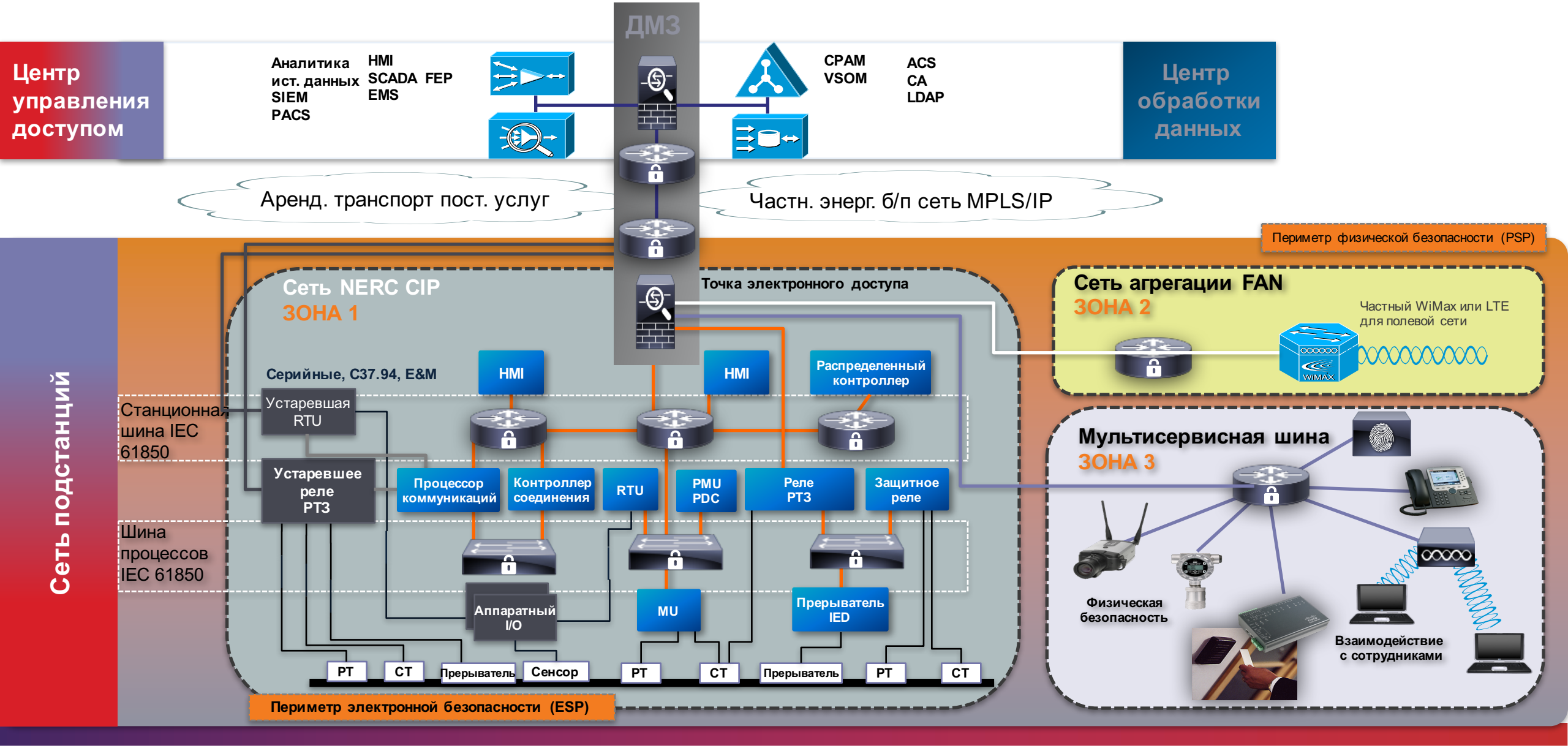
Передовой опыт обеспечения ИБ критических инфраструктур и возможность его применения в России

Алексей Лукацкий
Бизнес-консультант по безопасности
25 мая 2016 г.

Из чего состоит архитектура ИБ цифровой подстанции?



Международные требования для электроэнергетики

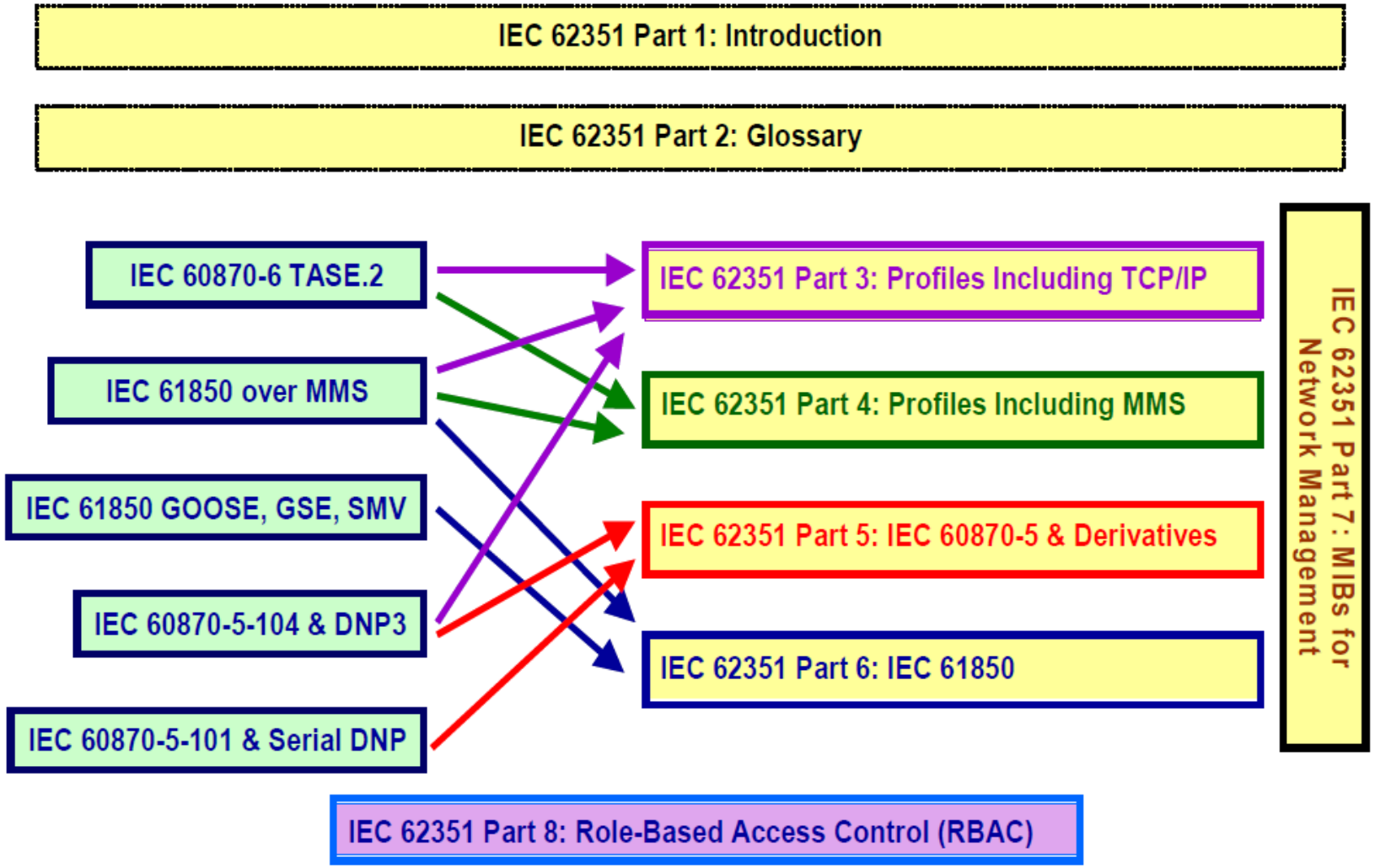
Стандарты International Electrotechnical Commission

- IEC 62210 «Initial Report from IEC TC 57 ad-hoc WG06 on Data and Communication Security»
- IEC 61784-4 «Digital data communications for measurement and control – Profiles for secure communications in industrial networks»
- IEC 62443 «Security for industrial process measurement and control – Network and system security»
- IEC 62351 «Data and Communication Security»

Стандарт IEC 62351

- IEC 62351 «Data and Communication Security»
  - IEC 62351-1: Data and Communication Security – Introduction
  - IEC 62351-2: Data and Communication Security – Glossary of Terms
  - IEC 62351-3: Data and Communication Security – Profiles Including TCP/IP
  - IEC 62351-4: Data and Communication Security – Profiles Including MMS
  - IEC 62351-5: Data and Communication Security – Security for IEC 60870-5 and Derivatives (i.e. DNP 3.0)
  - IEC 62351-6: Data and Communication Security – Security for IEC 61850 Profiles
  - IEC 62351-7: Data and Communication Security – Security Through Network and System Management

Связь стандартов IEC по PCN с IEC62351



Другие стандарты для энергетики

- Проект ISO 27009. Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002
- Advanced Metering Infrastructure(AMI) System Security Requirements
- Security Profile for Advanced Metering Infrastructure

Стандарты IEEE

- IEEE 1402 «IEEE Guide for Electric Power Substation Physical and Electronic Security»
- IEEE 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities
- IEEE P1711 - Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links

Стандарты NIST

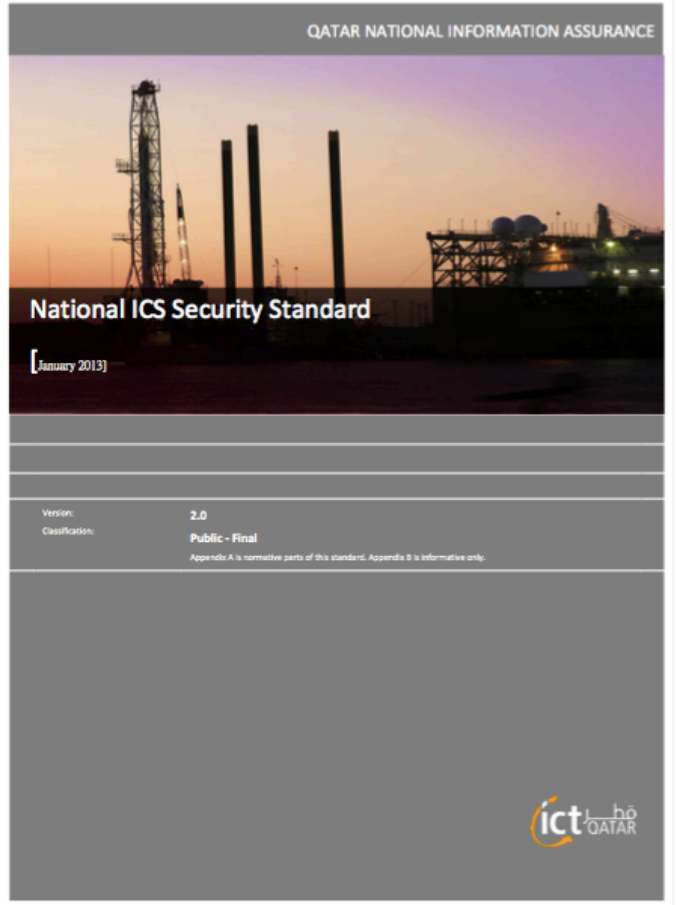
- NIST SP800-82 «Guide to Industrial Control Systems (ICS) Security»
- NIST SP800-53 «Security and Privacy Controls for Federal Information Systems and Organizations»
- NISTIR 7628 Guidelines for Smart Grid Cyber Security
- NIST PCSRF Security Capabilities Profile for Industrial Control Systems

Другие стандарты

- FERC Security Standards for Electric Market Participants Security Guidelines for the Natural Gas Industry
- Cisco SAFE for PCN
- GB/T 22239-2008 “Baseline for classified protection of information system security”

  China National Information Technology Standardization
- National ICS Security Standard

  Qatar National Information Assurance



Рекомендации ENISA

Good Practice Guide

Network Security Information Exchanges

Smart Grid Security

Recommendations for Europe and Member States

[Deliverable – 2012-07-01]

Protecting Industrial Control Systems

Recommendations for Europe and Member States

[Deliverable – 2011-12-09]

Лучшие практики DHS

Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments

Draft

April 2007

Author

Ken Masica

Lawrence Livermore National Laboratory

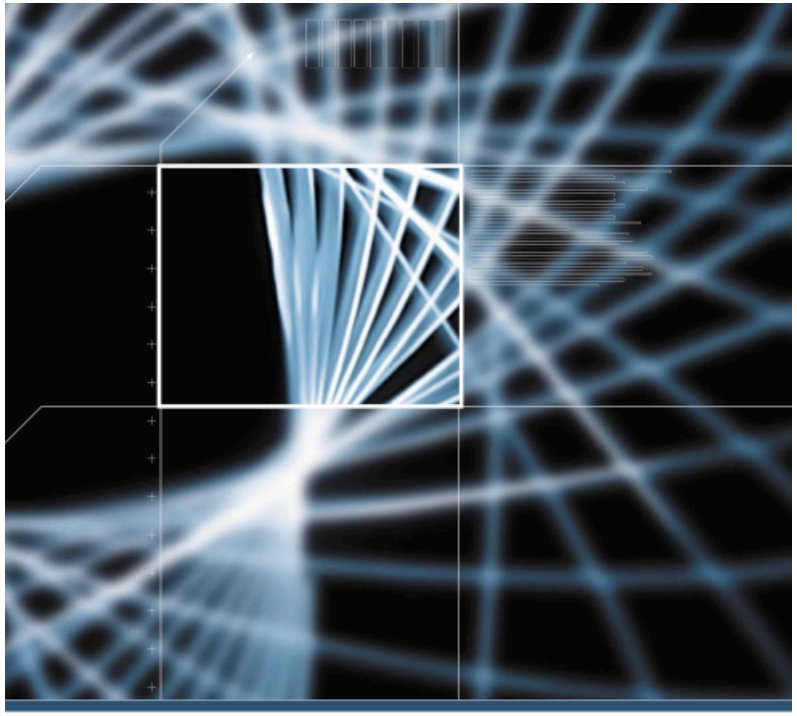
Homeland Security

Recommended Practice for Securing Control System Modems

January 2008

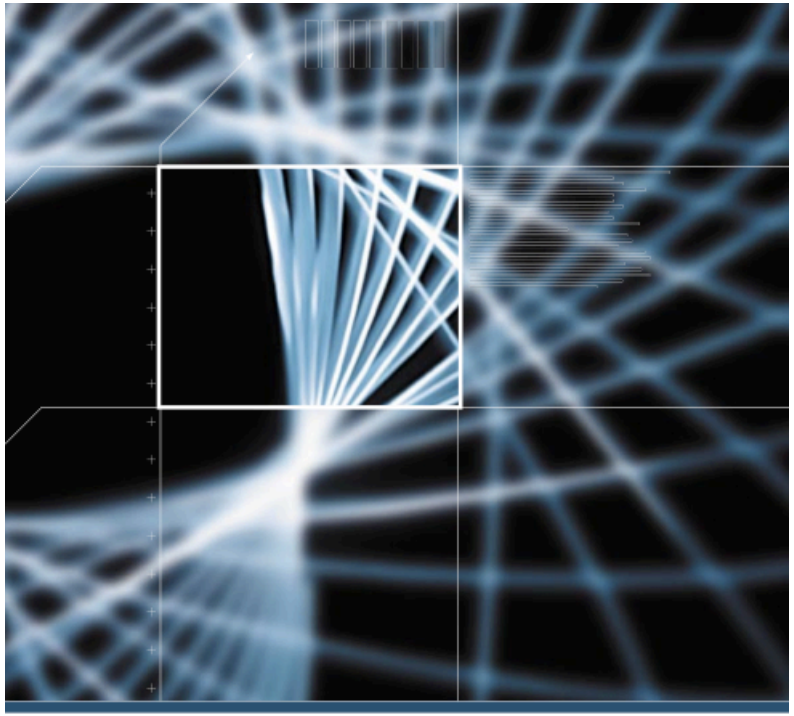
Homeland Security

Лучшие практики CPNI



GOOD PRACTICE GUIDE
PROCESS CONTROL AND SCADA SECURITY
GUIDE 1. UNDERSTAND THE BUSINESS RISK

CPNI
Centre for the Protection of National Infrastructure

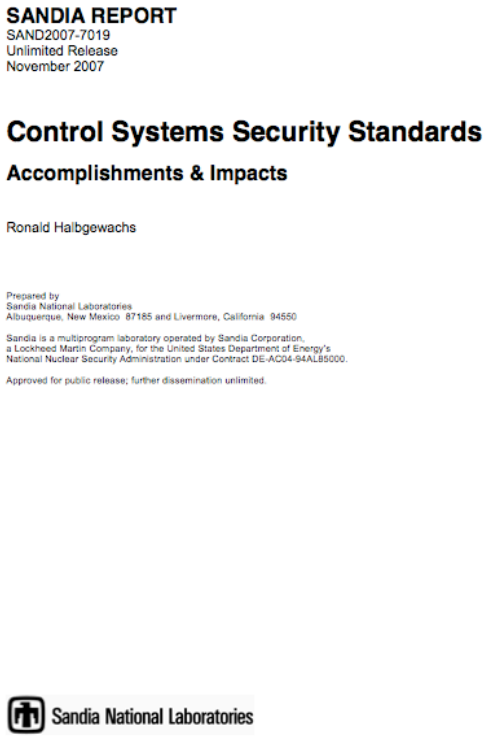


GOOD PRACTICE GUIDE
PROCESS CONTROL AND SCADA SECURITY
GUIDE 2. IMPLEMENT SECURE ARCHITECTURE

CPNI
Centre for the Protection of National Infrastructure

Есть ли лучший стандарт?

МинЭнерго США проводило соответствующую работу


SANDIA REPORT
SAND2007-7019
Unlimited Release
November 2007

Control Systems Security Standards

Accomplishments & Impacts

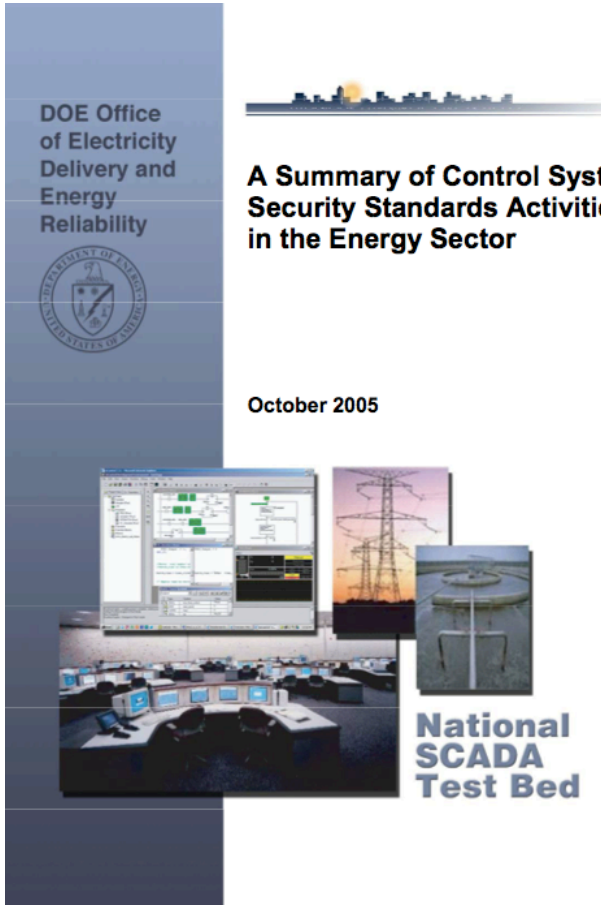
Ronald Halbgewachs

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

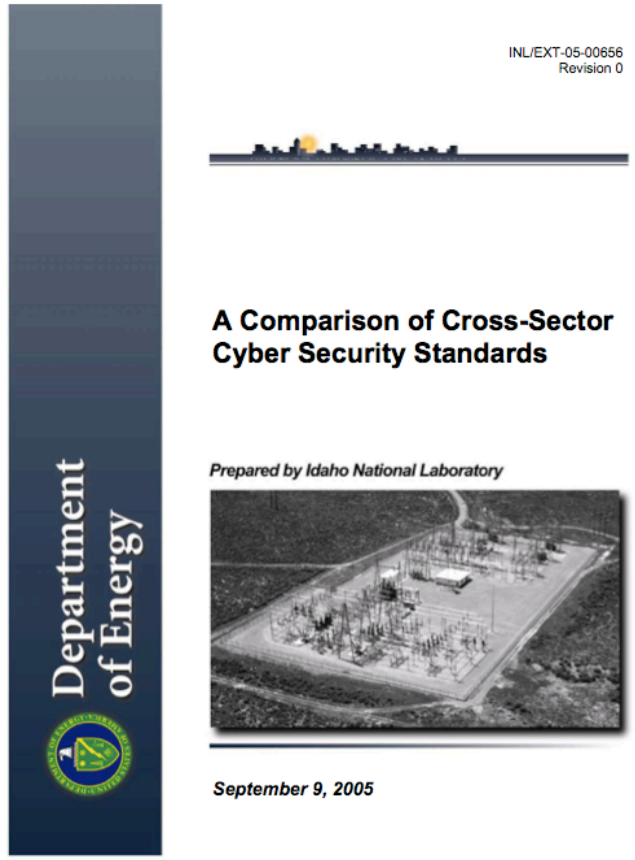
Sandia National Laboratories


DOE Office of Electricity Delivery and Energy Reliability

A Summary of Control System Security Standards Activities in the Energy Sector

October 2005

National SCADA Test Bed


Department of Energy

INL/EXT-05-00656
Revision 0

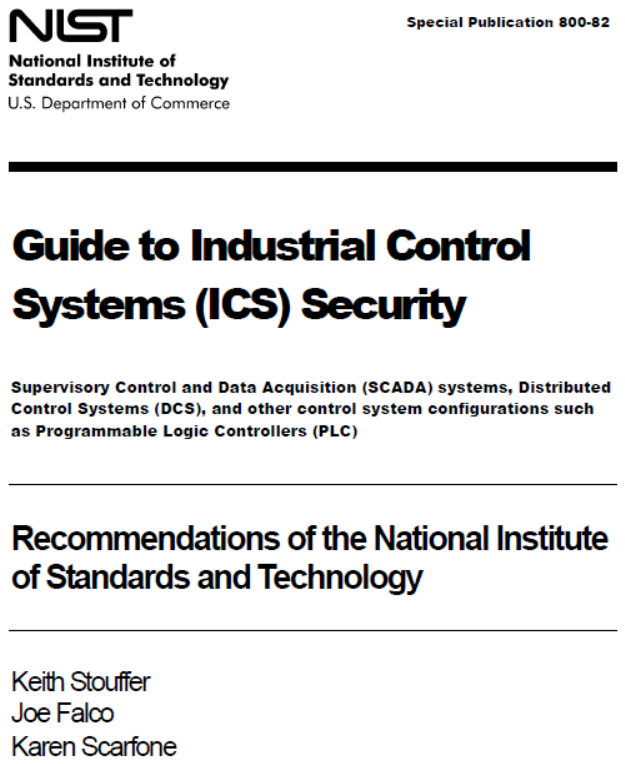
A Comparison of Cross-Sector Cyber Security Standards

Prepared by Idaho National Laboratory

September 9, 2005

Может быть NIST SP800-82?

- Общим руководством по защите АСУ ТП и выбору необходимого стандарта до недавнего времени являлось руководство NIST SP800-82
  - Выпущено в июне 2011 года


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-82

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Recommendations of the National Institute of Standards and Technology

Keith Stouffer
Joe Falco
Karen Scarfone

Как построен NIST SP800-82?

- FIPS PUB 2000

  Определяет 18 областей с минимальным набором требований по ИБ

- NIST SP800-53

  Определяет порядок выбора нужных защитных мер

- Все государственные ИС (включая и АСУ ТП) должны строиться на базе этих требований

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

Идеального стандарта нет
Мнение CIGRE

- При исследовательском комитете B5 CIGRE была создана специальная рабочая группа по кибербезопасности

  Отчет: «The Impact of Implementing Cyber Security Requirements using IEC 61850», CIGRE Working Group the B5.38, August 2010

- Однако, анализ существующих и разрабатываемых стандартов, выполненный рабочей группой исследовательского комитета СИГРЭ по релейной защите, показал, что ни один из рассмотренных стандартов не удовлетворяет всем требованиям по кибербезопасности в электроэнергетике

- Аналогичная ситуация и в других отраслях

Нужно комбинировать
Мнение CIGRE

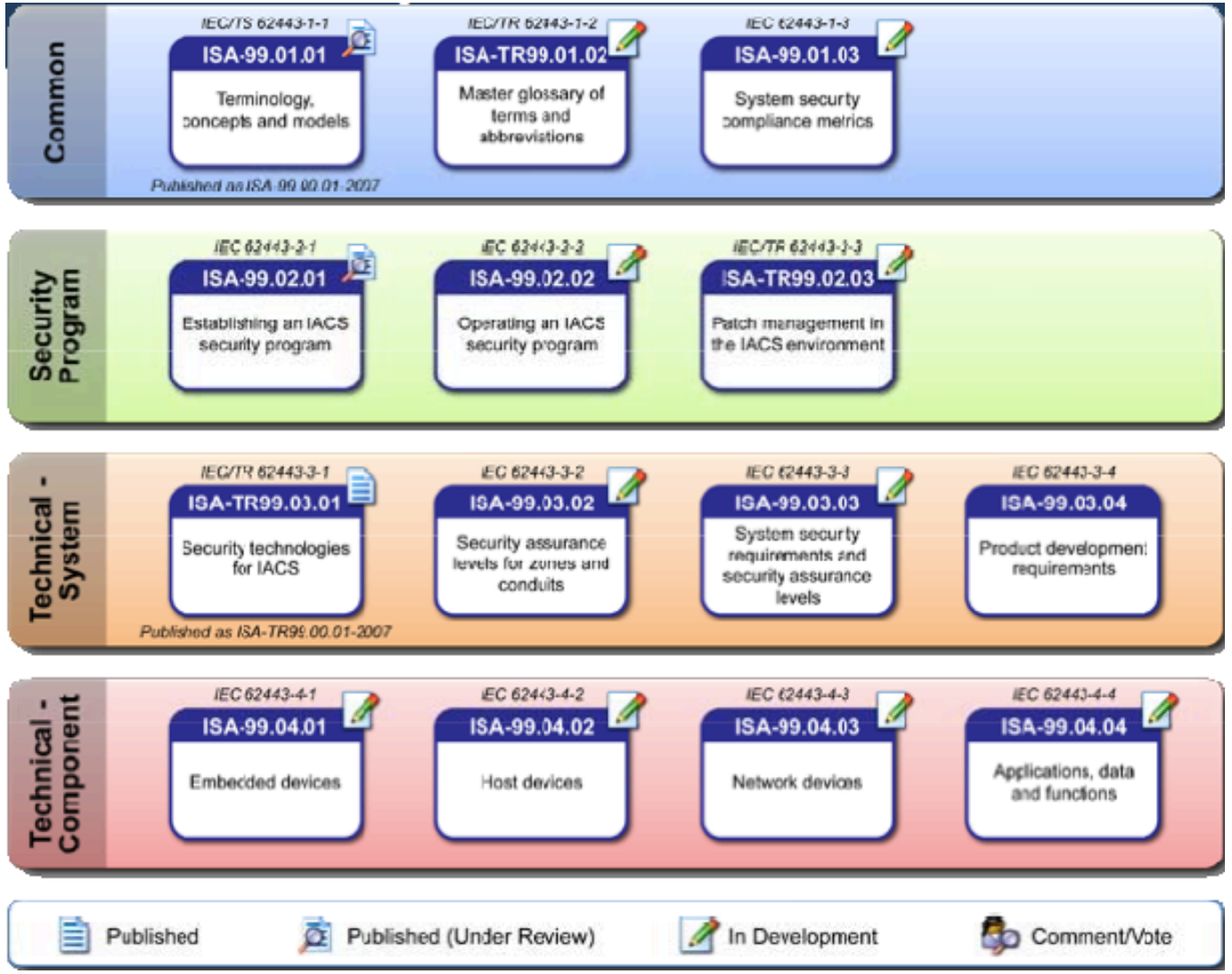
- CIGRE считает, что только стандарт IEC 62351 «Data and Communication Security» и ISA SP99 предлагают требования безопасности для передачи сообщений IEC 61850 в пределах цифровых подстанций

  При этом в рабочей группе CIGRE отмечает, что технические требования ISA SP99 еще находятся на ранней стадии развития

- Основополагающие стандарты ISA SP99 и NERC CIP, охватывают более широкую область требований по кибербезопасности, чем IEC62351

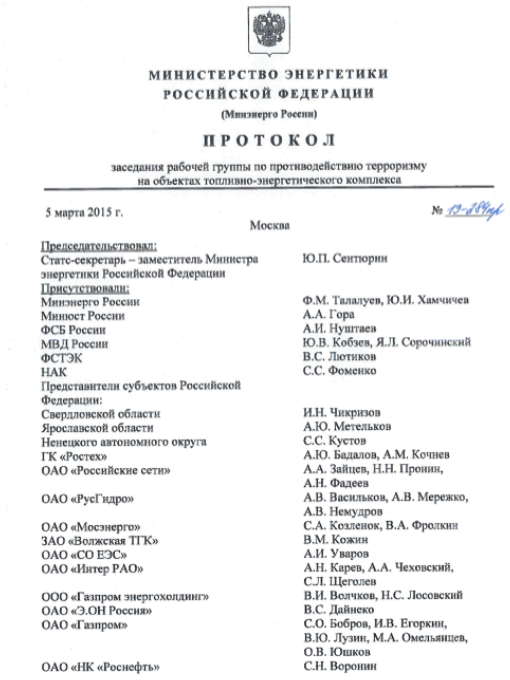
  но содержат высокоуровневые рекомендации, а не конкретные инструкции о том, что и как должно быть сделано

ISA SP99 умер, да здравствует IEC 62443



Российские требования

Что думает МинЭнерго?



МИНИСТЕРСТВО ЭНЕРГЕТИКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(Минэнерго России)

ПРОТОКОЛ

заседания рабочей группы по противодействию терроризму
на объектах топливно-энергетического комплекса

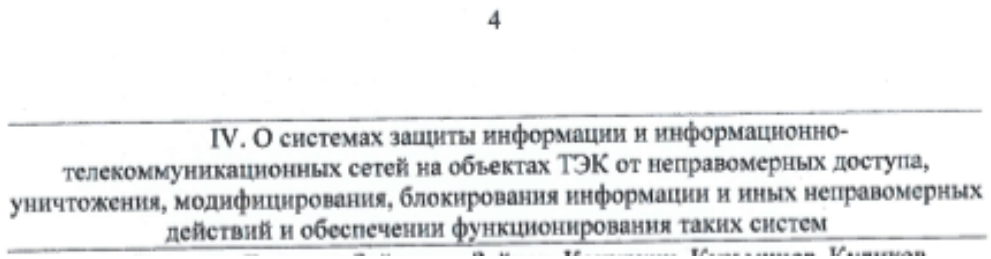
5 марта 2015 г. № 13-189пр

Москва

Председательствовал:
Статс-секретарь – заместитель Министра энергетики Российской Федерации — Ю.П. Сентюрин

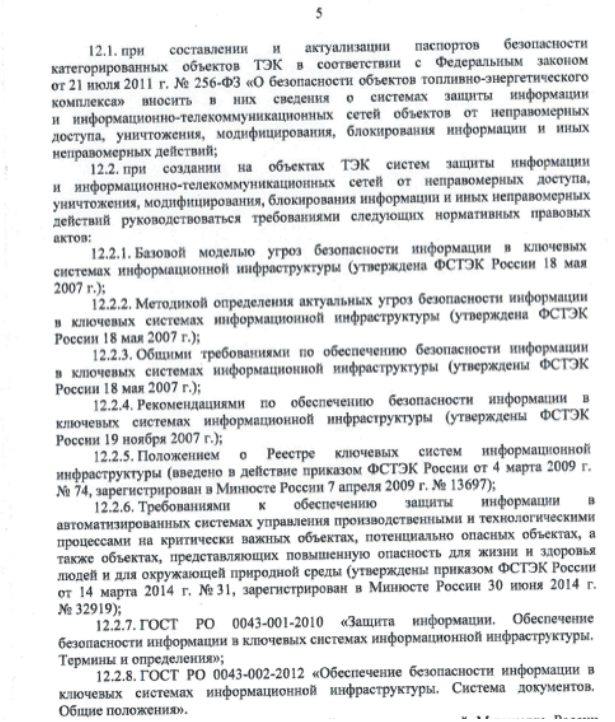
Присутствовали:
Минэнерго России — Ф.М. Талалуев, Ю.И. Хамчичев
Минюст России — А.А. Гора
ФСБ России — А.И. Нуштаев
МВД России — Ю.В. Кобзев, Я.Л. Сорочинский
ФСТЭК — В.С. Лютиков
НАК — С.С. Фоменко

Представители субъектов Российской Федерации:
Свердловской области — И.Н. Чикризов
Ярославской области — А.Ю. Метельков
Ненецкого автономного округа — С.С. Кустов
ГК «Ростех» — А.Ю. Бадалов, А.М. Кочнев
ОАО «Российские сети» — А.А. Зайцев, Н.Н. Пронин, А.Н. Фадеев
ОАО «РусГидро» — А.В. Васильков, А.В. Мережко, А.В. Немудров
ОАО «Мосэнерго» — С.А. Козленок, В.А. Фролкин
ЗАО «Волжская ТГК» — В.М. Кожин
ОАО «СО ЕЭС» — А.И. Уваров
ОАО «Интер РАО» — А.Н. Карев, А.А. Чеховский, С.Л. Щеголев
ООО «Газпром энергохолдинг» — В.И. Волчков, Н.С. Лосовский
ОАО «Э.ОН Россия» — В.С. Дайнеко
ОАО «Газпром» — С.О. Бобров, И.В. Егоркин, В.Ю. Лузин, М.А. Омельянец, О.В. Юшков
ОАО «НК «Роснефть» — С.Н. Воронин



4

IV. О системах защиты информации и информационно-телекоммуникационных сетей на объектах ТЭК от неправомерных доступа, уничтожения, модифицирования, блокирования информации и иных неправомерных действий и обеспечении функционирования таких систем



5

12.1. при составлении и актуализации паспортов безопасности категорированных объектов ТЭК в соответствии с Федеральным законом от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» вносить в них сведения о системах защиты информации и информационно-телекоммуникационных сетей объектов от неправомерных доступа, уничтожения, модифицирования, блокирования информации и иных неправомерных действий;

12.2. при создании на объектах ТЭК систем защиты информации и информационно-телекоммуникационных сетей от неправомерных доступа, уничтожения, модифицирования, блокирования информации и иных неправомерных действий руководствоваться требованиями следующих нормативных правовых актов:

12.2.1. Базовой моделью угроз безопасности информации в ключевых системах информационной инфраструктуры (утверждена ФСТЭК России 18 мая 2007 г.);

12.2.2. Методикой определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утверждена ФСТЭК России 18 мая 2007 г.);

12.2.3. Общими требованиями по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утверждены ФСТЭК России 18 мая 2007 г.);

12.2.4. Рекомендациями по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утверждены ФСТЭК России 19 ноября 2007 г.);

12.2.5. Положением о Реестре ключевых систем информационной инфраструктуры (введено в действие приказом ФСТЭК России от 4 марта 2009 г. № 74, зарегистрирован в Минюсте России 7 апреля 2009 г. № 13697);

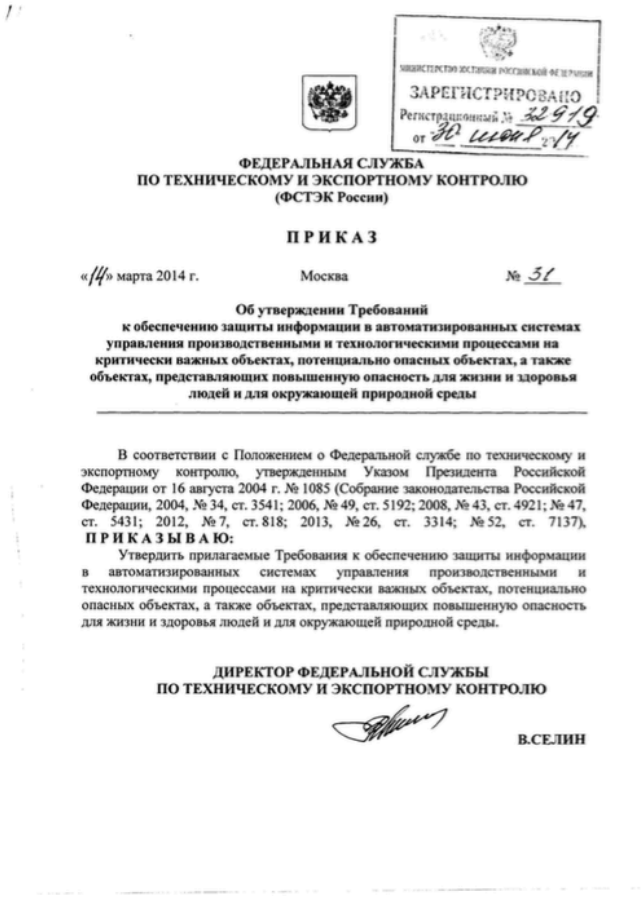
12.2.6. Требованиями к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (утверждены приказом ФСТЭК России от 14 марта 2014 г. № 31, зарегистрирован в Минюсте России 30 июня 2014 г. № 32919);

12.2.7. ГОСТ РО 0043-001-2010 «Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Термины и определения»;

12.2.8. ГОСТ РО 0043-002-2012 «Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Система документов. Общие положения».

Приказ ФСТЭК №31 по защите АСУ ТП

- №31 от 14.03.2014 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
- Все новые и модернизируемые системы должны создаваться по новому приказу, а не по документам ФСТЭК для КСИИ 2007-го и последующих годов
  - В тех случаях, если КСИИ управляют технологическими процессами
  - Остальные типы КСИИ продолжают подчиняться требованиям ФСТЭК к ключевым системами информационной инфраструктуры



ЗАРЕГИСТРИРОВАНО
Регистрационный № 32919
от 30 июня 2014

**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)**

ПРИКАЗ

«14» марта 2014 г. Москва № 31

**Об утверждении Требований
к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды**

В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 52, ст. 7137),

ПРИКАЗЫВАЮ:

Утвердить прилагаемые Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

**ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ**

В.СЕЛИН

Смена парадигмы

- Принимаемые организационные и технические меры защиты информации должны обеспечивать доступность обрабатываемой в АСУ ТП (исключение неправомерного блокирования информации), ее целостность (исключение неправомерного уничтожения, модифицирования информации), а также, при необходимости, конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации)
- Организационные и технические меры защиты информации должны быть согласованы с мерами по промышленной, физической, пожарной, экологической, радиационной безопасности, иными мерами по обеспечению безопасности АСУ ТП и управляемого (контролируемого) объекта и (или) процесса и не должны оказывать отрицательного (мешающего) влияния на штатный режим функционирования АСУ ТП

Меры по защите информации АСУ ТП

Защитная мера	АСУ ТП
Идентификация и аутентификация субъектов доступа и объектов доступа	+
Управление доступом субъектов доступа к объектам доступа	+
Ограничение программной среды	+
Защита машинных носителей информации, на которых хранятся и (или) обрабатывается КИ	+
Регистрация событий безопасности	+
Антивирусная защита	+
Обнаружение (предотвращение) вторжений	+
Контроль (анализ) защищенности персональных данных	+
Обеспечение целостности информационной системы и КИ	+
Обеспечение доступности персональных данных	+
Защита среды виртуализации	+
Защита технических средств	+
Защита информационной системы, ее средств, систем связи и передачи данных	+

Меры по защите информации АСУ ТП

Защитная мера	АСУ ТП
Управление инцидентами	+
Управление конфигурацией информационной системы и системы защиты КИ	+
Безопасная разработка прикладного и специального программного обеспечения разработчиком	+
Управление обновлениями программного обеспечения	+
Планирование мероприятий по обеспечению защиты информации	+
Обеспечение действий в нештатных (непредвиденных) ситуациях	+
Информирование и обучение пользователей	+
Анализ угроз безопасности информации и рисков от их реализации	+

- Планы ФСТЭК
  - Унификация перечня защитных мер для всех трех приказов
  - Выход на 2-хлетний цикл обновления приказов

NIST Cybersecurity Framework

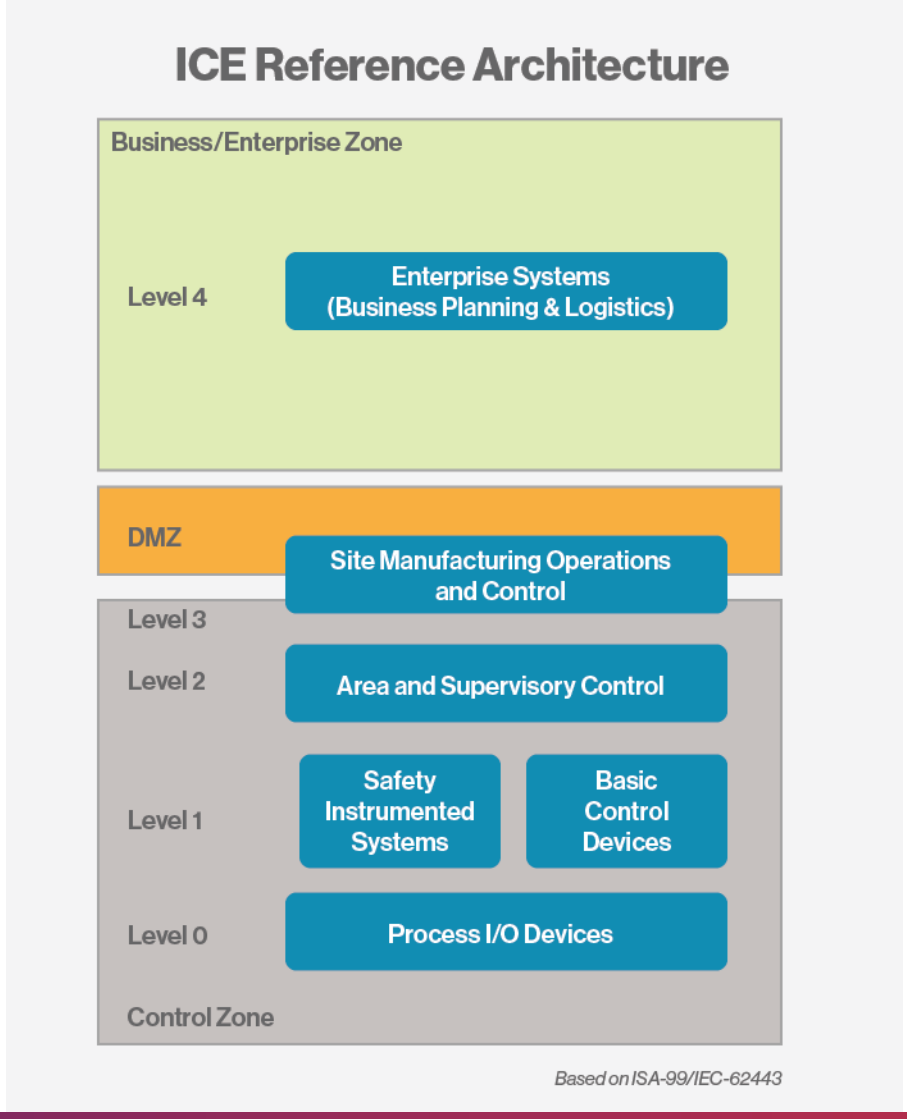
Цель Cybersecurity Framework

- Унификация подходов по безопасности информационных систем в разных отраслях на протяжении всего жизненного цикла
- Унифицированные требования
- Руководство по использованию международных стандартов
- Февраль 2014

- DCS
- PLC
- RTU
- IED
- SCADA
- Safety Instrumented Systems (SIS)
- Ассоциированные информационные системы
- Связанные люди, сети и машины

Основная парадигма

Основная сетевая модель



Три ключевых элемента CSF

- Ядро

  Определяет набор защитных мер

- Уровни реализации

  Определяет уровень зрелости в реализации CSF

- Профили

  Определяют текущий и желаемый профили защищаемой системы

Ядро CSF

Покрываемые CSF направления

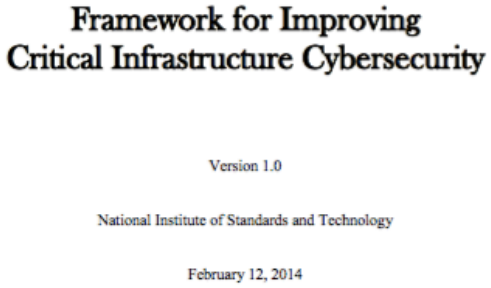
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Ссылки на другие стандарты

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	• **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	• **COBIT 5** APO02.06, APO03.01 • **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	• **COBIT 5** APO02.01, APO02.06, APO03.01 • **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 • **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	• **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 • **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	• **COBIT 5** DSS04.02 • **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	• **COBIT 5** APO01.03, EDM01.01, EDM01.02 • **ISA 62443-2-1:2009** 4.3.2.6 • **ISO/IEC 27001:2013** A.5.1.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	• **COBIT 5** APO13.12 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 • **NIST SP 800-53 Rev. 4** PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity,	• **COBIT 5** MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.7

Используемые стандарты

- Стандарты NIST 800-82 и 800-53
- ISA/IEC-62443
- ISO 27001/02
- Стандарты ENISA
- Стандарт Катара
- Стандарт API
- Рекомендации ICS-CERT
- COBIT
- Council on CyberSecurity (CCS)
  Top 20 Critical Security Controls (CSC)


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

Что можно взять от NIST CyberSecurity Framework?

Отличия CSF и 31-го приказа ФСТЭК

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Данный раздел в 31-м приказе отсутствует полностью

Процедура внедрения CSF

ENERGY SECTOR CYBERSECURITY FRAMEWORK IMPLEMENTATION GUIDANCE

JANUARY 2015

U.S. DEPARTMENT OF ENERGY
OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY

Пример текущего и желаемого профиля

Function	Category	Subcategory	Profiles
			Current
PROTECT (PR)	Access Control (PR.AC)	**PR.AC-3:** Remote access is managed	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1)

Function	Category	Subcategory	Profiles	
			Current	Target
PROTECT (PR)	Access Control (PR.AC)	**PR.AC-3:** Remote access is managed	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1)	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • ***NIST SP 800-53 Rev 4 AC-17 (3)*** • ***NIST SP 800-53 Rev 4 AC-17 (4)*** • NIST SP 800-53 Rev 4 AC-19 • ***NIST SP 800-53 Rev 4 AC-19 (5)*** • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1) • ***NIST SP 800-53 Rev 4 AC-20 (2)***

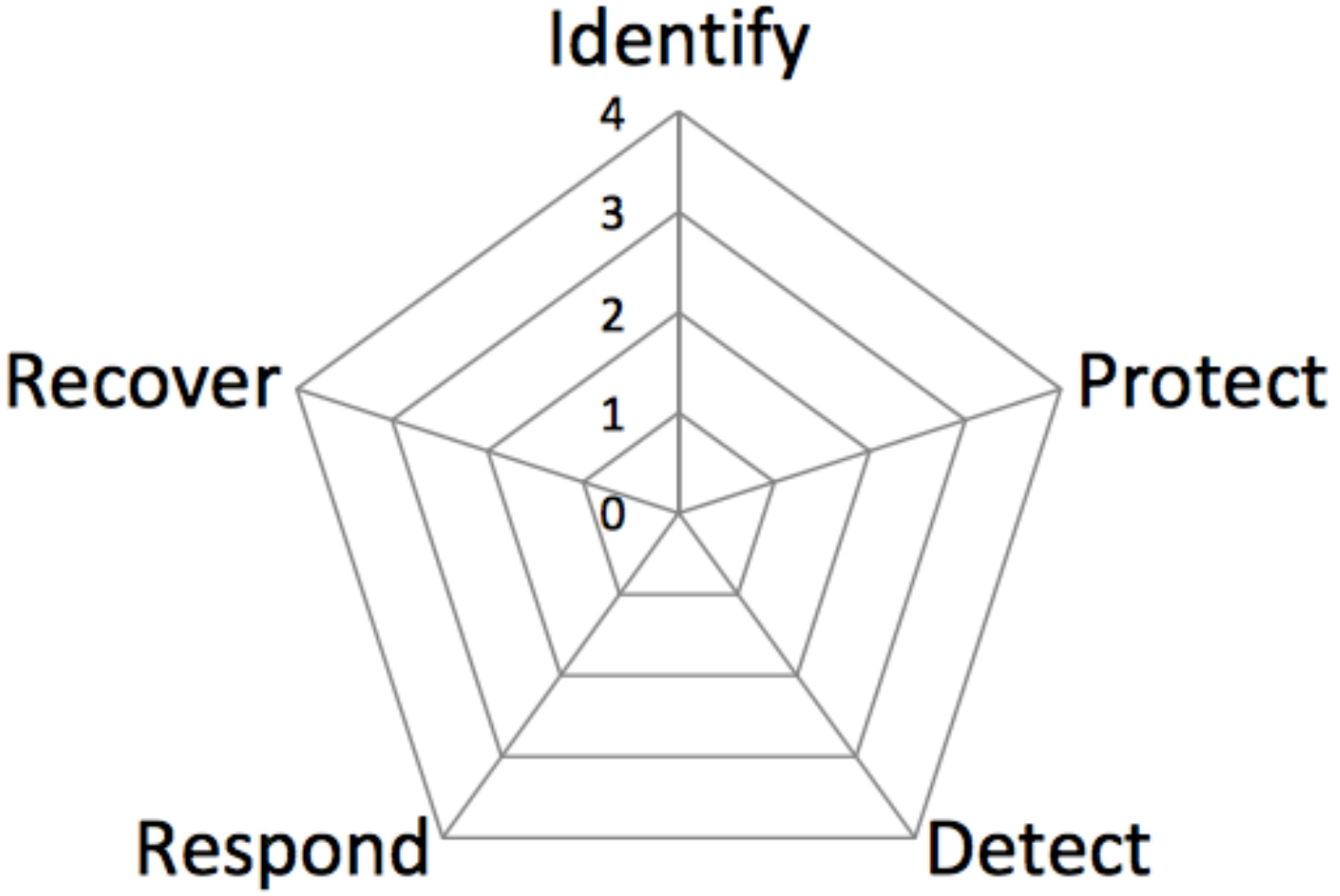
Анализ разрыва

Function	Category	Subcategory	Profiles		
			Current	Target	Gaps
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination • Supervisor signature required before VPN account issued • Bi-annual review of authorized VPN account list	• *Supervisor signature required before VPN account issued* • *Bi-annual review of authorized VPN account list*

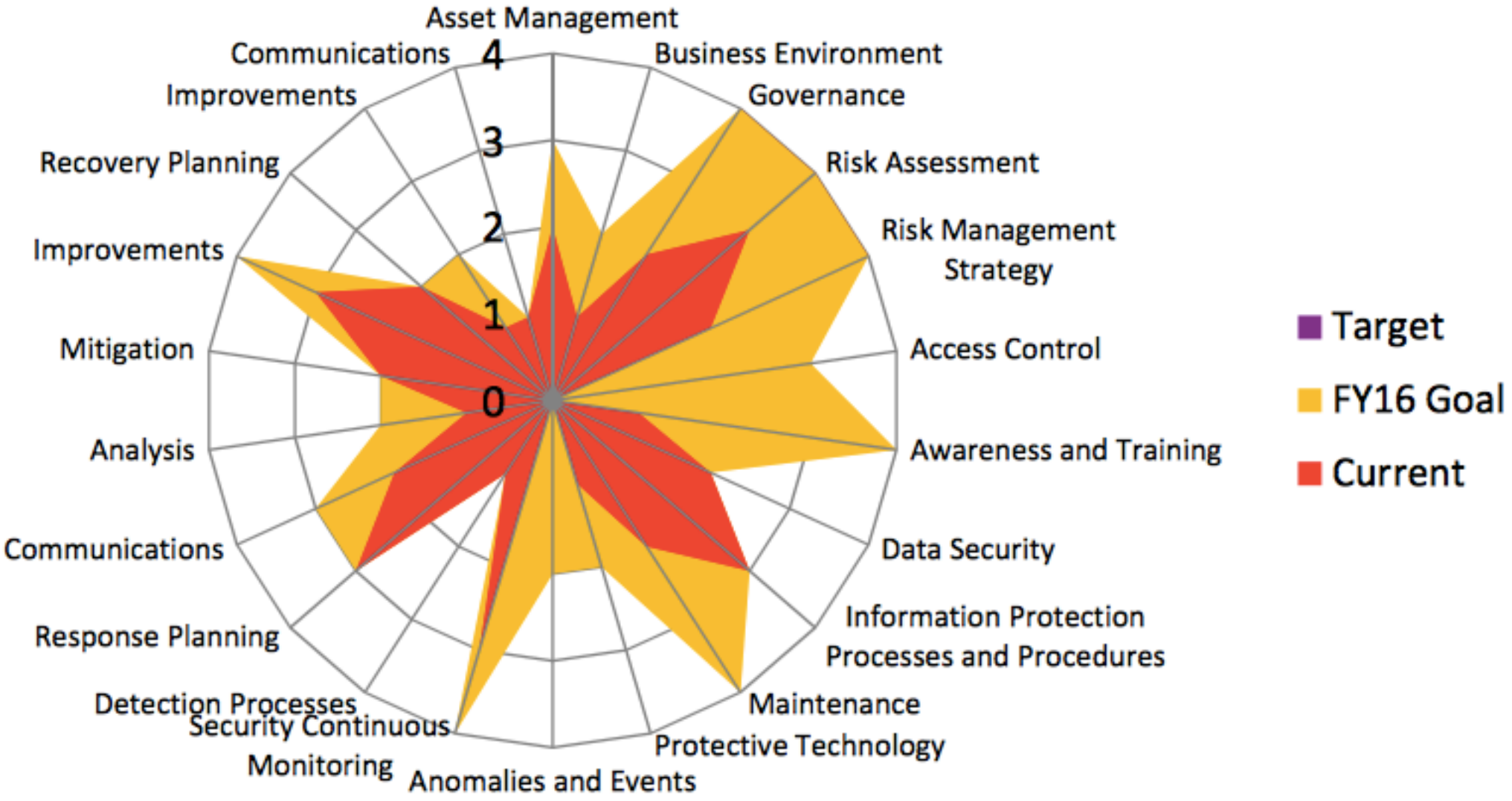
Анализ разрыва

Function	Category	Subcategory	Profiles		
			Current	Target	Gaps
PROTECT (PR)	Access Control (PR.AC)	**PR.AC-3:** Remote access is managed	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1)	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-17 (3) • NIST SP 800-53 Rev 4 AC-17 (4) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-19 (5) • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1) • NIST SP 800-53 Rev 4 AC-20 (2)	• ***NIST SP 800-53 Rev 4 AC-17 (3)*** • ***NIST SP 800-53 Rev 4 AC-17 (4)*** • ***NIST SP 800-53 Rev 4 AC-19 (5)*** • ***NIST SP 800-53 Rev 4 AC-20 (2)***

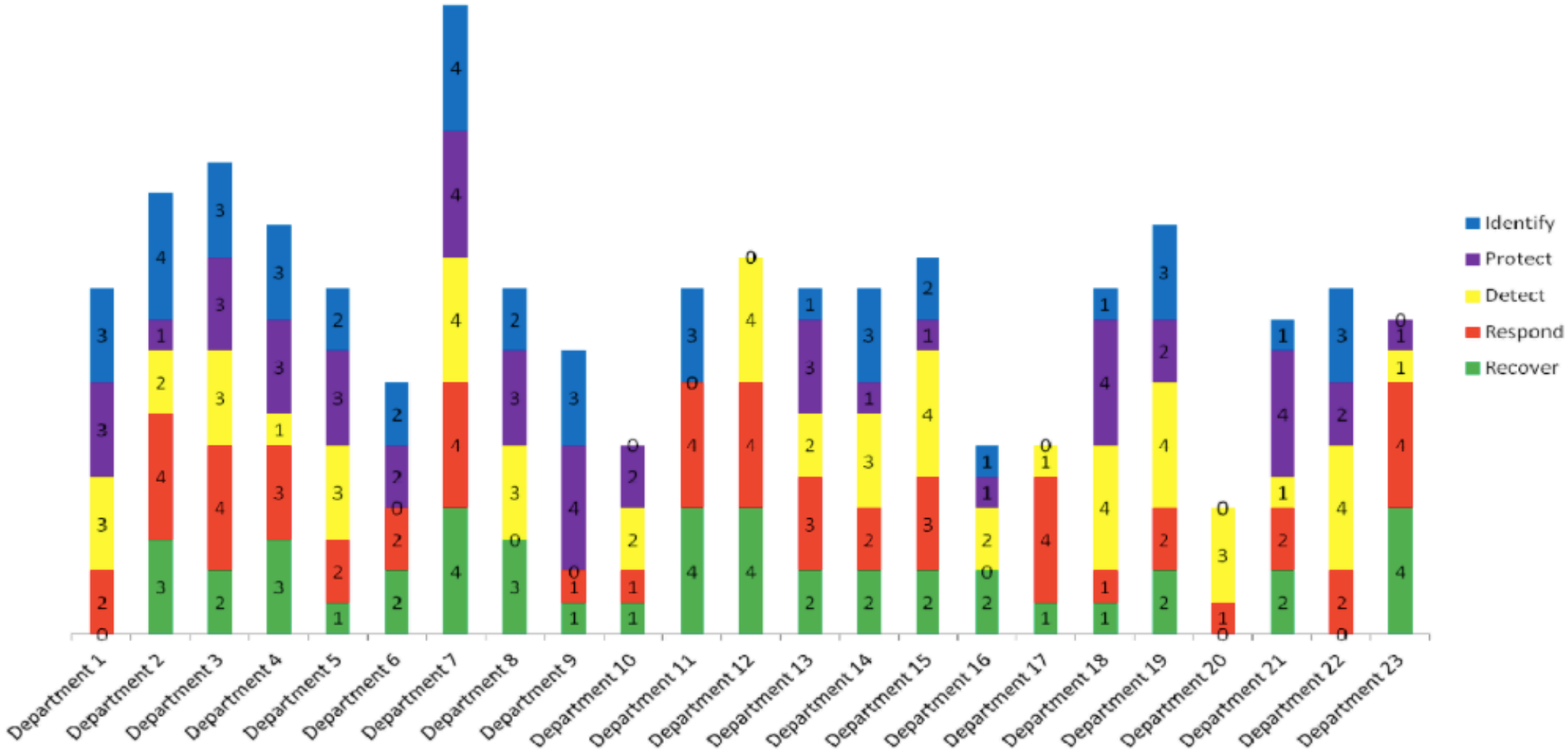
Оценка соответствия CSF (определение зрелости)



Пример оценки соответствия CSF



Соревнование между дочерними предприятиями



Где вы можете узнать больше?

Пишите на security-request@cisco.com

Быть в курсе всех последних новостей вам помогут:

- http://www.facebook.com/CiscoRu
- http://twitter.com/CiscoRussia
- http://www.youtube.com/CiscoRussiaMedia
- http://www.flickr.com/photos/CiscoRussia
- http://vkontakte.ru/Cisco
- http://blogs.cisco.ru/
- http://habrahabr.ru/company/cisco
- http://linkedin.com/groups/Cisco-Russia-3798428
- http://slideshare.net/CiscoRu
- https://plus.google.com/106603907471961036146/posts
- http://www.cisco.ru/

Благодарю за внимание