Технические требования к механизмам ИБ встроенных в интеллектуальные устройства

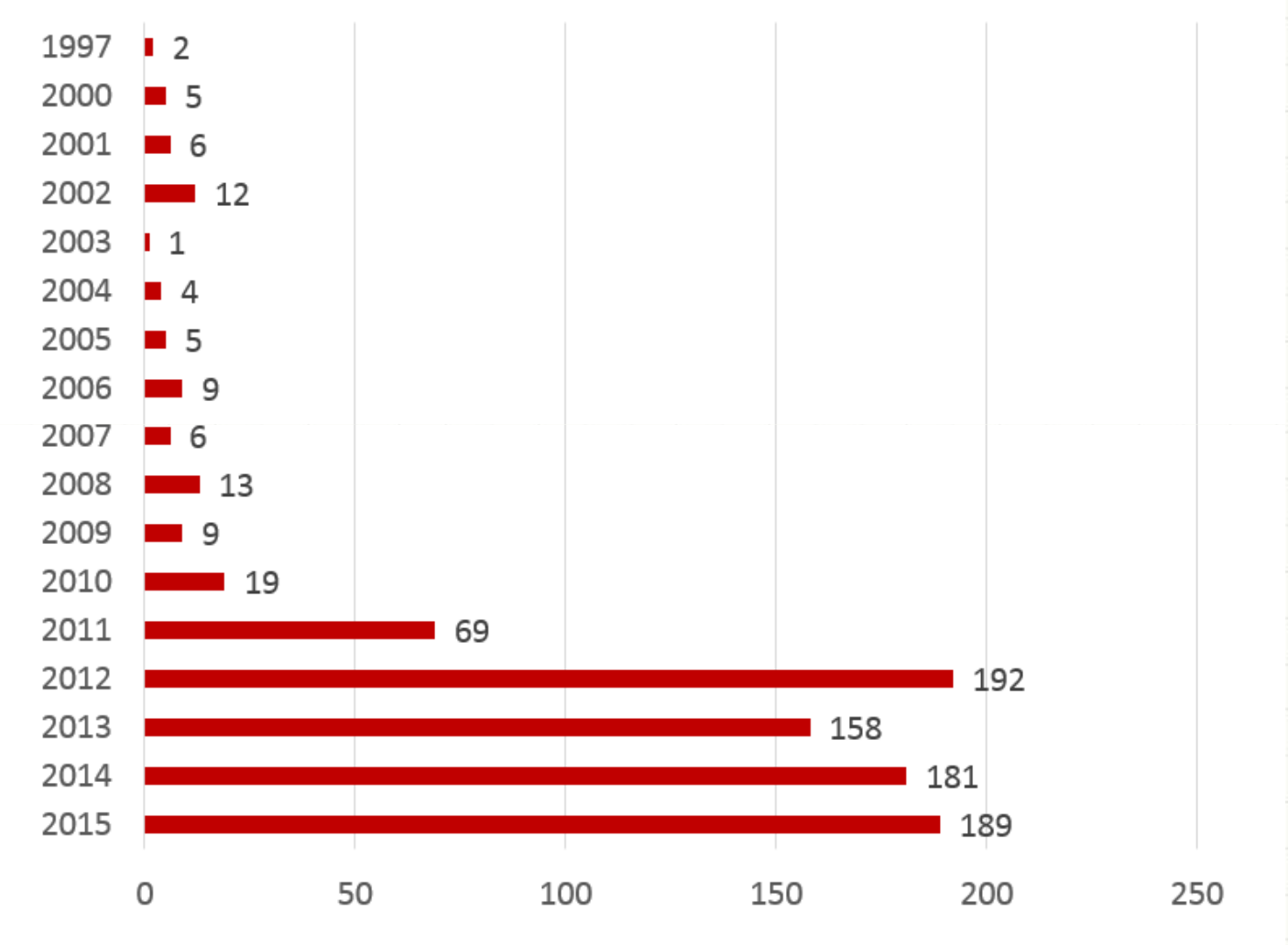
Никандров М.В.

IGRIDS
Интеллектуальные Сети

1. Текущая ситуация в области ИБ электроэнергетики

iGRIDS
Интеллектуальные Сети

Рост количества найденных уязвимостей в АСУ ТП



Positive Technologies «Безопасность АСУ ТП в цифрах, 2016 г.»

1. Текущая ситуация в области ИБ Электроэнергетики

Не удовлетворительная парольная политика

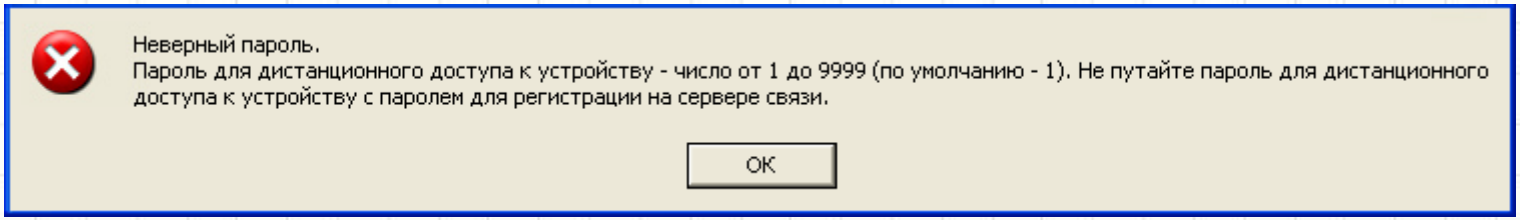
ВНИМАНИЕ!

ДО ИЗУЧЕНИЯ НАСТОЯЩЕГО РУКОВОДСТВА ПО ЭКСПЛУАТАЦИИ

ТЕРМИНАЛ **НЕ ВКЛЮЧАТЬ!**

Код (пароль), вводимый при операциях:

Запись уставок	**1**
Полная очистка электронного диска (карты памяти)	**2816**
Балансировка и настройка АЦП	**7892**



Пароль терминала - пароль терминала предназначен для ограничения доступа к уставкам и параметрам терминала через последовательный канал связи. Пароль представляет собой число от 0 до 9999. Заводским значением пароля является число 1. При установке пароля в значение 0 изменение уставок и параметров через последовательный канал связи становится невозможным;

Пароли по умолчанию собираются и используются

09:20 / 28 Декабря, 2015

Опубликован список логинов и паролей по умолчанию для SCADA-систем

Теги: SCADA, кибербезопасность, пароль

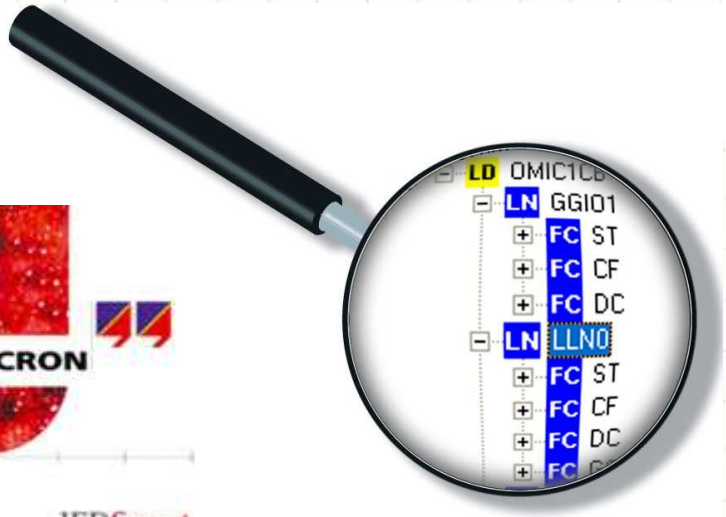
Группа ИБ-специалистов опубликовала учетные данные устройств 37 производителей SCADA-систем.

Группа исследователей безопасности SCADA StrangeLove опубликовала на GitHub список логинов и паролей по умолчанию SCADA-систем 37 производителей. Об этом специалисты сообщили в блоге StrangeLove.

Выпуск списка логинов и паролей приурочен к проводимому ежегодно Всемирному конгрессу хакеров (Chaos Communication Congress).

http://www.securitylab.ru/news/477999.php

«TEENAGER HACKS ELECTRICAL SUBSTATION AT PHDAYS»



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

Текущие проблемы ИБ для терминалов защиты

- **Не удовлетворительная парольная политика на изменение конфигурации;**
- **Пароли хранятся в открытом виде и легко доступны удаленно (CVE-2016-4785);**
- **Предустановленные заводские пароли «суперпользователя»**
- **Уязвимости приводящие к удаленному выводу из работы терминалов защит (CVE-2015-5374);**
- **Незадекларированные порты удаленного доступа**
- **Уязвимости типа RCE**
  Remote Code Execution (возможность несанкционированного запуска кода через сетевое соединение)

Получение сертификатов ФСТЭК

Предлагается - прохождение процедуры сертификации в соответствии с Постановлением Правительства Российской Федерации от 26.06.1995 № 608 «**О сертификации средств защиты информации**»;

Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных Федеральной службой безопасности Российской Федерации.

Получение сертификатов ФСТЭК

- Не дает гарантии от наличия уязвимостей и НДВ;
- Лаборатории пока не понимают на что проверять;
- На сегодня это дорого!!!
- Не продуман механизм обновления firmware
- Иностранные производители, в большинстве своем не готовы раскрывать свой программный код – могут уйти с рынка РФ.

2. Предлагаемая концепция технических требований к механизмам защиты

2. Предлагаемая концепция технических требований ВСЗИ

Предлагаемый вариант:

разработка простых и понятных технических требования к встроенным механизмам защиты информации интеллектуальных устройств (МП РЗА, контроллеры, измерители и т.д.)

Требования должны быть:

- реализуемыми;
- не требовать больших материальных и временных затрат от производителей оборудования;
- основываться на мировом опыте;
- реально повышать уровень ИБ (принцип Парето 20/80).

2. Предлагаемая концепция технических требований ВСЗИ

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-001: Sabotage Reporting
Отчеты по подозрительной активности

CIP-002: Critical Cyber Asset Identification
Критически важные IT-ресурсы

CIP-003: Security Management Controls
Кибернетическая безопасность - управление в области кибернетической б

CIP-004: Personnel and Training
Персонал и его обучение

CIP-005: Electronic Security Perimeters
Защита электронного периметра

CIP-006: Physical Security of Critical Cyber Assets
Физическая безопасность

CIP-007: Systems Security Management
Управление защитой систем

CIP-008: Incident Reporting and Response Planning
Управление инцидентами

CIP-009: Recovery Plans for Critical Cyber Assets
Планы восстановления ССА

- **ISO/IEC 15408-1:2005 Information technology - Security techniques – Evaluation criteria for IT security - Part 1: Introduction and general model (IDT);**
- **ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».**

Разделы технических требований

№ п/п	Функциональные показатели, требования
1.	**P.IDENT_ASSET** Идентификация и инвентаризация активов
2.	**P.DENY_UNAU** Защита от несанкционированного доступа
3.	**P.ACC_MON** Разграничение доступа
4.	**P.AUDIT** Контроль обеспечения информационной безопасности
5.	**P.SECURE** Защита критической информации

2. Предлагаемая концепция технических требований ВСЗИ

P.IDENT_ASSET

Идентификация и инвентаризация активов

В документации к устройству обязательна глава “Порты и сервисы” с описанием:

- открываемых на сетевых интерфейсах портов;
- предоставляемых сервисах;
- процессах запросов доступа и авторизации;
- методы аутентификации.

- **Исследование поверхности атаки**
- **Тесты на проникновения**
- **«Реверс инжиниринг»**

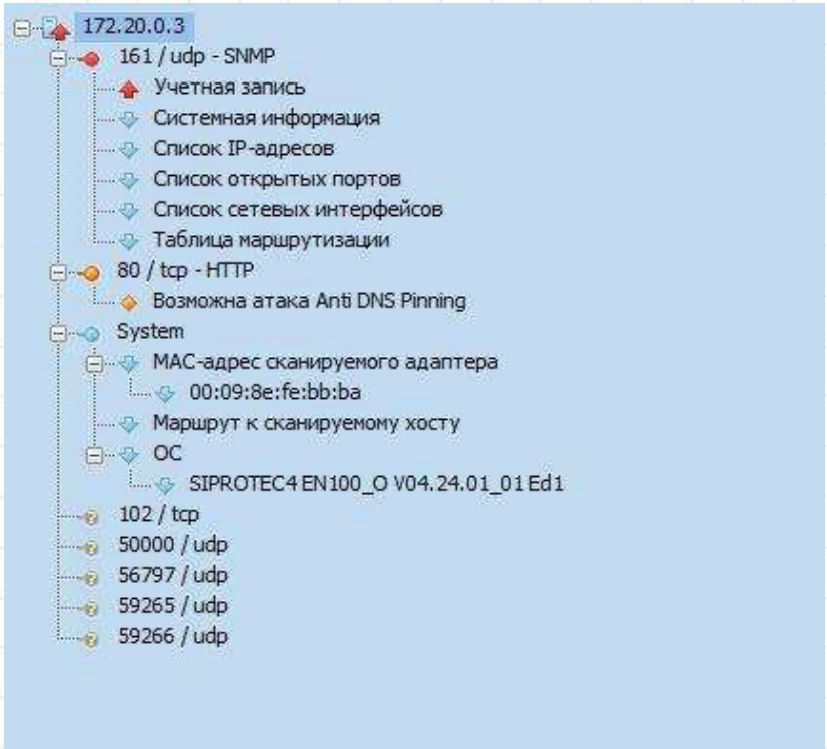
2. Предлагаемая концепция технических требований ВСЗИ

P.DENY_UNAU

Защита от несанкционированного доступа

На устройствах, вводимых в работу, должны быть доступны:

- только порты и сервисы необходимые для получения данных;
- удалённый доступ только тем пользователям, которые были созданы вручную, для которых был задан строгий пароль.



2. Предлагаемая концепция технических требований ВСЗИ

P.ACC_MON

Разграничение доступа

В устройствах должны быть организовано:

- гарантированное разграничение доступа к информации и управлению (по уровням ответственности и доступных возможностей). Минимальное количество ролей две: администратор и пользователь;
- обеспечение доступа только после предъявления идентификатора и пароля.

Парольная политика:

- заводские пароли должны меняться при первом же изменения конфигурации;
- должна быть предусмотрена система, не допускающая «простые» пароли;
- должна быть предусмотрена функция, защищающая от подбора паролей, рекомендована блокировка доступа при неуспешных попытках (время блокировки – не менее 30мин, количество попыток не более 3).

2. Предлагаемая концепция технических требований ВСЗИ

P.AUDIT

Контроль обеспечения информационной безопасности

Регистрация событий с меткой времени, имеющих отношение к защищенности информации:

- протоколы действий оператора, с указанием идентификатора оператора и его прав доступа к обслуживанию (конфигурированию);
  - входе/выходе пользователей из системы;
  - неудачные попытках входа;
  - о превышении количества неудачных попыток входа;
  - изменении конфигурации/уставок (с указанием что и кем было изменено, старое значение/новое значение);
- диагностические массивы информации, отражающие состояние аппаратной части и программ;
- начало работы, перезагрузка устройства
- включение/выключение портов/сервисов.

2. Предлагаемая концепция технических требований ВСЗИ

P.AUDIT

Контроль обеспечения информационной безопасности

Записи журнала доступа должны:

- храниться на устройстве в течении 90 календарных дней;
- удаление записей журнала доступа с удалённого рабочего места должно быть запрещено всем пользователям, включая администратора (учетной записи);
- опционально: устройство должно генерировать события, связанные с ИБ, для другой системы по открытому протоколу (например, генерация GOOSE-сообщений или syslog-сообщений).

Средство конфигурирования должно обеспечивать:

- проверку блокировки сервисов на портах или проверку блокировки портов;
- формирование отчётов о текущих привилегиях пользователей.

2. Предлагаемая концепция технических требований ВСЗИ

P.SECURE

Защита критической информации

Должен быть предусмотрен комплекс мер по недопущению несанкционированной подмены основного программного кода устройства (firmware). Предпочтительна организация возможности изменения основного программного кода устройства (firmware) только при физическом доступе к устройству.

Должна быть предусмотрена возможность верификации версии и целостности основного программного кода устройства (firmware).

Должна быть предусмотрена возможность возврата к заводским настройкам.

Предлагаемый план действий

1. Разработка технических требований к механизмам ИБ РЗА;
2. Корректировка ПО МП РЗА в соответствии с принятыми требованиями;
3. Обязательное проведение испытаний и тестов на проникновение;
4. Сертификация ФСТЭК на первом этапе добровольная;

Спасибо за внимание!

Никандров Максим
ООО «Интеллектуальные Сети»
nikandrov@igrids.ru