Никандров Максим

# Турниры по практической информационной безопасности как средство актуализации модели угроз и оценки эффективности средств киберзащиты в системах автоматизации электроэнергетики

24 июня 2016 г

iGRIDS
Интеллектуальные Сети

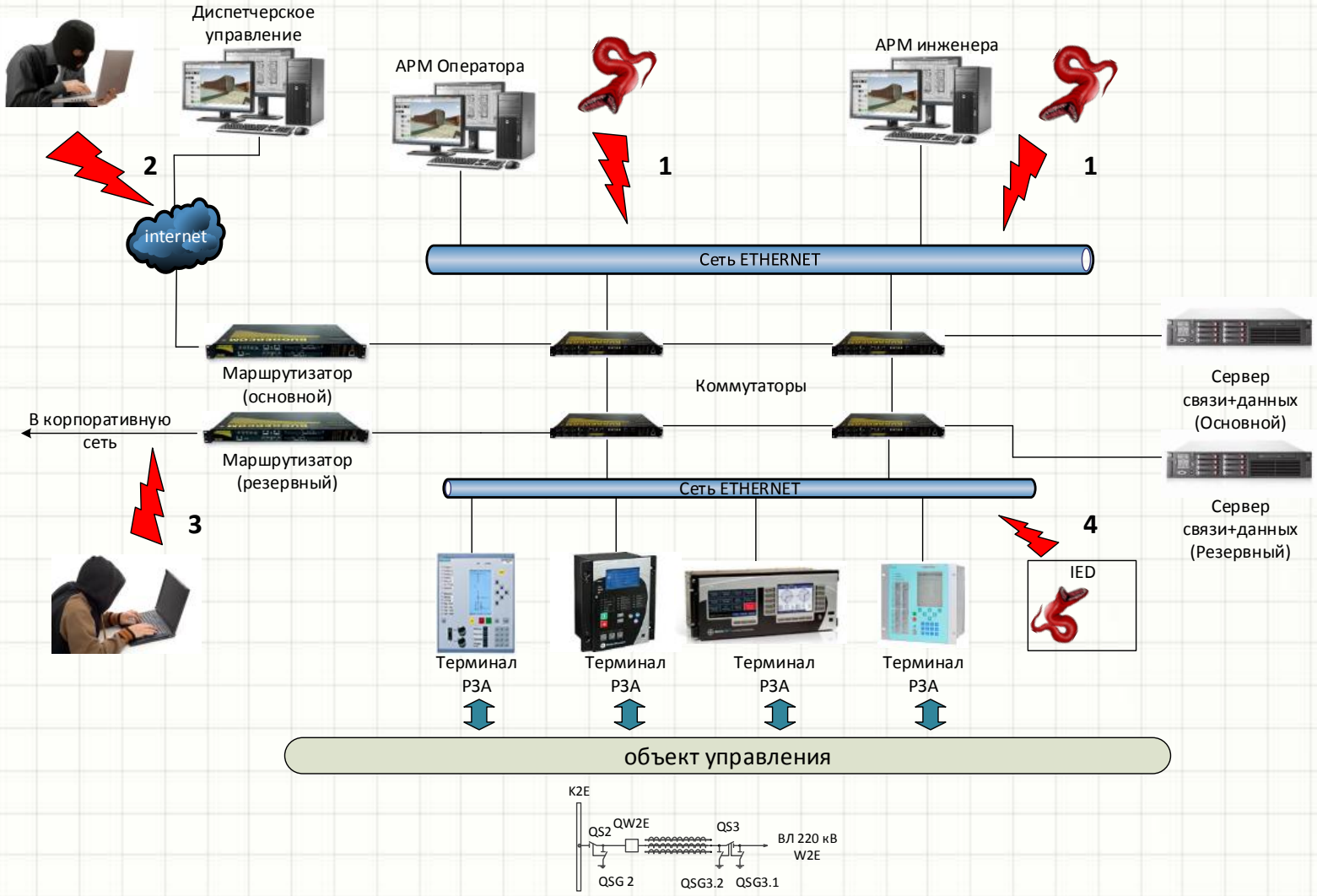
# Инциденты ИБ на объектах электроэнергетики

**Инциденты информационной безопасности на электроэнергетических объектах пока редки.**

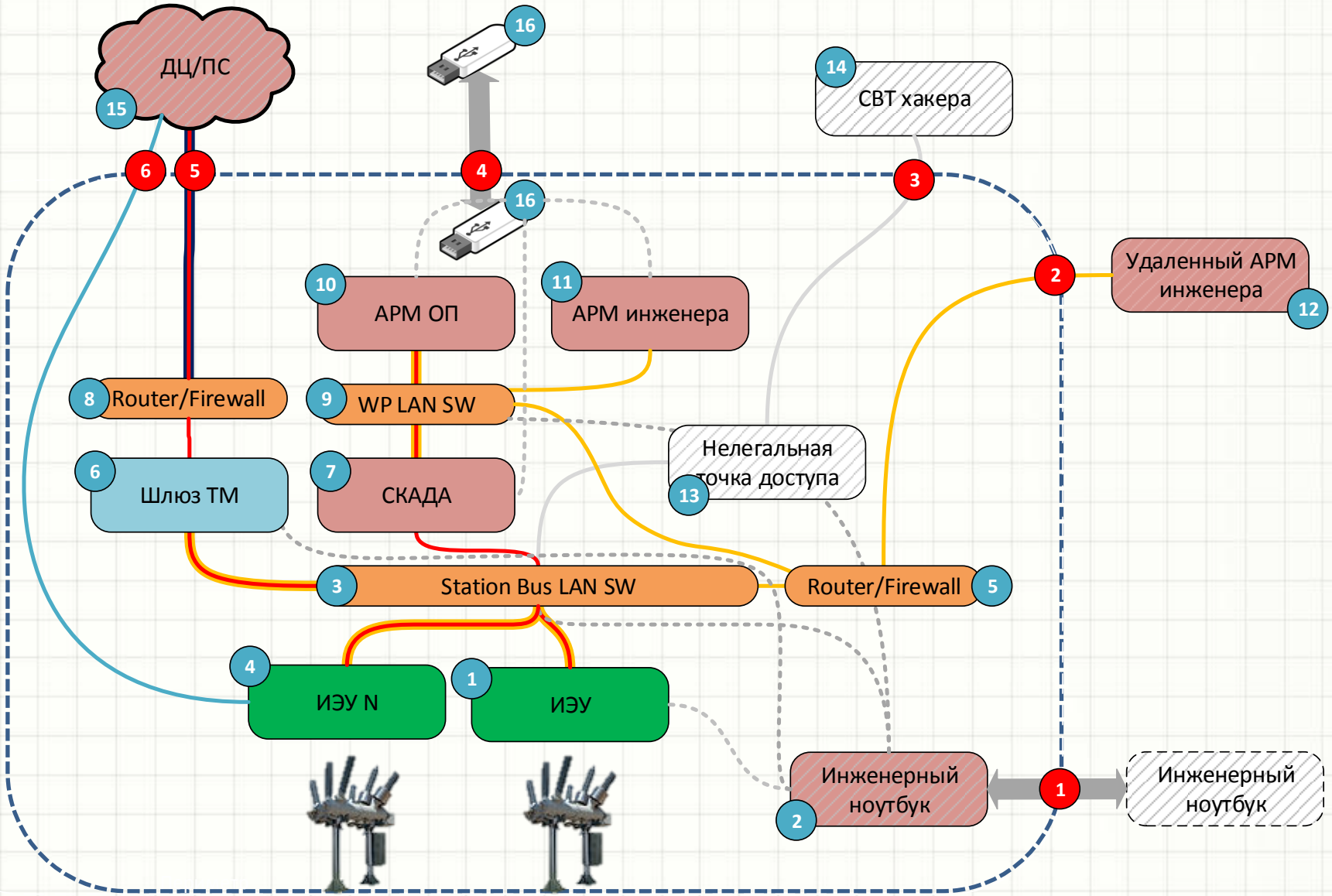
**Информация по реально случившимся инцидентам зачастую скрывается, так как ее обнародование несет серьезные репутационные риски.**

**В результате, вероятность возникновения инцидента, глубину проникновения и возможный ущерб оценить крайне сложно. Предлагаемые модели угроз часто не учитывают специфику электроэнергетических объектов, в результате, модели угроз и модели нарушителей ничем не подкреплены и не могут быть проверены на практике.**

# Модель системы



# Уязвимости периметра ПС



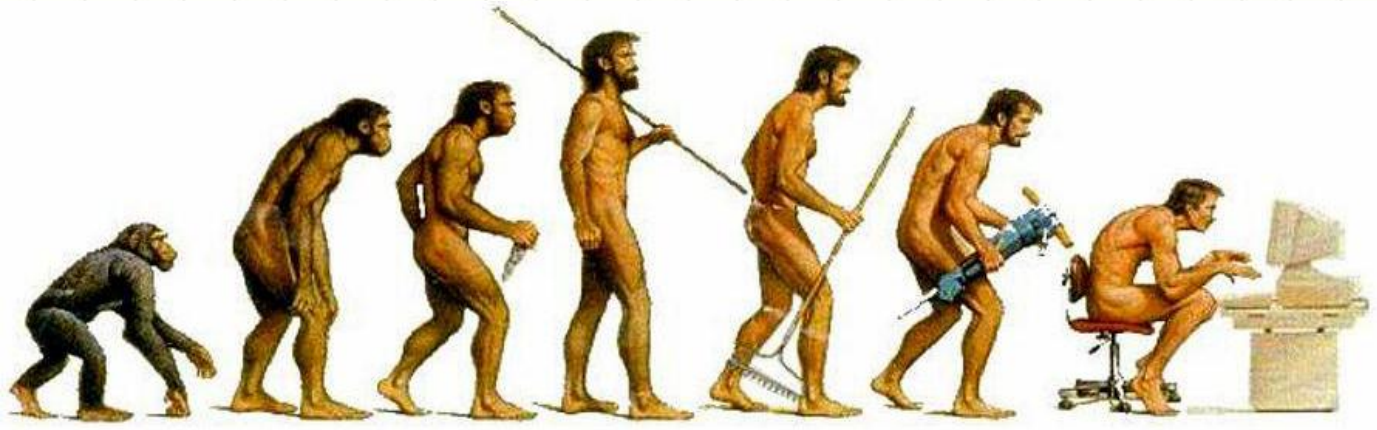

Из презентации Дорофеева Ивана

# Эволюция турниров

**1. Что могут сделать «ХАКЕРЫ» любители если их пустить в «огород»?**

**2. Что могут сделать «ОТБОРНЫЕ ХАКЕРЫ» за хороший приз?**

**3. Что смогут «ХАКЕРЫ» если им противодействовать?**

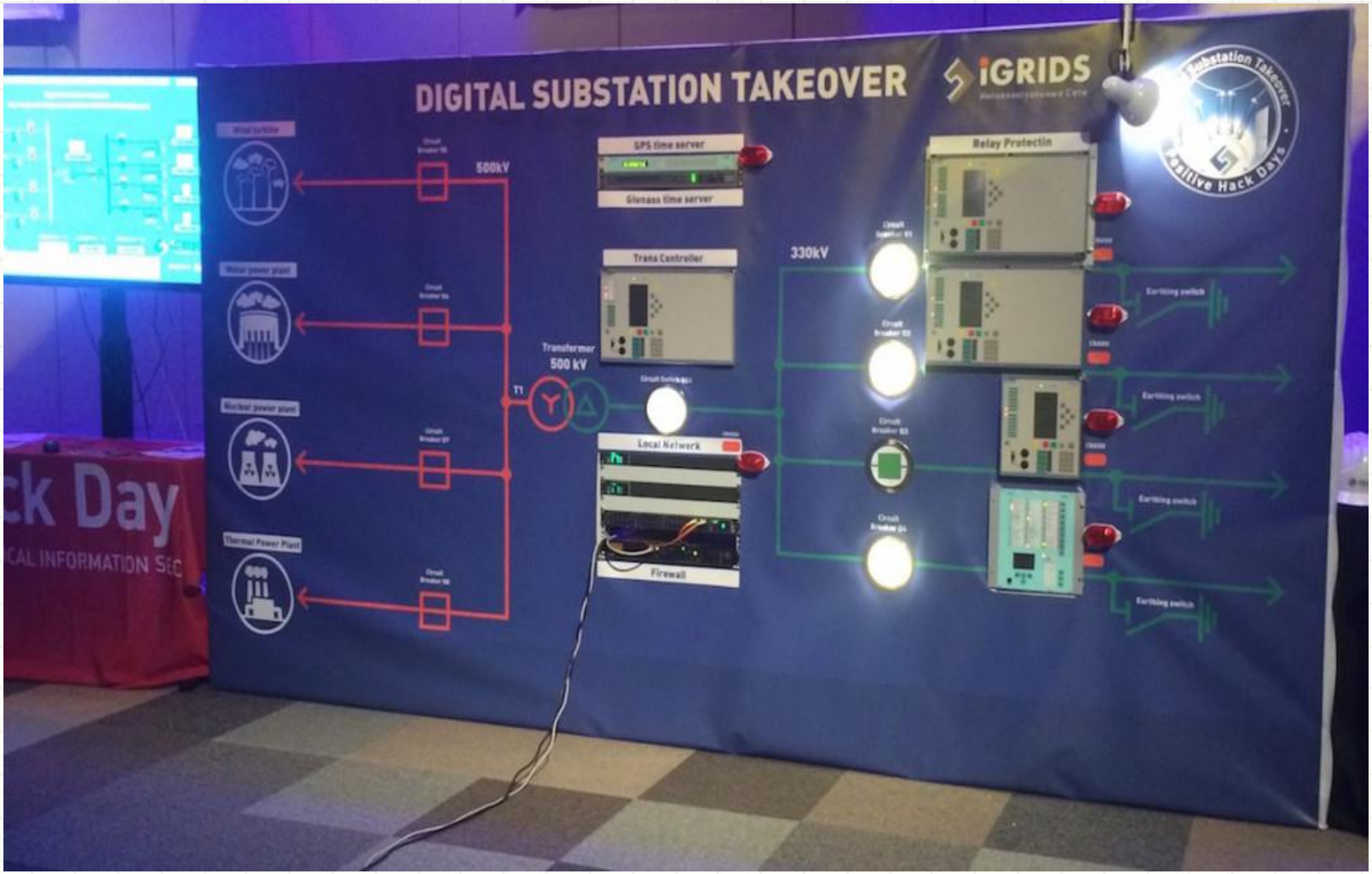


# Задачи конкурсов

- «Разведка» – тип атак, который позволяет получить дополнительную информацию о стенде, сети или атакуемых устройствах;
- «Взлом» – тип атак, которые привели к потери некоторых функций системы, снижении общей надежности, но не приведшие к разрушению технологического оборудования );
- «Диверсия» – тип атак, способных полностью нарушить технологический процесс, привести к возникновению ЧП (в нашем случае - короткое замыкание модели ЛЭП).

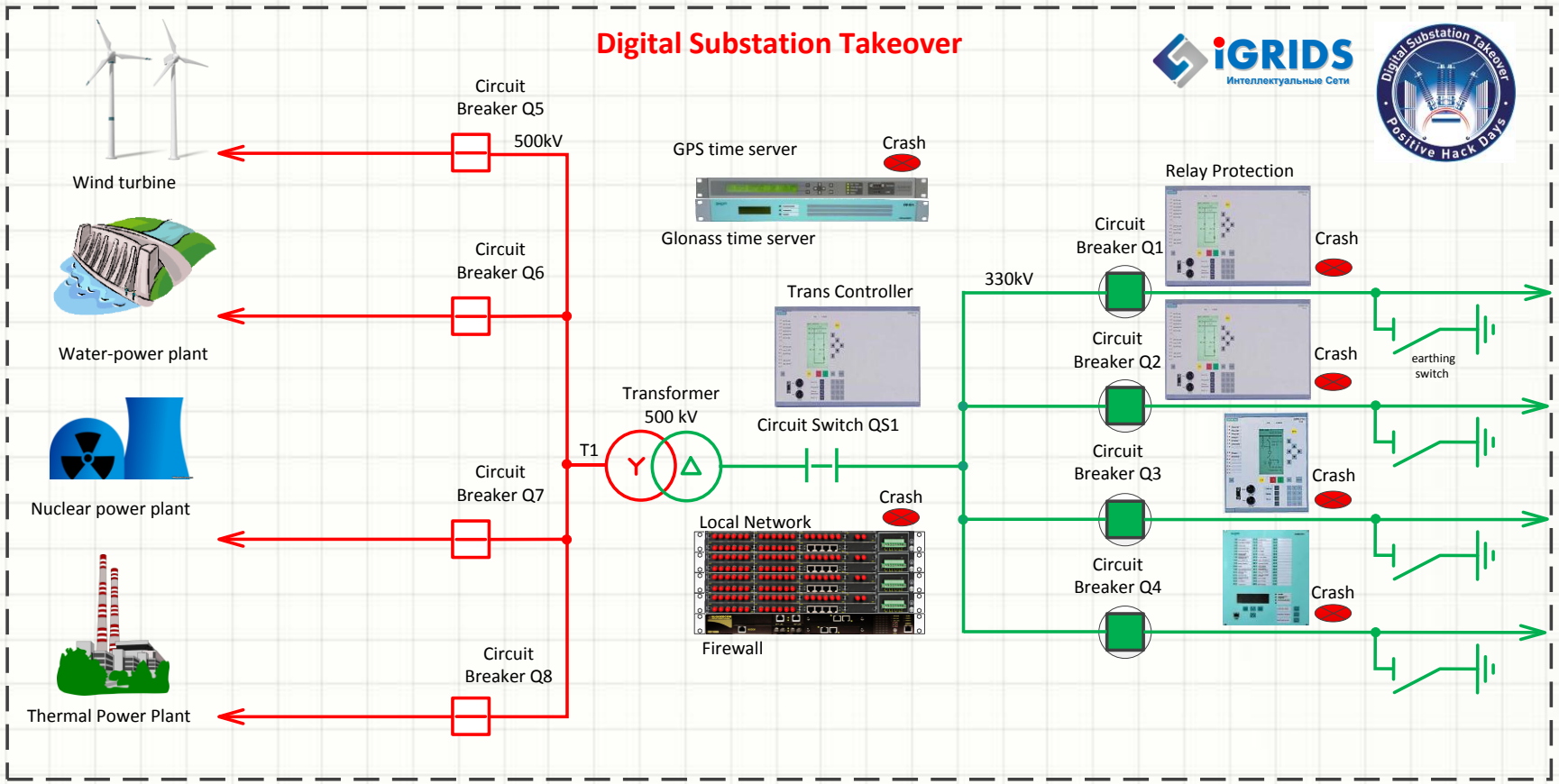
# Positive Hack Days V


# Конкурс Digital Substation Takeover




Международный форум по практической безопасности Positive Hack Days V проходил с 26 по 27 мая 2015 года. Организатор конференции ЗАО «Позитивные Технологии»

# Конкурс Digital Substation Takeover




«Легенда» конкурса

# Итоги конкурса

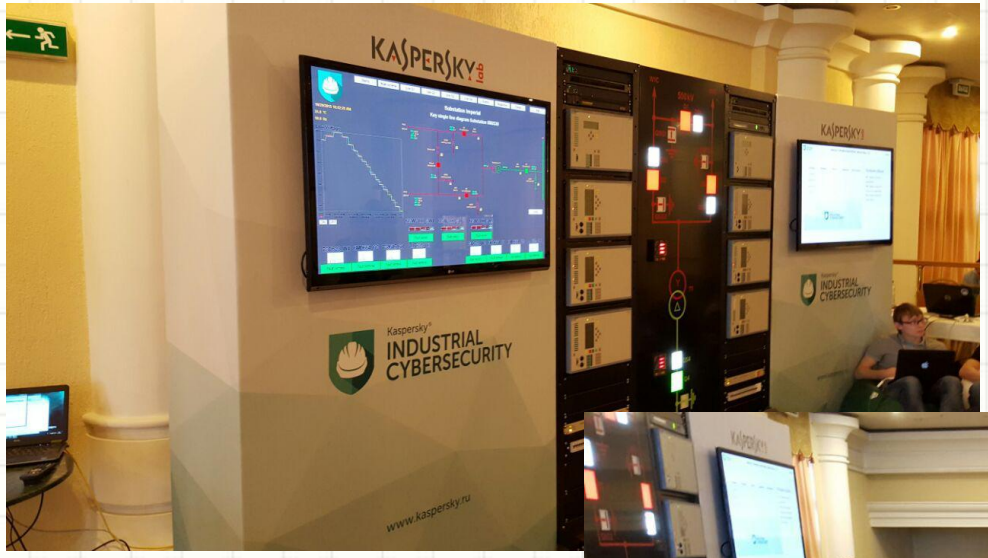
| Тип атаки | Количество |
|---|---|
| Вывод из строя информационной сети подстанции | 6 |
| Перепрограммирование сервера времени | 1 |
| Воздействие на терминал, приведшее к несанкционированному отключению | 2 |
| «Диверсии» | 0 |

# Не санкционированное отключение выключателя

- Две успешные атаки с отключением выключателя по средством сервисного ПО
- Одна «почти успешная» путем подключением клиентом IEC 61850
- Создание программы «GOOSE по заказу»

- Никто не смог сделать сложную многоходовую атаку

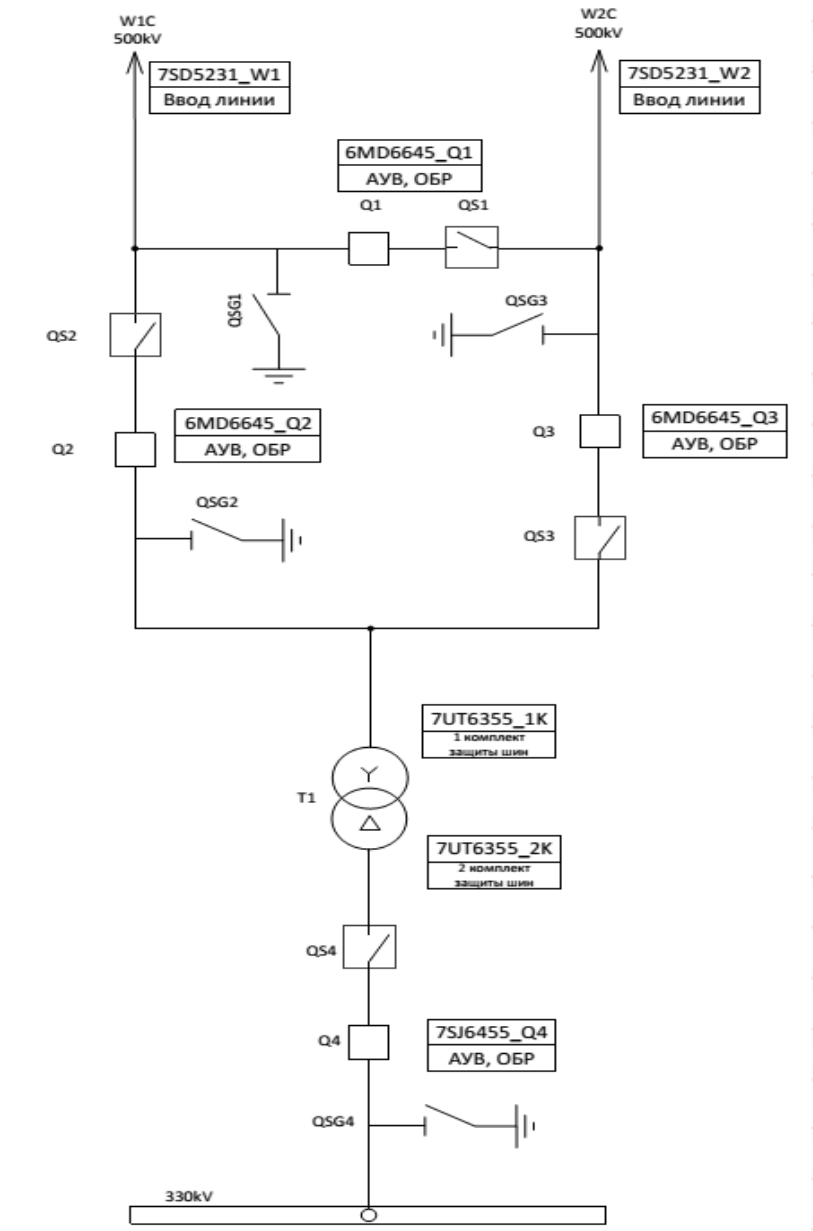
# Kaspersky Industrial CTF



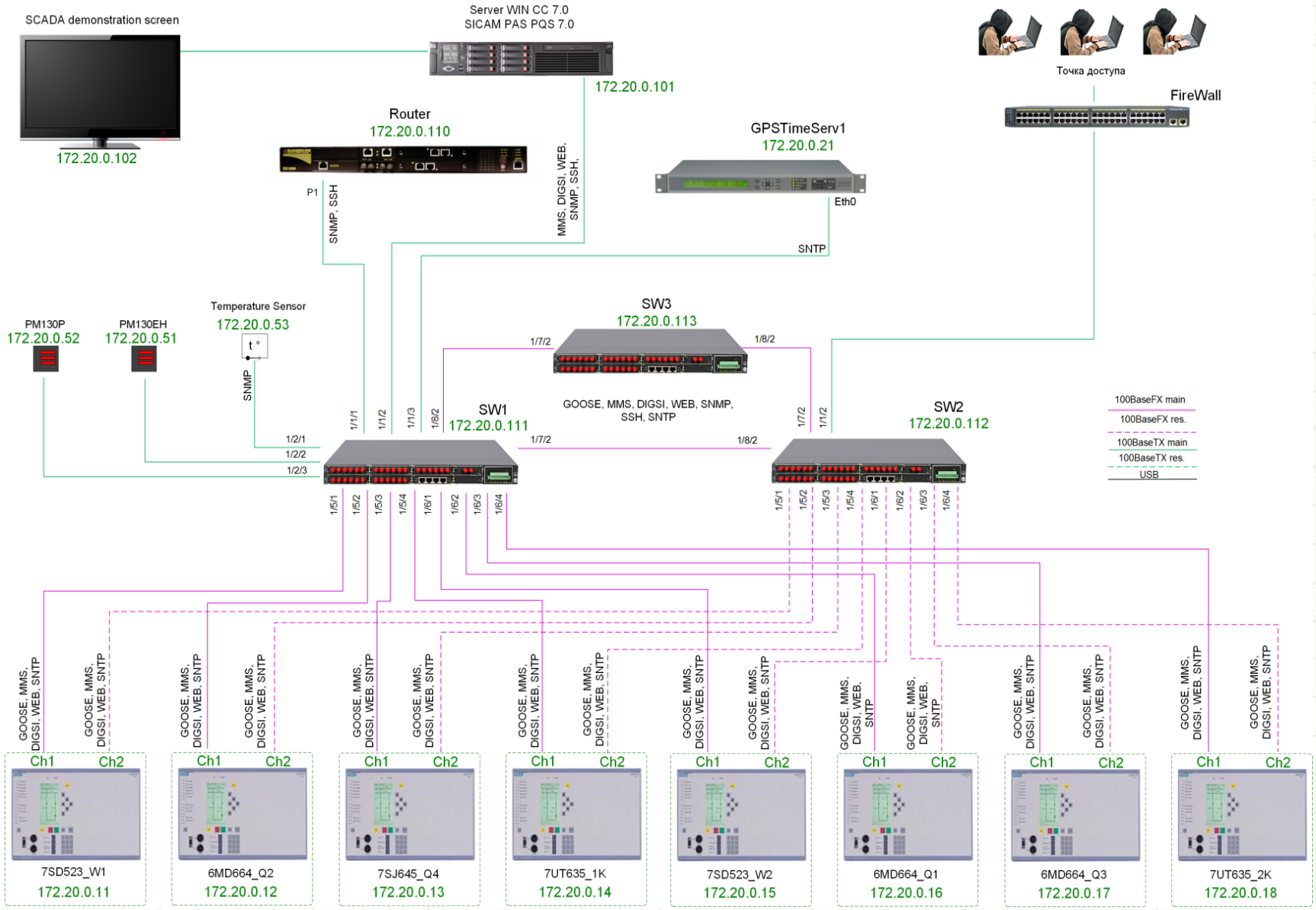

Kaspersky®
INDUSTRIAL
CYBERSECURITY

Финал Kaspersky Industrial CTF проходил с 29 по 30 октября 2015 года в рамках конференции «Кибербезопасность АСУ ТП: время действовать» Организатор конференции ЗАО «Лаборатория Касперского»

# Kaspersky Industrial CTF



# Kaspersky Industrial CTF



# Итоги CTF KICS 2015


| Тип атаки | Количество |
|---|---|
| «Разведка» | 7 |
| «Взломом» | 18 |
| «Диверсии» | 5! |

# Сценарии атак

**Сценарий А:**

1. Прохождение маршрутизатора, подключение в локальную сеть стенда;
2. Проведение разведки для определения типа устройств;
3. Подключение к контроллерам с использованием инженерного ПО путем подбора верных параметров подключения;
4. Снятие защитных блокировок с использованием инженерного ПО;
5. Отправка команды для совершения короткого замыкания.

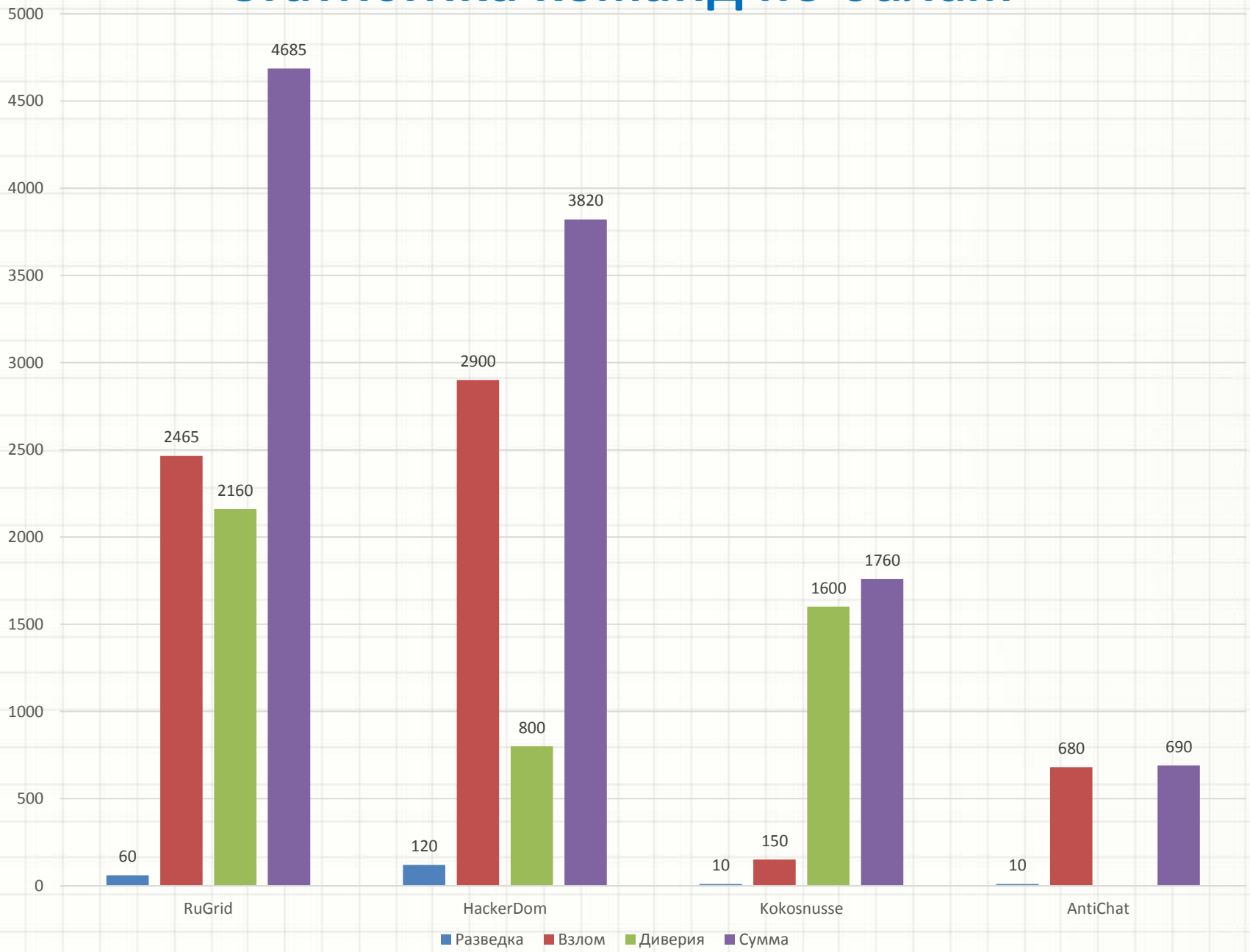
**Сценарий Б:**

1. Прохождение маршрутизатора, подключение в локальную сеть стенда;
2. Проведение разведки для определения типа устройств;
3. Генерация специально сформированных сообщений на основе протокола GOOSE для отключения защитных блокировок;
4. Подключение к контроллерам не легитимным клиентом MMS и подача команды на коммутационный аппарат для совершения короткого замыкания

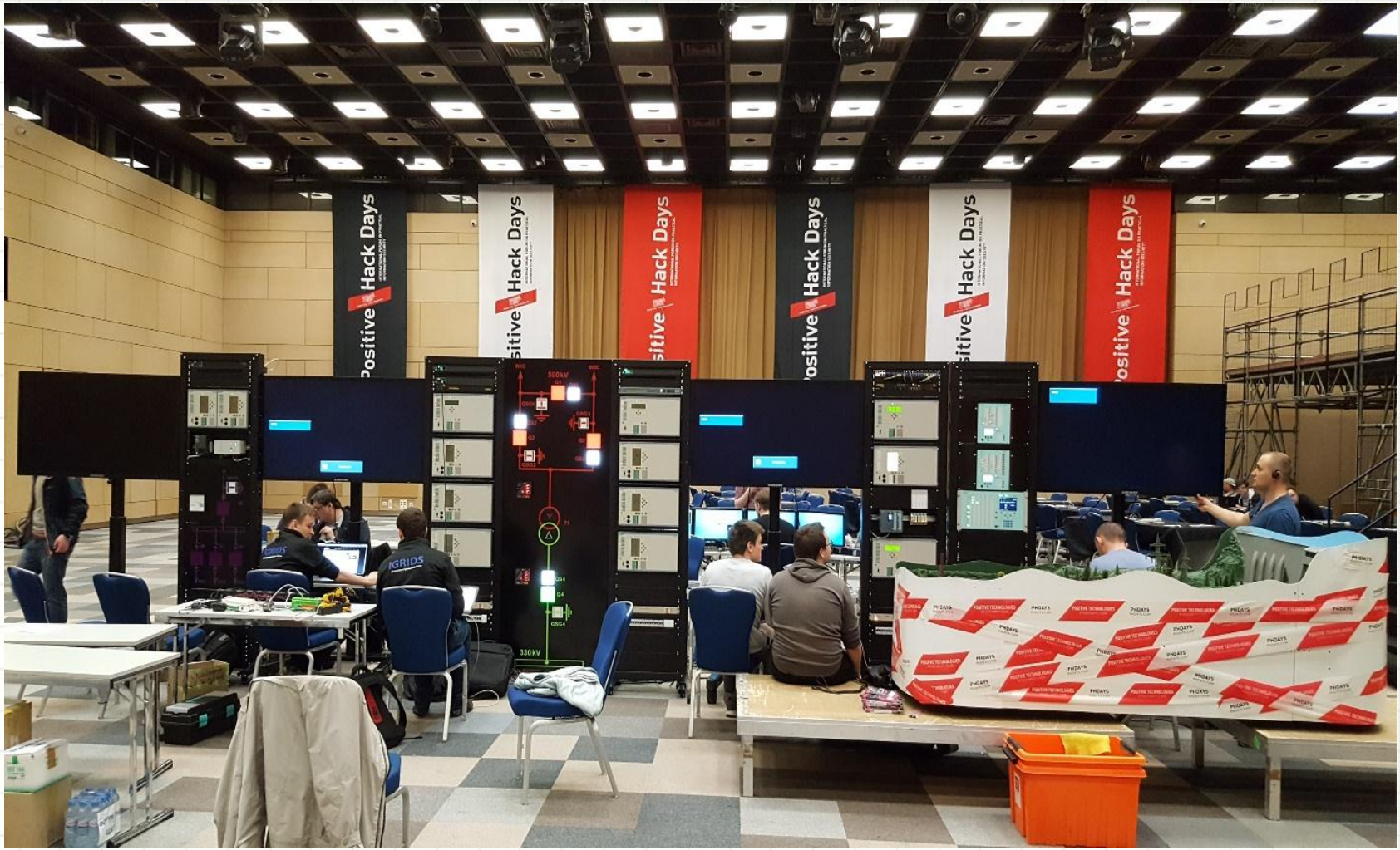
**Сценарий В (самый опасный):**

1. Прохождение маршрутизатора, подключение в локальную сеть стенда;
2. Проведение разведки для определения типа устройств;
3. Вывод из строя терминалов РЗА;
4. Подключение к контроллерам не легитимным клиентом MMS и подача команды на коммутационный аппарат для совершения короткого замыкания

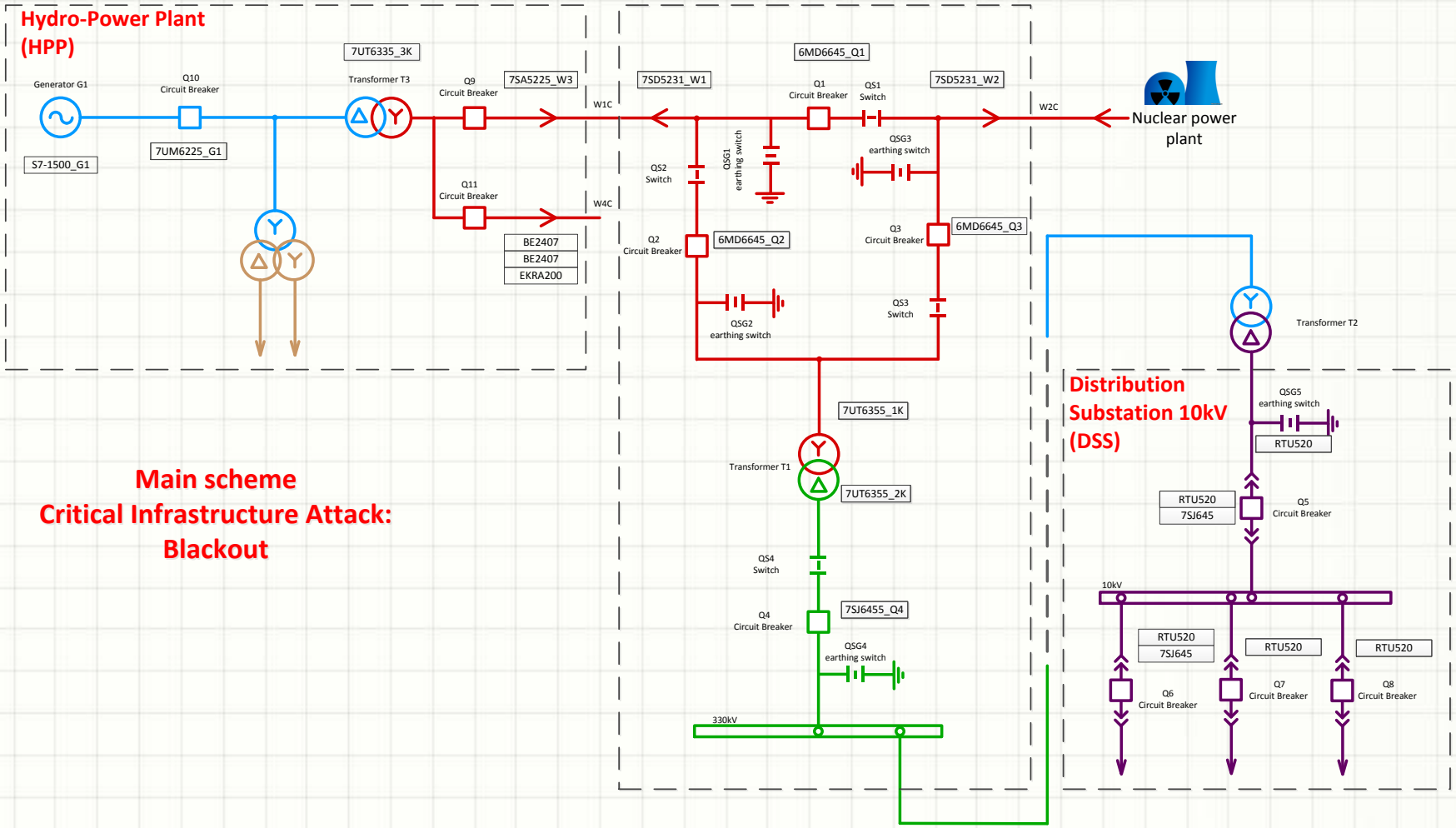
# Статистика команд по балам



# PHDays VI. The Standoff

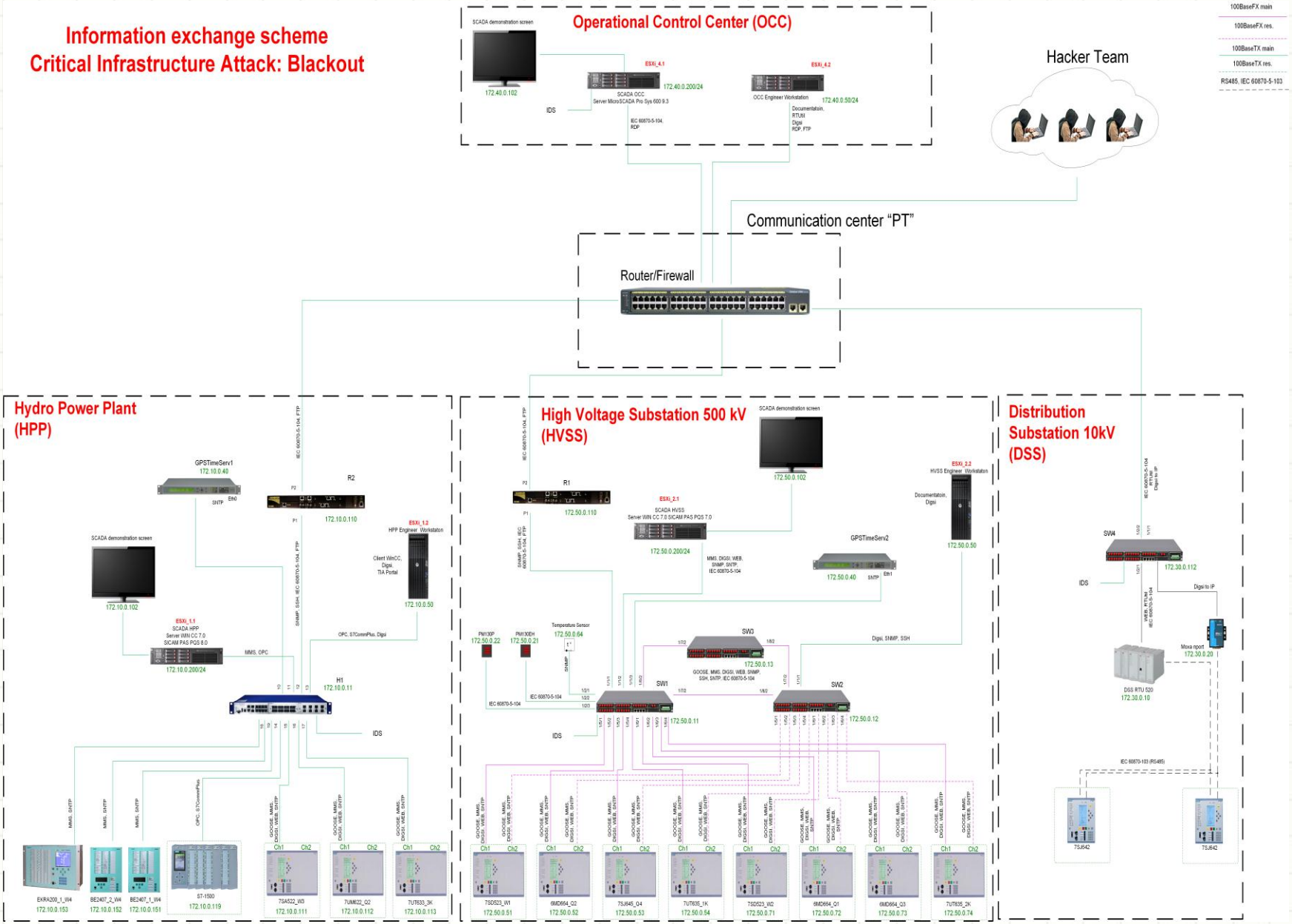



# Однолдинейная схема стенда




**Main scheme**
**Critical Infrastructure Attack: Blackout**

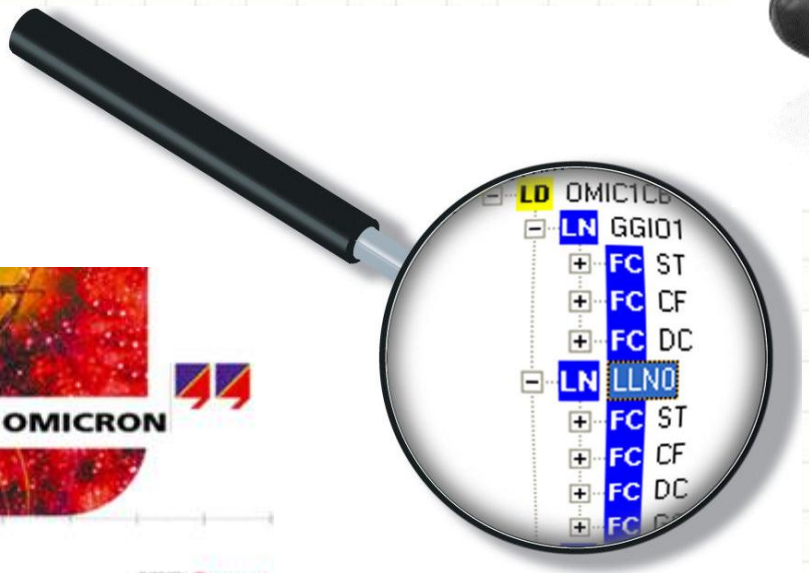
# Схема информационного обмена



# Особенность PHDays VI

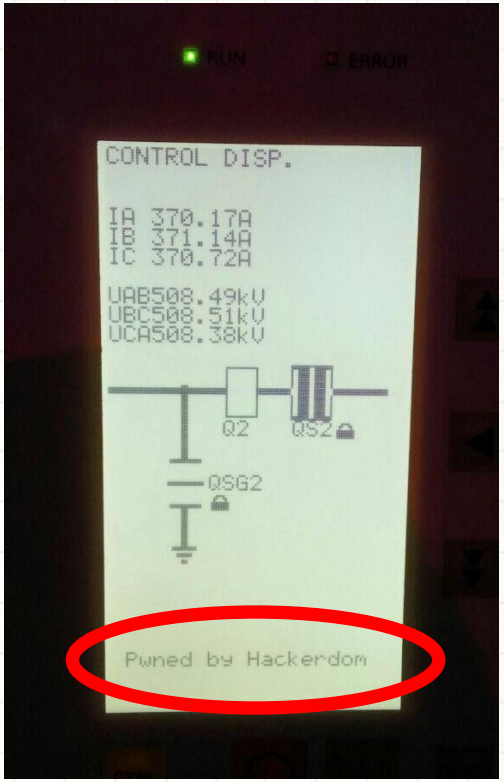

**Противостояние «Хакеров» и «Защитников»**

# «TEENAGER HACKS ELECTRICAL SUBSTATION AT PHDAYS»


**Из особенностей IEDScout можно отметить интуитивно понятный интерфейс и встроенный анализатор трафика с подробной расшифровкой информации...**

# Вскрытие пароля для конфигурирования РЗА



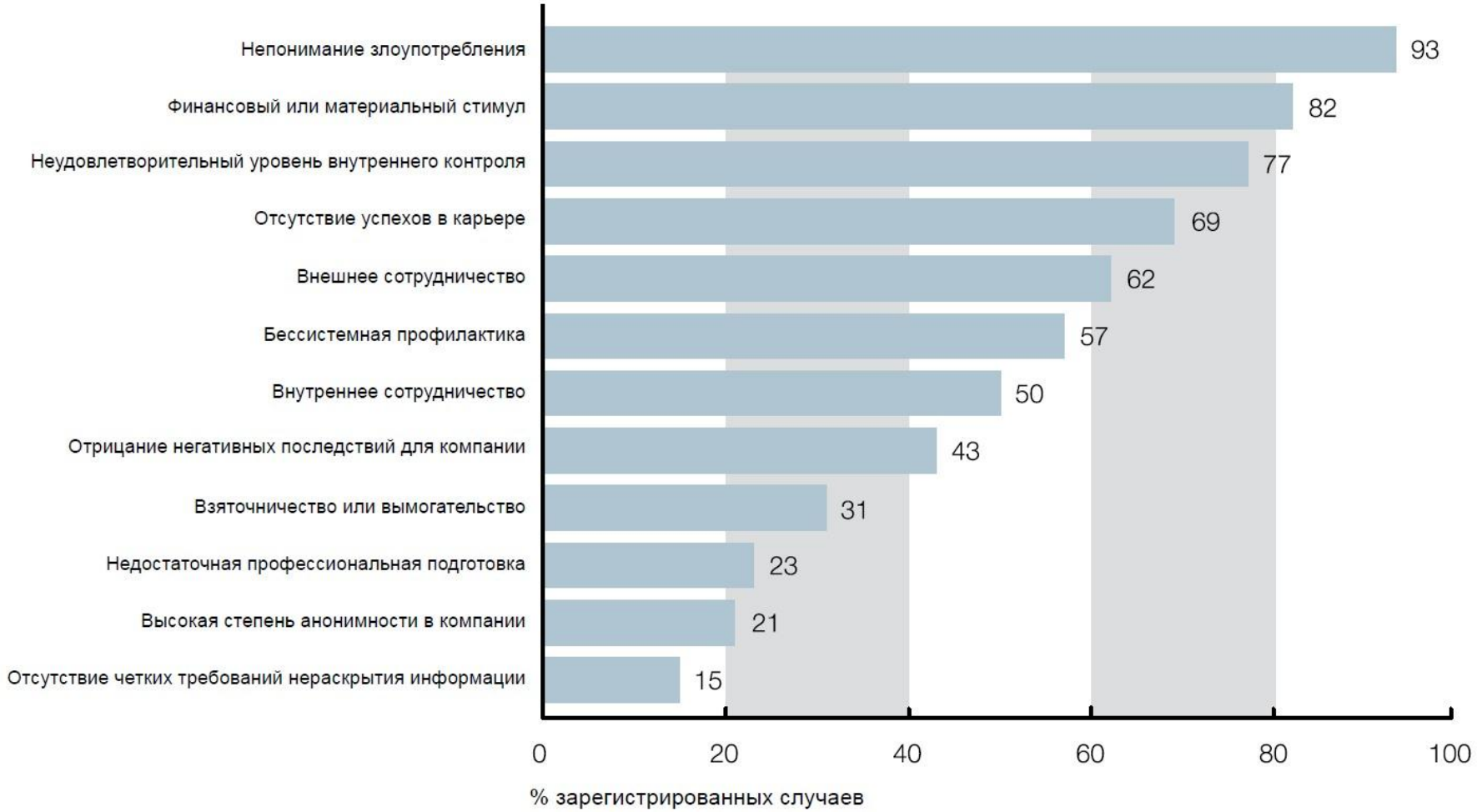

**Используя ранее не известную уязвимость МП РЗА команде «Хакердом» удалось устроить короткое замыкание в схеме имитируемого объекта.**

# Невидимая точка доступа

**Команде «Evil_Dwarfs» путем социального инжиниринга удалось подключить в локальную сеть ПС 500кВ (за защитным периметром) специально подготовленную точку удаленного доступа**


**До конца конкурса не легальное утройство не было обнаружено!!!**

# Мотивация внутренних нарушителей *




* SiFo-Studie 2009/10. Know-how-Schutz in Baden-Württemberg. Steinbeis-Edition Stuttgart, 2010 г.

# От кого больше вреда ?!?!

# Выводы

- **эффективно защитить электроэнергетический объект можно, но стоимость и трудоемкость защиты пока мало приемлемы;**
- **современные средства защиты «токсичны» по отношению к основному технологическому процессу, для работы на реальных объектах необходимы многосторонние проверки и тестирование на макетах, испытательных стендах;**
- **не обязательно досконально разбираться в технологическом процессе чтобы организовать атаку, достаточно информации из открытых источников и свободно распространяемого ПО;**
- **имеющиеся на сегодня в интеллектуальных устройствах (МП РЗА, контроллеры) встроенные средств защиты информации не позволяют эффективно противостоять угрозам ИБ. Необходимо их расширять и развивать.**

# Группа РНК СИГРЭ D2/B5

**«Кибербезопасность РЗА и систем управления современных объектов электроэнергетики»**

# Спасибо за внимание!

iGRIDS
Интеллектуальные Сети