Проблемы обеспечения информационной безопасности в системах промышленной автоматизации

ООО «ИНСАЙД РУС»

Александр Крутиков

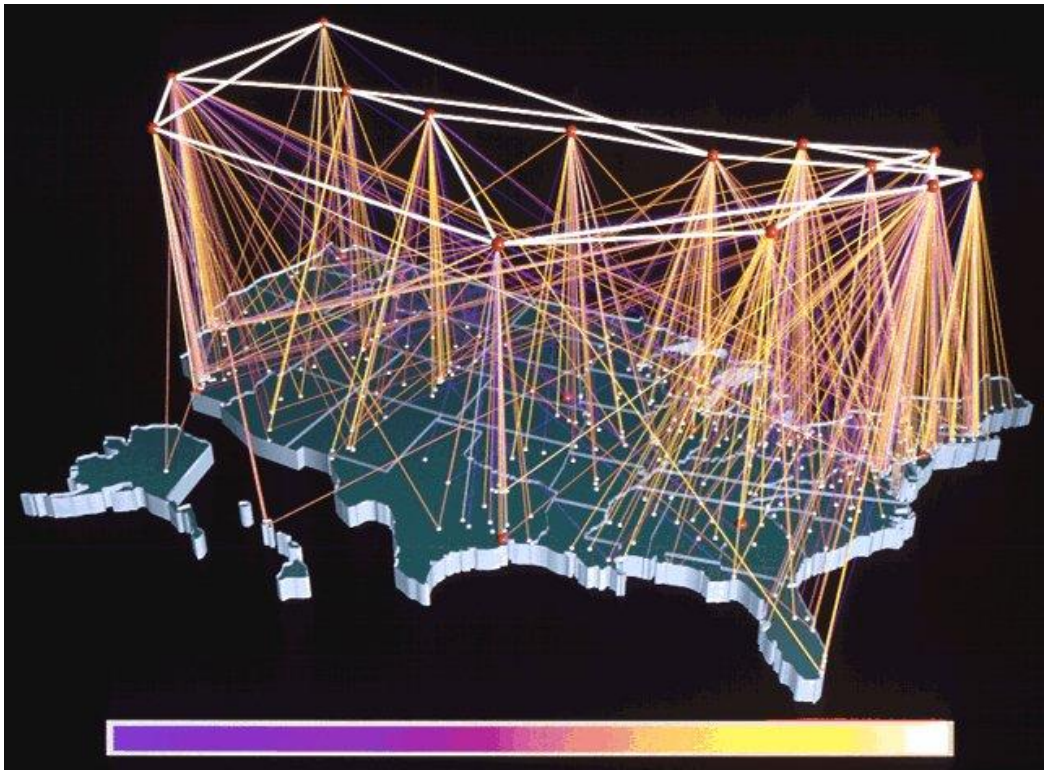
Руководитель направления

Промышленная автоматизация сегодня

- Использование сложных компьютеризированных систем и комплексов
- Широкое распространение удаленной диспетчеризации
- Резкий рост объема собираемой и контролируемой информации
- Рост числа M2M соединений
- Использование беспроводных технологий
- Использование стандартных протоколов: TCP/IP и подобных

Глобализация систем автоматизации

- Выход за пределы одного предприятия
- Создание и развитие сетей городского и национального уровня
- Использование стандартных каналов связи
- Следствие: те же проблемы, что и в «классической» информационной безопасности



Угрозы

- Вирусы, в том числе и «специализированные»
- Нарушение конфиденциальности
- Подмена данных
- Саботаж, несанкционированное воздействие
- Инсайдерская угроза

Как защитить SCADA?

- **Обеспечить:**
  - **уверенность в подключение «правильных» устройств к системе**
  - **целостность и неизменяемость передаваемых данных**
  - **надежный режим разграничения доступа к системе и ее компонентам**
  - **удобство применения средств ИБ с учетом индустриальных требований**

Средства ИБ и SCADA – конфликт интересов?

Средства ИБ:

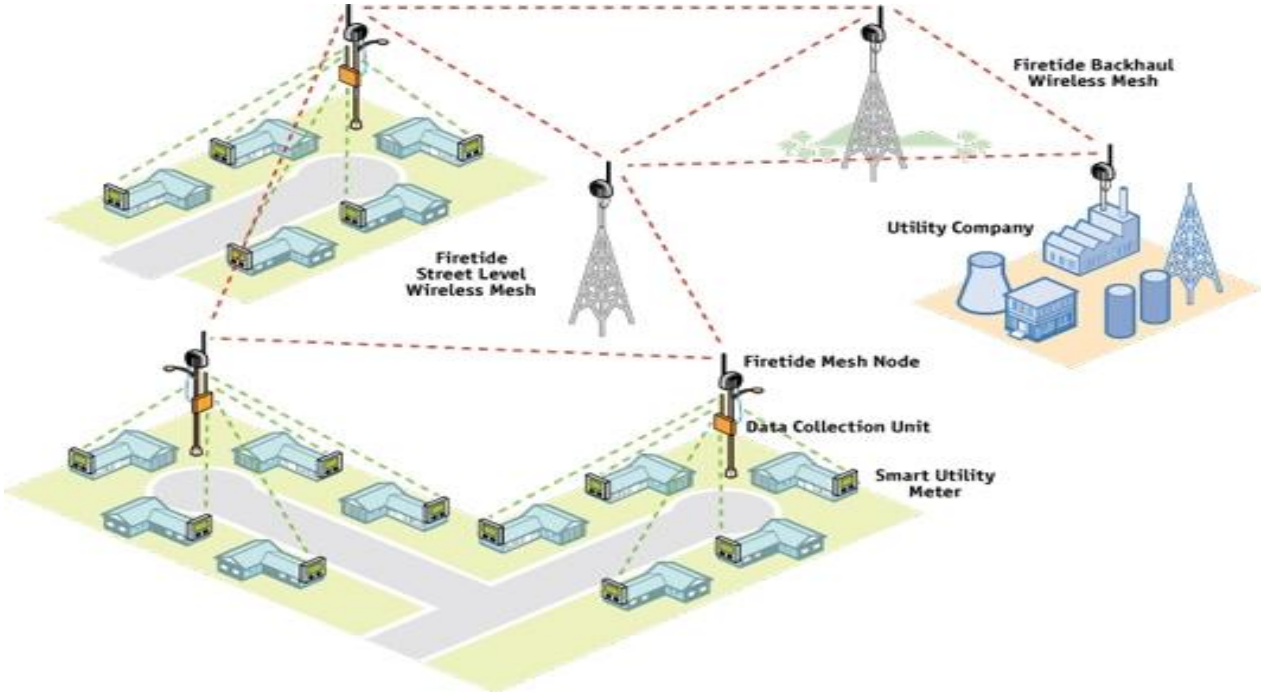
- **Ориентация на пользователя ПК:**
- **Гегемония USB**
- **Использование ПК-интерфейсов и стандартов**
- **Слабая возможность адаптации к конкретной задаче**

SCADA:

- **Работа с протоколами «низкого» уровня**
- **Широкое использование микроконтроллеров и «легких» цифровых систем**
- **Коммуникации M2M**
- **Индустриальные требования к системам и компонентам**

Шаги на встречу SCADA

- **Open Smart Grid Protocol**
- **Универсальный модуль безопасности «ИНСАЙД РУС. ГОСТ»**



«ИНСАЙД РУС. ГОСТ»: функционально законченное решение

- Средства загрузки и генерации ключей
- Средства поддержки PKI
- Поддержка функционирования в терминальных устройствах
- Поддержка разработок пользователя
- Широкие возможности адаптации к конкретным задачам

«ИНСАЙД РУС. ГОСТ»: международные стандарты

- **Соответствие международным стандартам:**
  - ISO 7816-3 (протоколы T=0 и T=1)
  - ISO 7816-4 (внутреннее устройство и команды)
  - ISO 7816-8 (криптография)
  - ISO 7816-9 (жизненный цикл)

«ИНСАЙД РУС. ГОСТ»: стандарты криптографии

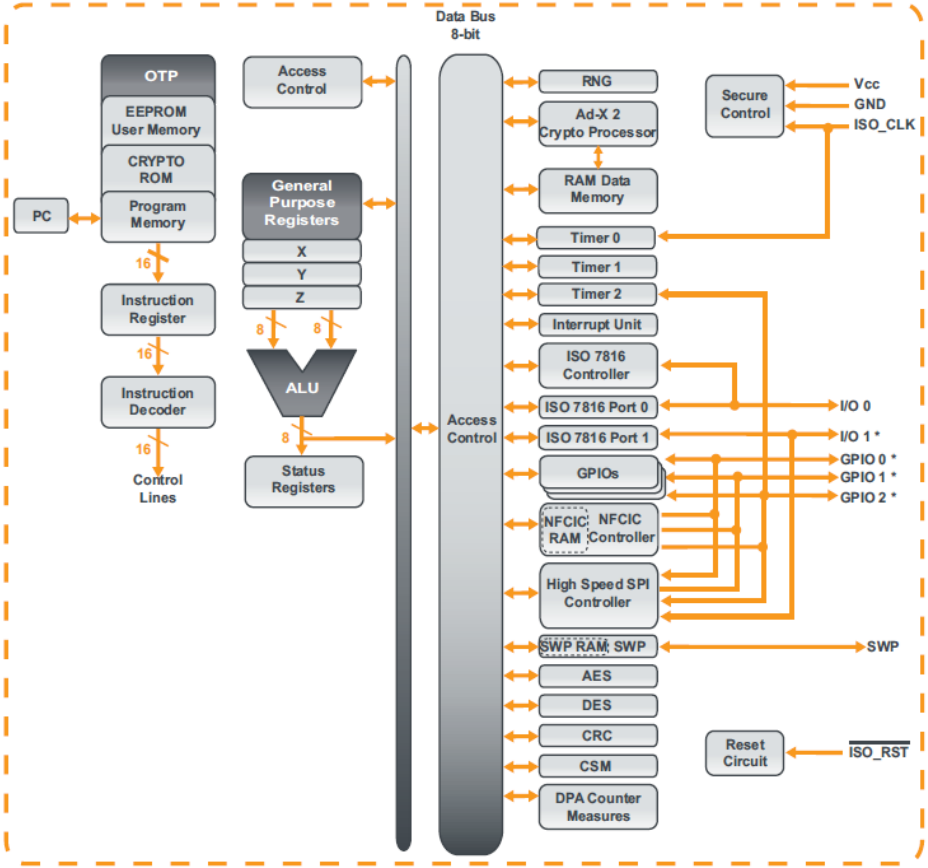
- ГОСТ 28147-89 (шифрование, имитовставка, аутентификация, защищенный обмен сообщениями, генерация сессионного ключа)
- ГОСТ Р34.11-94 (ХЭШ-функция)
- ГОСТ Р34.11-2012 (ХЭШ-функция)
- ГОСТ Р34.10-2001 (выработка и проверка ЭЦП, аутентификация, выработка ключевой пары, генерация сессионного ключа)
- ГОСТ Р34.10-2012 (выработка и проверка ЭЦП, аутентификация, выработка ключевой пары, генерация сессионного ключа)
- DES / 3DES (аутентификация, шифрование, MAC, защищенный обмен сообщениями)
- SHA-1
- RSA (выработка и проверка ЭЦП, аутентификация, выработка ключевой пары (1024/2048), генерация сессионного ключа)

«ИНСАЙД РУС. ГОСТ»: комплексное решение для промышленности

- Загрузка и генерация ключевой пары по ГОСТ Р34.10-2001 с возможностью выгрузки открытого ключа
- Загрузка и генерация ключевой пары по ГОСТ Р34.10-2012 с возможностью выгрузки открытого ключа
- Формирование и проверка Электронной Подписи (ЭП) по ГОСТ Р34.10-2001
- Формирование и проверка Электронной Подписи (ЭП) по ГОСТ Р34.10-2012
- Шифрование и расшифрование данных по ГОСТ 28147-89
- Выработка и проверка имитовставки по ГОСТ 28147-89
- Хеширование по ГОСТ Р34.11-94
- Хеширование по ГОСТ Р34.11-2012
- Взаимная аутентификации с выработкой сеансового ключа в соответствии со спецификацией RFC4357
- Хранение данных

«ИНСАЙД РУС. ГОСТ»: на базе МК IS AT90SC104104CV

- **Защищенный МК Inside Secure AT90SC104104CV:**
  - 8/16 RISC архитектура
  - 104 Kb Flash
  - 104 Kb EEPROM
  - Криптоакслератор Ad-X
  - Расширенная защита от физических атак
  - Интерфейсы ISO-7816
  - Сертификаты:
    - CC EAL5+
    - EMVCo



«ИНСАЙД РУС. ГОСТ»: для российскойй промышленности

- **На базе:**
  - ОС «Магистра»
  - МК Inside Secure AT90CS104104CV
- **Сборка на российских аттестованных**
- **36 Кбайт для размещения прикладных данных**
- **Варианты поставки:**
  - Смарт-карта
  - SOIC8
  - QNF44
- **Готов к сертификации**

«ИНСАЙД РУС. ГОСТ»: производительность

- **По результатам тестирования:**
  - ГОСТ 28147-89 (ECB): 1286.786128 bytes/sec
  - ГОСТ Р 34.11-94: 1774.796853 bytes/sec
  - ГОСТ 34.11.2012: 339.233766 bytes/sec
  - Генерация ключевой пары:
    - ГОСТ Р 34.10-2001: 0.707900 sec/key
    - ГОСТ Р 34.10-2012: 1.203200 sec/key
  - Расчет цифровой подписи:
    - ГОСТ Р 34.10-2001: 0.278200 sec/ds
    - ГОСТ Р 34.10-2012: 0.787600 sec/ds
  - Проверка цифровой подписи:
    - ГОСТ Р 34.10-2001: 0.353100 sec/ds
    - ГОСТ Р 34.10-2012: 1.306300 sec/ds

СПАСИБО ЗА ВНИМАНИЕ!

Александр Крутиков

Руководитель направления

ООО "Инсайд РУС"

kao@inside-rus.ru

тел. +7-812-331-0967