

## Обеспечение кибербезопасности при организации терминального доступа к микропроцессорным устройствам информационно-технологических систем подстанций

**Ю. В. МАШИНСКИЙ**  
**ЗАО «РТСофт»**  
**РОССИЯ**  
**mashinskiy\_yv@rtsoft.msk.ru**

### КЛЮЧЕВЫЕ СЛОВА

Информационная безопасность, МЭК 61850, микропроцессорные терминалы, удаленный доступ, релейная защита, сетевое оборудование, шифрование.

### 1 ВВЕДЕНИЕ

Микропроцессорные устройства (далее IED) сегодня являются преобладающими при строительстве или реконструкции систем релейной защиты, противоаварийной автоматики, АСУ ТП и других информационно-технологических систем подстанций. Возможности, предоставляемые терминальным доступом к этим устройствам, зачастую не просто добавляют удобства к использованию, но и жизненно необходимы для эксплуатации систем. Например, считывание внутренних журналов событий для множества устройств доступно только в этом режиме. В то же время безопасность такого доступа, не выделяется в отдельную задачу и решается на уровне общих угроз удаленного доступа к технологическим системам ПС, и мер по их купированию. Сложившаяся ситуация объясняется разным пониманием удаленного доступа (Remote Access) у специалистов нашей страны и стран Запада, что ясно видно из докладов секции CIGRE B5-2xx, опубликованных в 2012 году.

Данный доклад посвящен определению степени угрозы и сложности защиты именно систем терминального доступа к IED, а также необходимым мерам по снижению рисков использования данного способа доступа к устройствам. Используемые в докладе предпосылки и выводы актуальны для магистральных подстанций ОАО «ФСК ЕЭС», оснащенных современными системами РЗА, АСУ ТП, ССПТИ и т. п.

### 2 ОСНОВНАЯ ЧАСТЬ

#### 2.1 Применение терминального доступа.

Под терминальным доступом, здесь и далее, понимается чтение и запись информации в IED, осуществляющиеся одновременно, по инициативе человека, с применением программных средств и технологий, отличных от используемых для оперативного обмена информацией между IED.

Применение терминального доступа обуславливается двумя основными причинами:

- Необходимость получения журналов событий и конфигураций устройств, во время расследование происшествий;
- Необходимость изменения конфигураций устройств (уставок).

Иные задачи для использования терминального доступа к устройствам, например описанные в [1] и [2], являются либо подмножеством выше перечисленных задач, либо решаются штатными средствами систем сбора и передачи технологической информации.

Наиболее распространенными являются следующие технологии терминального доступа:

- Использование интерфейса командной строки (CLI). Данный способ наиболее распространен среди сетевого оборудования.

- Использование встроенного Web-сервера. На сегодня является наиболее типовым и поддерживается большинством современных IED.
- Использование специализированного инструментального программного обеспечения. Данный способ реализован в большинстве технологических IED и обеспечивает максимальный уровень доступа к устройству.

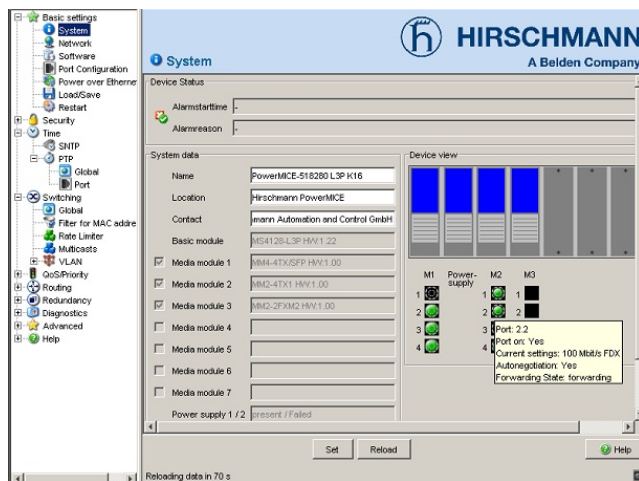


Рисунок 1. Интерфейс встроенного Web сервера коммутатора Power Mice

Способов реализации терминального доступа на сегодняшний день также несколько:

- 1й способ. Локальное подключение по последовательным интерфейсам, с помощью инженерного ноутбука;
- 2й способ. Удаленное подключение по последовательным интерфейсам, с помощью инкапсуляции их в IP;
- 3й способ. Удаленное подключение, с помощью сетевых интерфейсов устройства.

Первый и второй способ реализации терминального доступа функционально идентичны, а третий зачастую имеет некоторые функциональные ограничения, вызванные, в том числе, необходимостью соблюдать хоть какой-то уровень информационной безопасности. Так при третьем способе терминального доступа, некоторыми производителями, разрешается только чтение информации из устройства или замена не критических параметров конфигурации.

ЦУС ПМЭС

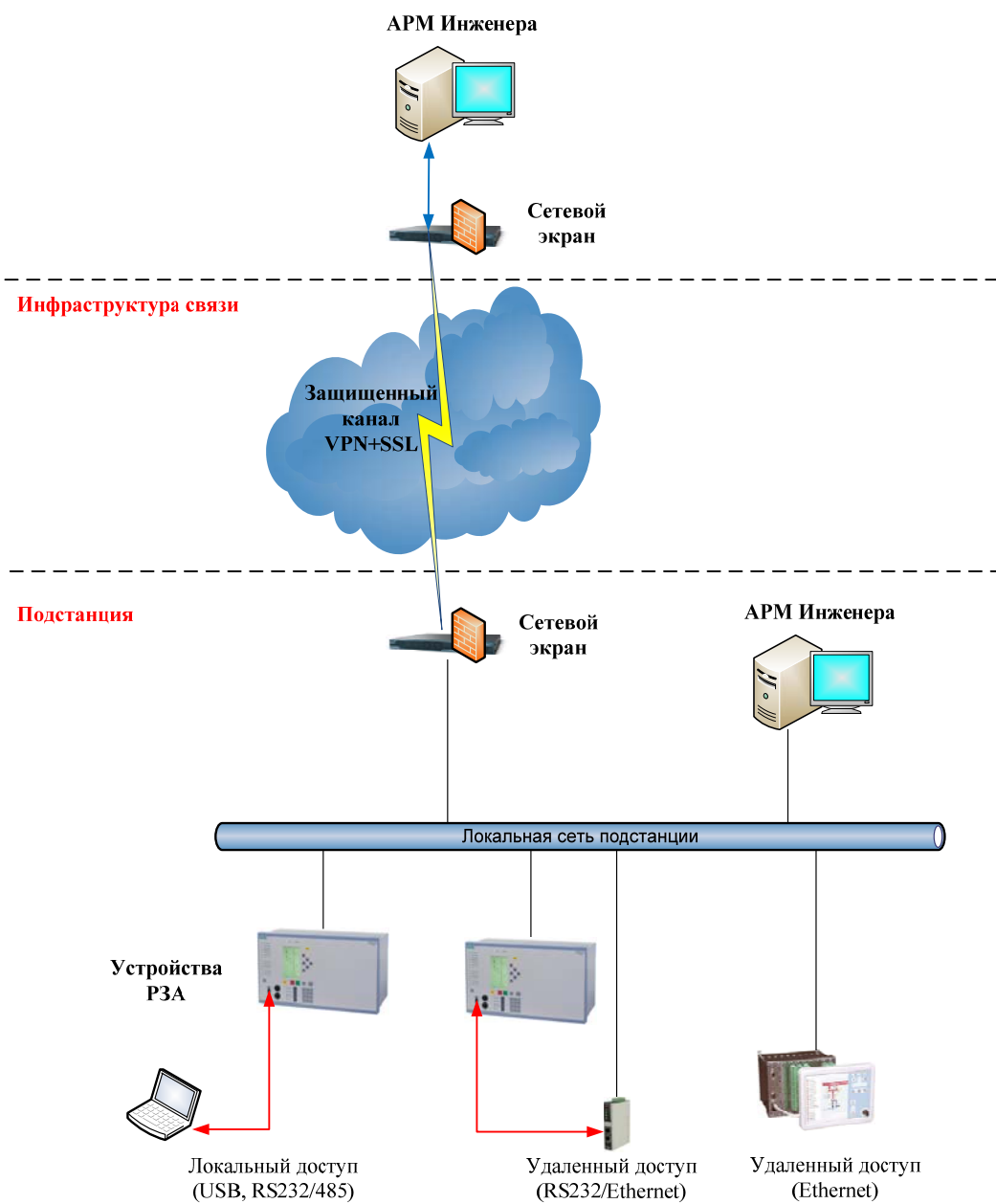


Рисунок 2. Способы реализации терминального доступа.

## 2.2 Безопасность терминального доступа.

В качестве сценариев угроз терминального доступа рассмотрим наиболее очевидный вариант: **получение злоумышленником терминального доступа к устройству РЗА.**

На первый взгляд, степень угрозы в данном случае является максимальной, так как злоумышленник получает полный доступ к управлению уставками устройства. Именно на защиту от такого типа угроз и направлены основные меры безопасности, изложенные в рекомендациях NERC и других организаций. Основным способом защиты от этого и подобных сценариев является сегментация сети и защиту удаленных каналов связи с помощью создания зашифрованных туннелей. Пример такого подхода изображен на Рисунок 3.

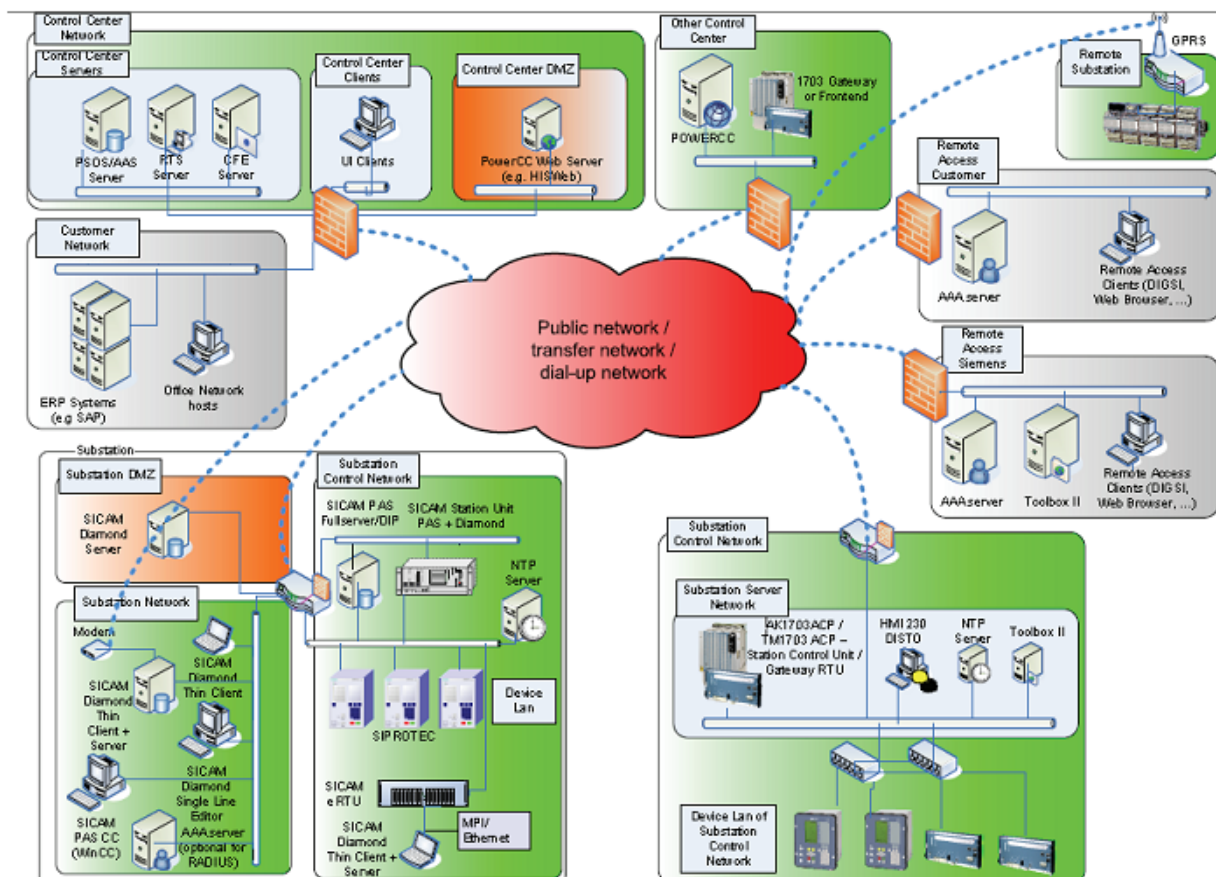


Рисунок 3. Защита сетей передачи данных способом сегментирования [3].

Приведенный способ защиты не подразумевает угроз внутри защищаемых сегментов сети. Если рассматривать это в контексте терминального доступа, то получается, что устройство всегда считает подключающегося к нему клиента терминального доступа – доверенным и заслуживающим уважение партнером. Для исключения этой ситуации, производители предусматривают меры парольной защиты к терминальному доступу к устройству. Однако, реализация этой парольной защиты, сколько-нибудь надежна только у производителей сетевого оборудования, но и у них регулярно находят уязвимости. Реализация же паролей на доступ к устройствам РЗА разбивается об необходимость изменения в процессе наладки и эксплуатации устройств. Если провести аудит установленных на объектах ОАО «ФСК ЕЭС» современных комплексов РЗА и АСУ ТП, то по нашему мнению, в большинстве случаев пароль совпадет с записанным в заводской инструкции по эксплуатации.

Вопросы организации доверенной среды на технологических АРМ, особенно на инженерных ноутбуках, достойны отдельного обсуждения. В рамках данного доклада стоит отметить, что применение обычного антивируса не гарантирует чистоты инженерной станции, так как многие инструментальные средства для конфигурирования микропроцессорных

устройств настолько сложные и одновременно хрупкие, что попытка антивируса обратить внимание на уязвимость или подозрительную активность не будет воспринята всерьез.

Таким образом, перед злоумышленником или перед вредоносной программой, по сути стоит только одна задача – проникнуть в защищаемую сеть, а так как сеть это довольно большая и строится по стандартным технологиям, то и задача эта становится вполне выполнимой. Следовательно, то что мы не слышали о «Stuxnet» для систем РЗА говорит либо об отсутствии заказчика на эту разработку, либо о его хорошей маскировке.

Конечно, сообщество производителей и специалистов в области информационной безопасности, также озабоченно решением этих проблемам. Одним из средств решения выступают меры, изложенные в стандартах серии МЭК 62351 [4]. Но если посмотреть на эти стандарты с практической точки зрения, то для проблем терминального доступа там предлагается уменьшение защищаемого сегмента сети до размера одного устройства.

При всем при этом с нашей точки зрения, главная уязвимость терминального доступа к устройствам это его вседозволенность или широта возможностей. Таким образом, мы втягиваемся в бесконечную борьбу между производителями средств устройств и противостоящими им потенциальными злоумышленниками с постоянным преимуществом вторых. В то же время напрашивается, возможно не очень элегантно, но довольно простое решение – ограничить функциональную необходимость терминального доступа.

Как уже говорилось в начале доклада подавляющее большинство случаев использования терминального доступа к устройствам в процессе эксплуатации, составляют операции чтения из устройств конфигурационных данных и внутренних журналов событий. Конечно, существуют сценарии, когда требуется изменение конфигурации уставок внутри устройств, но операции, выполняемые в этих сценариях, не должны быть удаленными. В докладе [1], несмотря на некоторые спорные суждения, сделан один из основных выводов, позволяющих, радикально уменьшить частоту использования терминального доступа – необходимость обязательной реализации в устройствах всех параметров модели данных МЭК 61850 [5], в том числе и опциональных (см. пример на Рисунке 4). Не реализуя в своих устройствах возможности считывания уставок стандартными средствами, производитель пытается навязать нам использование своего проприетарного инструментального ПО, одновременно с этим повышая уязвимость своих устройств.

| PDIS class                |                   |                                                                                                                       |   |       |
|---------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------|---|-------|
| Data object name          | Common data class | Explanation                                                                                                           | T | M/O/C |
| LNName                    |                   | The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22. |   |       |
| <b>Data objects</b>       |                   |                                                                                                                       |   |       |
| <b>Status information</b> |                   |                                                                                                                       |   |       |
| Str                       | ACD               | Start                                                                                                                 |   | M     |
| Op                        | ACT               | Operate                                                                                                               | T | M     |
| <b>Controls</b>           |                   |                                                                                                                       |   |       |
| OpCntRs                   | INC               | Resettable operation counter                                                                                          |   | O     |
| <b>Settings</b>           |                   |                                                                                                                       |   |       |
| PoRch                     | ASG               | Polar reach is the diameter of the Mho diagram                                                                        |   | O     |
| PhStr                     | ASG               | Phase start value                                                                                                     |   | O     |
| GndStr                    | ASG               | Ground start value                                                                                                    |   | O     |
| DirMod                    | ENG               | Directional mode                                                                                                      |   | O     |
| PctRch                    | ASG               | Percent reach                                                                                                         |   | O     |
| Ofs                       | ASG               | Offset                                                                                                                |   | O     |
| PctOfs                    | ASG               | Percent offset                                                                                                        |   | O     |
| RisLod                    | ASG               | Resistive reach for load area                                                                                         |   | O     |
| AngLod                    | ASG               | Angle for load area                                                                                                   |   | O     |
| TmDIMod                   | SPG               | Operate time delay mode                                                                                               |   | O     |

**Рисунок 4.** Фрагмент описания типа дистанционной защиты в стандарте IEC61850-7-4.

Для тех случаев, когда без терминального доступа не обойтись, механизм авторизации для изменения уставок или микропрограммы (firmware) устройства должен быть дополнен аппаратной блокировкой, выполненной на устройстве.

### 3 ЗАКЛЮЧЕНИЕ

Необходимость терминального доступа к микропроцессорным устройствам – это данность нынешнего уровня развития систем автоматизации подстанций. Потенциальная уязвимость данного вида информационного обмена, до сих пор адекватно не оценена, хотя наиболее известный инцидент в промышленной информационной безопасности – StuxNet – использовал именно этот вид доступа к ПЛК. Существующие способы защиты терминального доступа не представляют серьезной угрозы для злоумышленников или специально разработанного вредоносного программного обеспечения. Применяя стандартные протоколы и способы доступа к информации, получаемой обычно с помощью терминального доступа, мы существенно упрощаем защиту этой информации и уменьшаем возможный ущерб.

За пределами данного доклада намеренно оставлен вопрос обеспечения доверенной среды, особенно на ноутбуках инженерного персонала.

### ЛИТЕРАТУРА

- [1] CIGRE 2012-B5-211, Paris 2012-08, K. P. BRAND, M. HERZIG, W. WIMMER, Remote access to substations: state, possibilities, challenges.
- [2] CIGRE 2012-B5-208, Paris 2012-08, D. ESPINOSA, C. MELENDEZ, M. MANRIQUEZ, Present and future for remote access solutions to IEDs
- [3] CIGRE 2012-B5-202, Paris 2012-08, N. SCHUSTER, H-J. HERRMANN, A. SUHR, Advantages of solutions for remote access in protection and control applications via communication networks
- [4] IEC 62351, Communication network and system security.
- [5] IEC 61850Ed2 (2010): Communication networks and systems for Power Utility Automation.