НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
НЕОБИТ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ АСУ ТП ПУТЕМ ОБНАРУЖЕНИЯ И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

конференция
РусКрипто'2013

http://www.ruscrypto.ru/conference/

Москвин Д.А.

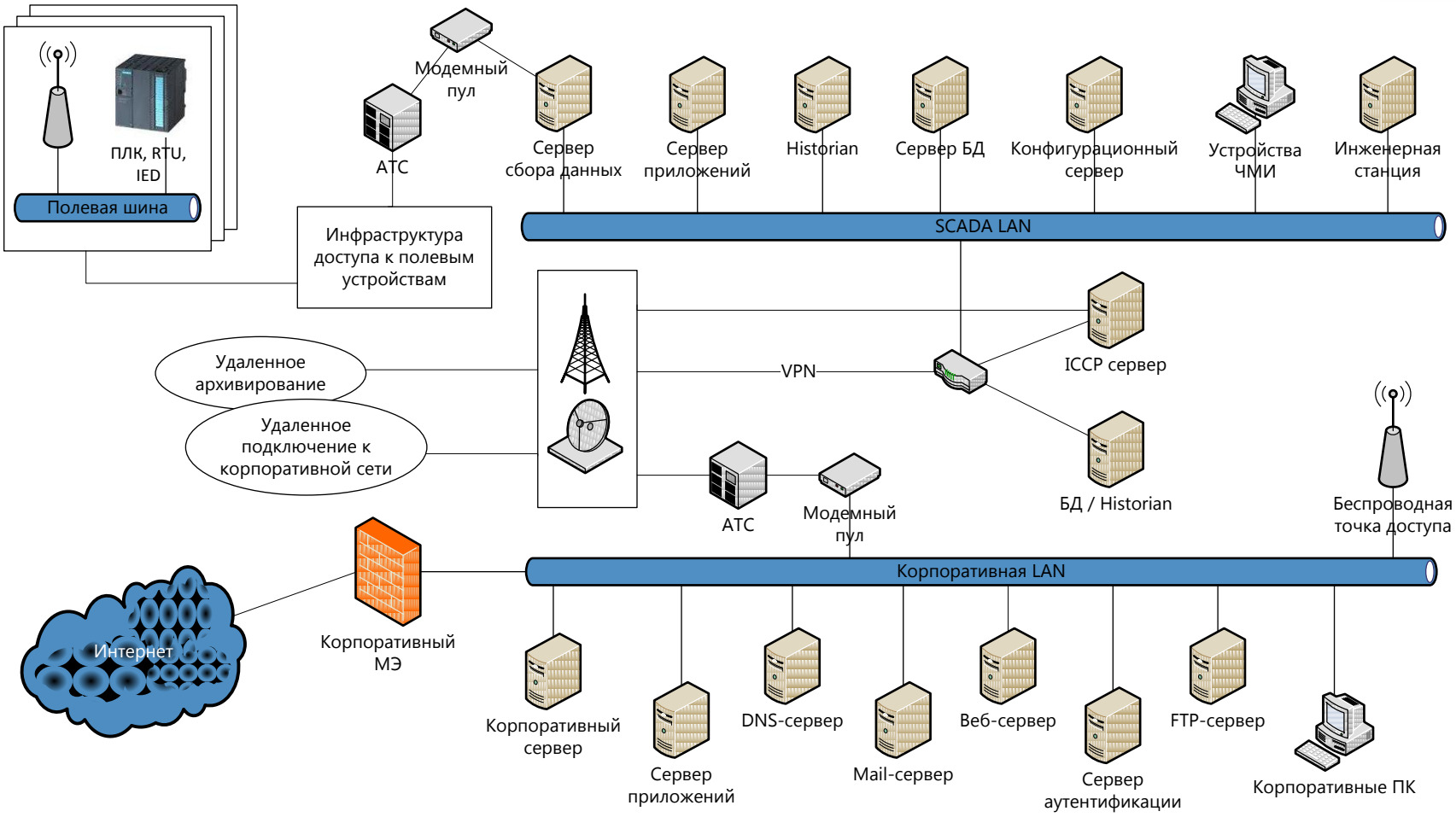
Определение

АСУ ТП – человеко-машинная система управления, обеспечивающая автоматизированный сбор и обработку информации, необходимой для оптимизации управления технологическим объектом в соответствии с принятым критерием.

Функции АСУ ТП:
- управляющие
- информационные
- вспомогательные

SCADA-система – это программная составляющая РСУ / ПАЗ

Типовая архитектура АСУ ТП



Стандарты обеспечения безопасности АСУ ТП

NIST SP800-82 «Guide to Industrial Control Systems (ICS) Security» (проект)

IEEE 1402 «IEEE Guide for Electric Power Substation Physical and Electronic Security»

API Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries

Security Guidelines for the Natural Gas Industry

API Security Guidelines for the Petroleum Industry

IEC 62351 «Data and Communication Security»

NIST PCSRF Security Capabilities Profile for Industrial Control Systems

Guidance for Addressing Cyber Security in the Chemical Industry

American Gas Association (AGA) 12 Cryptographic Protection of SCADA Communications (4 части)

NERC

American Petroleum Institute (API) 1164 «SCADA Security»

ISA SP99

IEC 61784-4

КСИИ ФСТЭК

Cisco SAFE for PCN

Стандарты Газпрома

IEC 62210 «Initial Report from IEC TC 57 ad-hoc WG06 on Data and Communication Security»

FERC Security Standards for Electric Market Participants (SSEMP)

Специфика обеспечения безопасности АСУ ТП и SCADA-систем

Распределенность компонентов и гетерогенность (неоднородность) информационной и программной составляющей

Географическая удаленность объектов информатизации и управления

Активное влияние человеческого фактора, усиленного фактором критичности управляемого объекта или технологии промышленного цикла

Отсутствие универсального подхода, "заточенность" решения под конкретную задачу управления определенным технологическим процессом или производством

Типовые проблемы безопасности АСУ ТП

- Ошибки в ПО автоматического управления
- Ошибки в задании системной конфигурации
- Уязвимости сред передачи данных, позволяющие осуществить несанкционированное подключение к каналу передачи данных
- Уязвимости управляющих сетевых протоколов, позволяющие осуществить перенаправление пакетов на другой хост сети
- Отсутствие необходимой физической защиты каналов передачи данных

Модели негативного программного воздействия на АСУ ТП

s7otbxdx.dll

s7blk_read

Блок кода STL

Скачивание проекта для ПЛК (Duqu?)

Модификация проекта для ПЛК (Stuxnet) + спуфинг

Поиск и эксплуатация уязвимостей

VNC (Simatic), RDP (Citect, inTouch), …

Keylogger + запись сессии удаленного рабочего стола (chaosrecorder)

Классификация угроз безопасности АСУ ТП

- По используемым типам уязвимостей
  - Организационные
  - Конфигурации
  - Программные
  - Периметра сети
  - Систем связи
- По типу последствий
  - Раскрытие информации
  - Отказ в обслуживании
  - Отказ в доступе
  - Отказ в управлении
  - Отказ в представлении
  - Подмена представления
- По объекту угрозы
  - SCADA
  - ПЛК
  - Инфраструктура и ОС
  - Транспортные протоколы

Сценарий пентеста

Выявление компонентов АСУ ТП

Идентификация компонентов АСУ ТП

Выявление уязвимостей компонентов АСУ ТП

Эксплуатация уязвимостей

Модификация системы обеспечения безопасности АСУ ТП

Этапы пентеста

Пассивная разведка

- Whois
- Shodan, Google, Eripp

Получение доступа к интерфейсам оператора

- Панель оператора SCADA
- Web-интерфейс контроллера

Сканирование подсети

- Идентификация оборудования и ПО
- Сканирование на уязвимости
- Проникновение в локальную сеть

Прослушивание и анализ трафика

Перехват управления контроллерами

- Использование уязвимостей
- Атака «человек посередине»

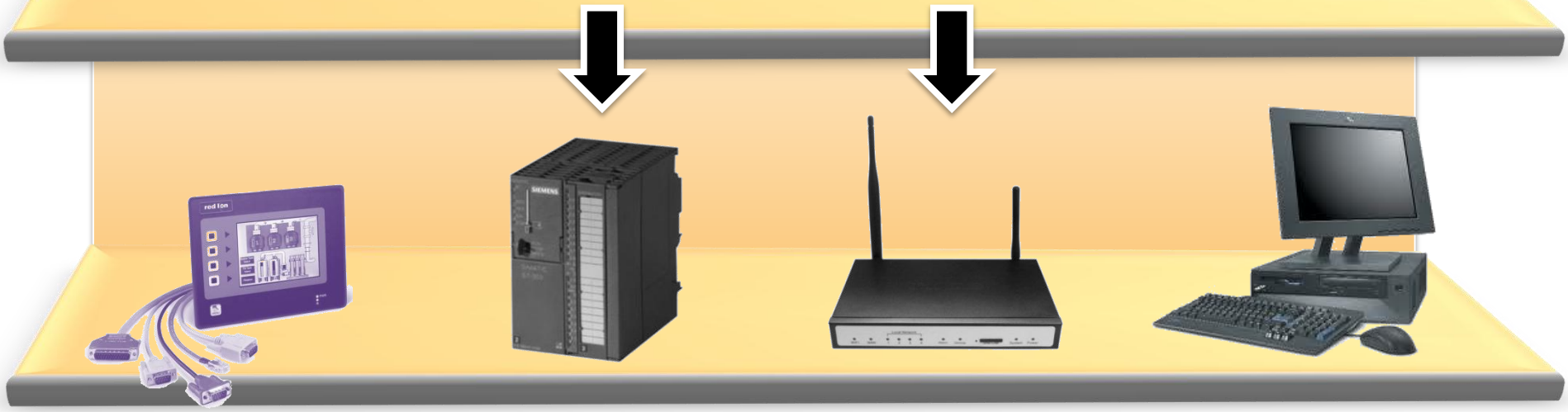
Объекты поиска в сети Интернет

Функциональные сервера

FTP-сервера

Веб-сервера

Устройства с поддержкой SNMP



Операторские панели

ПЛК

Маршрутизаторы

ПК

Пассивная разведка

Whois

- Определение диапазона IP-адресов подсети
- Геопривязка

Shodan

- Идентификация оборудования подсети
- Анализ баннеров

Резу

HMI

Comment

---- -------

Workgroup Master

--------- -------

PLC

TELEMECANIQUE BMX NOR 0200 REV015(Modicon M340 Ethernet 1 Port 10/100 RJ45

Доступ к интерфейсам оператора

К панели оператора SCADA

- Доступ по VNC – пустой пароль

К Web-интерфейсу контроллера

- Пустой логин/пароль для гостевого входа

Сканирование подсети

Использование nmap

- Информация о топологии сети
- Детализация оборудования
- Выявление сервера обработки данных на Windows Server 2003

Использование Nessus и SCADA plugins

- Уязвимость в Windows Server 2003 сервера обработки данных
- Уязвимости в ПО контроллеров (Schneider Modicon Ladder Logic Upload/Download; Schneider Modicon Remote START/STOP Command)

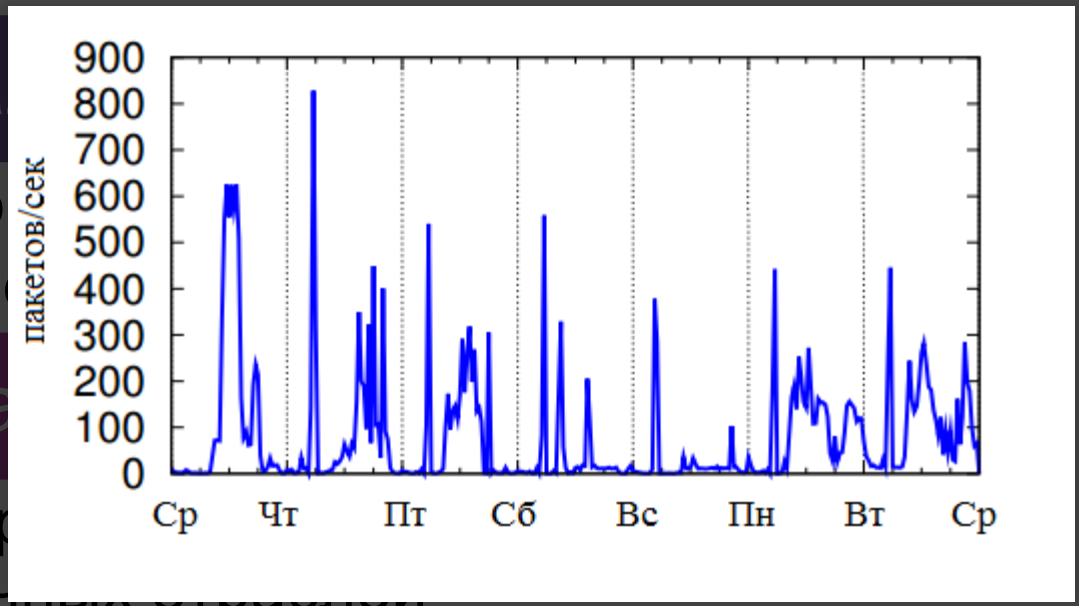
Анализ сетевого трафика

Сигнатурный ана

- Определение прото
- Заголовки протокол

Статистический а

- Шаблоны типового р
предприятий различ



Анализ информационных полей

- Анализ тэгов modbus (уровень воды, средняя температура, работа фильтров и др.)

Перехват управления контроллером

Команда RECV [0x5a 0x33, 0x34, 0x35]

Проект ПЛК

Команда STOP [0x5a 0x41]

Команда SEND [0x5a 0x30, 0x31, 0x32]

Проект ПЛК

ПЛК Modicon

Команда RUN [0x5a 0x40]

Функция 0x90 [Modbus] выполняется без аутентификации

Наиболее уязвимые компоненты АСУ ТП

Содержат проект управления / диагностики ТП. Обычно без таблиц символов и комментариев.

Содержат или имеют доступ к проекту ЧМИ.

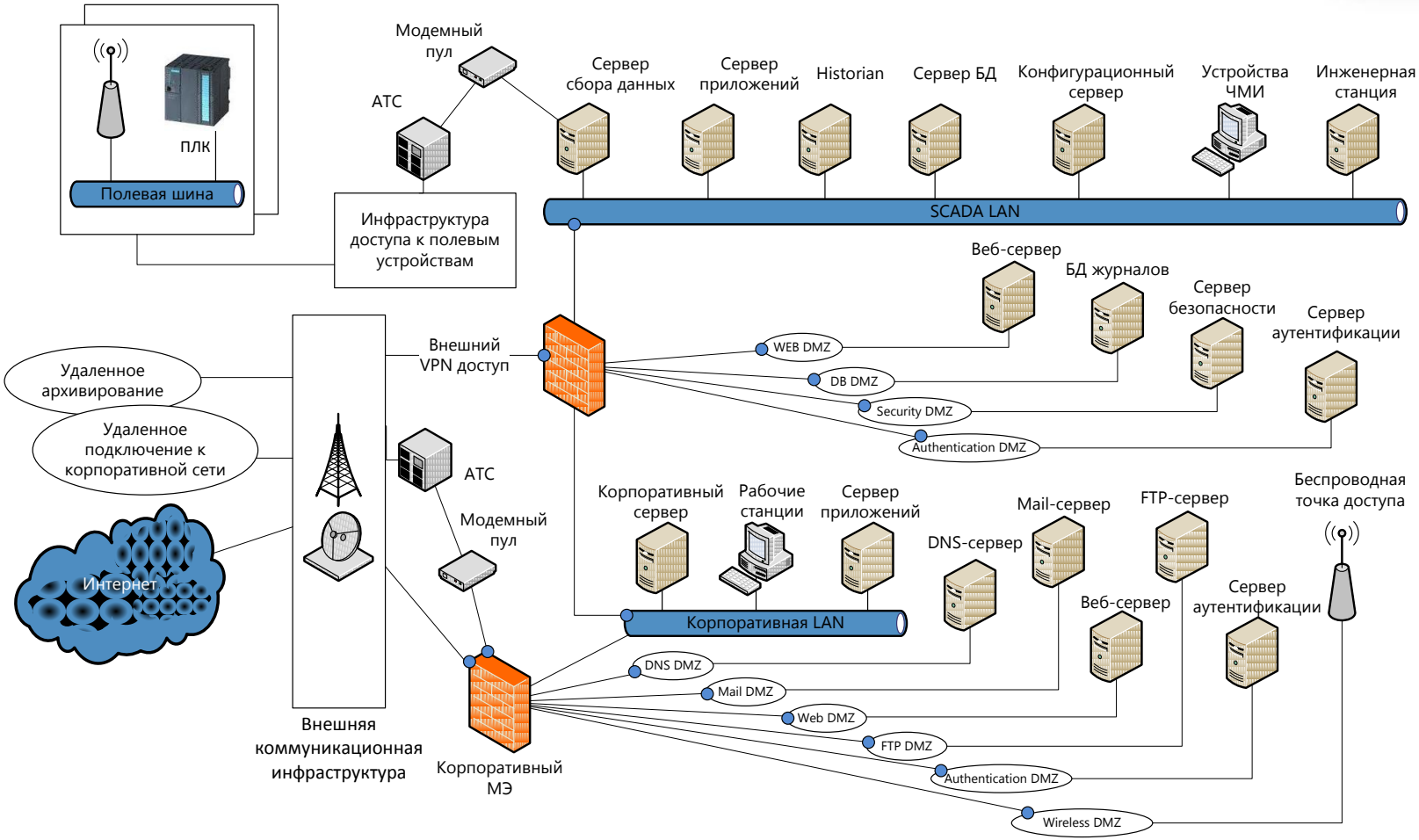
Содержат проект управления / диагностики ТП. Имеют доступ к управляемым устройствам.

ПЛК

Операторская панель

Инженерная станция

Многоуровневая архитектура защиты АСУ ТП




НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
НЕОБИТ