



Проектирование 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.

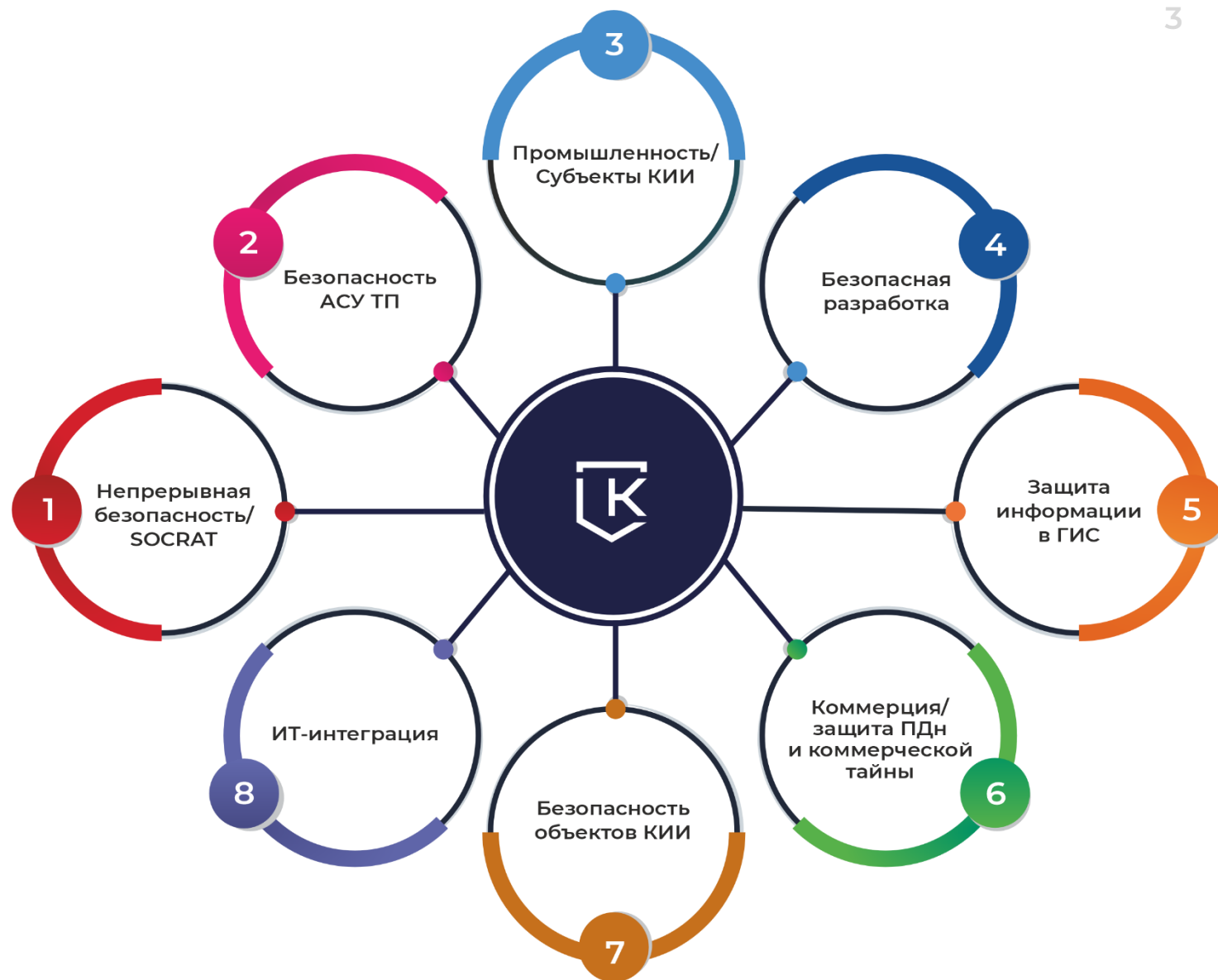
80+

регионов
внедрения

4000+

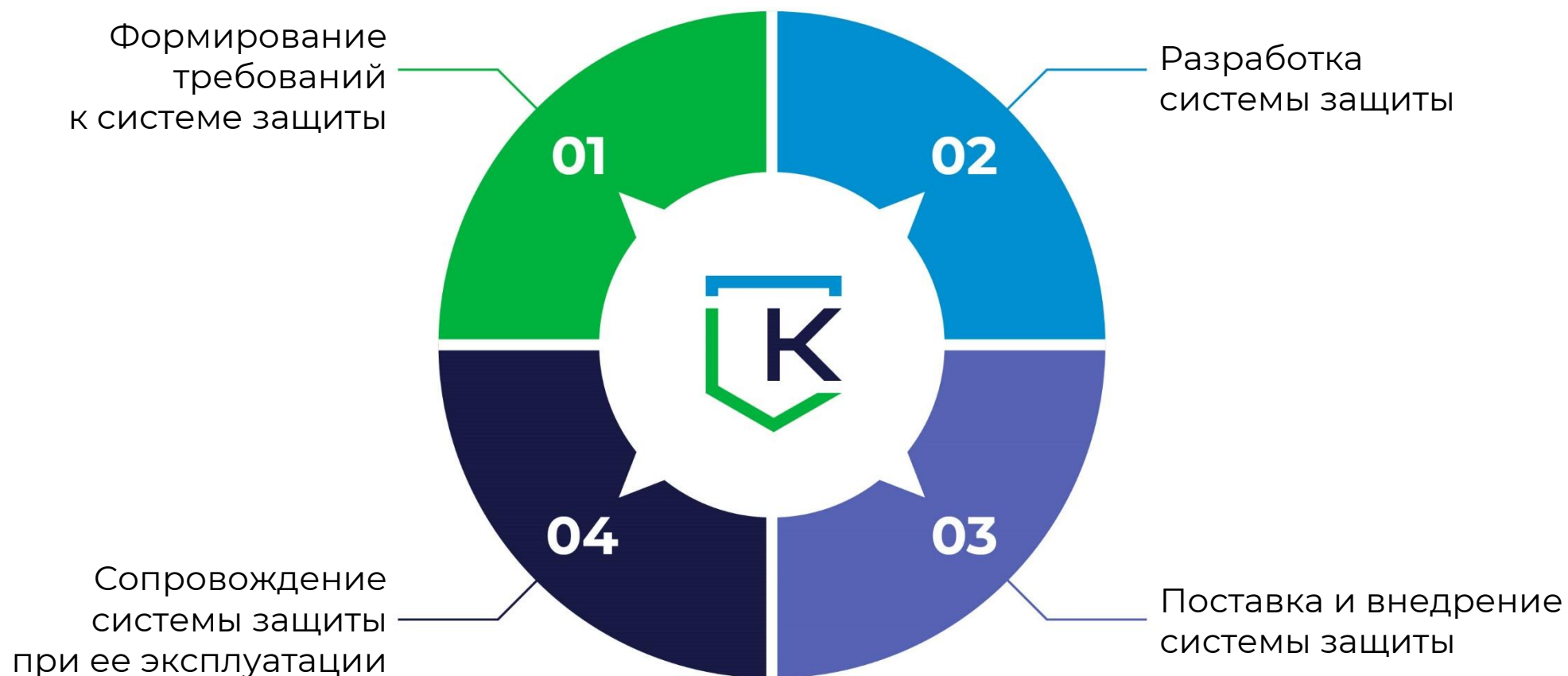
реализованных
проектов

НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ



ЭТАПЫ СОЗДАНИЯ СИСТЕМ ИБ АСУ ТП

4



ПОРТФОЛИО В ЧАСТИ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ 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

ВЗГЛЯД СО СТОРОНЫ ИНТЕГРАТОРА – ПРОБЛЕМЫ

6



**ИБ
по «остаточному
принципу»**



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



**Отсутствие методик
определения сметной
стоимости ИБ**

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ – ЛИЦЕНЗИРУЕМЫЙ ВИД ДЕЯТЕЛЬНОСТИ

7

Согласно требованиям Постановления Правительства РФ **от 3 февраля 2012 г. № 79**
«О лицензировании деятельности по технической защите конфиденциальной информации»:

«4. При осуществлении лицензируемого вида деятельности лицензированию подлежат:
....

д) **работы и услуги по проектированию в защищенном исполнении:**

- средств и систем информатизации;
- помещений со средствами (системами) информатизации, подлежащими защите;
- защищаемых помещений;

.....»



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



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

Типичный пример ТЗ:

Требования к обеспечению информационной безопасности	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.
--	---

НТД в сфере ИБ актуализируются быстрее, чем формируются ТЗ.

Актуализация НТД – задача разработчика системы ИБ.

Актуализация исходных данных – задача всех участников процесса.



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»

13



"У семи нянек дитя без глазу"

ДОРОЖНАЯ КАРТА – ЗАЛОГ УСПЕХА

- 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

Указ Президента Российской Федерации
от 30.03.2022 № 166

«О мерах по обеспечению технологической
независимости и безопасности критической
информационной инфраструктуры Российской
Федерации»

а) с 31 марта 2022 г. запрещено закупать иностранное
ПО в целях его использования на значимых ОКИИ РФ

б) с 1 января 2025 г. запрещается использовать
иностранное ПО на значимых ОКИИ



Постановление Правительства Российской Федерации
от 14.11.2023 № 1912

«О порядке перехода субъектов критической
информационной инфраструктуры Российской
Федерации на преимущественное применение
доверенных программно-аппаратных комплексов
на принадлежащих им значимых объектах
критической информационной инфраструктуры
Российской Федерации»

- переход субъектов КИИ РФ на преимущественное
применение доверенных программно-аппаратных
комплексов (ПАК) на значимых ОКИИ осуществляется
до 1 января 2030 г.;
- с 1 сентября 2024 г. не допускается использование
субъектами КИИ РФ на значимых ОКИИ ПАК,
приобретенных с 1 сентября 2024 г. и не являющихся
доверенными ПАК (за исключением подтвержденного
заключением Министерства промышленности
отсутствия аналогов доверенных ПАК)



Постановление Правительства Российской Федерации от 14.11.2023 № 1912:

- Непосредственно касается вопросов ИБ
- Большое количество новых «оптовых» проектов
- Дорожная карта – требование на уровне законодательства
- Пересмотр подходов к объектам КИИ

ВЗГЛЯД СО СТОРОНЫ ИНТЕГРАТОРА - РЕШЕНИЕ

19



Создание и актуализация в реальном времени дорожной карты СОИБ



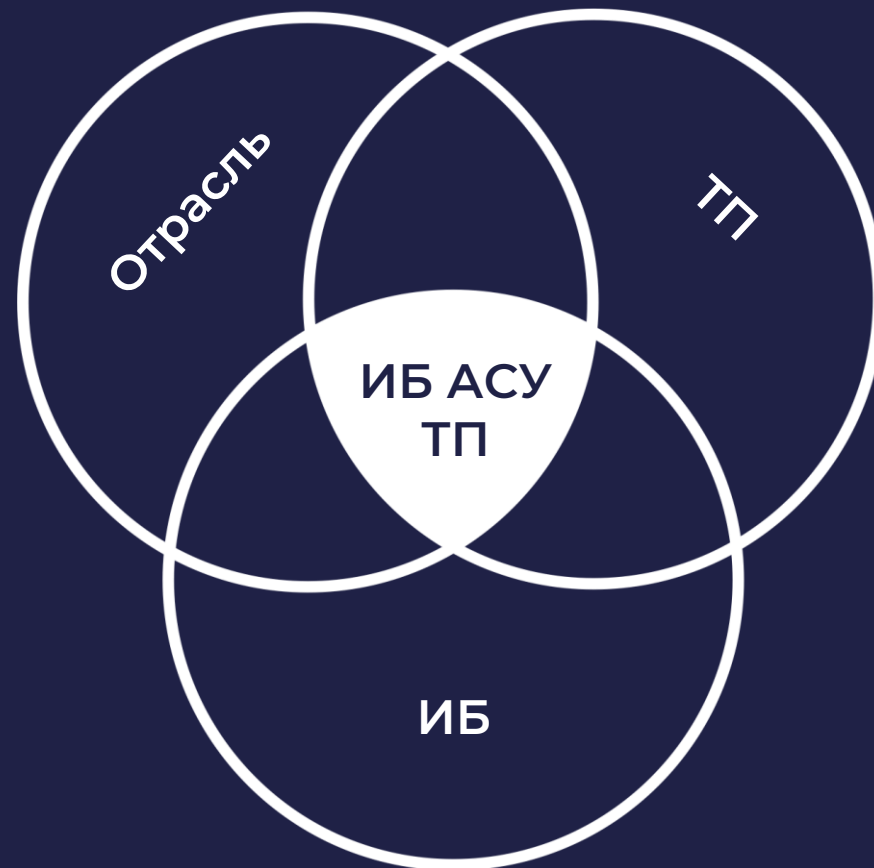
Наличие ответственного и уполномоченного лица Заказчика



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.

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