КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11 ОКТЯБРЯ 2017
САМАРА

#CODEIB

ОРГАНИЗАЦИЯ ЦЕНТРА КРУГЛОСУТОЧНОГО МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

на примере Отдела мониторинга событий ИБ
Акционерное общество «Системный оператор Единой энергетической системы»

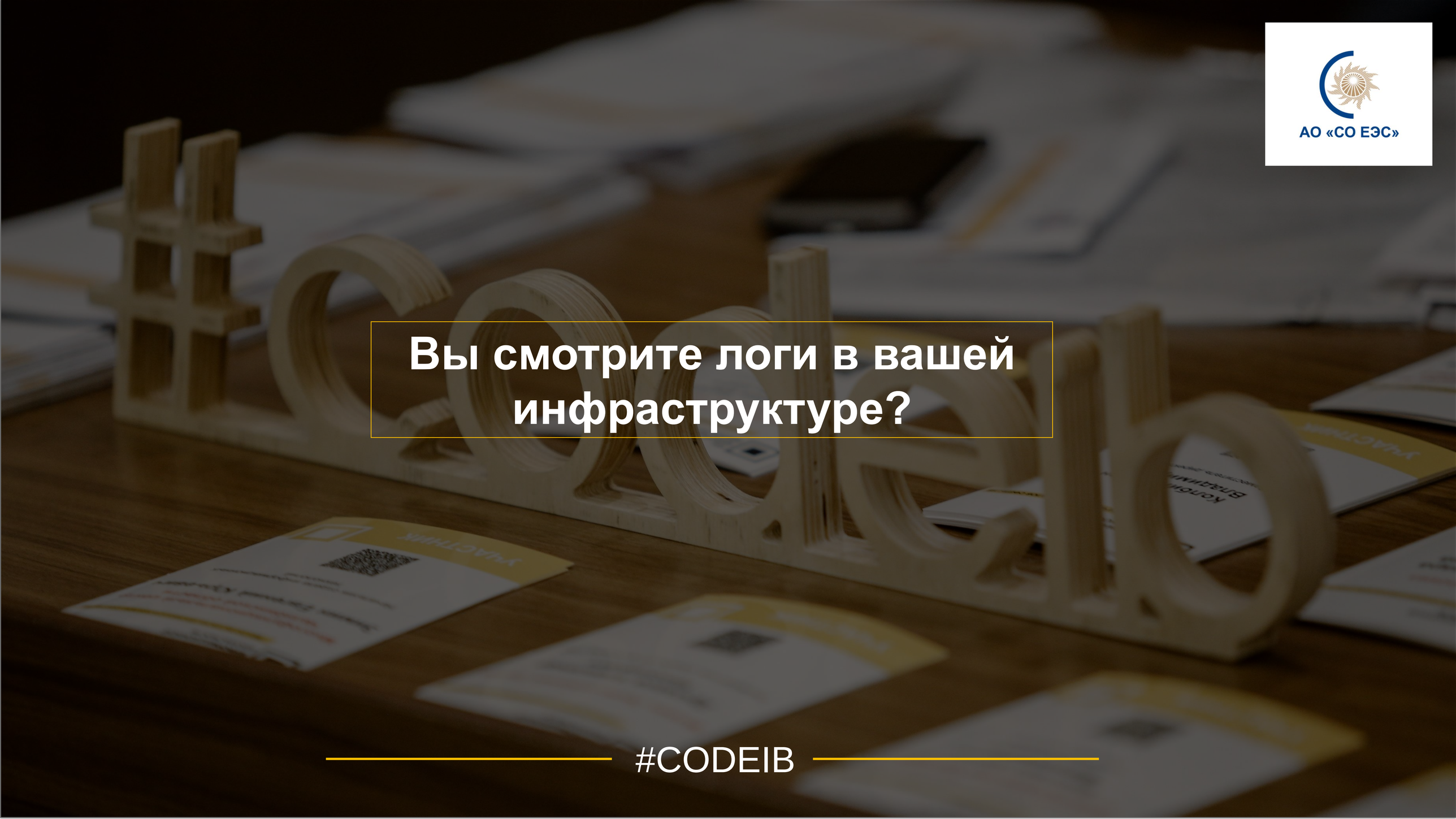
Андрей Степанов

Начальник Отдела мониторинга событий ИБ
АО «СО «ЕЭС»

ТЕЛЕФОН: +7 (909) 343-11-25

EMAIL: StepanovAV@odusv.ru

АО «СО ЕЭС»


АО «СО ЕЭС»
Вы смотрите логи в вашей инфраструктуре?
#CODEIB

АО «СО ЕЭС»

Анализируете причины зависаний/сбоев сетевого оборудования и систем?

#CODEIB

АО «СО ЕЭС»

Ландшафт атак в 2017-2018г.г.

Вредоносный код

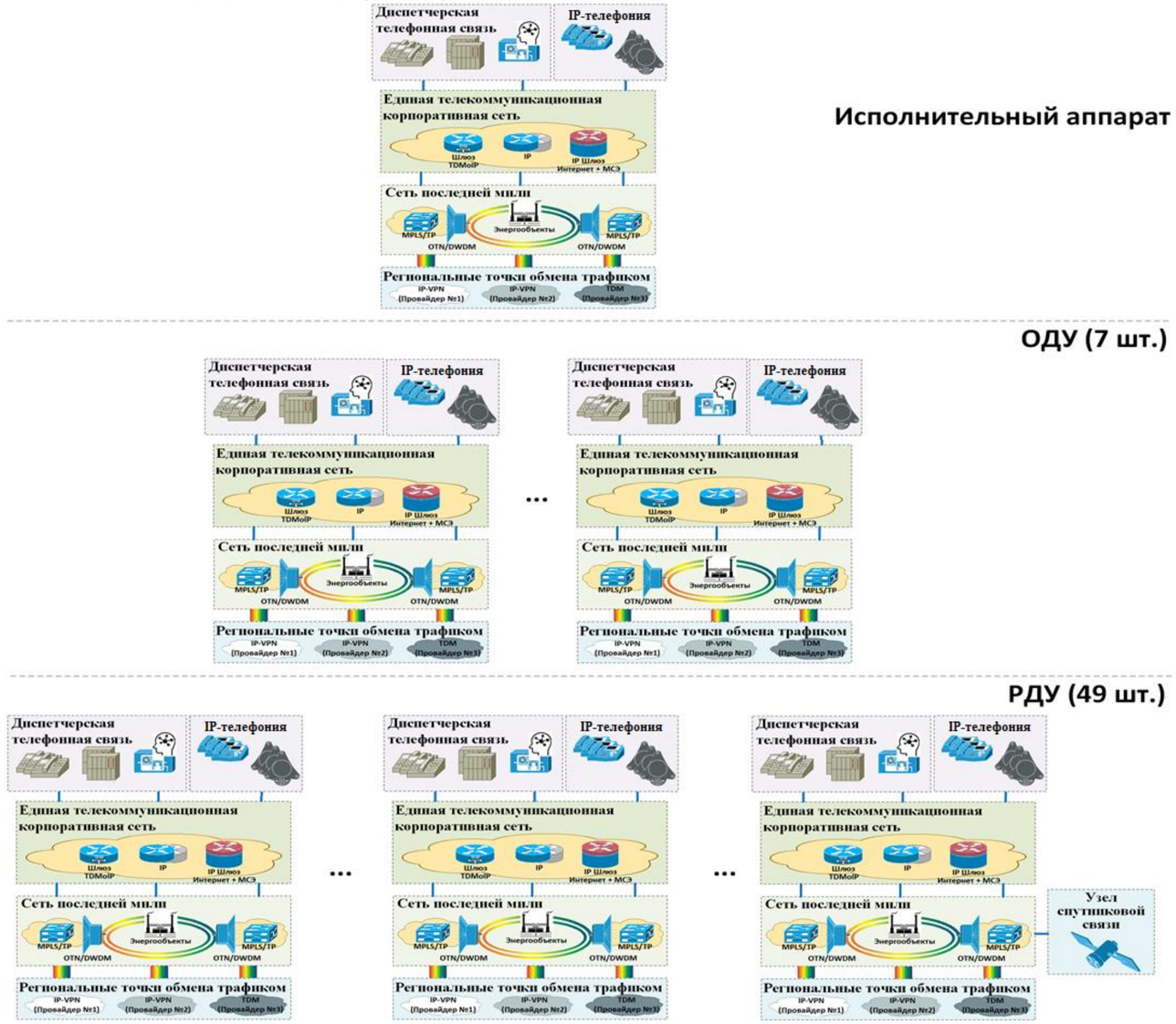
Фишинг

IoT и DDoS-атаки

Сетевые атаки

#CODEIB

Инфраструктура АО «СО «ЕЭС»

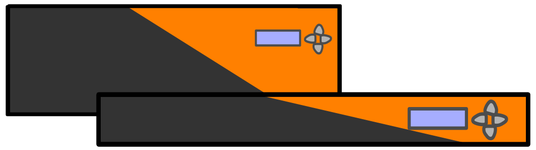


#CODEIB

Система оперативного контроля информационной безопасности АО «СО «ЕЭС»

Источники событий

Работники обрабатывающие события в СОКИБ



СОКИБ

СОКИБ является составной частью системы обеспечения информационной безопасности в АО «СО ЕЭС» и предназначена для централизованного сбора и анализа событий ИБ, регистрируемых средствами защиты информации, а также оперативного обнаружения и реагирования на события и инциденты ИБ.

АО «СО ЕЭС»

Причины организации Центра мониторинга событий ИБ

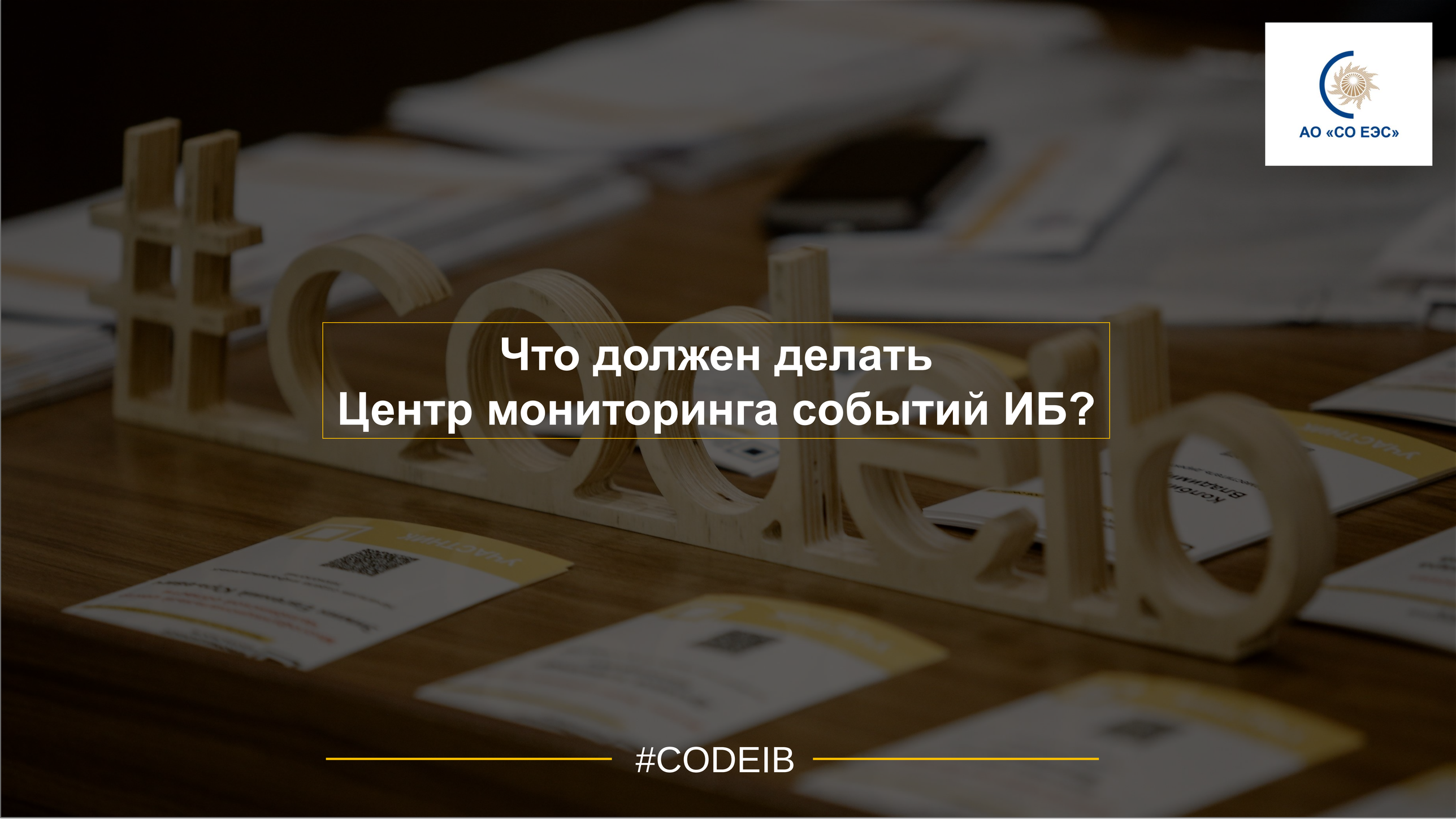
1 БОЛЕЕ 15.000 ХОСТОВ

2 ТЕРРИТОРИАЛЬНО-РАЗНЕСЕННАЯ ИНФРАСТРУКТУРА

3 ~15 ТЫС. СОБЫТИЙ В СЕКУНДУ

4 В КАЖДОМ РЕГИОНЕ СВОЙ ОТВЕТСТВЕННЫЙ ЗА ИНФРАСТРУКТУРУ

5 РАСПРЕДЕЛЕННЫЕ АТАКИ ОСТАЮТСЯ НЕЗАМЕЧЕННЫМИ



АО «СО ЕЭС»

Что должен делать Центр мониторинга событий ИБ?

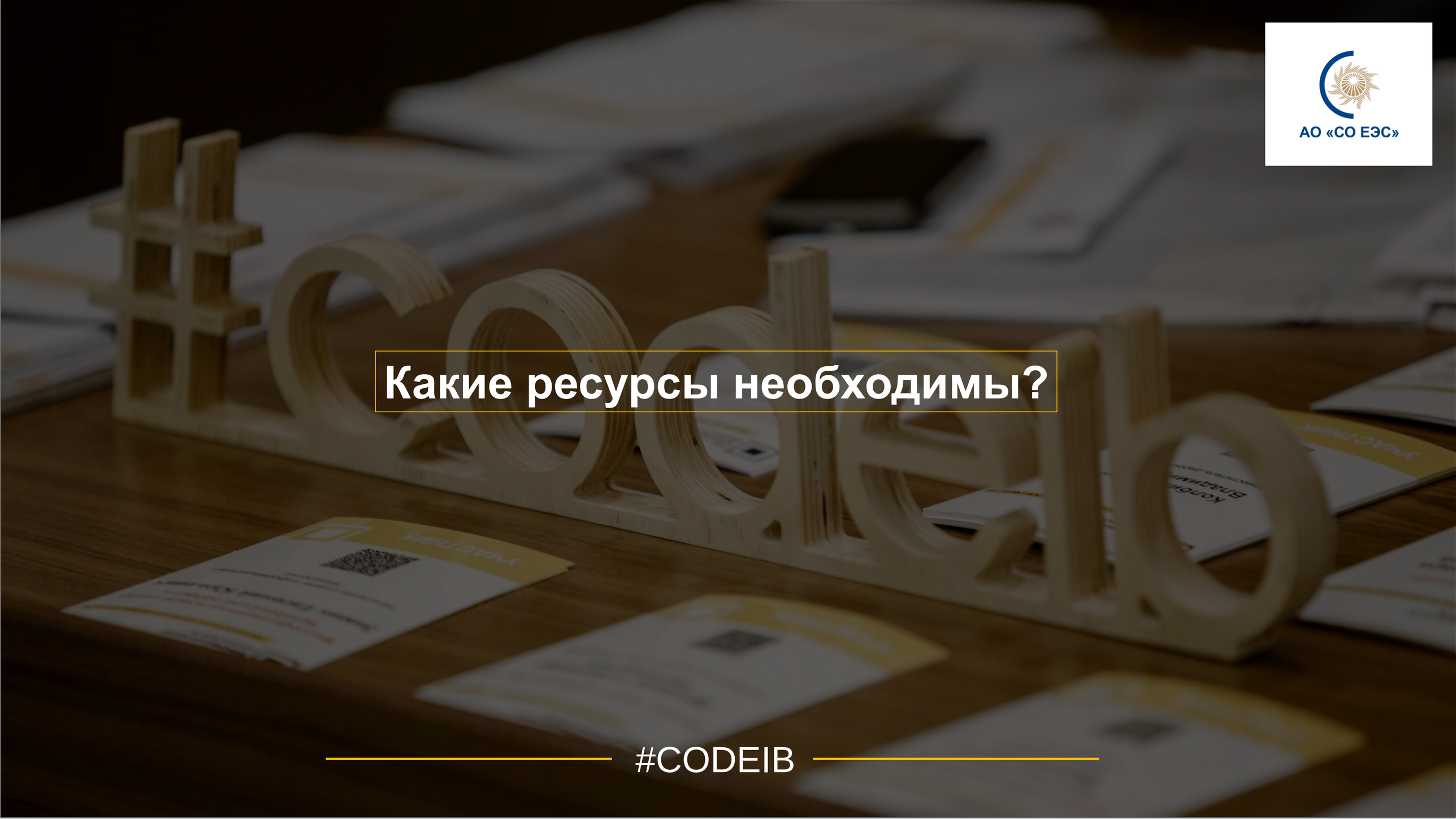
#CODEIB

Центр мониторинга событий ИБ

АО «СО ЕЭС»

- ✓ **Централизованный мониторинг в режиме 24x7x365**
- ✓ **Высокий уровень экспертизы**
- ✓ **Выстроенные процессы**
- ✓ **Продвинутая аналитика, включающая Threat Intelligence и Threat Hunting**
- ✓ **Изучение каждого события безопасности**
- ✓ **Регистрация инцидентов**
- ✓ **Алгоритмы реагирования на типовые инциденты**

#CODEIB



АО «СО ЕЭС»

Какие ресурсы необходимы?

#CODEIB

Какие ресурсы необходимы и на что?

АО «СО ЕЭС»

- ✓ **Распределенная система сбора и корреляции событий (SIEM). 57 ресиверов по всей территории РФ.**
- ✓ **Подключенные источники событий. Участие системных администраторов**
- ✓ **Настроенные правила корреляции и оповещений**
- ✓ **Разработанные процессы мониторинга событий, реагирования и совершенствования правил корреляции**
- ✓ **Справочная система с информацией об элементах инфраструктуры**
- ✓ **Специалисты. Минимум 1 дежурный в смену (5 человек)**
- ✓ **Обучение работников**

АО «СО ЕЭС»

Какие процессы пришлось организовывать?

#CODEIB

Какие процессы пришлось организовывать?

АО «СО ЕЭС»

- ✓ **Операции выполняемые дежурными в смену**
- ✓ **Регистрация и обработка инцидентов**
- ✓ **Ручной мониторинг событий ИБ**
- ✓ **Анализ публикаций о новых уязвимостях и проверка их актуальности для инфраструктуры**
- ✓ **Создание новых и актуализация действующих правил корреляции**
- ✓ **Ретроспективный анализ события для новых актуальных угроз**
- ✓ **Проверка отчетов об ИТ нарушениях и событий ECM на наличие связанных событий ИБ**
- ✓ **Реагирование на типовые инциденты**
- ✓ **Ежеквартальное общение с администраторами в регионах через WebEX (нововведения, обучение, разбор инцидентов)**

АО «СО ЕЭС»

Формализация деятельности Центра мониторинга событий ИБ?

#CODEIB

Формализация деятельности Центра мониторинга событий ИБ

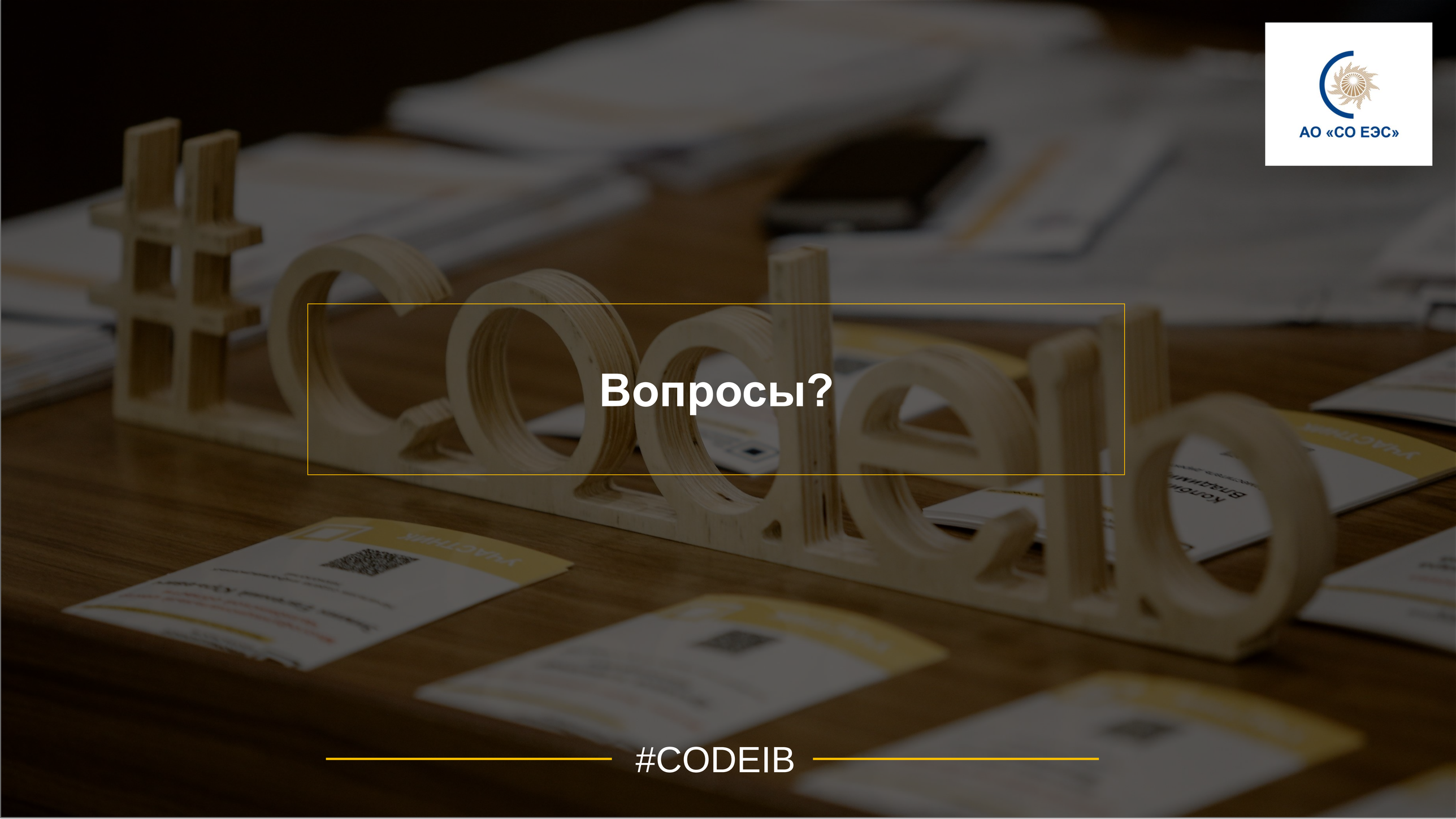
АО «СО ЕЭС»

- **Разработка и утверждение общих требований и правил мониторинга событий ИБ**
  Регламент эксплуатации ПАК «СОКИБ»
- **Разработка и утверждение Перечня источников событий ИБ**
  Перечень источников ПАК «СОКИБ»
- **Разработка и утверждение справочника по эксплуатации SIEM**
  Руководство по эксплуатации ПАК «СОКИБ»
- **Разработка инструкций для персонала**
  Инструкция Администратора ПАК «СОКИБ»
  Инструкция Оператора ПАК «СОКИБ»
- **Разработка алгоритмов реагирования на типовые инциденты ИБ**
  более 11 шт. инструкций
- **Разработка инструкций для системных администраторов по подключению источников событий ИБ**
  более 30 шт. инструкций

Пример. Инструкция Оператора ПАК «СОКИБ»

АО «СО ЕЭС»

Оглавление



АО «СО ЕЭС»

Вопросы?

#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11 ОКТЯБРЯ 2018
САМАРА

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ!

Андрей Степанов

Начальник Отдела мониторинга событий ИБ
АО «СО «ЕЭС»

ТЕЛЕФОН: +7 (909) 343-11-25

EMAIL: StepanovAV@odusv.ru

АО «СО ЕЭС»