



5-я Международная научно-техническая конференция
«Современные направления развития систем релейной
защиты и автоматики энергосистем»

КОНЦЕПЦИЯ ПОСТРОЕНИЯ КОМПЛЕКСА КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ СОВРЕМЕННЫХ ОБЪЕКТОВ ЭЛЕКТРОСЕТЕВОГО ХОЗЯЙСТВА

Никандров М.В.
К.Т.Н.

ООО «Интеллектуальные сети»



Брагута М.В.
К.Т.Н.

ОАО «НТЦ ФСК ЕЭС»



Содержание

- I. Особенности информационной инфраструктуры современных энергообъектов**
- II. Модель технологического объекта**
- III. Векторы кибератак**
- IV. Обобщенная модель угроз**
- V. Практика PHDays V (2015)**
- VI. Классификация объектов защиты**
- VII. Комплексная система защиты технологических объектов**

Изменение инфраструктуры

Повышение уровня автоматизации

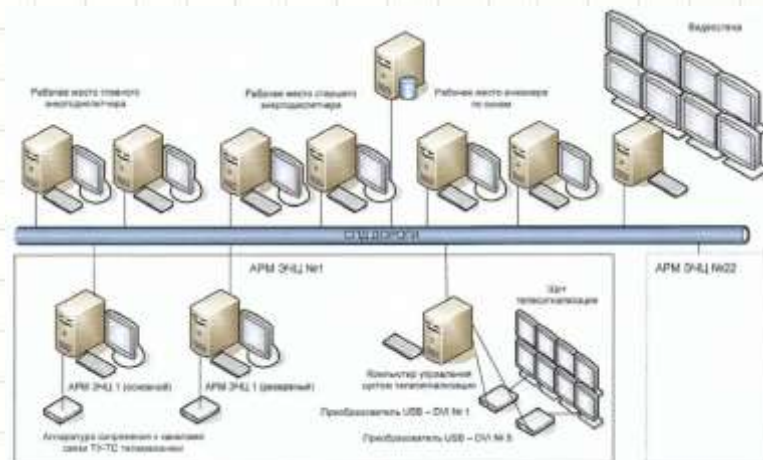
высокая плотность интеллектуальных цифровых устройств на один объект

Увеличение размеров ЛВС объекта

тотальный переход на Ethernet сети

Открытые протоколы

переход на унифицированный протокол IEC 61850



Отсутствие контроля сети

Отсутствие сегментирования сети и контроля трафика

Мы сами строим благоприятную среду для развития кибератак

Отсутствие полной изолированности

Необходимость передачи информации в режиме реального времени на вышестоящие диспетчерские центры

Наличие арендованных каналов связи и точек соприкосновения с корпоративными и внешними сетями

Отсутствие внедренных механизмов контроля и защиты внешнего трафика



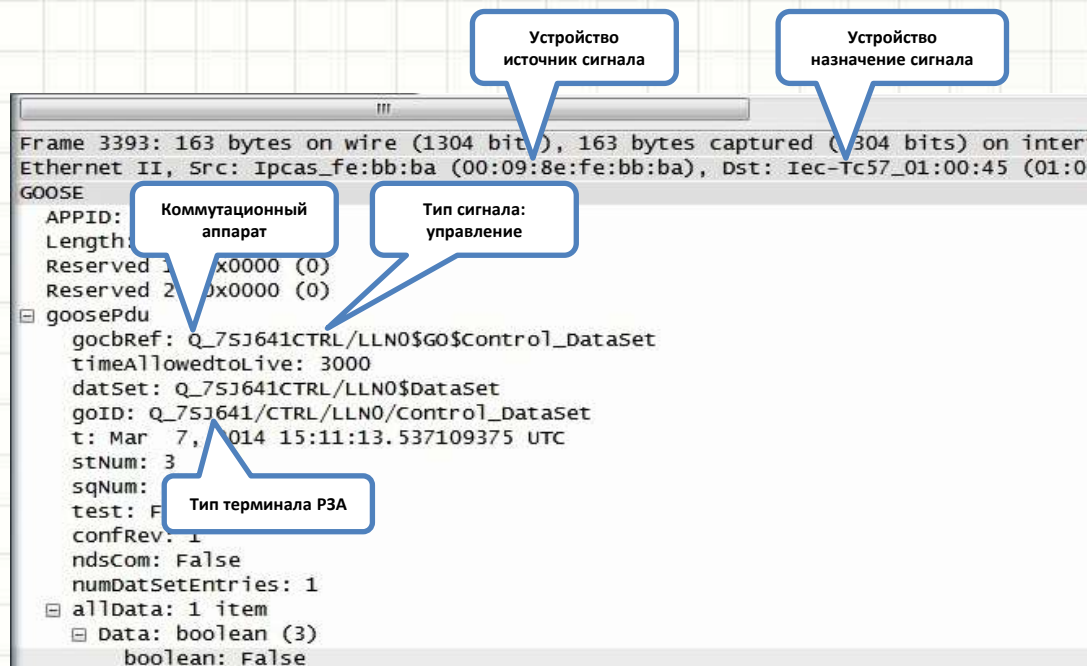
Отсутствие защиты

Доступность информации

- отсутствие шифрования межобъектовой информации
- логическая открытость внутренней структуры объекта (IEC 61850)

Доступность источников информации

- сохранение заводских паролей «по умолчанию»;
- наличие заводских паролей суперпользователя.



Изменение конъюнктуры

Доступность технологий и знаний

- культура «киберпанков»
- доступность средств вычислительной техники
- развитые рынки продажи уязвимостей



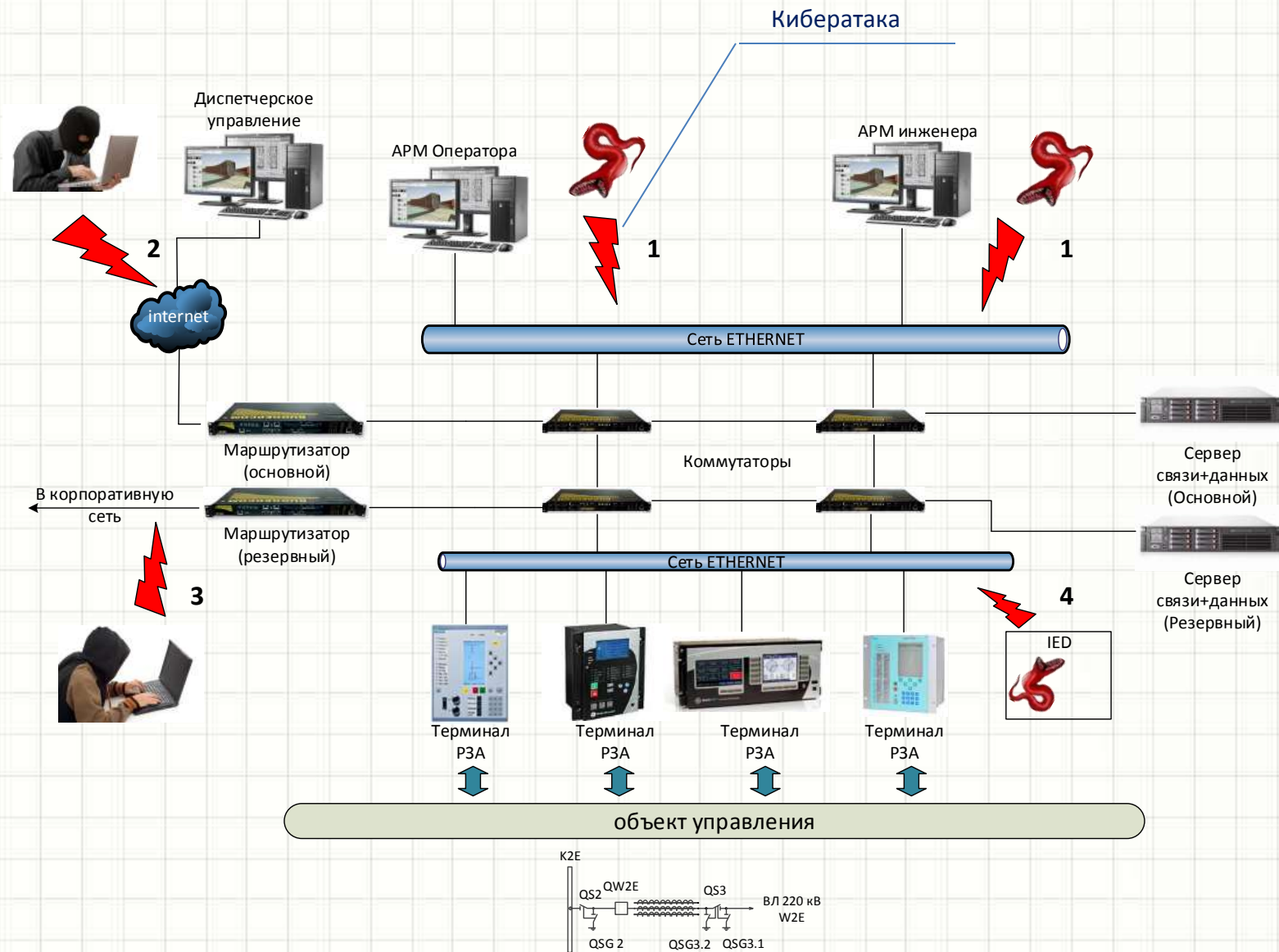
Актуальность

- повышенное внимание со стороны хулиганов, «хактивистов» и профильных криминальных группировок
- повышенное внимание со стороны спецслужб



II

Модель технологического объекта



III Векторы атак

- SCADA, сервера системы управления
- АРМы управления и инженеров
- Сервера времени и другое вспомогательное оборудование
- Сетевое оборудование
- Каналы связи
- IED (контроллеры и МП РЗА)
- Сотрудники (социальная инженерия)



Трехуровневая миссиоцентрическая классификация угроз:

© С. Гордейчик

1. Снижение функциональной безопасности и надежности системы сети передачи энергии
2. Снижение эффективности процесса передачи электрической энергии
3. Нарушение безопасности основного технологического процесса

1. Снижение функциональной безопасности и надежности системы сети передачи энергии:

- временный вывод из строя компонентов, не отвечающих за безопасность процесса передачи электроэнергии (оборудование связи, сервера времени, второстепенные датчики и т.д.)
- временный вывод из строя системы телемеханики и диспетчерского управления
- отображение ложной диагностики на АРМ оперативного персонала



2. Снижение эффективности процесса передачи электрической энергии:

- долговременный вывод из строя системы телемеханики и диспетчерского управления
- несанкционированное отключение потребителей
- дезинформирование центра диспетчерского управления



3. Нарушение безопасности основного процесса:

- отключение и/или модификация оперативных блокировок
- ложные команды управления, приводящие к повреждению силового оборудования (например, включение заземляющего ножа под напряжением)
- несанкционированное отключение крупных генераторов энергии
- отключение и/или **вывод из работы терминалов релейной защиты и противоаварийной автоматики**

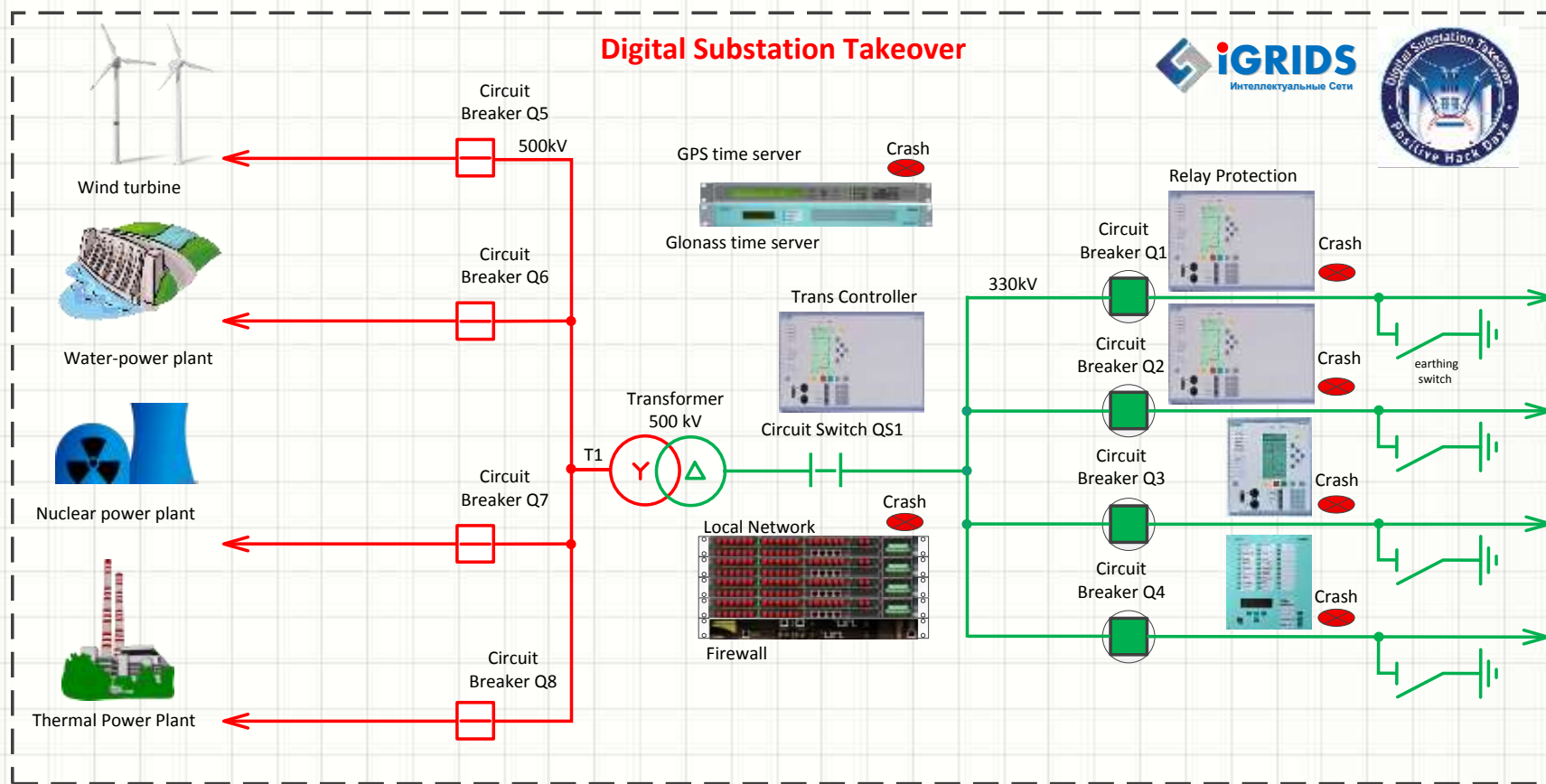




Конкурс Digital Substation Takeover



Схема стенда



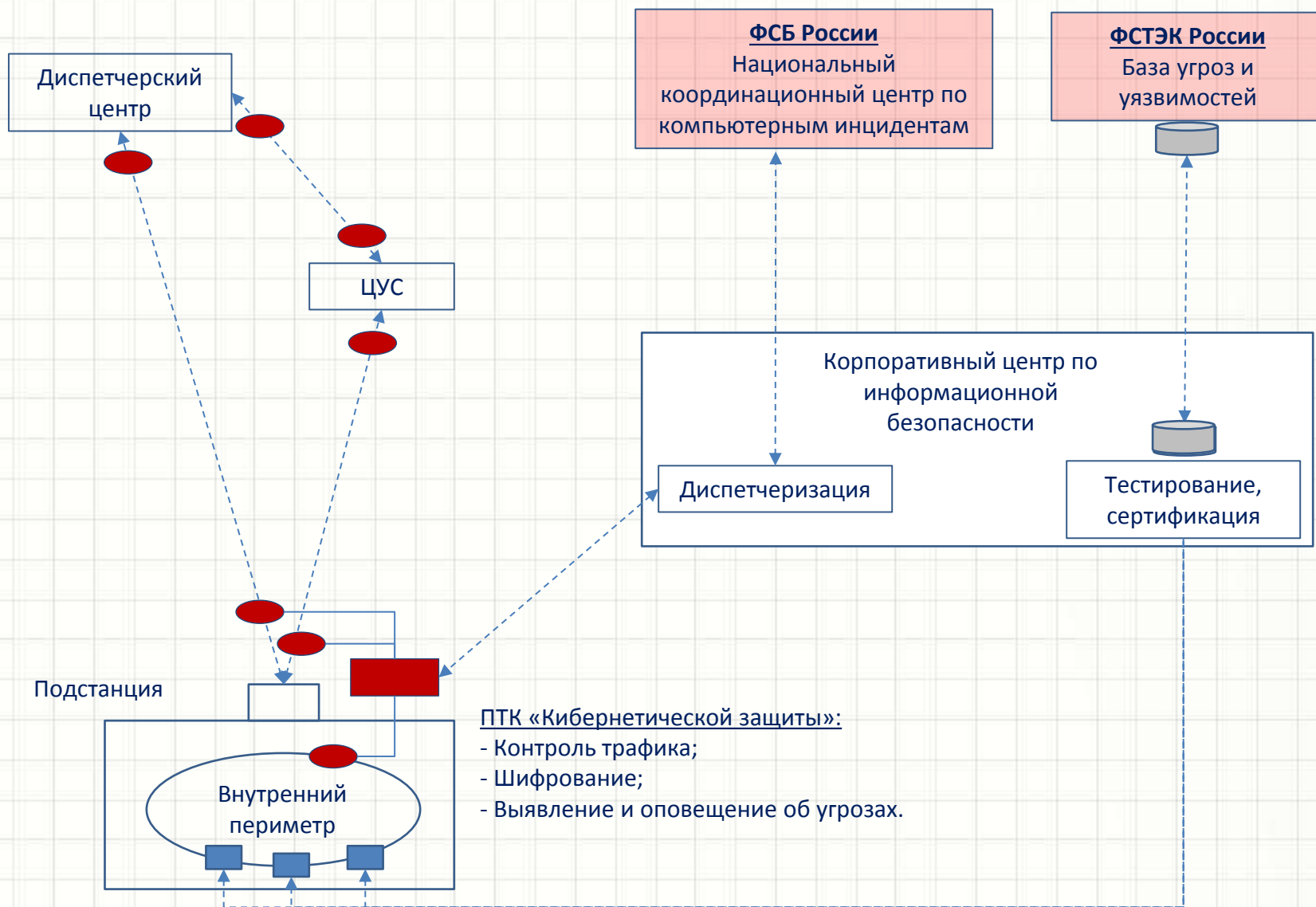
Итоги конкурса



- Вывод из строя информационной сети подстанции - 6 раз
- Перепрограммирование сервера времени - 1 раз
- Воздействие на терминал, приведшее к несанкционированному отключению - 2 раза

Особенность объекта	Класс защищенности
1) Объект построен на ИЭУ, оснащен полноценной АСУ ТП с возможностью дистанционного управления; 2) Работа объекта, влияет на устойчивость ЕНЭС. 3) Федеральное и межрегиональное влияние нарушения работы объекта.	Первый класс (К1)
1) Объект построен на ИЭУ, оснащен полноценной АСУ ТП с возможностью дистанционного управления; 2) Работа объекта мало влияет на устойчивость ЕНЭС; 3) Региональное влияние нарушения работы объекта.	Второй класс (К2)
1) Объект построен на основе электромеханических и полупроводниковых систем РЗА, оснащен системой телемеханики без возможности дистанционного управления;	Третий класс (К3)
1) Муниципальное (локального) влияние нарушения работы объекта.	Третий класс (К3)

Комплексная система защиты технологических объектов (концепт)



Спасибо за внимание!



ООО «Интеллектуальные Сети»
www.igrids.ru



ОАО «НТЦ ФСК ЕЭС»
www.ntc-power.ru