USSC

серия вебинаров

«SecOps от УЦСБ»

Подключение к ГосСОПКА:

решать задачу самостоятельно или выбрать услуги коммерческого центра?

Николай Домуховский

Заместитель генерального директора ООО «УЦСБ»

Екатеринбург, 2021

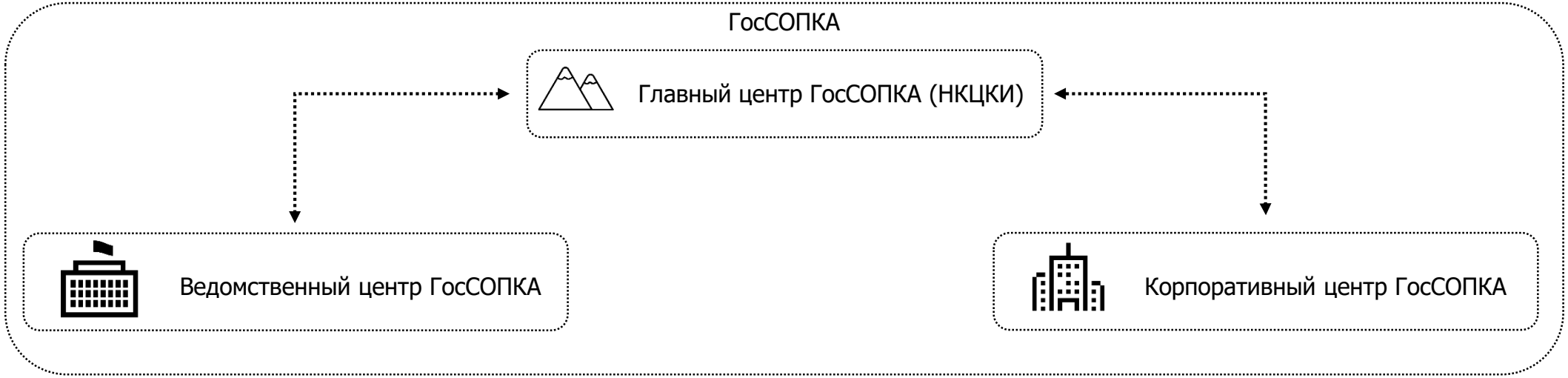
Новая серия вебинаров

1. Выбор между своим и коммерческим центром ГосСОПКА
2. Зачем нужен SOC для АСУ ТП
3. Выявляем инциденты в корпоративных сетях
4. Как оценить работу SOC
5. SOC и его команда
6. Автоматизация SecOps: IRP/SOAR
7. Threat Hunting и Threat Intelligence
8. Red Team, pentest и причем тут SOC
9. Самый SOC: примеры реальных кейсов

И много полезной информации в ранее проведенных вебинарах:
https://www.ussc.ru/events/zapisi-vebinarov/

ГосСОПКА – история создания

Структура ГосСОПКА



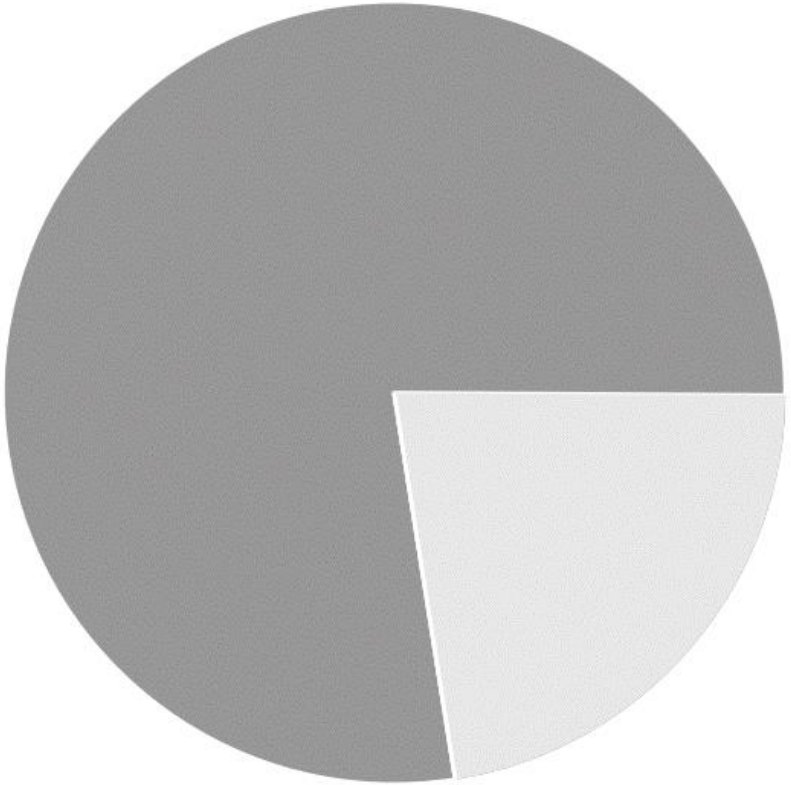
- Информация о признаках компьютерных инцидентов
- Индикаторы вредоносной активности (IOC)
- Сведения об угрозах безопасности информации
- Методические рекомендации по противодействию угрозам

- Информация о реагировании на компьютерные инциденты
- Информация о выявленных компьютерных атаках
- Информация о результатах ликвидации последствий КИ

Информационные ресурсы РФ – это не только КИИ

USSC

Участники ГосСОПКА



1853 субъекта ГосСОПКА

535 субъектов КИИ

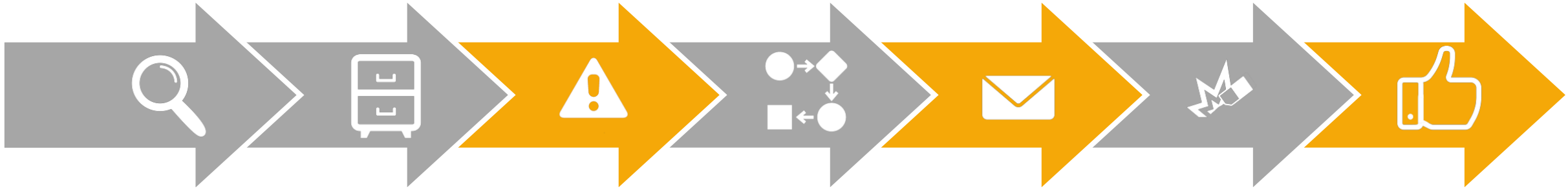
«ГосСОПКА. Для кого же?», Сергей Корелов, НКЦКИ, SOC Forum, 2019 г.

Организация прямого взаимодействия с ГосСОПКА

- **Передача сведений о выявленных атаках**
- **Передача сведений о результатах реагирования**
- **Передача сведений о ликвидации последствий КИ**

Организация прямого взаимодействия с ГосСОПКА

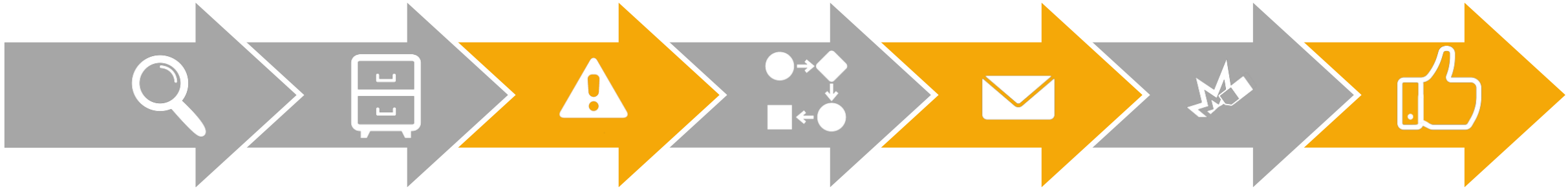
- Сбор и анализ событий
- Управление активами
- **Передача сведений о выявленных атаках**
- реагирование на инциденты
- **Передача сведений о результатах реагирования**
- Восстановление ресурсов после КИ
- **Передача сведений о ликвидации последствий КИ**



Организация прямого взаимодействия с ГосСОПКА

- Сбор и анализ событий
- Управление активами
- **Передача сведений о выявленных атаках**
- реагирование на инциденты

- **Передача сведений о результатах реагирования**
- Восстановление ресурсов после КИ
- **Передача сведений о ликвидации последствий КИ**

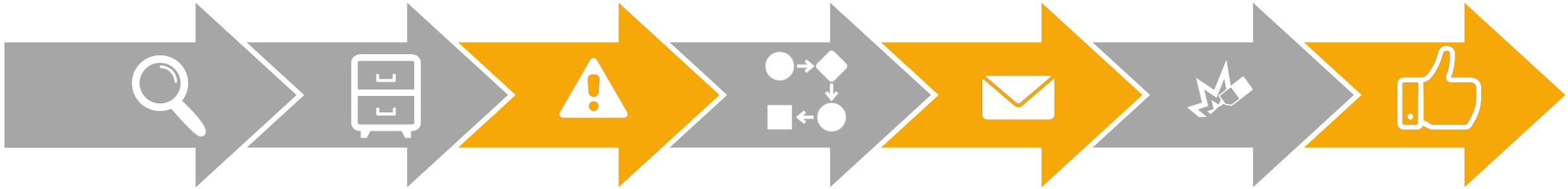


Группа реагирования на КИ

Группа ликвидации последствий КИ

Организация прямого взаимодействия с ГосСОПКА

- Сбор и анализ событий
- Управление активами
- **Передача сведений о выявленных атаках**
- реагирование на инциденты
- **Передача сведений о результатах реагирования**
- Восстановление ресурсов после КИ
- **Передача сведений о ликвидации последствий КИ**



Группа реагирования на КИ

Группа ликвидации последствий КИ

Средства обнаружения

Средства предупреждения

Средства ликвидации последствий

Средства поиска признаков КА

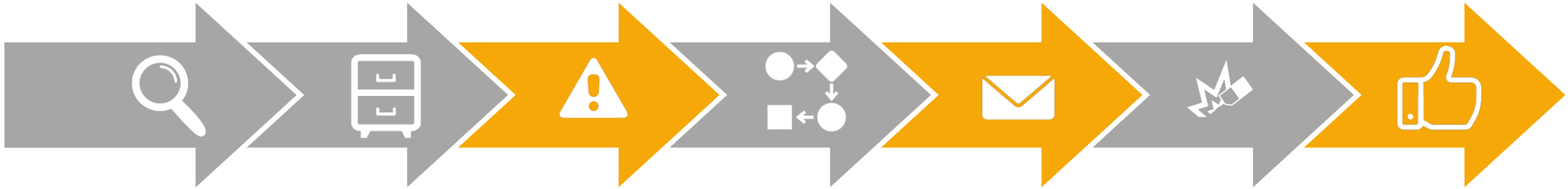
СКЗИ

Средства обмена

Организация прямого взаимодействия с ГосСОПКА

- Сбор и анализ событий
- Управление активами
- **Передача сведений о выявленных атаках**
- реагирование на инциденты

- **Передача сведений о результатах реагирования**
- Восстановление ресурсов после КИ
- **Передача сведений о ликвидации последствий КИ**



Группа реагирования на КИ

Группа ликвидации последствий КИ

Средства обнаружения

Средства предупреждения

Средства ликвидации последствий

Средства поиска признаков КА

СКЗИ

Средства обмена

Группа эксплуатации средств ГосСОПКА

Самостоятельное внедрение средств взаимодействия с ГосСОПКА

- Приказ ФСБ России №196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»
- Приказ ФСБ России № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»

- Выбор средств ГосСОПКА
- Разработка структурно-функциональной схемы
- Назначение лиц, ответственных за эксплуатацию

- Установка, настройка , проверка работоспособности
- Подключение средств к информационным ресурсам
- Информирование НКЦКИ

- Обеспечение круглосуточной бесперебойной работы средств ГосСОПКА

Технические средства ГосСОПКА - требования

Средства обнаружения	• Сбор событий с источников • автоматический анализ • повторный анализ собранных событий • хранение событий не менее 6 месяцев
Средства поиска признаков КА	• Выявление признаков КА в трафике • обнаружение признаков управления АСО • обнаружение изменений параметров • хранение копий трафика не менее 6 месяцев • анализ и экспорт трафика
Средства предупреждения	• Инвентаризация инфраструктуры • анализ уязвимостей • учет угроз ИБ • формирование рекомендаций по минимизации угроз ИБ
СКЗИ	• Криптографическая защита при обмене • Должны быть сертифицированы
Средства ликвидации последствий	• Учет инцидентов • управление процессом реагирования • взаимодействие с НКЦКИ посредством технической инфраструктуры
Средства обмена	• Передача и прием информации с контролем целостности

Центры ГосСОПКА - альтернативный метод взаимодействия

USSC

Класс В

- Обмен с НКЦКИ
- Эксплуатация средств ГосСОПКА
- Регистрация атак и инцидентов
- Инвентаризация информационных ресурсов
- Сбор и автоматический анализ событий

Класс Б

- Анализ угроз ИБ
- Повышение уровня защищенности
- Поиск уязвимостей
- Ведение перечня инцидентов
- Поиск причин инцидентов
- Ведение перечня угроз ИБ

Класс А

- Ликвидация последствий компьютерных инцидентов
- анализ результатов

Надо ли создавать свой центр?

Потенциально много центров

40 Центров ГосСОПКА в процессе создания (конец 2018)

72 Организации запросили методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА (конец 2018)

189 Организаций, обладающих лицензией ФСТЭК России с видом деятельности «услуги по мониторингу информационной безопасности средств и систем информатизации» (2021-й год)

Но, что конкретно они могут предложить?

Отсутствует централизованный реестр центров ГосСОПКА с указанием класса

Отсутствует механизм контроля качества работы центров ГосСОПКА

Как не ошибиться при выборе центра ГосСОПКА?

- Запросить структурно-функциональную схему средств ГосСОПКА
- Запросить политики и регламенты выполнения структурными элементами центра ГосСОПКА своих функций
- Оценить опыт центра по обеспечению ИБ схожих объектов
- Провести аудит второй стороны
- Иметь запасной вариант и сменить поставщика услуги, при необходимости

Собственное подключение или услуги центра?

USSC

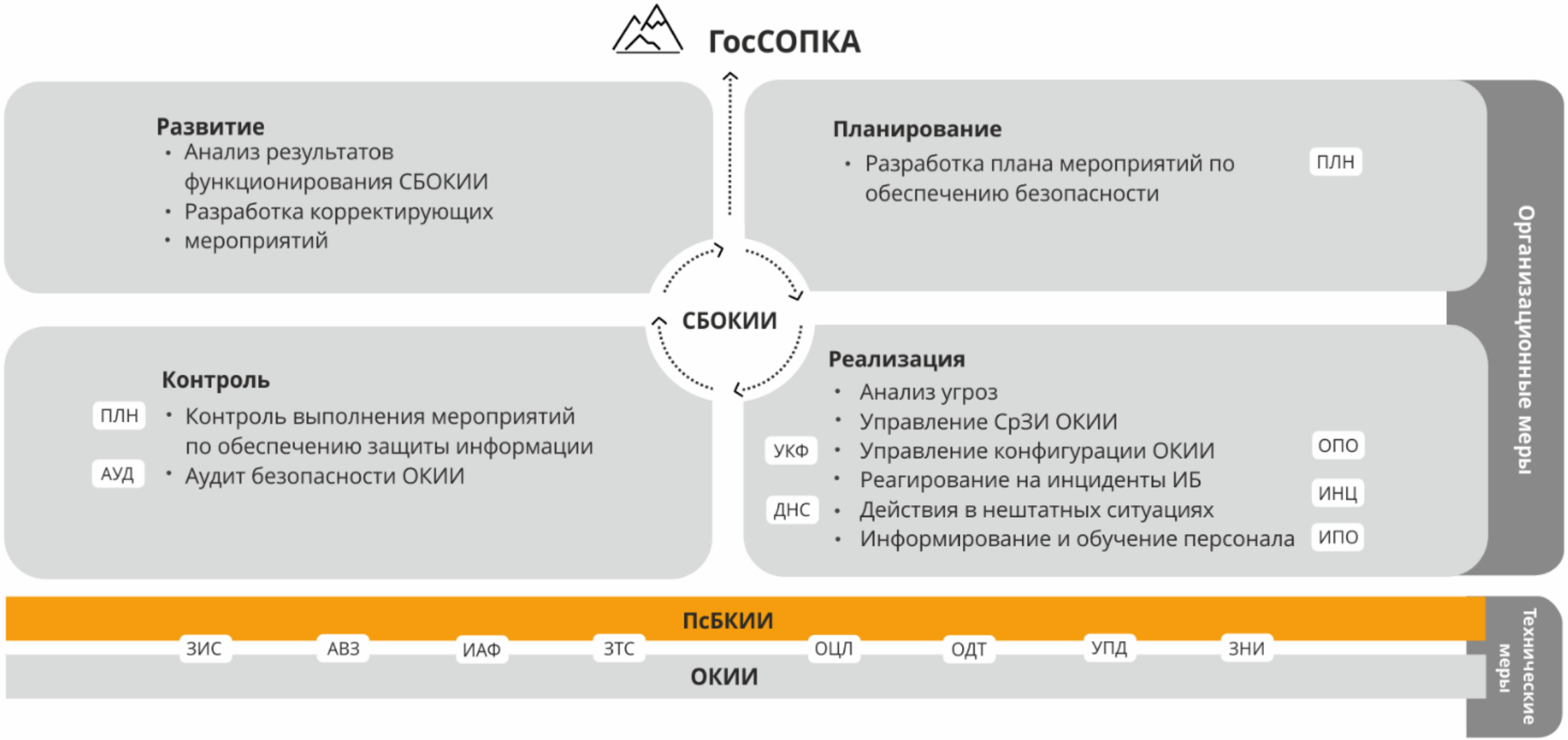
Услуги центра

- \+ Быстрый запуск
- \+ Нет необходимости подбора сотрудников в штат
- \+ Есть необходимые лицензии, выстроено взаимодействие с НКЦКИ
- \+ «Перенос» опыта с других объектов, подключенных к SOC
- — Операционные затраты
- — Нет накопления собственной компетенции

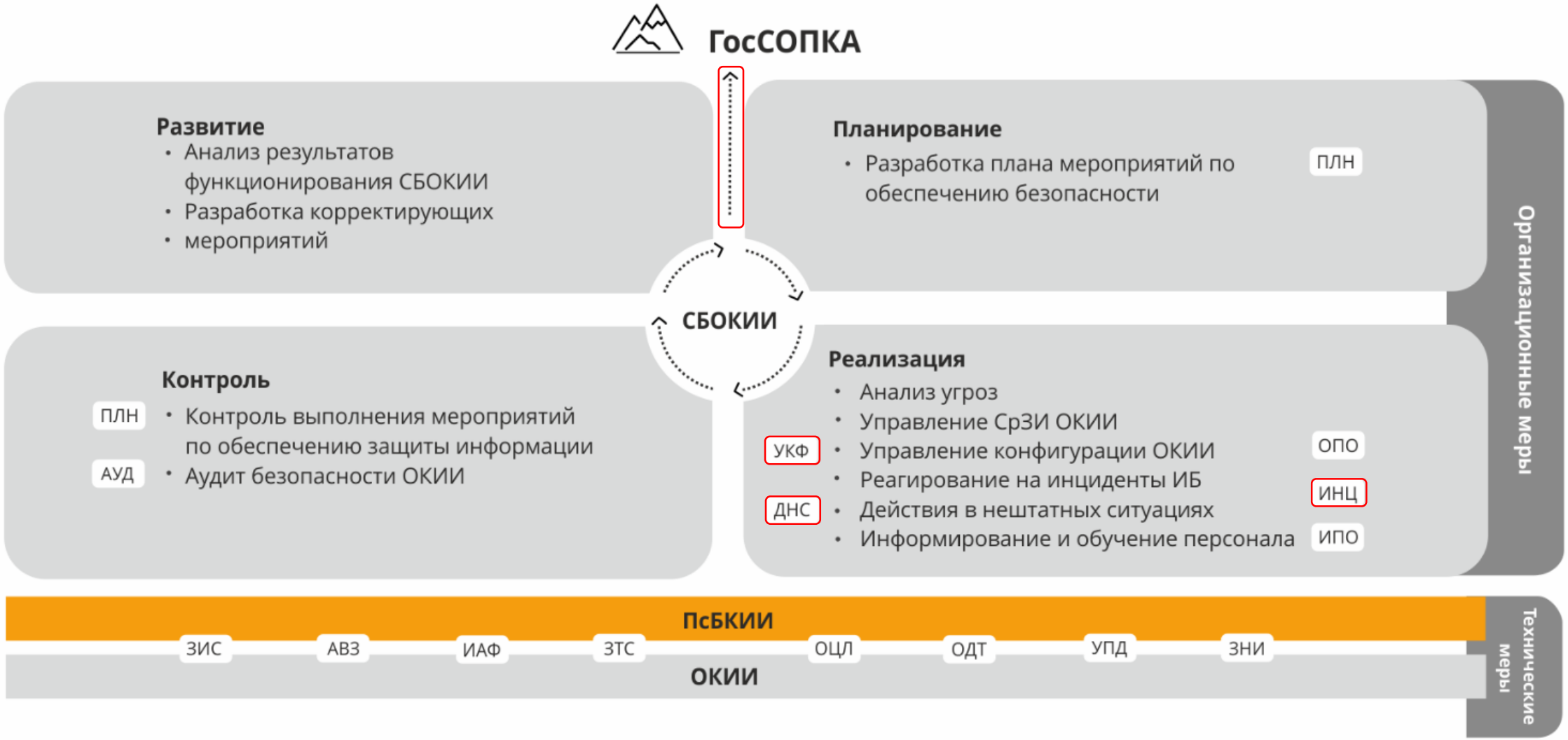
Собственное подключение

- \+ Минимизация операционных затрат
- \+ Развитие собственной экспертизы ИБ
- \+ Гибкая адаптация под требования бизнеса
- — Подключение к ГосСОПКА – длительный процесс
- — Сложно найти квалифицированные кадры
- — Высокие капитальные затраты
- — Необходимо получать лицензии ФСТЭК (в некоторых случаях)

ГосСОПКА – не серебряная пуля!



ГосСОПКА – не серебряная пуля!



USSC

СПАСИБО ЗА ВНИМАНИЕ

ВОПРОСЫ?

Николай Домуховский

Заместитель генерального директора
ООО «УЦСБ»

ndomukhovsky@ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU