логарифмування над скінченими полем та еліптичними кривими, в результаті складена порівняльна таблиця цих алгоритмів. Описані базові стандарти, такі як DSA, ElGamal, ECDSA, ГОСТ Р 34.10-2001. Окрім цього розглядалися алгоритми, які аналогічно алгоритму RSA надають можливості відновлення повідомлення безпосередньо при верифікації цифрового підпису. Вони вирішують важливу задачу підпису – забезпечення, окрім цілісності даних, їх конфіденціальний захист. Проте можливості щодо відновлення всіх цих алгоритмів виявилися обмеженими: вони або не підходять для відновлення довгих повідомлень, коли потрібно вираховувати послідовно кілька підписів або один, що має великий розмір (схема p-NEW), або просто не були здатні на відновлення повідомлень довільної довжини (або їх частини довільної довжини) – схема Zhang.

Література: ***1.*** *Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си. - М.: Изд. ТРИУМФ, 2008. – 816 с.* ***2****. Nyberg K., Rueppel R. A New Signature Scheme Based on the DSA Giving Message Recovery / K. Nyberg, R. Rueppel // 1st ACM Conference on Computer and Communications Security. – Springer-Verlag, 1998. – P. 182 – 193.* ***3.*** *Ateniese, G., Medeiros, B.D. A Provably Secure Nyberg-Rueppel Signature Variant with Applications./ G. Ateniese, B.D Medeiros // IACR Cryptology ePrint Archive 2004.– 2004. – P. 93-110.* ***4****. Sujata M., Banshidhar M. A Digital Signature Scheme with Message Recovery and without One-Way Hash Function / M. Sujata, M. Banshidhar // International Conference on Advances in Computer Engineering. – Bangalore, 2010. – P. 265-267.* ***5.*** *Miyaji A. A message recovery signature scheme equivalent to DSA over elliptic curves // In Proceedings of ASIACRYPT'96. – Springer-Verlag, 1996. – P. 1-14.* ***6.*** *Pintsov L., Vanstone S. Postal Revenue Collection in the Digital Age / L. Pintsov, S. Vanstone // Financial Cryptography, Lecture Notes in Computer Science 1962. – Springer, 2000. – P. 105-120.* ***7.*** *Zhang. F. Identity-based partial message recovery signatures (or How to shorten ID-based signatures) / F. Zhang, W. Susilo, Y. Mu // Lecture Notes in Computer Science, 3570. – 2005. – P. 45–56.* ***8.*** *An Efficient ID-based Digital Signature with Message Recovery Based on Pairing / Raylin Tso, Chunxiang Gu, Takeshi Okamoto, and others // IACR Cryptology ePrint Archive, Vol. 2006. – 2006/195.* ***9.*** *Мао В. Современная криптография: теория и практика. – Пер. с англ. – М.: Издательский дом Вильямс, 2005. – 768 с.*

УДК 004.056.5

АНАЛИЗ И ОЦЕНКА НОРМАТИВНЫХ ДОКУМЕНТОВ, ПРИМЕНЯЕМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SMART GRID СИСТЕМ

Алексей Юдин, Глеб Пирогов
ГосНИИ Спецсвязи

Аннотация: **Статья описывает требования и нормы, устанавливаемые нормативными документами, применяющимися в мире для обеспечения информационной безопасности Smart Grid.**
Abstract: **This paper describes the requirements and standards set by regulations which apply in the world of information security Smart Grid.**
Ключевые слова: **Информационная безопасность, Smart Grid, международный стандарт.**

Введение

Актуальность проведения анализа зарубежных нормативных документов, касающихся информационной безопасности, вызвана тем, что на сегодня в мире Smart Grid системы только начинают создаваться и развиваться, а в Украине они вообще нормативно не закреплены и не описаны. Под термином Smart Grid будем понимать электрическую сеть которая использует информационные и коммуникационные технологии, а также информацию о поведении поставщиков и потребителей, с целью автоматизации процесса улучшения продуктивности, надежности, экономичности и стойкости производства и распространения электрической энергии. Также, необходимо подчеркнуть, что внедрение Smart Grid систем направлено на обеспечение энергетической безопасности Украины, то есть способности государства обеспечить максимально надежное, технически безопасное, экологическое и обоснованно достаточное энергообеспечение экономики и населения [1].

В статье будем рассматривать Smart Grid систему как совокупность подсистемы передачи электрической энергии и информационно-телекоммуникационной подсистемы [2 – 4] и в соответствии с этим осуществлять анализ существующих нормативных документов.

I Объект анализа

В ходе проведения исследований нормативных документов, которые относятся к обеспечению информационной безопасности систем управления, систем диспетчерского управления и сбора данных (SCADA), автоматизированных систем управления технологическим процессом (АСУ ТП) и Smart Grid, были выделены следующие документы:

Международные стандарты

1. Institute of Electrical and Electronics Engineers (IEEE)

- IEEE 1402. IEEE Guide for Electric Power Substation Physical and Electronic Security;
- IEEE 1686. 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.

2. International Organization for Standardization (ISO)

ISO 27019. Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002.

3. International Electrotechnical Commission (IEC)

- IEC TR 62210. Power system control and associated communications. 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/TS 62443-1-1. Industrial communication networks - Network and system security - Part 1-1: Terminology;
  - IEC/TR 62443-3-1. Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems;
  - IEC/PAS 62443-3. Security for industrial process measurement and control - Network and system security.
- 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;
  - 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;
  - IEC 62351-8 (project): Data and Communication Security – Power systems management and associated information exchange. Role-based access control.
- IEC/TR 62357. Power system control and associated communications - Reference architecture for object models, services and protocols.

Национальные отраслевые стандарты

4. National Institute of Standards and Technology (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:
  - Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements;
  - Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid;
  - Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References.

5. Industrial Automation and Control Systems Security (ISA)

ISA SP-99:

- ISA 99.00.01. Security for Industrial Automation and Control Systems: Concepts, Models and Terminology;
- ISA 99.00.02. Establishing an Industrial Automation and Control Systems Security Program;
- ISA 99.00.03. Operating an Industrial Automation and Control Systems Security Program;
- ISA 99.00.04. Specific Security Requirements for Industrial Automation and Control Systems.

6. American Gas Association (AGA)

- AGA 12-1 Background, Policies and Test Plan;
- AGA 12-2 Retrofit Link Encryption for Asynchronous Serial Communications;
- AGA 12-3 Protection of Networked Systems;
- AGA 12-4 Protection Embedded in SCADA Components.

7. North American Electric Reliability Corporation (NERC)

- NERC CIP-002. Cyber Security - Critical Cyber Asset Identification;
- NERC CIP-003. Cyber Security - Security Management Controls;
- NERC CIP-004. Cyber Security - Personnel & Training;
- NERC CIP-005. Cyber Security - Electronic Security Perimeter(s);
- NERC CIP-006. Cyber Security - Physical Security of Critical Cyber Assets;
- NERC CIP-007. Cyber Security - Systems Security Management;
- NERC CIP-008. Cyber Security - Incident Reporting and Response Planning;
- NERC CIP-009. Cyber Security - Recovery Plans for Critical Cyber Assets;
- NERC CIP-010. Cyber Security - Configuration Change Management and Vulnerability Assessments;
- NERC CIP-011. Cyber Security - Information Protection.

II Общее описание нормативных документов

1. IEEE 1402. IEEE Guide for Electric Power Substation Physical and Electronic Security.

Стандарт носит общий характер и определяет основные подходы к планированию, проектированию, строительству и эксплуатации электрических подстанций. Данный стандарт не содержит детальных спецификаций по обеспечению информационной безопасности.

2. IEEE 1686. IEEE Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities.

Стандарт описывает спецификации, которые необходимо выполнить для оценки защищенности интеллектуальных электронных устройств (ИЭУ). Этот документ дает возможность оценить функции обеспечения кибербезопасности как уже примененных ИЭУ, так и тех, которые планируется использовать.

3. IEEE P1711. Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.

Документ разработан на базе отраслевого стандарта AGA 12-2 «Retrofit Link Encryption for Asynchronous Serial Communications» и описывает механизм шифрования для асинхронного последовательного канала связи. Стандарт предписывает использовать криптографические алгоритмы, которые утверждены NIST и реализованы в соответствии с федеральным стандартом FIPS PUB 140-2.

4. ISO 27019. Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002.

На сегодня указанный стандарт находится в стадии разработки. Основным его назначением будет детализация общих требований ISO/IEC 27002 для предприятий энергетической отрасли, которые эксплуатируют системы реального времени. Планируется использовать стандарт совместно с ISO/IEC 27002. Также планируется, что стандарт будет содержать требования к системам безопасности расширенной измерительной инфраструктуры (Advanced Metering Infrastructure, AMI) и соответствующие профили безопасности.

5. IEC TR 62210. Power system control and associated communications. Data and communication security.

Этот документ является техническим отчетом, делающим акцент на механизмах защиты коммуникационных протоколов, которые применяются в сетях управления электрических систем. Также в документе приведены примеры уязвимости систем и возможные пути их блокирования. В отчете уделено особенное внимание отсутствию механизмов аутентификации устройств.

6. IEC 61784-4. Digital data communications for measurement and control – Profiles for secure communications in industrial networks.

Стандарт описывает возможные угрозы и порядок анализа последствий их реализации, требования к системам безопасности связи, порядок осуществления удаленного доступа посредством модема, а также устанавливает профили безопасности управляющего центра, корпоративной сети, сети высшего уровня управляющего центра, удаленного управления с помощью сети Интернет или Интранет.

7. IEC 62443. Security for industrial process measurement and control – Network and system security.

Данный стандарт разработан на базе отраслевых стандартов ANSI/ISA 99 и на сегодня состоит из следующих частей:

- IEC/TS 62443-1-1. Industrial communication networks - Network and system security - Part 1-1: Terminology;
- IEC/TR 62443-3-1. Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems;
- IEC/PAS 62443-3. Security for industrial process measurement and control - Network and system security, а также, на сегодня разрабатывается четвертая часть IEC 62443-4-1, которая будет описывать требования к поставщикам оборудования и решений.

В целом, стандарт описывает:

- основные понятия и термины, которые связаны с безопасностью производства и системой управления;
- практические рекомендации по составлению планов направленных на обеспечение безопасности;

- конкретные требования к безопасности производства и системам управления с учетом специфики промышленных сетей;
- жизненный цикл программного обеспечения защиты систем управления, а также планирования промышленного производства

8. IEC 62351. Data and Communication Security.

Стандарт рассматривает вопросы информационной безопасности подсистем управления энергосистемами. Также документ говорит о необходимости модернизации ряда стандартов, определенных IEC TC 57, для обеспечения безопасности коммуникационных протоколов. В частности, речь идет о стандартах описывающих коммуникационные сети энергосистем, а именно: IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970, IEC 61968. В стандарте вводится базовое понятие «конечной безопасности» под которым понимается защита информации во всем тракте передачи, от пункта создания до пункта использования. Опираясь на это понятие 3 – 6 части документа определяют механизмы улучшения безопасности коммуникационных профилей. В тоже время 7 и 8 части стандарта посвящены вопросам авторизованного доступа и обеспечения безопасности информации во время ее передачи между различными подсистемами.

9. ISA-99

Этот отраслевой стандарт описывает подходы к обеспечению информационной безопасности системы производства и управления производством. Стандарт был опубликован как ANSI/ISA-99 в 2007 году, а в 2010 переиздан как ANSI/ISA-62443. Стоит отметить, что на базе ANSI/ISA-62443 разработан стандарт IEC 62443. Security for industrial process measurement and control – Network and system security (рассмотрен выше). Таким образом, ISA-99 полностью вошел в IEC 62443 и развивается как ANSI/ISA и IEC. Зоны ответственности частей стандарта IEC 62443 представлены на рис. 1.

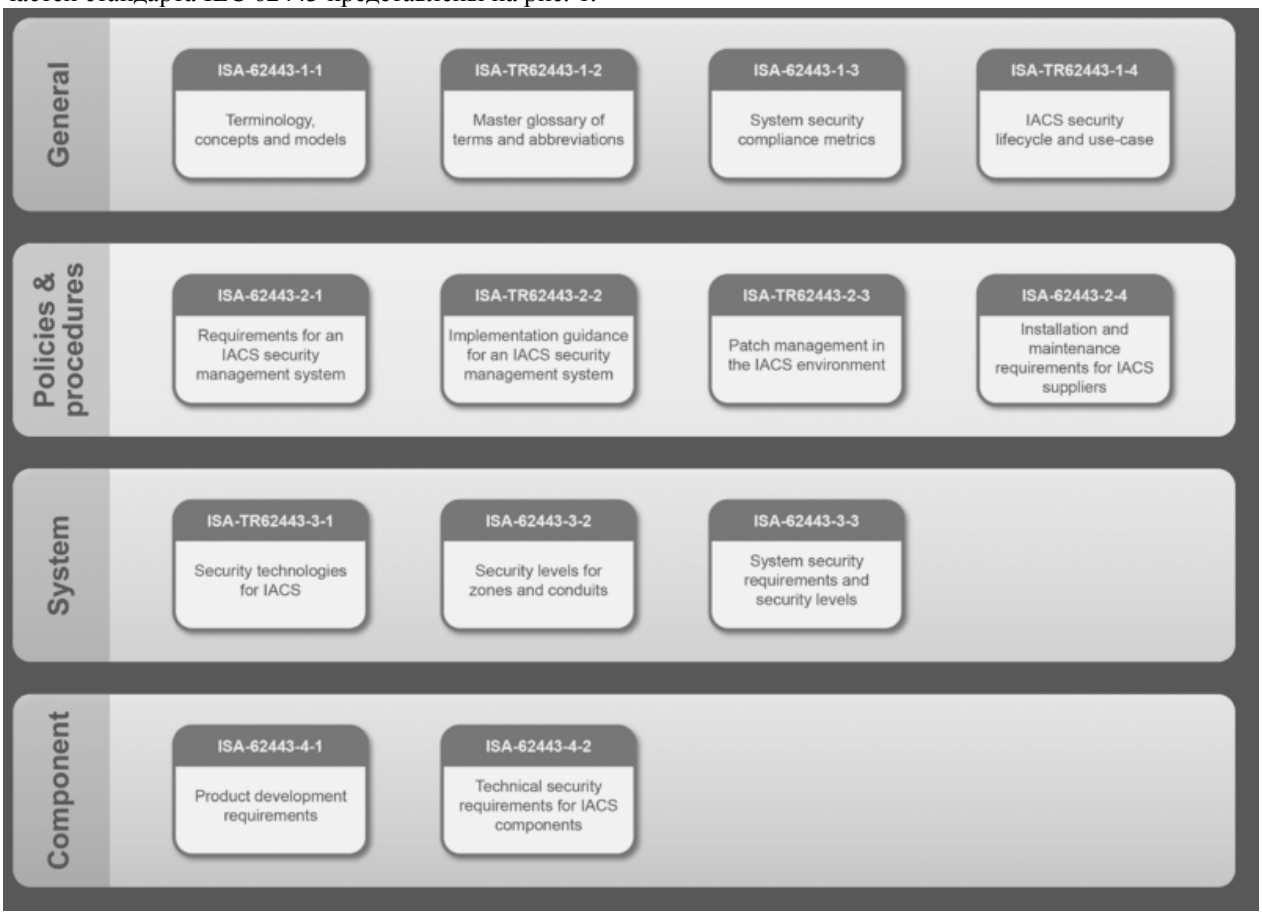

Рисунок 1 - Зоны ответственности частей стандарта IEC 62443

10. AGA 12

AGA 12 является пакетом документов, который предлагает практические решения, связанные с защитой SCADA от кибер-атак. Акцент делается на обеспечении конфиденциальности связи как механизма

авторизации пользователя. На сегодня эти документы описывают механизмы шифрования асинхронных последовательных протоколов, защиты сетевых систем и защиты встроенных компонент SCADA.

Следует отметить, что AGA 12 предлагает использовать криптографические алгоритмы, утвержденные NIST и соответствующие FIPS PUB 140-2.

Учитывая то, что документ направлен на описание защиты SCADA в целом, его можно использовать в сферах деятельности отличных от газовой промышленности, например водопроводные системы, электро- и трубопроводы и др.

11. NERC CIP. Cyber Security.

Документ является группой из 11 нормативных актов, регламентирующих вопросы обеспечения кибербезопасности в SCADA и других критически важных объектов инфраструктуры электросистем. Также, он определяет минимальные требования необходимые для обеспечения соответствия и надежности электросистем. Стандарт описывает практически все уровни обеспечения безопасности от физической охраны до защиты систем управления. В то же время необходимо отметить, что степень детализации этих требований довольно низкая, а сами требования носят декларативный характер.

12. NIST SP800-53. Security and Privacy Controls for Federal Information Systems and Organizations

Документ регламентирует обеспечение безопасности систем управления типа SCADA федеральных информационных систем и ориентирован на широкую аудиторию – от разработчика до поставщика услуг. В стандарте дано подробное описание профилей безопасности и механизмов их обеспечения. Профили группируются по семействам (таблица).

Таблица - Семейства профилей

AC	Access Control (Управление доступом)	MP	Media Protection (Защита носителей информации)
AT	Awareness and Training (Компетентность и обучение)	PE	Physical and Environmental Protection (Физическая защита и защита окружающей среды)
AU	Audit and Accountability (Аудит и отчетность)	PL	Planning (Планирование)
CA	Security Assessment and Authorization (Оценка безопасности и авторизация)	PS	Personnel Security (Безопасность персонала)
CM	Configuration Management (Управление конфигурацией)	RA	Risk Assessment (Оценка рисков)
CP	Contingency Planning (Планирование чрезвычайных обстоятельств)	SA	System and Services Acquisition (Системы и сервисы сбора данных)
IA	Identification and Authentication (Идентификация и аутентификация)	SC	System and Communications Protection (Защита систем и коммуникаций)
IR	Incident Response (Реагирование на инциденты)	SI	System and Information Integrity (Целостность систем и информации)
MA	Maintenance (Сопровождение)	PM	Program Management (Управление ПО)

Также следует отметить, что данный документ является одним из серии стандартов, направленных на реализацию управления рисками. Взаимосвязь стандартов представлена на рис. 2.

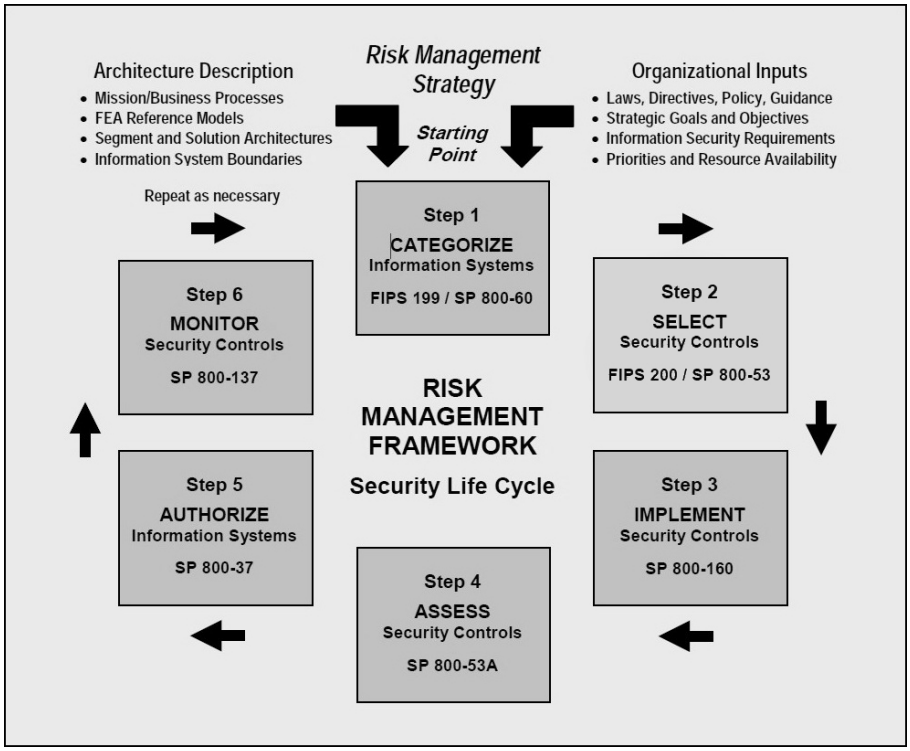

Рисунок 2 - Взаимосвязь стандартов по управлению рисками

13. NIST SP800-82. Guide to Industrial Control Systems Security

Стандарт дает рекомендации по обеспечению безопасности систем промышленного управления (ICS), в том числе и SCADA, а также распределенных систем управления (DCS). В документе содержится обзор ICS и их стандартных топологий, определяются типовые угрозы и уязвимости. Стандарт также предоставляет рекомендации по контрмерам угрозам безопасности.

NIST SP800-82 состоит из нескольких разделов, которые описывают:

- обзор SCADA и других ICS, а также обоснование необходимости обеспечения их безопасности;
- отличия между ICS и информационно-телекоммуникационными системами;
- угрозы, уязвимости и инциденты;
- процесс разработки и внедрения программного обеспечения ICS;
- рекомендации по интеграции механизмов обеспечения безопасности в сетевых архитектурах ICS;
- выводы по управлению, оперативным и техническим средствам контроля, которые описаны в NIST SP800-53, а также указания о том, как эти средства обеспечения безопасности применяются в ICS.

14. NISTIR 7628. Guidelines for Smart Grid Cyber Security.

Данный нормативный документ является первым, который описывает кибербезопасность в Smart Grid системах. Как и IEC 62351 и NIST SP800-53 он устанавливает профили безопасности, а также приводит соответствие профилей безопасности по отношению к NIST SP800-53 и NERC CIP.

Этот документ интересен тем, что рассматривает вопросы безопасности в таких доменах Smart Grid как генерирующие компании, передающие и распределяющие компании, потребители, поставщики услуг, операторы и рынок, таким образом, охватывая все сегменты взаимодействия Smart Grid. Это взаимодействие изображено на рисунке 3 [5].

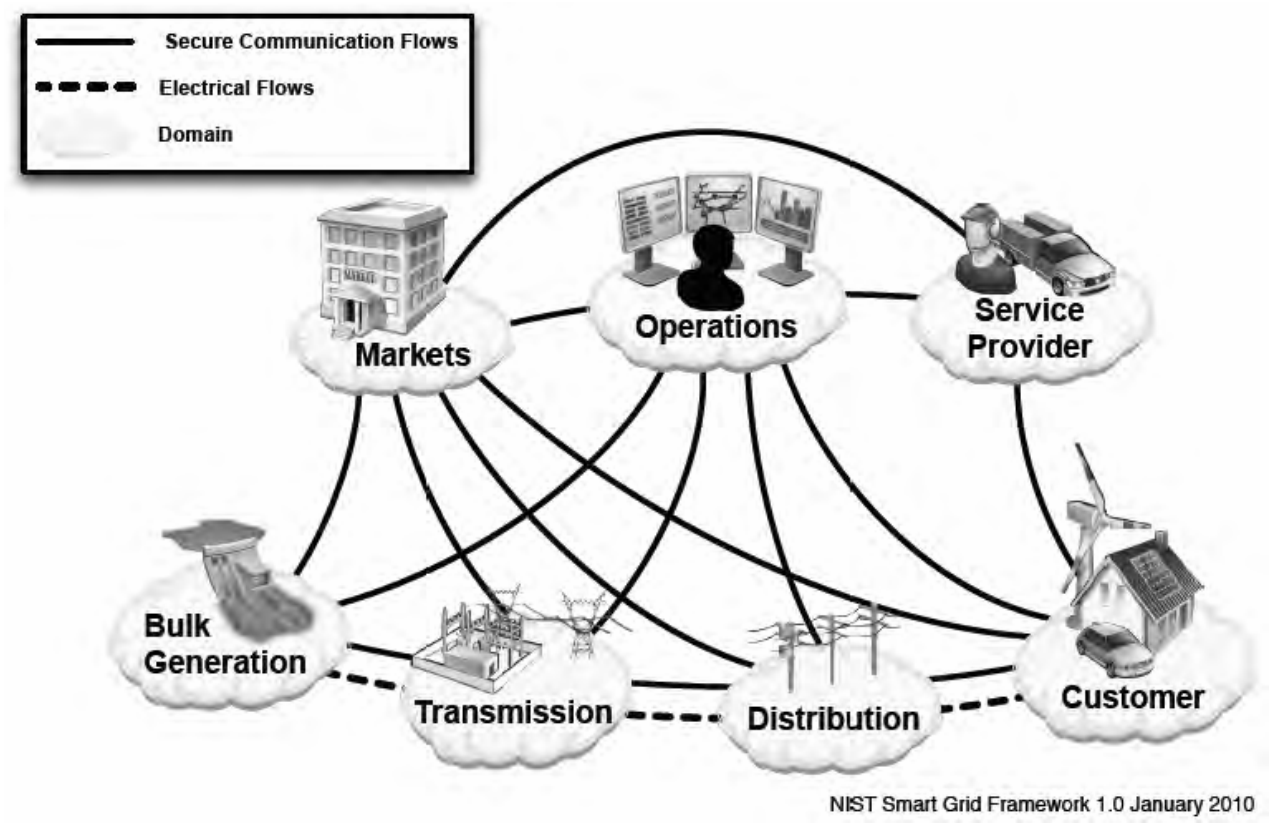

Рисунок 3 - Взаимодействие доменов Smart Grid

Также, в NISTIR 7628 дано описание множества объектов и субъектов, которые принадлежат к обозначенным доменам, и определены взаимосвязи между ними. Причем, взаимосвязи объектов и субъектов описаны с точки зрения необходимости обеспечения целостности, конфиденциальности и доступности. Еще одним интересным обстоятельством является то, что NISTIR 7628 описывает требования к криптографическим механизмам защиты информации. Эти требования изложены с учетом дальнейшей перспективы развития (2030 год) систем безопасности.

Выводы

1. Стандарты, разработанные Институтом инженеров по электротехнике и электронике, касаются электрических подстанций и различных интеллектуальных устройств. Данные документы не описывают вопросы обеспечения безопасности во всех доменах Smart Grid.

2. Документы Международной организации по стандартизации на сегодня находятся на стадии разработки. Стандарт ISO 27019, судя по содержанию проекта документа, будет содержать сведения о базовых механизмах защиты электрических подстанций и интеллектуальных устройств. То есть, стандарты этой серии смогут охватить четыре из семи доменов – генерирующие, передающие, распределяющие организации и потребителя.

3. Стандарты, разработанные Международной электротехнической комиссией, а именно IEC 61784, 62443, 62351 и TR 62210, также ориентированы на обеспечение информационной безопасности систем производства и управления производством. Данная серия довольно детально и полно описывает защиту трех доменов - генерирующих, передающих и распределяющих организаций.

4. Серия стандартов NERC CIP, в основном, ориентирована на обеспечение кибербезопасности в SCADA. Эти документы носят декларативный характер и также не учитывают специфику обеспечения информационной безопасности в Smart Grid.

5. Стандарты Национального института стандартизации и технологий описывают вопросы безопасности в промышленных системах. В тоже время технический отчет NISTIR 7628 вводит понятие кибербезопасности в Smart Grid системах. Данный документ является первым ориентированным именно на

Smart Grid и наиболее полно дает описание множества объектов и субъектов Smart Grid, их взаимодействия и механизмов защиты.

Таким образом, можно предположить, что для понимания процесса обеспечения информационной безопасности Smart Grid систем наиболее полно подходит технический отчет NISTIR 7628, так как именно этот документ описывает отличия в подходах к обеспечению информационной безопасности SCADA, АСУ ТП и Smart Grid.

*Литература: **1**. Енергетична безпека України: стратегія та механізми забезпечення / [Шевцов А. І., Земляний М. Г., Бараннік В. О. та ін.] / За ред. А. І. Шевцова. - Дніпропетровськ: Пороги, 2002. – 264 с. **2**. Україна. Закони. Про електроенергетику : офіц. текст : [прийнятий Верховною Радою 16 жовтня 1997 р.]. - К.: Відомості Верховної Ради України, 1998, № 1. **3**. Україна. Закони. Про захист інформації в інформаційно-телекомунікаційних системах : офіц. текст : [прийнятий Верховною Радою 5 липня 1994 р.]. - К.: Відомості Верховної Ради України, 1994, №31. **4**. The path of the smart grid / H. Farhangi. // IEEE Power and Energy Magazine, - 2010. - Vol. 8, № 1. – P. 18-28. **5**. NISTIR 7628. Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements // National Institute of Standards and Technology. – 2010. – 15 p.*