



Москва, 29 сентября - 1 октября



МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ И ВЫСТАВКА  
**РЕЛЕЙНАЯ ЗАЩИТА И АВТОМАТИКА ЭНЕРГОСИСТЕМ 2021**

**ДОЛЖНЫ ЛИ МЫ ПРИМЕНЯТЬ МЕТОДЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ  
РАСПРЕДЕЛИТЕЛЬНЫХ СЕТЕЙ: ВЫЗОВЫ И РЕШЕНИЯ**

E. Weerathunga, A. Appukuttan, M. Kanabar

GE Renewable Energy

Канада, Великобритания

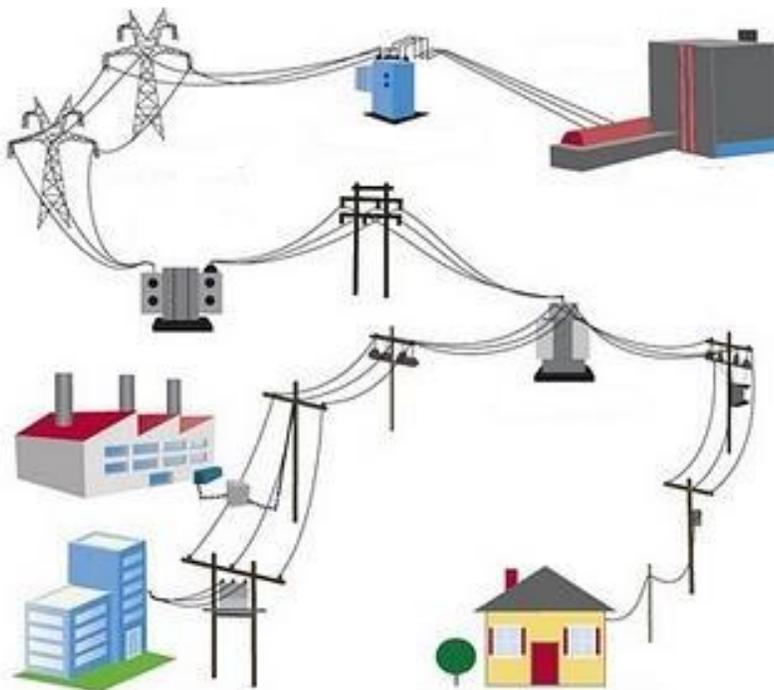
**Соколов Г.А.**



## ЕСТЬ ЛИ ПРОБЛЕМЫ С КИБЕР БЕЗОПАСНОСТЬЮ?

---

Распределительная сеть уязвима



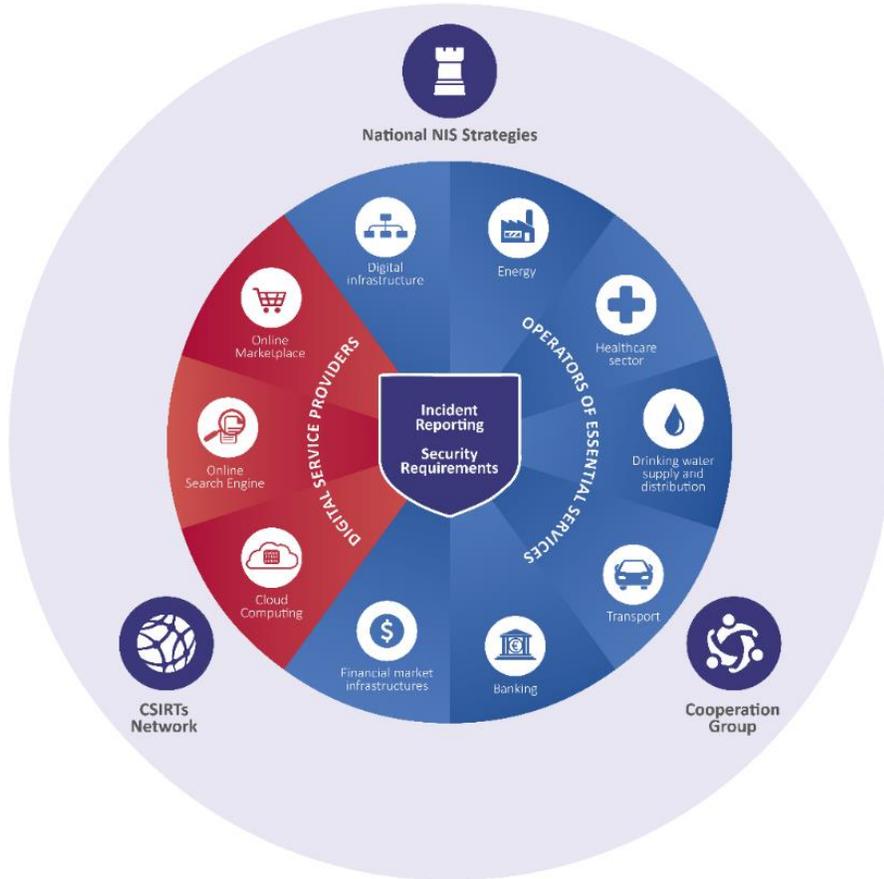
23 декабря 2015 года в Украине произошла первая известная успешная атака на информационную безопасность, нацеленная на энергосистему



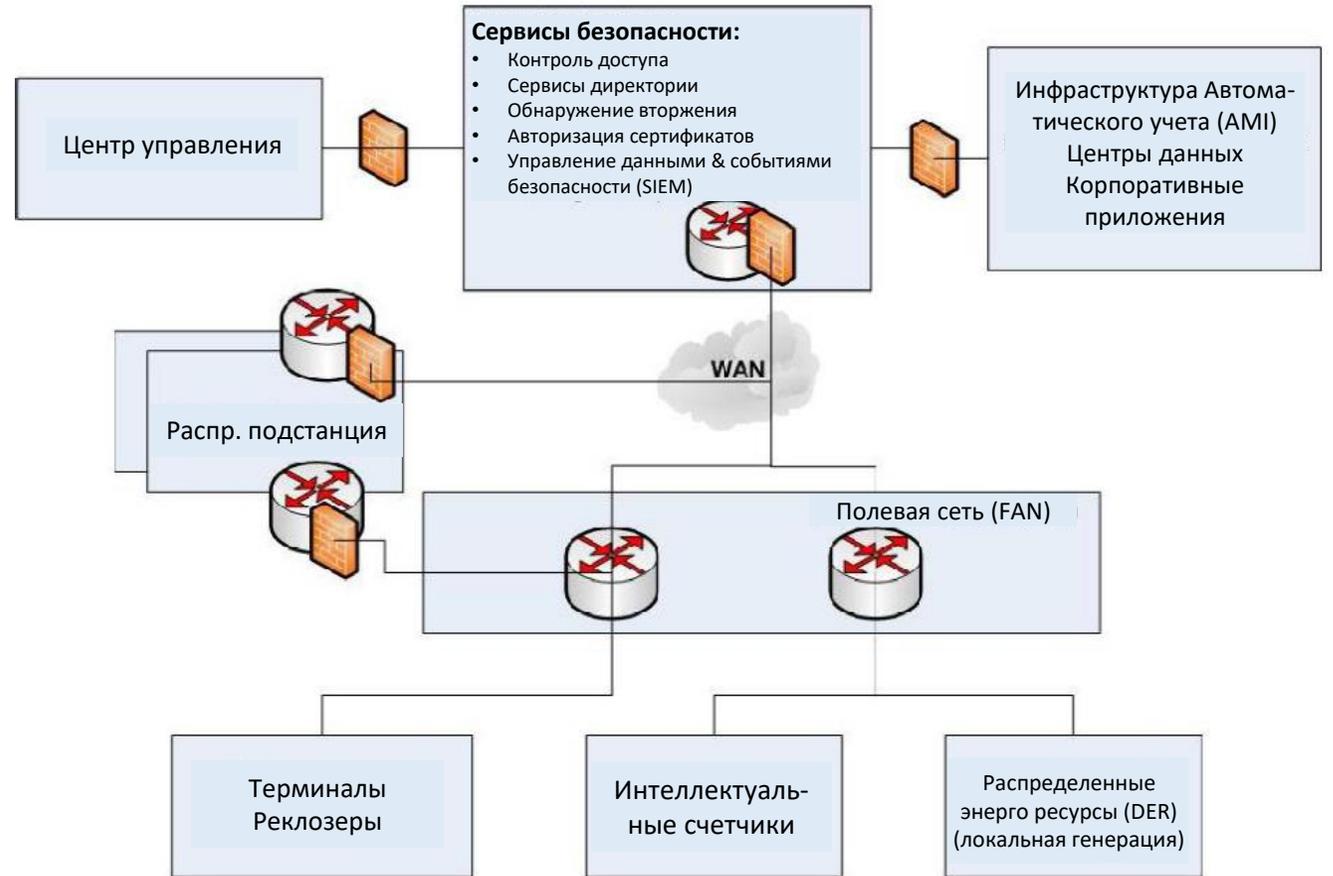


## ЕВРОПЕЙСКИЙ ПОДХОД

### Директива NIS



### Архитектура информационной безопасности



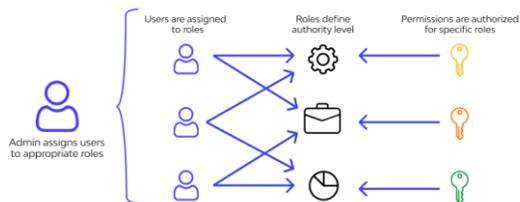


## ИНТЕГРАЦИЯ ПОДСТАНЦИИ/УСТРОЙСТВА В АРХИТЕКТУРУ БЕЗОПАСНОСТИ

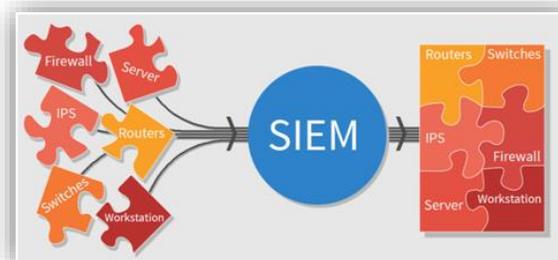
Глубокоэшелонированная защита - наложение элементов защиты

### Доступ на основе ролей (RBAC)

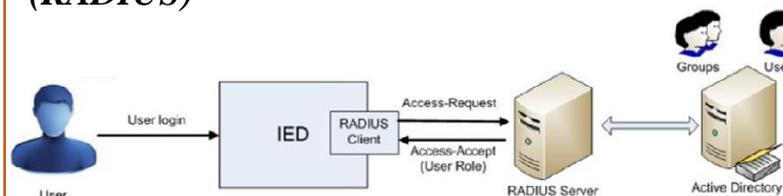
Role-Based Access Control



### Регистрация системных событий (SIEM) (системный журнал)



### Идентификация удаленных пользователей (RADIUS)

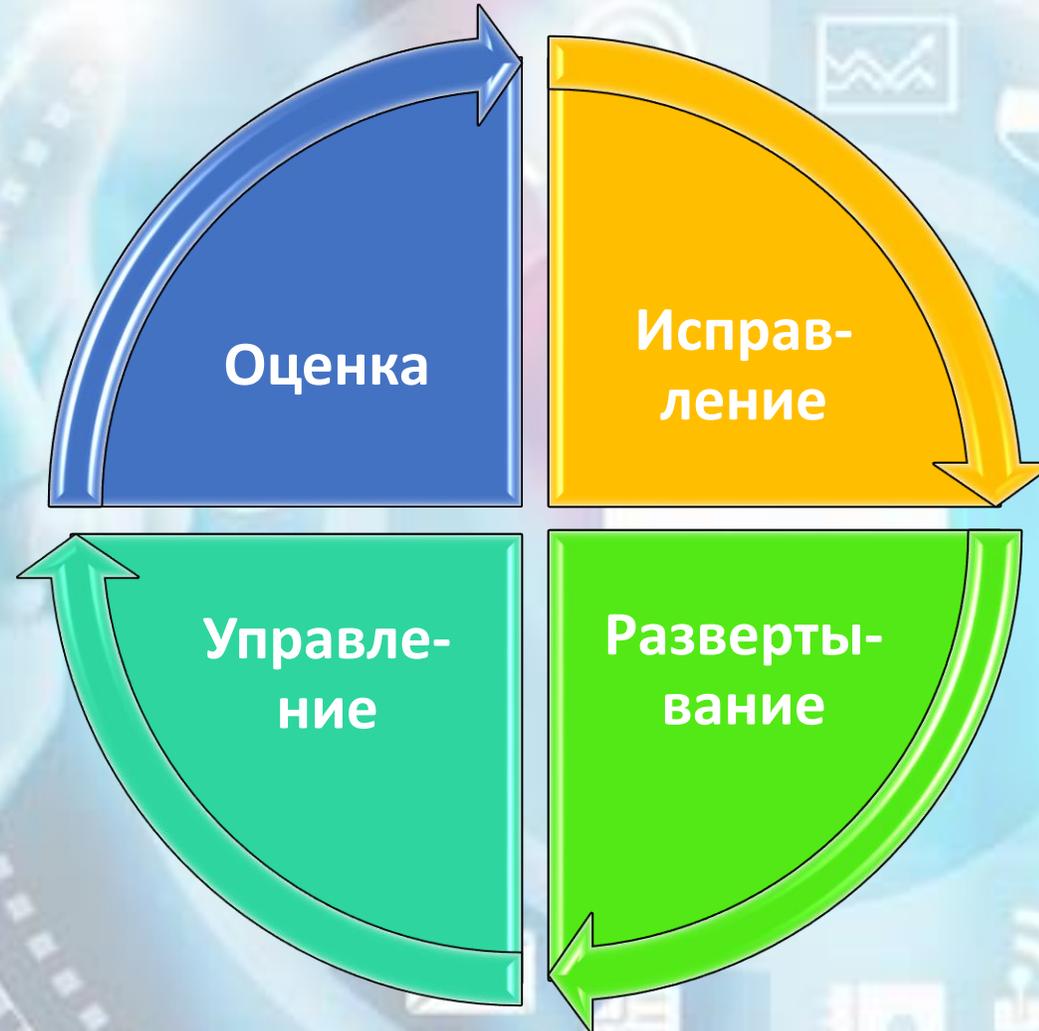


Управление  
идентификацией  
привилегий





## СТРАТЕГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ





## ЗАКЛЮЧЕНИЕ

---

- Сети усложняются – нарастают риски кибер атак
- Европейский подход (NIS) глубокоэшелонированная защита
- На каждом уровне должны реализовываться свои требования
- Опыт Украины показал, что слабое звено всегда пользователь
- Кибербезопасность это не только технические меры, но организационные, а также регулярное обучение персонала



# СПАСИБО ЗА ВНИМАНИЕ!

---

Контакты:  
[gleb.sokolov@ge.com](mailto:gleb.sokolov@ge.com)