**

- Текущее или планируемое состояние СОИБ
- Последовательность внедрения
- Совместимость технических решений

- **ОПЕРАТИВНАЯ АКТУАЛИЗАЦИИ ИСХОДНЫХ ДАННЫХ**

- Одновременная реализация нескольких проектов и их взаимное влияние

- **ОТВЕТСТВЕННЫЕ ЛИЦА**

- Цепочка предоставления информации
- Цепочка согласования документации



Отсутствие методик определения сметной стоимости ИБ:

- Недостаточная оценка стоимости ПИР в условиях нехватки и высокой стоимости специалистов
 - Стремление сэкономить на разработчике системы ИБ
 - Ущерб качеству результатов проектирования – ущерб безопасности
- Недостаточная оценка стоимости реализации в условиях регулярного роста стоимости СЗИ
 - Вынужденная необходимость экономии на СЗИ при реализации
 - Ущерб безопасности
- Недостаточная оценка стоимости ПНР в условиях нехватки и высокой стоимости специалистов
 - Стремление сэкономить на внедрении
 - Ущерб безопасности



Залог успеха:

- Разработка методик определения сметной стоимости ИБ близкой к реальности рынка
- Знание особенностей рынка СЗИ
- Актуализация стоимости СЗИ
- Экспертиза в части формирования карт-заказов СЗИ

НАШЕ ПРЕДЛОЖЕНИЕ ПО РЕШЕНИЮ



Создание и актуализация в реальном времени дорожной карты СОИБ



Наличие ответственного и уполномоченного лица Заказчика



Экспертиза и вовлеченность в процесс всех участников



Экспертиза в АСУ ТП интегратора ИБ

Компания КСБ-СОФТ оказывает полный комплекс услуг по защите объектов КИИ

Мы поможем Вам защитить данные и выполнить требования НПА



Безопасность объектов КИИ

Выявление и категорирование объектов КИИ, разработка и внедрение комплексного решения по обеспечению безопасности значимых объектов КИИ, организация взаимодействия с центром ГосСОПКА, анализ уязвимостей и пентест



Импортозамещение

Решение задач импортозамещения в соответствии со стратегией развития информационного общества в Российской Федерации



SOCRAT - центр мониторинга и реагирования на инциденты информационной безопасности

Мониторинг и предотвращение атак на начальных стадиях, либо выявление следов проникновения



Оценка показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры

Выполнение работ по новой методике ФСТЭК России от 02.05.2024 г.

альфа:реестр

- Учет информационных систем
- Автоматизированное формирование единого реестра ГИС/ИС
- Создание портала для публикации сведений об информационных системах
- Формирование графического ИТ-ландшафта

альфа:док

- Реализация организационных мер по обработке и защите ПДн, КИИ, ГИС, включая разработку и актуализацию документации
- Контроль корректности и достаточности применения СЗИ
- Управление процессом по защите информации в курируемых организациях

альфа:крипто

- Электронный учет СКЗИ в соответствии с требованиями ФСБ России
- Автоматизация процесса выдачи СКЗИ, включая электронную очередь
- Контроль сроков действия лицензий и сертификатов

альфа:коннект

- Цифровизация регламентов подачи и обработки заявок на подключение пользователей к ИС
- Контроль выполнения требований по подключению пользователей к ИС
- Ведение реестра пользователей

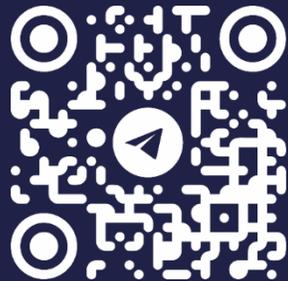


СПАСИБО ЗА ВНИМАНИЕ!

Сделайте первый шаг к новому видению
информационной безопасности вместе с нами!

ПРИГЛАШАЕМ ВАС ПОСЕТИТЬ НАШ СТЕНД!

ОСТАЛИСЬ ВОПРОСЫ?



ksb-soft.ru

+7 (8352) 322-322

info@ksb-soft.ru