kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Лев Палей

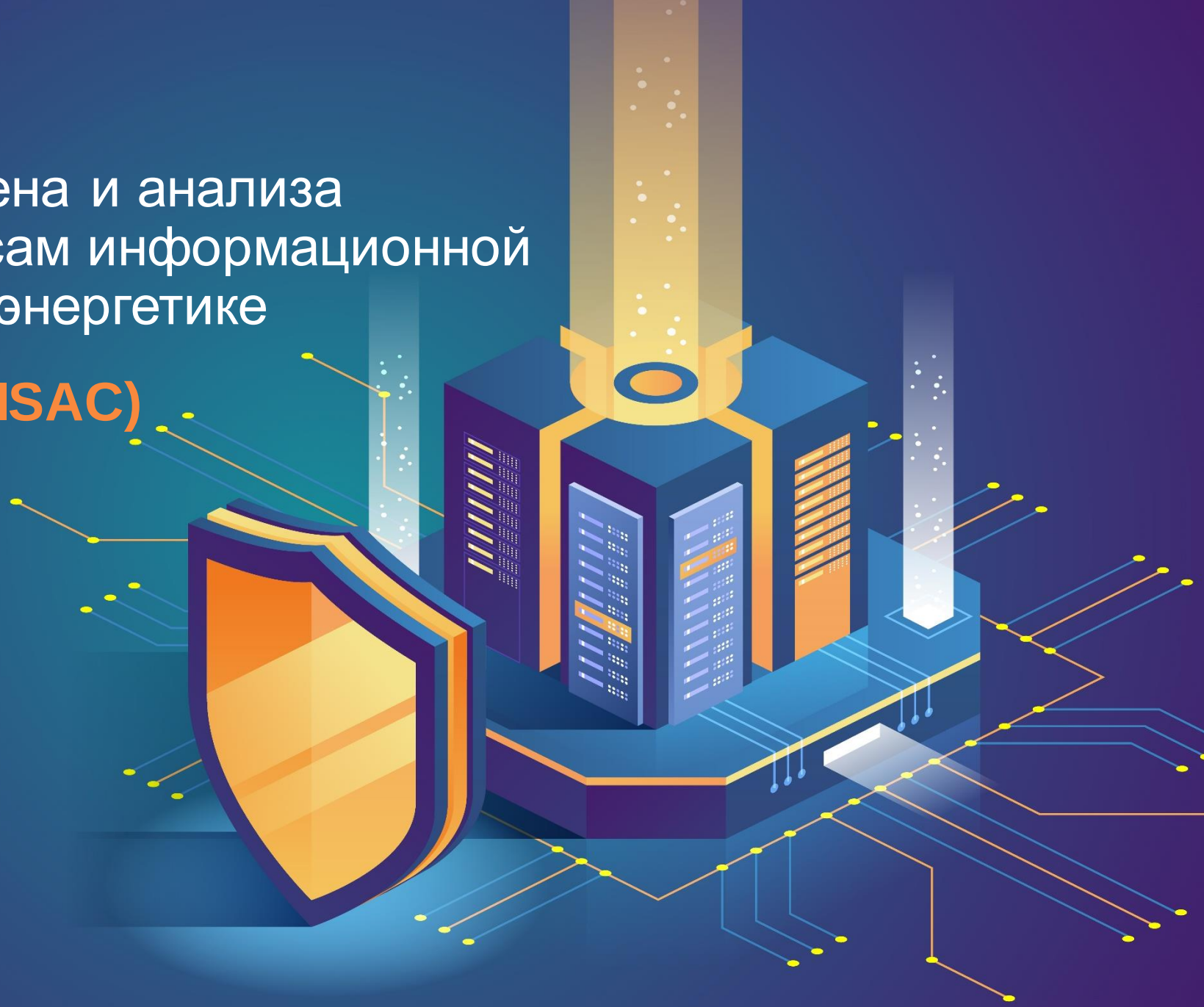
Начальник службы ИБ,
АО «СО ЕЭС», Россия

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

Центр экспертизы (обмена и анализа информации) по вопросам информационной безопасности в электроэнергетике

Энерго ЦИБ (ENERGY ISAC)

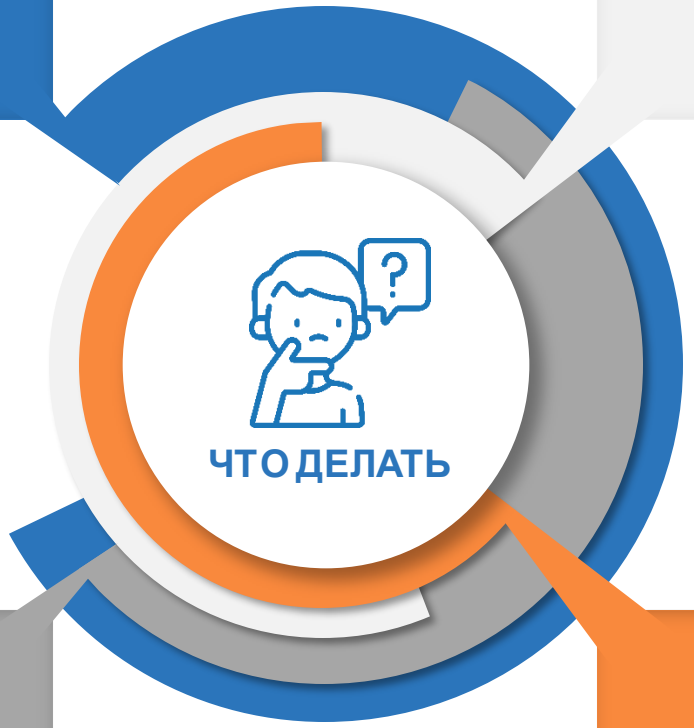


Ассоциация «Цифровая энергетика»

Предпосылки создания центра обмена и анализа информации

Активный рост числа и видов компьютерных атак

Усложнение современных систем управления технологическими процессами в отрасли



Широко известные случаи успешных целевых атак на энергосистемы

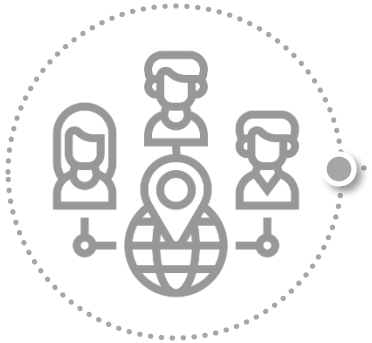
Большое взаимное влияние предприятий ТЭК в рамках Единой энергосистемы России

Главные тезисы проекта

СОЗДАНИЕ ЦЕНТРА ЭКСПЕРТИЗЫ В ВИДЕ ДОБРОВОЛЬНОГО СООБЩЕСТВА КОМПАНИЙ НЕСЕТ В СЕБЕ СЛЕДУЮЩИЕ ПРЕИМУЩЕСТВА

- Создается система с учетом бизнес-процессов и технологических особенностей ИБ предприятий
- Более высокая динамика и становление процессов внутри него за счет отсутствия бюрократических издержек
- Использование существующей инфраструктуры Ассоциации «Цифровая энергетика», обеспечивающей функции бухгалтерского и кадрового учета, офиса и т.д.
- Выделение финансирования компаниями на создание и функционирование данного Центра и наращивания отраслевой компетенции

Одной из задач Центра является обеспечение консолидированной позиции в подготовке предложений для нормативной базы и оказание поддержки Минэнерго России по формированию регуляторных инициатив по информационной безопасности отрасли



Создание Центра на базе Ассоциации «Цифровая энергетика» позволит создать отраслевую площадку для взаимодействия компаний по ИБ

Международный и российский опыт CERT и ISAC

>500

Центров создано в мире, как государственных, так и специализированных отраслевых

<10 лет

У энергетиков в других странах есть свои CERT

В России с 2013 года функционируют:

RU-CERT

Функционирует в сфере безопасности российского сегмента сети Интернет

НКЦКИ

Национальный координационный центр по компьютерным инцидентам

ФинЦЕРТ

Центральный Банк России

CERT-GIB

Коммерческий CERT частной компании Group IB

BI-ZONE

Сбербанк

Создание отраслевого центра кибербезопасности (CERT) планируется Минэнерго России на базе ведомственного центра. Для содействия обмена информацией о передовой практике в отношении киберугроз при Ассоциации создается Центр обмена информацией и ее анализа (Information Sharing and Analysis Centres, ISAC)

Распределение функции участников обеспечения ИБ электроэнергетики

Минэнерго России

- Разработка Стратегии развития ИБ отрасли
- Координация деятельности в области информационной безопасности в электроэнергетике
- Взаимодействие с регуляторами по вопросам ИБ электроэнергетики
- Координация реагирования на компьютерные инциденты в электроэнергетике
- Оценка защищенности объектов электроэнергетики и системы в целом

Ведомственный центр ГосСОПКА

- Организации ИБ для Министерства и подведомственных предприятий
- Проведение мероприятий по ИБ на подведомственных предприятиях и объектах электроэнергетики
- Мониторинг состояние ИБ и реагирование на инциденты ИБ
- Круглосуточный мониторинг информационной безопасности центрального аппарата Минэнерго и подведомственных предприятий

Отраслевой центр кибербезопасности Минэнерго России (CERT)

- Круглосуточное информирование об атаках и угрозах и оперативное оповещение Минэнерго, ведомственного центра и предприятий отрасли о новых уязвимостях, угрозах и атаках
- Сбор информации о фактическом состоянии внешней инфраструктуры, оценка актуальности рисков и угроз для отрасли
- Взаимодействие с разработчиками ПО в части ИБ
- Проведение совместных киберучений, обучающих мероприятий
- Проработка методологий и отраслевых стандартов в области ИБ
- Проведение аудитов по ИБ и оценка защищенности совместно с предприятиями и регуляторами (ФСБ России, ФСТЭК России, ведомственный центр ГосСОПКА Минэнерго России)

Энерго ЦИБ (ENERGO ISAC)

- Содействие организациям электроэнергетики в предотвращении и устранении последствий киберугроз, путем сбора, анализа и распространения среди своих членов информации, которая может быть использована для принятия мер, а также путем предоставления своим партнерам инструментов для уменьшения рисков и повышения устойчивости функционирования информационной инфраструктуры
- Содействие отраслевому (ведомственному) центру кибербезопасности Минэнерго России (в качестве аналитического центра экспертизы консолидированной информации и обеспечения оперативного взаимодействия с компаниями электроэнергетики)

Подразделения ИБ компании энергетического сектора

- Разработка корпоративных планов развития ИБ
- Реализация мероприятий по ИБ на предприятиях и объектах электроэнергетики, включая оценку защищенности объектов КИИ
- Мониторинг состояния ИБ и реагирование на инциденты ИБ

Что даст создание центра обмена и анализа информации

Формирование Энерго ЦИБ

Участники:

Предприятия энергетики

- ПАО «Россети»
- ПАО «Интер РАО»
- АО «Интертехэлектро»
- АО «СО ЕЭС»
- АО «Концерн Росэнергоатом»

Предприятия отрасли ИБ

Этапы создания

1 этап

2021 – 2022 года

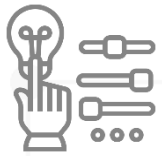
Становление центра на базе Ассоциации «Цифровая энергетика» и формирование отраслевой компетенции

2 этап

2023 год

Развитие компетенций центра, выделение в отдельную организацию

Функции на 1 этапе



Функции Подразделения на 1 этапе

Сотрудничество, накопление и обмен знаниями, отраслевая методология, в том числе:

- Формирование экосистемы для реализации перспективных задач и обеспечения обмена информацией
- Обеспечение «профилирования» компаний электроэнергетики по результатам обмена информацией по заключенным соглашениям
- Привлечение к реализации перспективных задач регуляторов ИБ, внешних организаций – экспертов в области ИБ

1. Информационно-аналитическая (5\2)
2.
3. Популяризация и распространение знаний

Функции на 2 этапе

1. Сотрудничество, накопление и обмен опытом, отраслевая методология
2. Популяризация и распространение знаний
3. Оповещение объектов о новых атаках и угрозах (24\7)
4. Сбор информации о фактическом состоянии внешней инфраструктуры, оповещения об изменениях и уязвимостях (24\7)
5. Экспертная аналитика и помощь при развитии инцидента
6. Оказание услуг по индивидуальному заказу

Концепция создания Энерго ЦИБ

Разработана Концепция создания Энерго ЦИБ с учетом предложений Минэнерго России, ФСТЭК, Минцифры России, НКЦКИ

Подготовлен план работ Энерго ЦИБ на 2021-2022 гг

Сформирован состав Комитета по кибербезопасности при Наблюдательном совете Ассоциации

(для контроля деятельности Энерго ЦИБ)