Роман Краснов

Руководитель направления информационной безопасности промышленных систем

Практический анализ кибербезопасности компонентов ЦПС .. и не только

Вчера, сегодня и завтра

POSITIVE TECHNOLOGIES

14:55 / 10 Апреля, 2018

Positive Technologies обнаружила опасные уязвимости в оборудовании Siemens для электроподстанций

POSITIVE TECHNOLOGIES

Теги: Positive Technologies, Siemens, АСУ ТП

Атакующие могли получить полный доступ к устройствам релейной защиты и автоматики, что чревато нарушениями в работе энергосистемы.

Эксперты Positive Technologies Илья Карпов, Дмитрий Скляров и Алексей Стенников выявили уязвимости высокого уровня риска в устройствах релейной защиты и автоматики (РЗиА) производства Siemens, которые используются для управления и защиты силового оборудования на электроэнергетических объектах (подстанции, ГЭС и др.). Siemens устранил уязвимости и выпустил соответствующие рекомендации.

Обнаруженным уязвимостям могут быть подвержены устройства SIPROTEC 4, SIPROTEC Compact и Reyrolle, использующие коммуникационный модуль EN100 и программное обеспечение DIGSI 4. Эксплуатируя эти уязвимости, злоумышленник может удаленно внести изменения в конфигурацию отдельно взятых устройств РЗиА, что может привести к отказу функции защиты силового оборудования (и потенциально к аварии) или отключению потребителей.

Наибольшая опасность связана с уязвимостью CVE-2018-4840 , которая может эксплуатироваться удаленно, при этом от злоумышленников не требуется высокий уровень квалификации. Механизм работы позволяет неаутентифицированному удаленному пользователю загружать модифицированную конфигурацию устройства посредством перезаписи авторизационных паролей доступа.

Решения по кибербезопасности АСУ ТП

POSITIVE TECHNOLOGIES

Сервисы

- Анализ защищенности
- Тест на проникновение

POSITIVE TECHNOLOGIES

PT ISIM

- Непрерывный мониторинг защищенности
- Поддержка основных платформ АСУ ТП
- Нулевое влияние на технологическую сеть
- Эффективное управление инцидентами ИБ
- Оперативный анализ бизнес-рисков
- Распределенная архитектура (SOC)

Главная задача нашей работы по анализу защищенности

POSITIVE TECHNOLOGIES

~~Найти максимальное количество уязвимостей~~

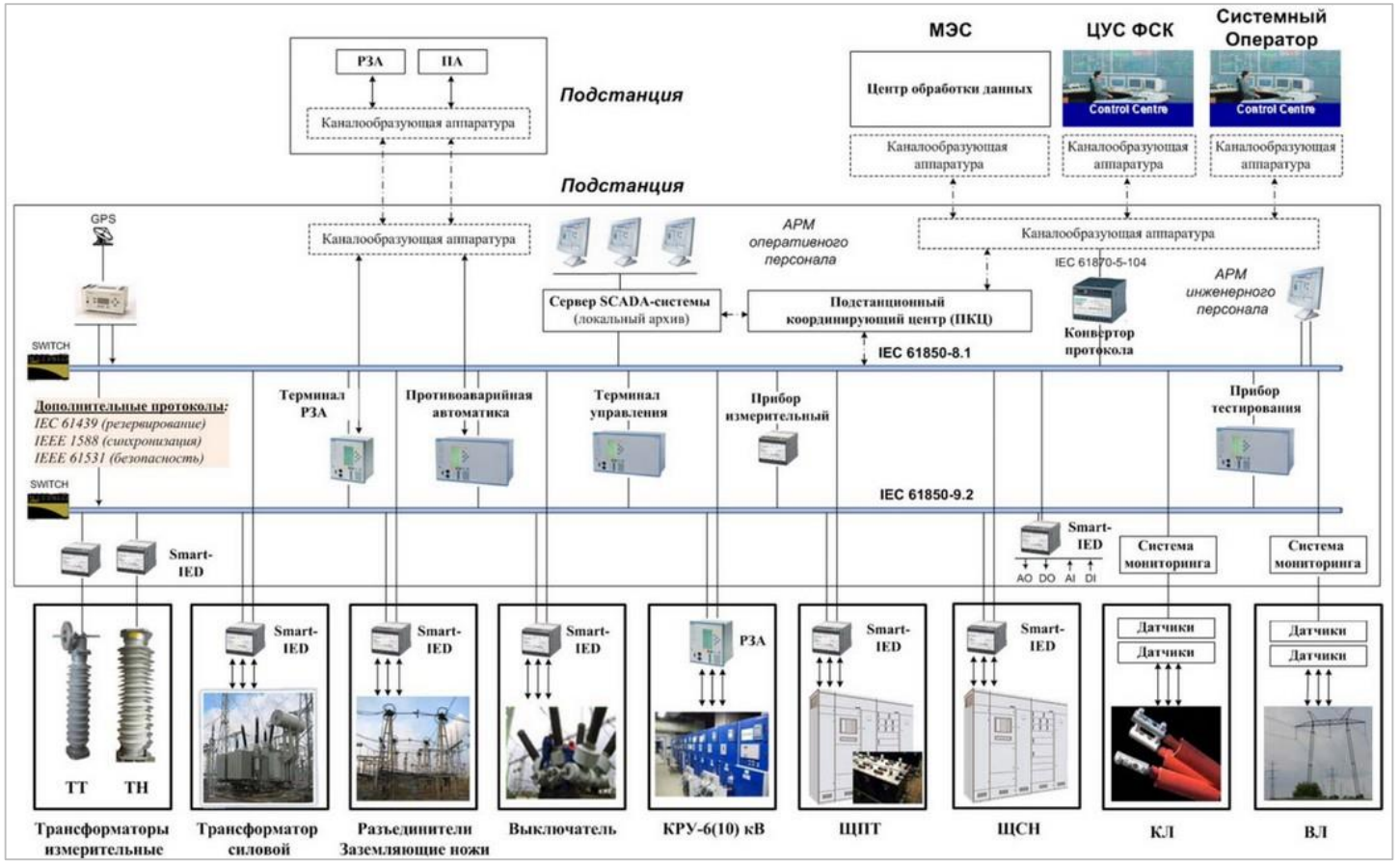
Выявить пути негативного влияния на техпроцесс:

- Создание условий аварийной ситуации (обход блокировок, защит и так далее)
- Остановка элементов и всего техпроцесса (чаще всего это DoS)
- Внесение изменений в штатную работу (изменение параметров и уставок)

Типовые объекты анализа

POSITIVE TECHNOLOGIES

- **Нижний уровень**
- **ПЛК / РЗА**
  - Каждый модуль
  - Интерфейсы (eth, com, …)
  - Firmware / Прошивка
  - Проект
- **Устройства коммутации сети**
- **Серверы + АРМ-ы**
- **Другие узлы в сети**
  - Принтеры
  - UPS
  - …



Взгляд на каждый и все компоненты сразу

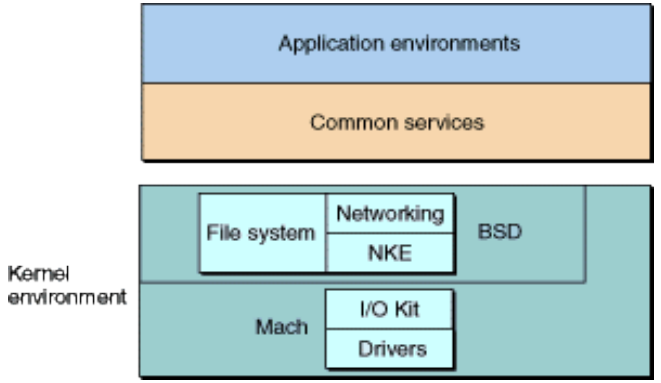
POSITIVE TECHNOLOGIES

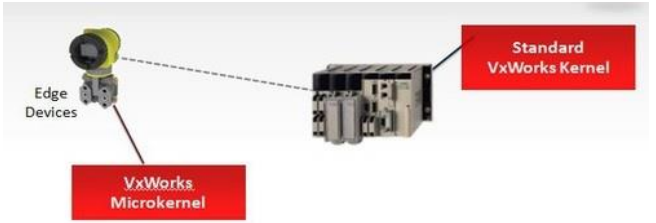
Рассматриваем каждое устройство

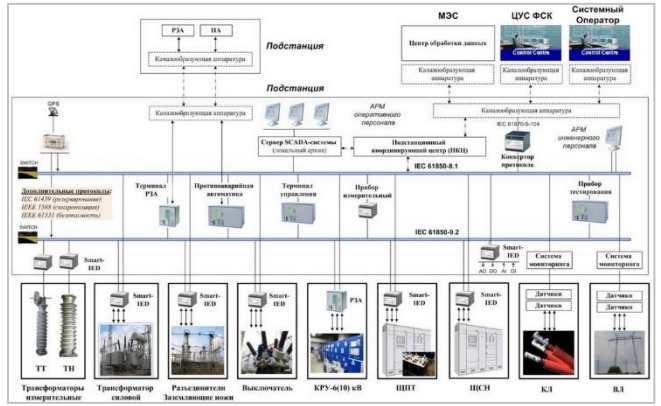
1. **Как отдельную сущность**
   - Аппаратная платформа
   - Аппаратные интерфейсы (порты)
   - Файловая система и её содержимое
   - Прошивка / Firmware
     - Операционная система
     - ПО
     - Конфигурация ОС и ПО
     - Используемые сетевые протоколы и службы

2. **Как устройство в сети**

3. **Как компонент АСУ ТП**







Зачем нужны эти знания об исследуемом объекте?

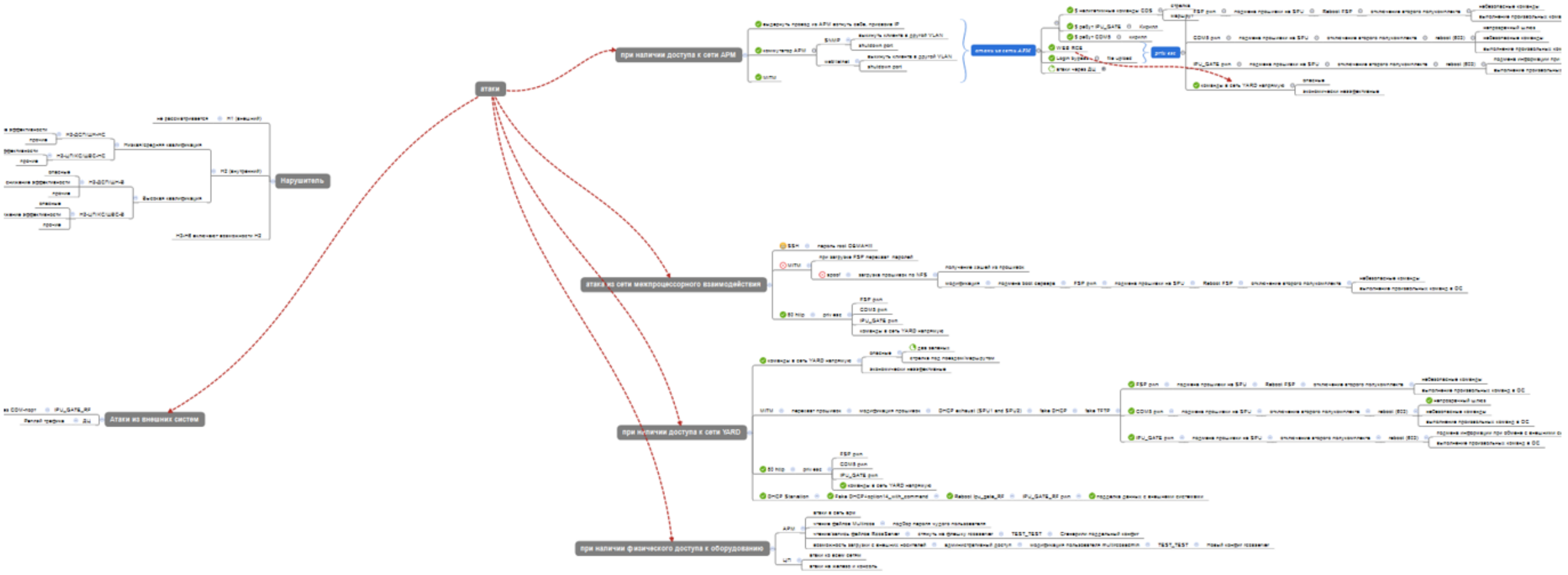
POSITIVE TECHNOLOGIES

На выходе подобного детального анализа получаем:

- Уязвимости и недостатки каждого устройства информационной системы (ИС)
- Понимание сетевого взаимодействия в ИС
- Понимание того, как устроен конкретный техпроцесс и чего он боится

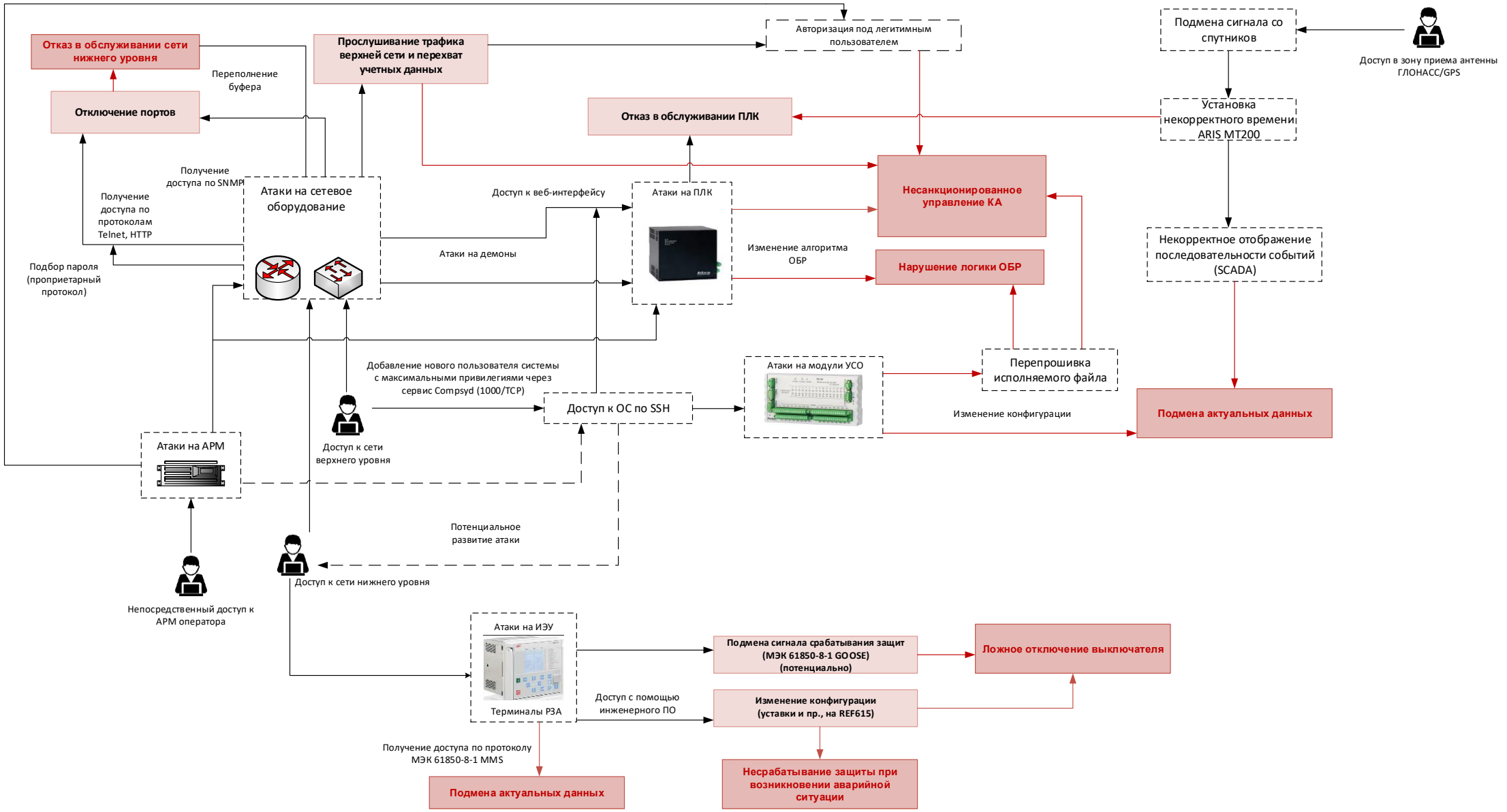
Строим вектора атак: через возможности к страшному

POSITIVE TECHNOLOGIES



Вектора атак для типовой подстанции

POSITIVE TECHNOLOGIES



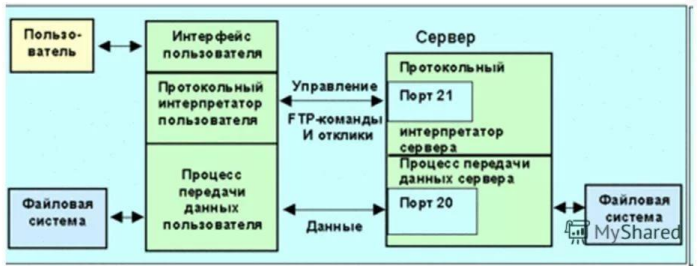
Что может дать изучение прошивки ПЛК (РЗА)

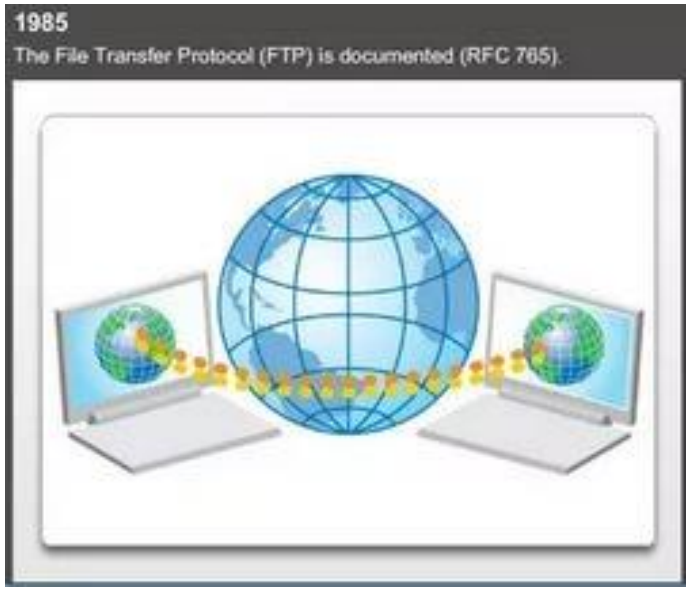
POSITIVE TECHNOLOGIES

Протокол FTP

FTP (англ. File Transfer Protocol — протокол передачи файлов) — протокол, предназначенный для передачи файлов в компьютерных сетях.

FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер.



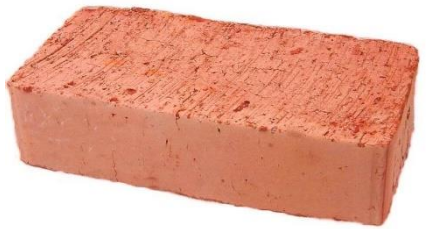


Пример: «Deutsch FTP von Schneider Electric»

REBOOT
FORMAT
BURNKER

Зачем нужна полезная команда «FORMAT»?

POSITIVE TECHNOLOGIES



Schneider PLC

FTP-команда **FORMAT**

Результат

Почему всё это плохо

- Вы об этом не знаете (пока мы вам об этом не расскажем)
- Это невозможно отключить
- Вероятно, это уязвимость «навсегда»

Примеры атак на элементы ЦПС и цели атакующего

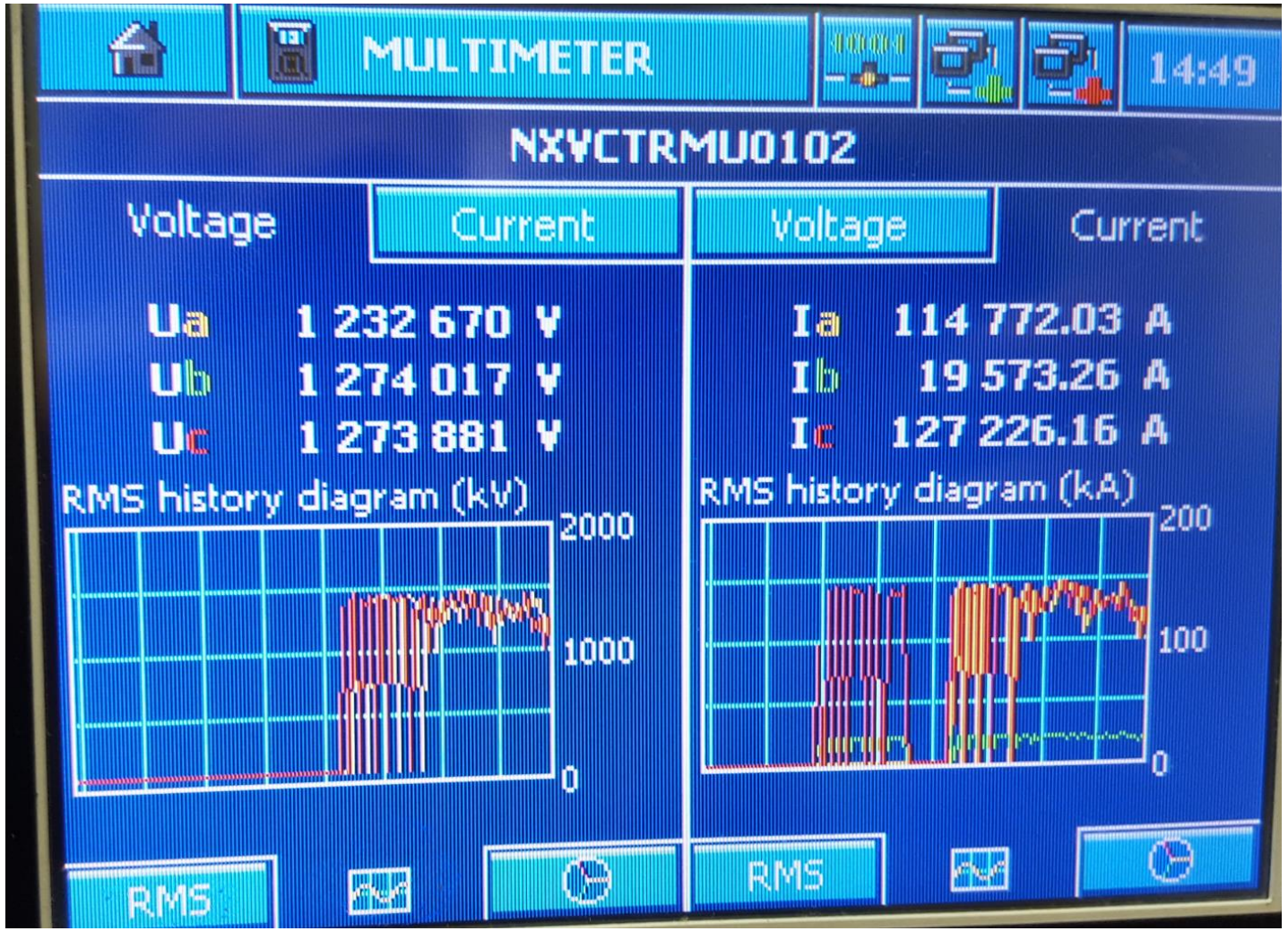
POSITIVE TECHNOLOGIES

– Несанкционированное управление выключателями (коммутационными аппаратами)

– Выведение атакуемой компьютерной сети и её элементов из строя с целью нарушения штатного режима работы цифровой подстанции.

Подмена данных SV-потока на ПС 110 кВ

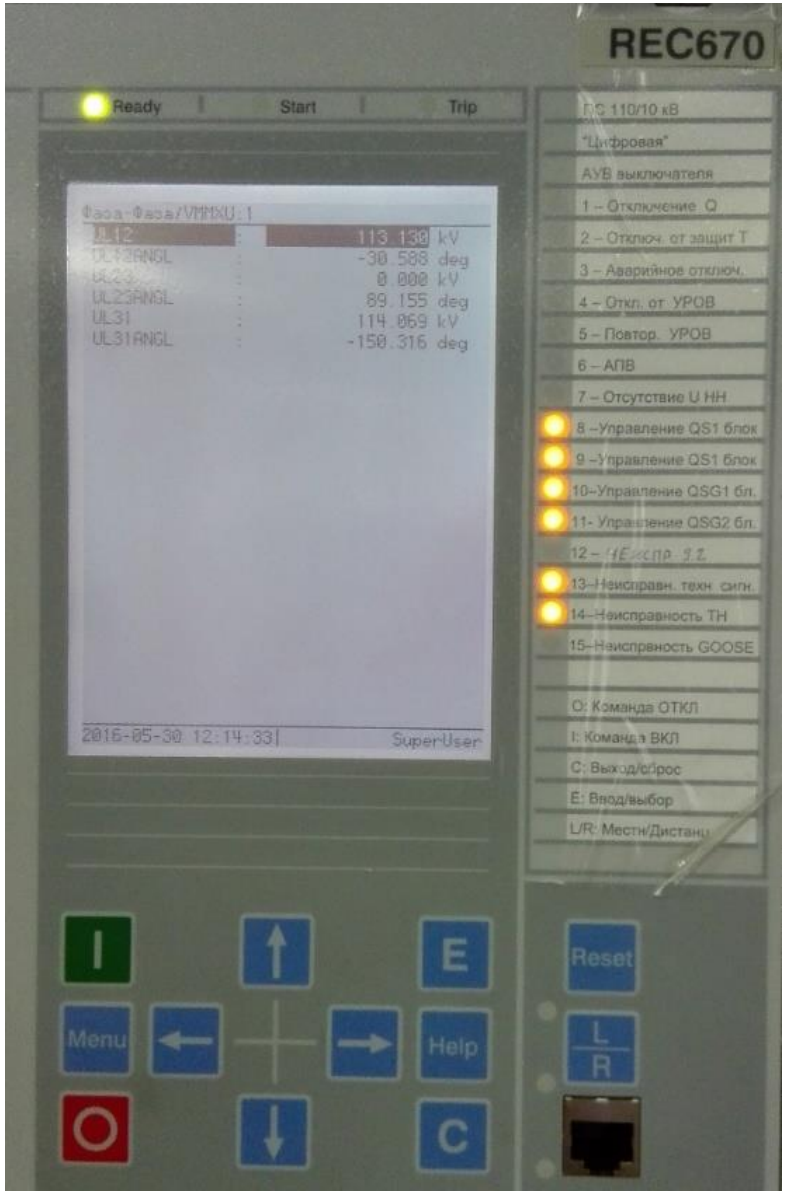
POSITIVE TECHNOLOGIES



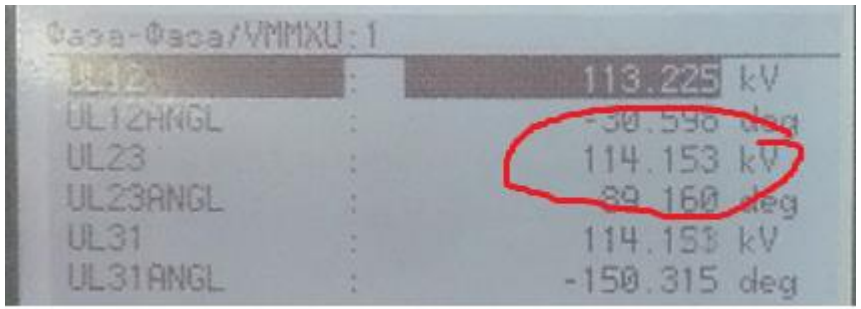
Подмена значения параметра «UL23» на устройстве РЗА

POSITIVE TECHNOLOGIES

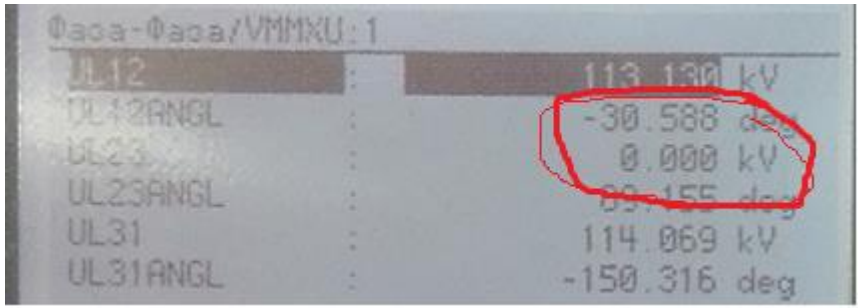
Была выполнена отправка команды на замещение значения измерения напряжения на устройстве REC670



Истинные значения



Подделанные значения



Спасибо за внимание!

Роман Краснов, rkrasnov@ptsecurity.com

POSITIVE TECHNOLOGIES