

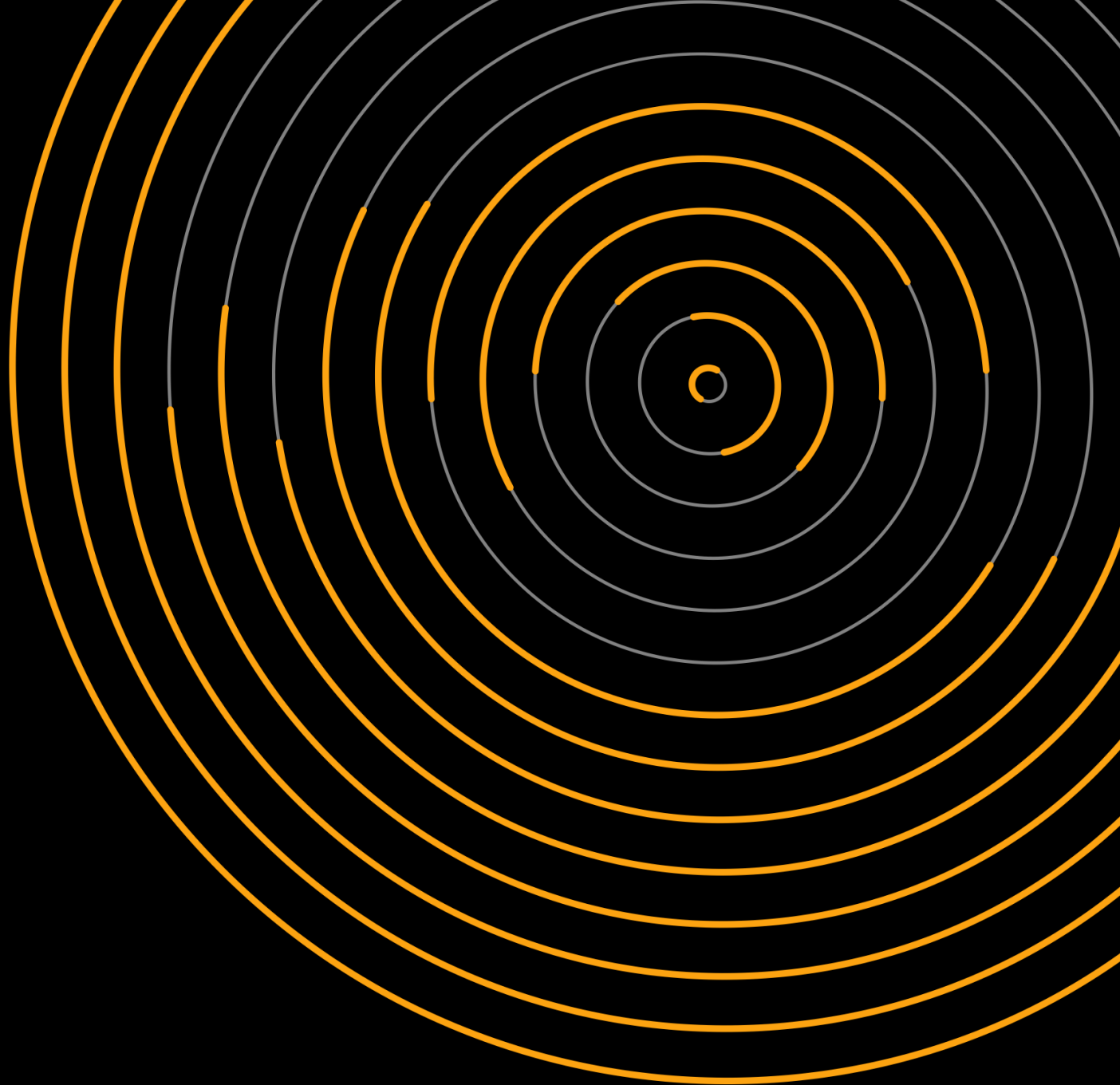


Уменьшаем влияние человеческого фактора в процессах выявления и противодействия угрозам безопасности АСУ ТП

Руслан Амиров

Директор USSC-SOC

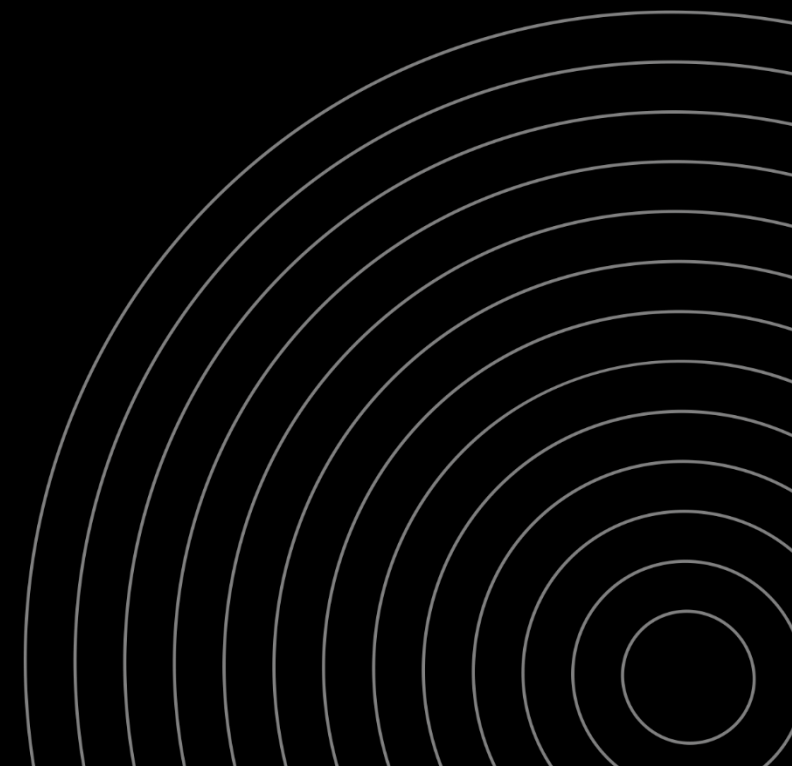
Конференция ИБ АСУ ТП КВО
Москва, 2022 г.



ПЛАН ДОКЛАДА



- Как выявляются угрозы ИБ в АСУ ТП
- Как противодействуют угрозам ИБ в АСУ ТП
- Опасения администраторов АСУ ТП
- Опасения специалистов по ИБ АСУ ТП
- Снижаем влияние человеческого фактора



КАК ВЫЯВЛЯЮТСЯ УГРОЗЫ ИБ в АСУ ТП



1

Модель угроз:

- при создании АСУ ТП
- при создании системы ИБ для существующей АСУ ТП

2

Пересмотр модели угроз:

- на регулярной основе
- при возникновении внешних и внутренних факторов
- при проведении работ по обслуживанию и сопровождению АСУ ТП

Работы по обслуживанию АСУ ТП проводятся регулярно.
Это же касается и вопросов ИБ

КАК ВЫЯВЛЯЮТСЯ УГРОЗЫ ИБ В АСУ ТП



Когда выявлять:

СЕРВИСНОЕ
ОБСЛУЖИВАНИЕ
В ЧАСТИ ИБ

ТО В ЧАСТИ ИБ

ПОСТОЯННО

Как выявлять:

постоянный мониторинг ИБ
или периодический сбор и
анализ лог-файлов

ручной и инструментальный
анализ защищенности

проверка изменений по
сравнению с результатами
предыдущих работ

СПОСОБЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИБ



ПОСТОЯННЫЕ

- встроенные механизмы защиты
- наложенные СрЗИ
- дополнительные СрЗИ
- организационные мероприятия

ПЕРИОДИЧЕСКИЕ

- поддержка постоянных способов противодействия
- устранение уязвимостей ОС, ПО и конфигураций в рамках сервисного обслуживания/ТО в части ИБ
- повышение эффективности системы безопасности АСУ ТП на основании анализа результатов предыдущих работ

ОПАСЕНИЯ

АДМИНИСТРАТОРОВ АСУ ТП



Отсутствие доверия к качеству аутсорсинговых работ по ИБ

Работы по ИБ могут мешать выполнению основных работ по обслуживанию системы

Аутсорсер выявит ошибки обслуживающего АСУ ТП персонала

Ошибки при проведении обновлений приведут к необходимости восстановления ОС из резервной копии

ОПАСЕНИЯ

АДМИНИСТРАТОРОВ АСУ ТП



Аутсорсеру требуются реквизиты доступа или информация о конфигурации оборудования

Работоспособность АСУ ТП может быть нарушена при проведении инструментального анализа защищенности

По вине аутсорсера может возникнуть инцидент ИБ

Могут быть допущены критические ошибки в ходе работ по реагированию на инцидент ИБ

ОПАСЕНИЯ СПЕЦИАЛИСТОВ ИБ АСУ ТП



- Запланированные работы не будут выполнены в полном объеме

- Резервное копирование не будет проведено перед началом работ

- Не все уязвимости будут выявлены

- Лог-файлы не будут собраны в достаточном объеме для обнаружения следов инцидентов ИБ

ОПАСЕНИЯ СПЕЦИАЛИСТОВ ИБ АСУ ТП



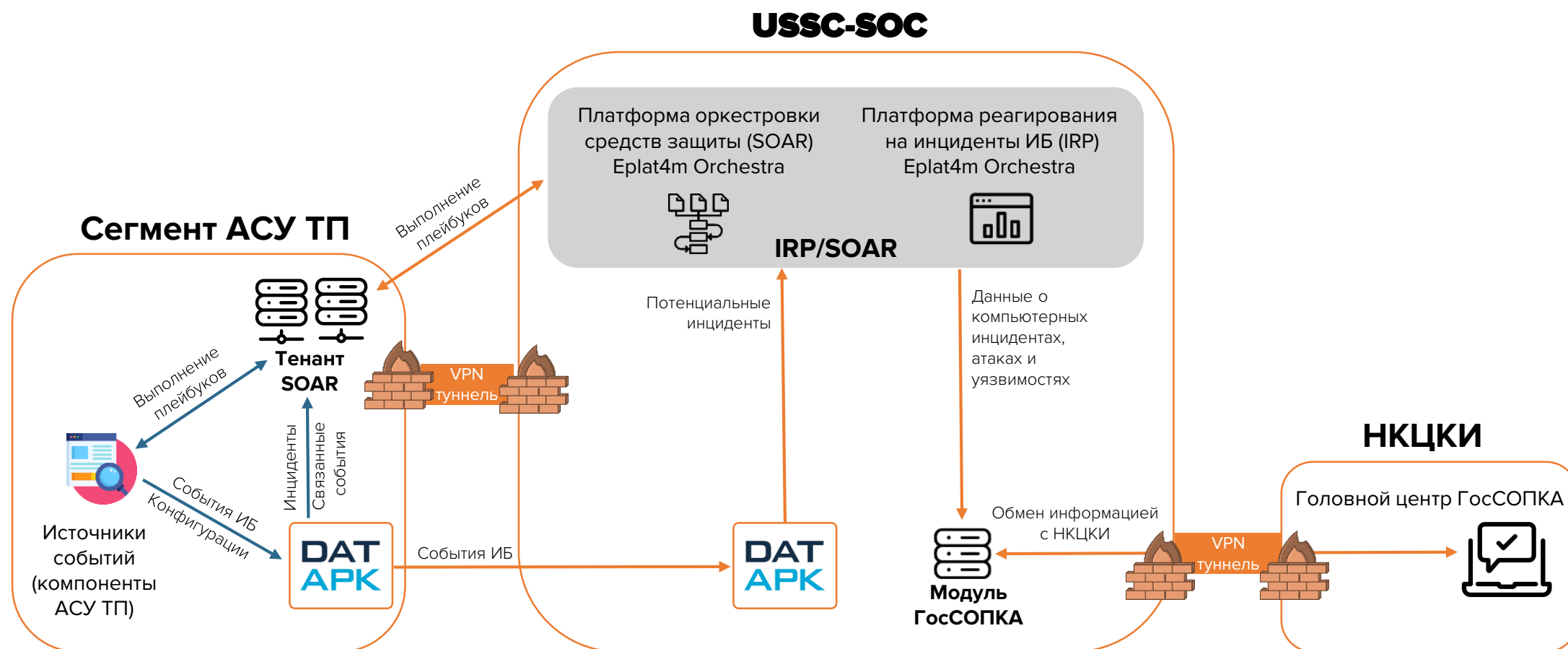
- Аутсорсер не будет соблюдать требования ОРД по ИБ АСУ ТП

- Аутсорсер передаст не всю информацию по выявленным ошибкам и уязвимостям

- Аутсорсер может вынести за пределы КЗ чувствительную информацию в части ИБ

- Проводимые мероприятия по ИБ не будут согласованы с разработчиком АСУ ТП

СНИЖАЕМ ВЛИЯНИЕ ЧЕЛОВЕЧЕСКОГО ФАКТОРА СРЕДСТВАМИ SOAR



СПАСИБО ЗА ВНИМАНИЕ! ВОПРОСЫ?



Руслан Амиров

Директор USSC-SOC

ramirov@ussc.ru

soc.ussc.ru

