DNV·GL

ЭНЕРГЕТИКА - СОВРЕМЕННЫЕ ПРОМЫШЛЕННЫЕ МЕТОДЫ - ИНТЕЛЛЕКТУАЛЬНЫЕ СЕТИ И КОММУНИКАЦИИ

# Текущие и будущие угрозы для устройств РЗА подстанций и сетевых объектов в энергетике и в мире автоматизации: векторы атак

**Г-жа Кимберли Лукин, старший консультант**

# Векторы атак  на подстанции с учетом архитектуры

1) Для удаленных подключений  на высоковольтных подстанциях используются стационарные подключения (не Wifi или GPRS): несанкционированный доступ возможен со стороны первичной подстанции.
2) Подключения по протоколам Wi-Fi / GPRS / LTE / ВЧ / GPS используются при эксплуатации подстанции средней мощности
3) В пределах подстанции ИЭУ подключены по волоконному или медному кабелю. не исключено, что на подстанции есть АРМ (локальный центр управления)
4) Большинство подстанций требуют модернизации! Пример одной из неназванных стран ЕС: 27 устройств в действующих цепях (трансформаторы, выключатели) требуют замены
5) Подключения к внешним сетям (например, к офисной  внутренней электронной сети - интранету)

6) ПС формируют важные каналы обмена информацией между генераторной станцией, системами передачи, системами распределения и точками потребления нагрузки, которые могут оказаться уязвимыми для атак

7) В отдельных случаях через каждые 4 километра монтируется соединительная коробка или точка подключения, через которую осуществляется маршрутизация (маршрутизатор или ретранслятор)

**Открытая публикация**

# Векторы атак на подстанции

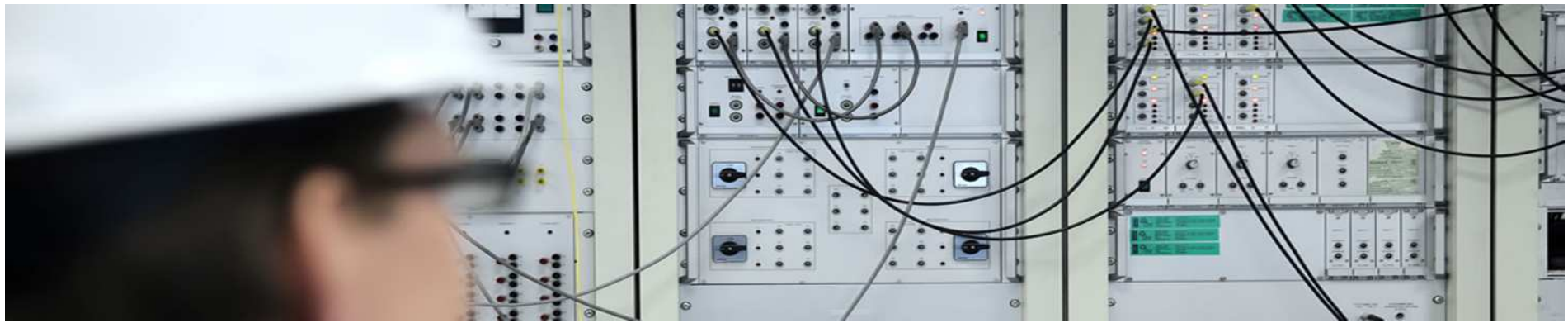
8) В некоторых случаях на старых подстанциях вместо ПЛК используются УОУ (удаленные оконечные устройства), эта ситуация чаще встречается в атомной энергетике.

9) В архаичных системах широко используются 4-х цифровые ПИН-коды доступа..

10) На уровне распределения они подкреплены резервными беспроводными устройствами или модемами.

11) В УОУ  используются беспроводные каналы связи или по модему (без защиты обратным вызовом) для организации дополнительного канала связи

12) На каждой подстанции установлено не менее 10 устройств с возможностью удаленного подключения: УОУ, ИЭУ, системы видеонаблюдения, локальные АРМ проектировщика, устройства регистрации нарушений и т.д.



# Векторы атак на подстанции

13) Инструмент конфигурации реле или FTP-соединение для изменения файлов конфигурации. Существует возможность удаления файла конфигурации или подключения к промежуточному инструменту

14) Архаичные подстанции используют собственные протоколы, более новые работают по протоколам TCP/IP и протоколы стандарта IEC

15) Отсутствие управления доступом

16) Большинство компьютеров с ОС Windows устарело, производители должны утверждать использование прошивок, любое внесение изменений в систему требует длительных согласований

17) Производительность аппаратных средства слишком низкая, чтобы поддерживать шифрование

# Векторы атак с учетом параметров программного обеспечения

- Невыявленные ошибки программного обеспечения, что приводит к эксплуатации энергообъекта по неверному алгоритму
- дефекты вредоносных программ, ПО встроенное в микропроцессор цифровой подстанции для противостояния отказам системы
- внешние кибер-атаки по цифровым каналам за счет перехвата каналов дистанционного управления или использования вредоносного кода в системе управления
- промахи эксплуатации и замена программного обеспечения
- отсутствие обновлений за весь срок эксплуатации устройства.
- коммерческое программное обеспечение

# Векторы атаки  по радиоканалам и каналам ВЧ

- Беспроводное подслушивание и считывание данных может иметь место практически во всех широко используемых беспроводных сетях, включая радио частоты, частоты работы спутникового телевидения, а также в диапазоне микроволнового излучения.
- Электронное подслушивание возможно прим эксплуатации всех средств обмена информацией путем перехвата или подключения к каналам связи.
- Все устройства на основе электрических принципов имеют «утечку» электромагнитных волн и являются источниками

электромагнитных помех

- Система СКАДА местных подстанций работает на

серверах с беспроводным подключением и выполняет

роль центра управления.

- Источники излучения:

✓печатные платы, кабели обогрева, провода и шины волны



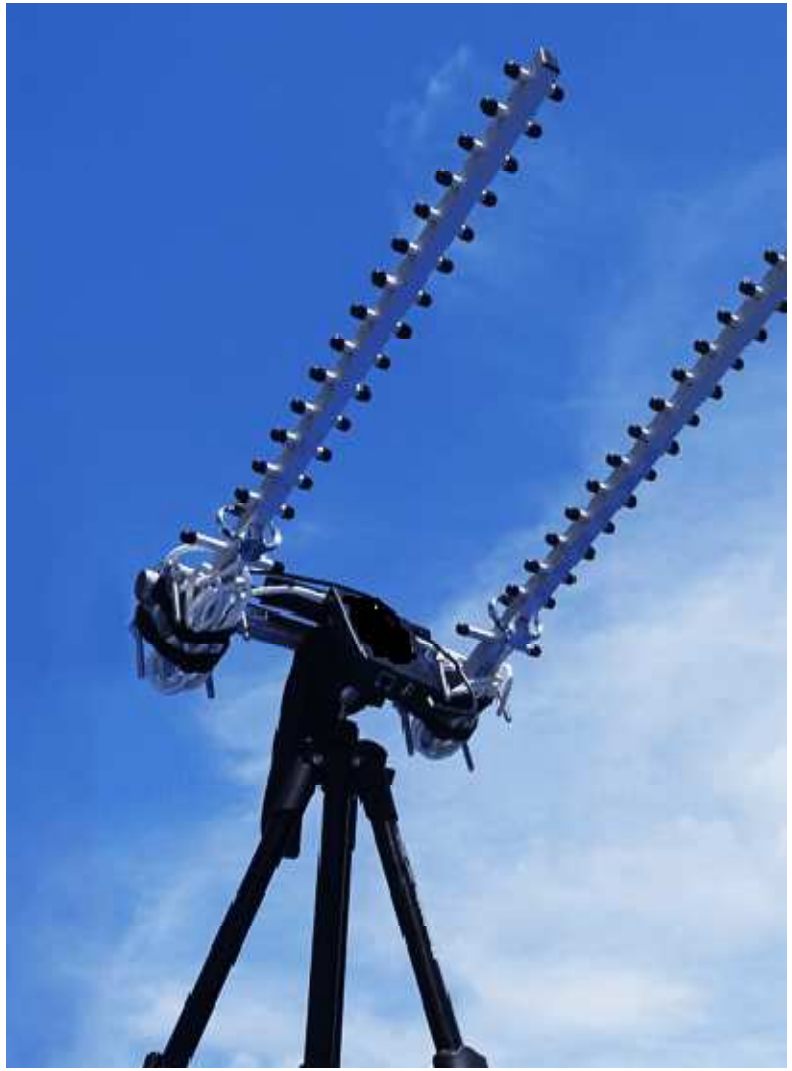
✓Экранированные корпуса являются источниками ЭМ

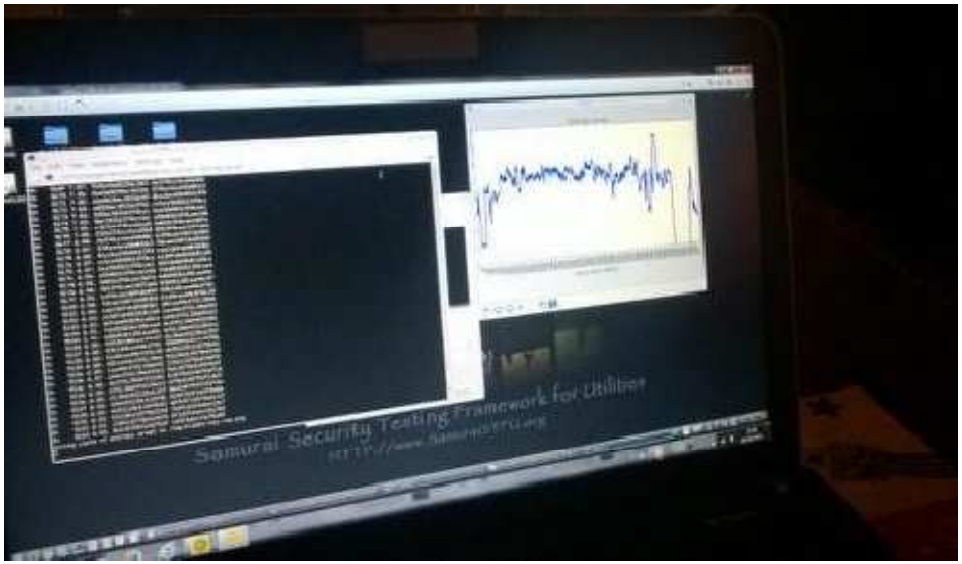
✓волн из зазоров, щелей и стыков ...

# Векторы атак с учетом инженерных решений на подстанциях

- Часто АРМ оснащено компьютером с ОС Windows
- Изменение фактической логики контроллеров
- Скачивание обновления ПО контроллеров через Интернет
- Не останавливает процесс, однако может его изменить
- Удаление логики инженерной безопасности
- Кража исходного кода ПЛК
- Получение доступа к встроенному аппаратному обеспечению

# Инструменты внешнего воздействия



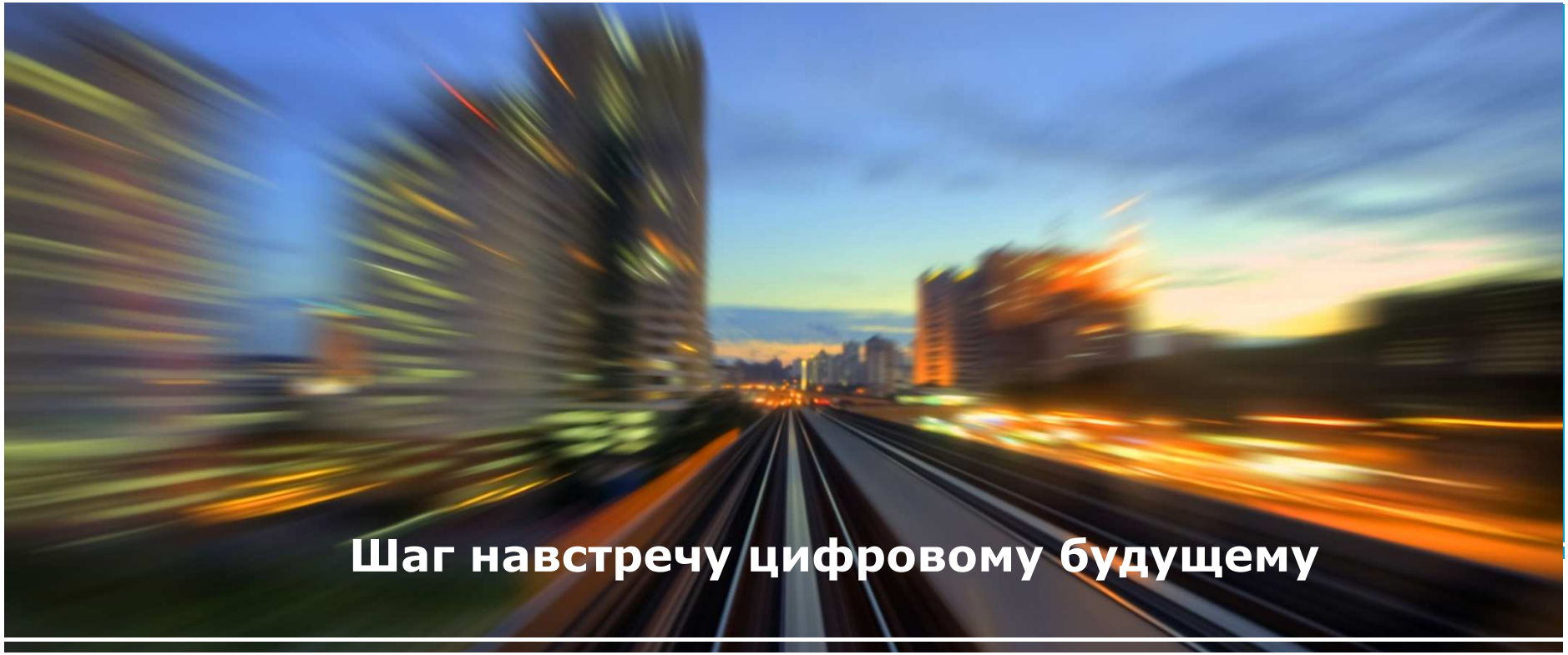

**Открытая публикация**

# Новые угрозы

- Взлом отдельно стоящей системы
- Для получения несанкционированного доступа к обособленной системе или для сбора информации (о рабочих частотах, номерах версий устройств, уязвимостях) могут использоваться  БЛА
- Беспилотники можно использовать для получения удаленного несанкционированного доступа, например, через системы на основе ОС Линукс или для целей глушения на известных рабочих частотах ..
- Дроны могут служить внешними базовыми станциями или "точками несанкционированного доступа"
- Беспилотники могут также нести оборудование для создания помех и перехвата сигналов

<u>Рабочие частоты:</u>

- Инженерные объекты работают в разных частотных диапазонах, которые требуется распознать (для составления диаграммы рабочих частот) для создания надежной защиты устройств от ЭМИ, атак по глушению; кроме того, необходимо разобраться на каких радиочастотах частотах и при каких параметрах электромагнитного поля возможно получить несанкционированный доступ к системе.



# Шаг навстречу цифровому будущему


**Контактная информация:**

Kimberly.Lukin@dnvgl.com

**www.dnvgl.com**

twitter @KimLukin


**SAFER, SMARTER, GREENER**