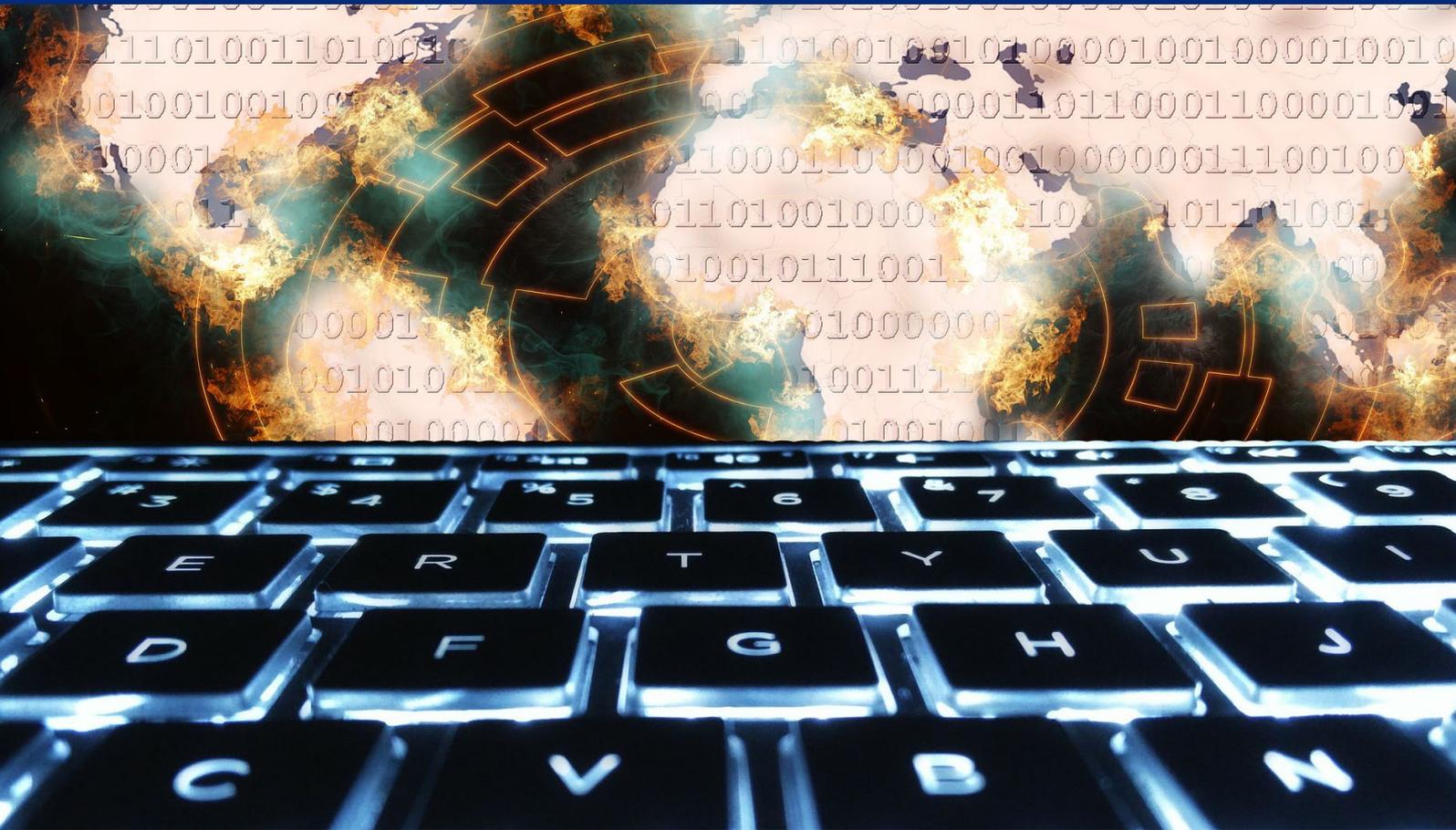




**USAID**  
FROM THE AMERICAN PEOPLE

# РОЛЬ ОРГАНОВ РЕГУЛИРОВАНИЯ КОММУНАЛЬНОЙ СФЕРЫ В УКРЕПЛЕНИИ КИБЕРБЕЗОПАСНОСТИ Отказоустойчивость, оценка риска и стандарты



**Апрель 2020**

Настоящая публикация разработана для рассмотрения Агентства США по международному развитию. Подготовлена Национальной ассоциацией членов комиссий по регулированию коммунальных предприятий.

# РОЛЬ ОРГАНОВ РЕГУЛИРОВАНИЯ КОММУНАЛЬНОЙ СФЕРЫ В УКРЕПЛЕНИИ КИБЕРБЕЗОПАСНОСТИ

## Отказоустойчивость, оценка риска и стандарты

Наименование проекта: Европейско-евразийская инициатива по кибербезопасности в энергетике

Отдел-спонсор в ЮСАИД: Бюро ЮСАИД по Европе и Евразии

Соглашение о сотрудничестве: AID-OAA-A-16-00049

Получатель: Национальная ассоциация членов комиссий по регулированию коммунальных предприятий (НАРУК)

Дата публикации: Апрель 2020 г.



*Настоящая публикация осуществлена при поддержке Отдела энергетики и инфраструктуры Бюро по Европе и Евразии согласно условиям Соглашения о сотрудничестве с Национальной ассоциацией членов комиссий по регулированию коммунальных предприятий No. AID – OAA-A-16-00049. Мнения, высказанные в настоящей публикации, принадлежат ее авторам и могут не отражать мнения Агентства США по международному развитию и Национальной ассоциации членов комиссий по регулированию коммунальных предприятий.*

## Благодарности

---

Пособие «Роль органов регулирования коммунальной сферы в укреплении кибербезопасности: отказоустойчивость, оценка риска и стандарты» разработано совместно с Национальной ассоциацией членов комиссий по регулированию коммунальных предприятий (НАРУК) при щедрой поддержке Агентства международного развития США (ЮСАИД).

НАРУК выражает признательность группе авторов, безвозмездно уделивших время подготовке настоящего документа, в целях помочь органам регулирования энергетики разных стран мира провести оценку возможных вариантов повышения кибербезопасности электроэнергетики. Следует особо отметить группу технических экспертов, которую удалось сформировать из специалистов трех различных организаций, расположенных на двух континентах, для совместного решения масштабной задачи по обмену опытом и наработками с национальными органами регулирования энергетики.

### Ведущие авторы

- **Стефано Бракко**, Агентство по сотрудничеству органов регулирования энергетики (ACER) Администратор базы знаний и начальник службы безопасности отдела по работе с корпоративными клиентами Агентства по сотрудничеству органов регулирования энергетики Европейского союза. Последние 22 года Стефано Бракко работает в различных структурах и органах Евросоюза, занимаясь в основном реализацией стратегий в различных областях. Исследователь и соавтор работ, опубликованных в международных рецензируемых научных журналах и представленных на международных научных конференциях, по ряду тематик (энергетика, ядерная энергетика, обработка естественно-языковых текстов и биоинформатика). Обладает обширными знаниями в области кибербезопасности энергосектора Европы. Председатель и сопредседатель Целевых рабочих групп по кибербезопасности энергетики в части нормативно-правового регулирования и член Целевой группы Комиссии Европейского союза по «умным» электросетям.
- **Франсис Кливленд**, Xanthus Consulting International, от имени Системного комитета-Целевой группы по «умной» энергетике – кибербезопасности Международной электротехнической комиссии (МЭК) ([www.iec.ch](http://www.iec.ch)).<sup>1</sup> Более 35 лет Франсис Кливленд занимается управлением и консультациями по вопросам информационно-контрольных систем, связанных с «умными» электросетями, в электроэнергетике. Ее опыт и экспертные знания включают информации о стандартах совместимости «умных» электросетей, функционале «умных» инверторов для распределенных источников энергии (РИЭ), вопросов кибербезопасности, отказоустойчивости электросети, а также интеграции систем, включая РИЭ, электромобили с подзарядкой от сети (ЭПС), инфраструктуры «умных» счетчиков (ИИС), системы автоматизации распределительной сети (АРС), системы автоматизации подстанций, производственные информационные системы (SCADA), и операции на рынке энергоресурсов. В Международной электротехнической комиссии (МЭК) и Институте по электротехнике и электронике (IEEE). В частности, Франсис Кливленд является:
  - научным руководителем Рабочей группы 15 ТК 57 МЭК по стандартам кибербезопасности работы энергетических систем МЭК 62351;
  - редактором Рабочей группы 17 ТК 57 МЭК по стандарту информационных моделей МЭК 61850-7-420 для систем РИЭ, электромобилей и автоматизации распределительной сети;

---

<sup>1</sup> [http://xanthus-consulting.com/about\\_xanthus/staff.html](http://xanthus-consulting.com/about_xanthus/staff.html)

- руководителем Целевой группы по разработке Принципов кибербезопасности для Системного комитета – Целевой группы по «умной» энергетике МЭК (SyC-SE) и член Рабочей группы 2, Рабочей группы 3, Рабочей группы 5 и Рабочей группы 6;
  - техническим консультантом от США Консультативного комитета по информационной безопасности и конфиденциальности данных (ACSEC) МЭК (кибербезопасность).
  - техническим консультантом по ТК 57 МЭК Рабочей группы 17 (Распределенные источники энергии), Рабочей группы 14 (Общая информационная модель распределения и интеграции развитой измерительной инфраструктуры), Рабочей группы 03 (Дистанционное управление удаленным оконечным устройством), Рабочей группы 07 (Протокол внутренней передачи данных между центрами управления (ICCP)), Рабочей группы 15 (Информационная безопасность), Рабочей группы 16 (Рыночные операции), Рабочей группы 19 (Гармонизация стандартов ТК 57);
  - секретарем IEEE 1547.3 по подготовке рекомендаций в области кибербезопасности для РИЭ, отвечающих требованиям по объединению энергосетей IEEE 1547.
- **Тим Конвей, SANS Institute**  
Технический директор программ Промышленных систем управления (ПСУ) и Производственных информационных систем (SCADA) в SANS. Отвечает за разработку, анализ и внедрение технических компонентов ассортимента продукции ПСУ и SCADA, предлагаемого SANS. Ранее занимал должность Директора по соблюдению требований к системам защиты важнейших объектов инфраструктуры и операционным технологиям Государственной компании по коммунальному обслуживанию северной Индианы (НИПСКО). Кроме того, он отвечает за операционные технологии, соблюдение требований СИП NERC и учебную базу NERC по подготовке персонала эксплуатационных служб компании в НИПСКО Электрик. До своей работы в SANS Тим Конвей в течение восьми лет занимал должность инженера по вычислительным комплексам систем управления энергопотреблением (СУЭП) в компании НИПСКО, отвечая за работу серверов систем управления и вспомогательной сетевой инфраструктуры. Он входил в состав различных комиссий, включая Группу подготовки рабочих предложений Комитета по защите важнейших объектов инфраструктуры (RFC CIPC), Группу подготовки проекта интерпретации требований СИП NERC (CIP NERC), Ресурсный центр по кибербезопасности национального электроэнергетического сектора (НЕСКОР) и другие.<sup>2</sup>

Авторы признательны бывшим сотрудникам НАРУК Жизель Рей и Крисси Годфри за рекомендации и редакторскую правку в процессе разработки настоящего пособия. Авторы также благодарят нижеперечисленных специалистов по регулированию в энергетике за предоставленное время, а также профессиональные знания и ценные соображения по разработке данного документа в целом.

#### **Экспертно-консультационный комитет**

- Линн Константины, Центр партнерства и инноваций НАРУК
- Майк Ассанте, SANS Institute
- Константинос Мулинос, Европейское агентство по сетевой и информационной безопасности (ЭНИСА)
- Ардиан Бериша, Региональная ассоциация органов регулирования энергетики (ЭРРА)

---

<sup>2</sup> <https://www.sans.org/security-awareness-training/tim-conway>

## Содержание

Благодарности.....	3
Аннотация .....	7
1 Введение.....	9
2 Важнейшие принципы кибербезопасности и отказоустойчивости с точки зрения органов регулирования .....	10
2.1 Отказоустойчивость как комплексная стратегия обеспечения безопасности коммунальных услуг .....	11
2.2 Система безопасности, встроенная в архитектуру, как наиболее экономически эффективный подход.....	12
2.3 ИТ и ЭТ: различия в требованиях к безопасности информационно-технического и эксплуатационно-технического комплексов .....	15
2.4 Оценка риска, снижение риска, процессы в жизненном цикле и оповещение о нарушениях .....	17
2.5 Стандарты и передовой опыт кибербезопасности в энергетике.....	19
3 Регламенты кибербезопасности, которые органы регулирования могут рекомендовать коммунальным предприятиям в целях повышения их безопасности .....	22
3.1 Подготовительные этапы .....	22
3.2 Порядок оценки рисков .....	23
3.3 Последующий переход на регламенты и типовые технические средства безопасности .....	25
4 Выводы .....	25
5 Приложение. Стандарты и передовой опыт в сфере кибербезопасности ...	27
A.1 NIST Базовая структура кибербезопасности .....	27
A.2 Стандарты ИСО/МЭК серии 27000 .....	29
A.2.1 Серия стандартов ИСО/МЭК 27001 .....	30
A.2.2 ИСО-МЭК 27002:2013.....	31
A.2.3 ИСО-МЭК 27019:2017.....	32
A.3 НЕРК Защита объектов критической инфраструктуры (CIP).....	33
A.3.1 Основные факты.....	33
A.3.2 Стандарт, разработанный специалистами отрасли для отрасли	34
A.3.3 Физические и кибер-угрозы стабильности электрических сетей	34
A.3.4 Требования к традиционным ИТ-ресурсам и ЭТ-ресурсам .....	34
A.3.5 Выводы.....	35
A.3.6 Четыре основных вопроса .....	36
A.4 NISTIR 7628 Пособие по кибербезопасности в «умных» электрических сетях.....	37
A.4.1 NISTIR 7628 Средства обеспечения кибербезопасности .....	37
A.4.2 NISTIR 7628 Эталонная логическая модель кибербезопасности	37
A.5 МЭК 62443 Стандарты на промышленные средства автоматизации ...	39
A.5.1 МЭК 62443 Основные факты .....	39
A.5.2 МЭК 62443 Основные факты .....	39
A.5.3 МЭК 62443 Уровни безопасности.....	41

А.6	Серия стандартов МЭК 62351 по кибербезопасности «умных» электрических сетей .....	42
А.6.1	МЭК 62351 Обзор .....	42
А.6.2	МЭК 62351 Стандарты кибербезопасности связи .....	43
А.6.3	МЭК 62351 Дополнительные стандарты по кибербезопасности и технические отчеты.....	44
А.6.4	МЭК 62351 Технические требования к проверке на соответствие стандартам.....	45
5.1.1	А.6.4. МЭК 62351 Технические требования к проверке на соответствие стандартам.....	46
6	Литература.....	48

## Перечень иллюстраций

Рис. 1.	Система безопасности, встроенная в архитектуру. Периметр защиты электронных средств.....	13
Рис. 2.	Сходство и различие задач безопасности в ИТ и ЭТ .....	16
Рис. 3.	Схема управления рисками. ....	18
Рис. 4.	Важнейшие стандарты и пособия Международной организации по стандартизации (МОС/ISO) и Международной электротехнической комиссии (МЭК/IEC).....	20
Рис. 5.	NIST Базовая структура повышения кибербезопасности критической архитектура.....	28
Рис. 6.	Схема процесса управления рисками на всех уровнях организации (NIST) 29	29
Рис. 7.	Стандарты серии ИСО/МЭК 27000, в частности, 27019 по АСУ ТП.....	30
Рис. 8.	ISMS Family of Standards Relationships .....	31
Рис. 9.	Действующие стандарты НЕРК по защите объектов критической инфраструктуры (сочетание версий 5 и 6). ....	33
Рис. 10.	Группа стандартов NISTIR 7628 по безопасности «умных» электрических сетей.....	37
Рис. 11.	Эталонная логическая модель с пересекающимися связями («спагетти») NIST IR 7628 .....	38
Рис. 12.	IEC 62443 Серия стандартов безопасности в промышленности МЭК 62443. Обзор.....	40
Рис. 13.	Разделы стандартов серии МЭК 62443 согласно функциям. ....	40
Рис. 14.	Уровни безопасности в стандарте МЭК 62443 .....	41
Рис. 15.	Серия стандартов кибербезопасности МЭК 62443 комитета ISA-99. ....	42
Рис. 16.	Серия стандартов МЭК 62351 по кибербезопасности. ....	43

## Аннотация

---

Начиная с 2016 года Бюро по Европе и Евразии Агентства США по международному развитию (ЮСАИД) играет ведущую роль, обеспечивая готовность регулирующих органов и предприятий коммунального обслуживания к принятию мер по кибербезопасности для защиты важнейших объектов инфраструктуры. Работая в странах Восточной Европы и Евразии, ЮСАИД и НАРУК предоставляют техническую информацию и проводят обучение в целях оказать содействие органам регулирования энергетики в усилении их потенциала, что позволит органам регулирования играть ведущую роль в защите и дальнейшем развитии энергетики своих стран.

Предлагаемое пособие первоначально было предназначено для расширения представлений регулирующих органов стран Европы и Евразии в области практического применения методов кибербезопасности в виду угроз, существующих внутри энергетического сектора.<sup>3</sup> Однако вопросы, оценки риска, определением мер борьбы с последствиями кибератак и выбором соответствующих стандартов, актуальны для органов регулирования любых стран мира.

Пособие подготовлено НАРУК в целях дать обобщенный анализ разнообразных концепций кибербезопасности на доступном языке, в виде удобного и простого руководства для сотрудников органов регулирования энергетики. Органы регулирования отвечают за выполнение ряда ключевых функций, таких как обеспечение надежности энергоснабжения, оценка инвестиционных планов коммунальных предприятий и установка тарифов. В виду продолжающегося роста киберугроз, органам регулирования энергетики необходимо повысить свой технический потенциал, чтобы играть ведущую роль в обеспечении кибербезопасности отрасли и координировать совместную работу государственных и негосударственных организаций. В этом пособии дан краткий практический обзор международных стандартов по кибербезопасности (дополнительная, более подробная информация приводится в приложении), которые могут стать точкой отсчета для последующего анализа возможных решений проблем кибербезопасности в контексте национальных и региональных потребностей.

В документе рассматриваются:

1. Кибербезопасность и отказоустойчивость
2. Система безопасности, встроенная в архитектуру (SbD)
3. Различия между информационно-техническими (ИТ) и эксплуатационно-техническими (ЭТ) составляющими
4. Оценка риска
5. Стандарты, которые необходимо учитывать при разработке нормативов и базовых структур кибербезопасности.

Настоящий документ построен таким образом, чтобы помочь органам регулирования энергетики получить представление об основных принципах кибербезопасности, на основе которых они смогут разработать и внедрить оптимальные структуры и механизмы надзора, учитывающие специфику конкретной страны. Эти принципы – строительный материал, который поможет заинтересованным участникам адаптироваться в условиях постоянно меняющихся киберугроз и новых технологий. В настоящее время уже разработано множество стандартов, и регулирующие органы и коммунальные предприятия должны опираться на эти существующие стандарты, использовать

---

<sup>3</sup> Бюро ЮСАИД по Европе и Евразии начало активно заниматься кибербезопасностью после атаки на энергосистему Украины в 2015 г. С помощью НАРУК и Энергетической ассоциации США (ЮСЕА) ЮСАИД решает проблемы кибербезопасности в регионе как на уровне органов регулирования, так и на уровне энергокомпаний.

накопленный международный опыт, при этом модифицируя структуры и механизмы, исходя из конкретных условий.

Хотя решение о том, с чего начать, всегда дается непросто, регулирующим органам следует начать с вопроса «Что?». В частности, одни стандарты содержат общие требования к организационной безопасности и детальные требования к средствам обеспечения безопасности (они отвечают на вопрос «Что?»), в других рассматриваются технологии обеспечения кибербезопасности (они отвечают на вопрос «Как?»).

В Приложении к настоящему документу содержится список основных стандартов и передовых методов обеспечения кибербезопасности, организованных по категориям «Что?» и «Как?», а также порядок соблюдения этих стандартов. НАРУК надеется, что Приложение послужит органам регулирования и другим директивным органам полезным источником информации при оценке множества существующих на сегодня стандартов. Их можно рассматривать в качестве отправной точки и затем адаптировать к местным условиям.

Органы регулирования должны обеспечить непрерывное обучение и усиление своего потенциала, обмениваясь информацией и опираясь на собственный опыт. Вот, например, несколько ключевых рекомендаций, подробнее рассмотренных в настоящем документе:

- **Стандарты имеют недирективный характер.** Стандарты указывают на цели (*что*) программы кибербезопасности, но не уточняют, *как* их достичь, оставляя предприятиям свободу в разработке и реализации собственных программ, отвечающих данным условиям.
- **Стимулировать разработку стандартов.** В условиях сложной операционной среды, такой как электроэнергетическая система, стандарты должны разрабатываться *самой отраслью и для целей отрасли*. Однако при определенных условиях регулирующему органу придется стимулировать этот процесс, приняв обязательные стандарты.
- **Низкая, средняя и высокая степень применимости требований.** Это позволяет гарантировать рациональный выбор мер и средств обеспечения безопасности, исходя из рисков для энергосистемы.

В заключение, регулирующие органы и коммунальные предприятия должны в первую очередь рассмотреть возможность **организационной реформы** (развитие корпоративной культуры). В стандартах, отвечающих на вопрос «Что?», рассматриваются организационные структуры высокого уровня и целенаправленные меры контроля, что составляет основу готовности к обеспечению кибербезопасности.

## Введение

---

Какова роль органов регулирования в обеспечении кибербезопасности и отказоустойчивости? Следует ли коммунальным предприятиям самостоятельно решать эти проблемы или же органы регулирования должны занять руководящую позицию в этом вопросе и разработать свои рекомендации (требования) по кибербезопасности и отказоустойчивости, обеспечив тем самым безопасность энергосети? Если этими вопросами займутся органы регулирования, то как должны выглядеть нормативные документы по кибербезопасности и отказоустойчивости? Далее, следует ли органам, которые регулируют экономические вопросы, вникать в технические аспекты работы энергосистем в отсутствие соответствующих, ясно-очерченных полномочий? Настоящий документ поможет органам регулирования ответить на подобные вопросы в сфере кибербезопасности и соответствующим образом расставить свои приоритеты.

Как минимум, органы регулирования энергетики имеют четкие полномочия по обеспечению качества энергоснабжения. Независимо от длительности или кратковременности отключения электроэнергии по причине человеческого фактора или по естественным причинам (например, из-за погодных условий), население хочет, чтобы энергоснабжение было восстановлено как можно быстрее. Органы регулирования также анализируют и утверждают заявки на тарифы, направленные коммунальными предприятиями. Они должны определить оптимальное соотношение между справедливыми и обоснованными тарифами на электроэнергию, с одной стороны, и потребностями коммунального предприятия в капитале, с другой. Поскольку коммунальные предприятия направляют свой капитал, в том числе, на повышение кибербезопасности и восстановительные работы, вызванные кибератаками, регулирующие органы должны проверять обоснованность соответствующих затрат.<sup>4</sup>

Во многих странах мира органы регулирования все чаще принимают на себя надзор над кибербезопасностью и решение связанных с кибербезопасностью проблем и, таким образом, признают расширение сферы своей ответственности. Органам регулирования следует развивать собственные ресурсы, которые помогут создать необходимую базу, включающую стандарты кибербезопасности и их последовательное внедрение. Необходима система надзора и принуждения, которая обеспечит внедрение стандартов кибербезопасности на должном уровне.<sup>5</sup>

С учетом этого, обеспечение кибербезопасности и отказоустойчивости в случае кибератак есть и будут важнейшими требованиями к любым компаниям, в особенности тем, которые отвечают за важнейшие объекты инфраструктуры. Операторам энергосистем необходимо и дальше управлять быстро растущими электросетями, обеспечивая надежность и высокое качество обслуживания. Однако их деятельность

---

<sup>4</sup> См. также Ragazzi et al., *Evaluating the Prudence of Cybersecurity Investments: Guidelines for Energy Regulators*.

<sup>5</sup> Разумеется, энергокомпании продолжают играть важнейшую роль в разработке и внедрении соответствующих стандартов. Как будет показано в данном руководстве, энергокомпаниям предлагается самим обращаться к органам регулирования в процессе разработки стандартов, чтобы защитить свои интересы, а также добиться понимания со стороны всех заинтересованных участников. Энергокомпаниям и органам регулирования важно объединить усилия и начать диалог, в ходе которого будут решаться эти сложные вопросы.

Так сложилось, что в некоторых странах, наших партнерах, органы регулирования и энергокомпании изолированы друг от друга. Тем не менее, в сегодняшнем динамичном мире, по мере усложнения общих задач сотрудничество между органами регулирования и энергокомпаниями необходимо. Развитие современных технологий, интеграция предложения на рынке электроэнергии и угроза кибератак означают, что настало время объединения усилий всех сторон, чтобы правильно формировать стратегию и обмениваться передовым опытом. Органы регулирования обязаны создать условия для сотрудничества с энергокомпаниями, обеспечить взаимное уважение и одинаковое понимание общих задач.

неуклонно усложняется из-за освоения новых рыночных структур, бурного развития технологий и новых социальных задач, которые ставит перед ними государство (расширение доступа и ценовой доступности энергосетей).

Важно отметить, что в условиях, когда все участники признают необходимость обеспечить кибербезопасность своих ресурсов, можно перейти к добровольным стандартам и оценке рисков, что содействует тесному сотрудничеству. Однако если какая-либо из сторон, участвующих в защите важнейших объектов инфраструктуры (например, энергосистемы), не способна добровольно выполнять заранее согласованные задачи и функции, возникает необходимость в обязательных стандартах. Обязательный подход также дает дополнительные гарантии, так как коммунальные предприятия получают уверенность в соответствующем возмещении затрат при условии выполнения обязательных стандартов. Кроме того, регулирующим органам, возможно, будет проще проводить проверки коммунальных предприятий, следующих обязательным стандартам. Настоящий документ предназначен для регулирующих органов, на которые возложено решение проблем кибербезопасности коммунальных и других предприятий в целях снижения вероятности кибератак и, в особенности, последствий «успешных» кибератак.

Изложенные ниже принципы формируют стойкую базу кибербезопасности и служат образцом того, как строить нормативные документы, чтобы они удовлетворяли требованиям отказоустойчивости.

## **Важнейшие принципы кибербезопасности и отказоустойчивости с точки зрения органов регулирования**

---

Прежде всего органам регулирования и коммунальным предприятиям следует ознакомиться с пятью важнейшими принципами кибербезопасности и отказоустойчивости, которые обсуждаются подробно далее в документе.

### ***Пять важнейших принципов в сфере кибербезопасности и отказоустойчивости***

**Принцип 1. Отказоустойчивость входит в стратегию обеспечения нормальной деятельности компании.**

**Принцип 2. Система безопасности, встроенная в архитектуру, является наиболее экономически эффективным подходом к безопасности.**

**Принцип 3. ИТ и ЭТ похожи, но не совпадают.**

**Принцип 4. Оценка риска, снижение риска и систематическое обновление процедур и систем оповещения об отказах — неотъемлемая часть повышения уровня безопасности.**

**Принцип 5. Внедрение программ и нормативов в сфере кибербезопасности должно опираться на стандарты кибербезопасности и руководства по передовому опыту для ЭТ.**

## 2.1 Отказоустойчивость как комплексная стратегия обеспечения безопасности коммунальных услуг

Кибербезопасность выходит далеко за рамки пресечения атак злоумышленников-хакеров. Современный подход к кибербезопасности включает повышение отказоустойчивости энергосистемы посредством предупреждения «инцидентов» с ИТ-ресурсами.<sup>6</sup> Если говорить конкретней, отказоустойчивость – это планирование обеспечения безопасности и надежности до инцидента (выявление и предотвращение), во время инцидента (обнаружение и реагирование) и после инцидента (восстановление).<sup>7</sup>

Устранение факторов, снижающих отказоустойчивость, требует сочетания методов кибербезопасности (регулирование доступа, обнаружение эксплуатационных аномалий, регистрация инцидентов) с организационными и техническими стратегиями, обеспечивающими готовность и адаптацию организации к изменению условий, повышение стойкости к нештатным ситуациям и скорости восстановления. К техническим стратегиям относятся традиционные средства повышения надежности в энергосистемах — резервное оборудование, анализ последствий аварий, резервные системы. Они потребуют модификаций, чтобы успешно защитить ИТ-ресурсы, включая планирование мер в случае выхода из строя нескольких ресурсов, отсечение пораженных кибератаками участков с целью не допустить «каскадного» распространения поражения, и даже обучение персонала выполнению вручную действий в экстренных ситуациях, когда автоматические системы вышли из строя либо отключены.

Наиболее распространенными т.н. ИТ-событиями являются ошибки персонала и неправильные настройки. Соответственно, в систему мер повышения отказоустойчивости следует включить проверки вводимых данных и команд управления. Самые опасные атаки организуют лица, хорошо осведомленные об эксплуатации энергосистем, поэтому, возможно, следует внедрить дополнительные технические стратегии нейтрализации данного типа уязвимости, в частности, двухфакторную аутентификацию и непрерывный оперативный контроль аномального трафика в сети. Грозная деятельность может повлиять не только на электротехническую часть энергосистемы, но и на ее ИТ-ресурсы. Соответственно, в хорошо защищенных, но при необходимости легко доступных местах следует разместить резервные генераторы, аппаратуру связи и запасное ИТ-оборудование.

При выработке нормативов кибербезопасности для коммунальных предприятий органам регулирования следует учитывать действующие стандарты и накопленный мировым сообществом опыт. Таким проверенным стандартом является, например, «базовая структура кибербезопасности», разработанная Национальным институтом стандартов и технологий США (NIST). Эту или иную «базовую структуру» можно взять за основу при разработке норм безопасности, направленных не только на предотвращение кибератак, но и на обеспечение готовности к устранению последствий неминуемой «успешной» кибератаки или инцидента, нарушающих штатную эксплуатацию технических ресурсов. Органам регулирования целесообразно предложить

---

<sup>6</sup> Информационно-техническим ресурсом считается любая техника, обладающая электронно-вычислительными мощностями, включая контроллеры технических средств, но не сама аппаратура (например, высоковольтный выключатель). Воздействие на ИТ-ресурсы может иметь как физический характер (обрыв провода, повреждение трансформатора), так и кибернетический (внедрение вредоносного программного обеспечения (ПО), случайный ввод некорректных данных и проч.).

<sup>7</sup> Следует отметить, что документ «Основы повышения качества кибербезопасности критической инфраструктуры» (Framework for Improving Critical Infrastructure Cybersecurity), разработанный Национальным институтом стандартов и технологий США (NIST), является одним из ряда аналогичных руководств, пользующихся международным признанием. Множество органов регулирования и энергетических компаний с успехом применили это руководство на практике. См. NIST, *Framework*.

энергокомпаниям базовую структуру кибербезопасности такого рода для формирования подхода к разработке собственных планов по кибербезопасности. В качестве примера, базовая структура системы кибербезопасности, разработанная Национальным институтом стандартов и технологий США (NIST) включает:

- инвентаризацию технических ресурсов, угроз, уязвимостей и возможных последствий инцидентов;
- защиту информационных ресурсов на стадии проектирования, а также посредством контроля над доступом к ресурсам, регламентации работы персонала, инструктажа персонала по безопасности и соответствующих технологий;
- обнаружение инцидентов, связанных с безопасностью, посредством непрерывного оперативного контроля и обнаружения событий, а также оценки степени их серьезности;
- реагирование на инциденты с целью смягчения их последствий посредством заблаговременного планирования и применения процедур и соответствующих технических средств, в сотрудничестве с национальными группами реагирования на инциденты ИТ-безопасности (computer security incident response teams (CSIRT));
- восстановление штатной эксплуатации после инцидентов посредством планирования, совершенствования и регулярной переоценки угроз и уязвимостей.

## **2.2 Система безопасности, встроенная в архитектуру, как наиболее экономически эффективный подход**

Ущерб от киберпреступности возрастает год от года. В течение суток в мире из-за нарушений безопасности теряется около 780 тысяч записей данных и 33 тысячи фишинговых сообщений, а также 4000 атак с помощью программ-вымогателей.<sup>8</sup> По мнению аналитиков, мировой ущерб от киберпреступности в 2019 г. составляет два триллиона долларов, что вчетверо больше, чем в 2015 г.<sup>9</sup>

С учетом этого, наиболее эффективным подходом к кибербезопасности информационно-технических комплексов представляется безопасность, изначально встроенная в общую архитектуру (SbD, security by design). Такой подход позволяет свести к минимуму риск и финансовые издержки. «Встроенный» подход (SbD) гарантирует единообразие всех систем общей архитектуры, в которой конфигурации сетей и потоки информации четко определены. Используя этот подход, пользователи получают единообразный регламент вместо ситуативных (разовых) процедур безопасности.

Эффективные средства безопасности невозможно наложить в качестве «заплат» на действующие регламенты эксплуатации, они должны стать неотъемлемой составляющей общей архитектуры и конфигурации, эксплуатационных регламентов и информационных технологий. Запоздалое внедрение регламентов и технических средств безопасности, то есть, внедрение их после создания системы, сопряжено с повышенными издержками в силу случайного (ситуативного) характера изменений в конфигурации системы, их сложности и необходимости всякий раз проводить повторный инструктаж персонала. Если же меры безопасности изначально встроены в общую архитектуру системы, они

---

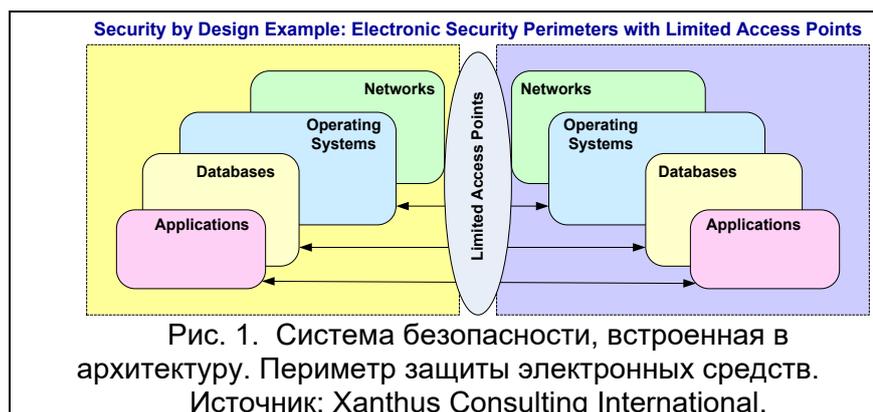
<sup>8</sup> Lewis, *Economic Impact*.

<sup>9</sup> Morgan, "Cyber Crime."

становятся штатной составляющей жизненного цикла ИТ-ресурсов и эксплуатационных регламентов энергосистем.

Термин *встроенная в архитектуру безопасность* (SbD) охватывает целый ряд понятий,<sup>10</sup> в частности, конфигурации системы, конфигурации сетей, порядок планирования, управление данными и пр. Встроенная в архитектуру система безопасности полезна даже в случае модернизации или поэтапной замены систем, т.к. тщательно продуманный план обеспечения безопасности эффективен и при внедрении на отдельных этапах модернизации или замены.

Одним из аспектов выявления угроз и уязвимых узлов системы до окончательного утверждения конфигурации системы и сетей. Например, если критически важные системы можно расположить внутри



ограниченной зоны безопасности электронных средств (т.н. «электронный периметр безопасности», или периметр защиты электронных средств), то доступ к этим системам можно ограничить, защищенным и тщательно наблюдаемым уже на стадии проектирования (см. рис. 1). Подобная конфигурация позволяет уменьшить *площадь* атак, которые могут быть предприняты злоумышленниками или произойти случайно вследствие ошибки в эксплуатации.

SbD-подход позволяет повысить эффективность мер по предотвращению атак, т.к. планирование действий в случае неизбежных «успешных» нарушений безопасности («сценарии неудачи») позволяет заблаговременно пройти необходимое обучение, принять соответствующие меры и разработать стратегии для смягчения последствий нарушений. Если безопасность встроена в архитектуру, регулирование доступа можно осуществлять на уровне данных, а не только на общесистемном уровне. Тогда безопасность действий пользователей и их доступа к данным приобретает комплексный характер, поскольку удастся с высокой точностью ограничить, кому разрешается контролировать те или иные данные и манипулировать ими. Тот же подход к

<sup>10</sup> Система безопасности, встроенная в архитектура (security by design, SbD) — понятие, разработанное с целью решения вопроса о защите основных элементов информационной безопасности: конфиденциальности, целостности и доступности. В рамках Проекта по обеспечению безопасности открытых веб-приложений (OWASP) составлен перечень принципов интеграции мер безопасности в архитектуру системы, которым рекомендуется следовать специалистам в области ИТ. Принципы OWASP позволяют существенно повысить уровень безопасности и снизить риск «успешных» кибератак.

Некоторые примеры мер безопасности, встроенных в архитектуру: 1) максимально ограничить площадь, открытую для атаки; 2) сделать безопасными настройки по умолчанию; 3) применять принцип «пользователь получает минимальный, насколько это возможно, уровень прав»; 4) предусмотреть меры безопасности в случае отказа; 5) не доверять сервисным и сетевым ресурсам; 6) разделять обязанности; 7) стараться не применять принцип «безопасность через неясность», т.е. сокрытие внутреннего устройства системы для обеспечения ее безопасности; 8) не усложнять систему безопасности; 9) не допускать ошибок при устранении недостатков в системе безопасности; 10) применять принцип глубокого эшелонирования защиты (defense in depth).

Эти принципы заслуживают отдельного подробного рассмотрения, но в рамках данной публикации они приведены в сугубо ознакомительных целях.

регулированию доступа можно применить и к обмену данными между прикладными программами.

Важнейшим требованием к работе системы является ее способность своевременно направлять потоки проверенной информации в установленный пункт назначения. Методика SbD позволяет выполнить эти требования, благодаря защищенным протоколам, которые изначально встроены в системы и являются одной из их основных функций. Например, проверка корректности данных может способствовать нейтрализации угрозы злонамеренных действий со стороны лиц, знакомых с энергосистемой и знающих, как нарушить штатную эксплуатацию. В данном случае проверка корректности данных может быть встроенной функцией каждой подсистемы. Параллельно, доступ к данным может быть ограничен общими мерами безопасности, которые определены политикой безопасности.

Общая политика безопасности, разработанная на этапе SbD-проектирования, может, в частности, включать регламент и порядок закупки и модернизации электронных средств. Наличие такой политики позволяет должным образом спроектировать конфигурации сетей связи, а также позволяет лучше контролировать и управлять цепью поставок.

Тем не менее, общепризнано, что быстро встроить средства безопасности в архитектуру действующих энергосистем сложно, особенно потому, что жизненные циклы различных компонентов коммунальных систем существенно различаются. Для систем, находящихся сегодня в эксплуатации, меры безопасности следует внедрять в эксплуатационные регламенты, а также следует продумать методику модернизации.

Сотрудничество органов регулирования и коммунальных предприятий позволит сформировать SbD-подход к обеспечению кибербезопасности, в том числе, при замене устаревшего оборудования на оборудование с более высоким уровнем безопасности. Органы регулирования могут порекомендовать энергокомпаниям определить, какие принципы SbD они применяют или намереваются применить. Это можно сделать, например, запросив следующую информацию:

- общую политику безопасности коммунального предприятия, в части, где описана общая структура и регламенты безопасности;
- функции сотрудников (например, эксплуатационный персонал, персонал по техническому обслуживанию, инженер по защите, инженер по безопасности) и их обязанности, полномочия и ограничения (принципы наименьшего уровня полномочий и разделения обязанностей);
- меры, обеспечивающие реализацию полномочий и ограничений в строгом соответствии с установленными функциями сотрудника;
- порядок инструктажа по безопасности и проверки усвоения;
- конфигурация эксплуатационных систем, в частности, электронных периметров безопасности, контрольно-пропускных пунктов, технических средств обеспечения безопасности при перетоках информации сквозь периметры;
- планы регистрации, оценки и отчетности по случаям нарушения безопасности различных уровней;
- планы эксплуатации после инцидентов различных категорий (например, отказы оборудования, ошибки персонала, стихийные бедствия, кибератаки);
- планы восстановления после случаев нарушения кибербезопасности.

В зависимости от специфики конкретной страны, безопасность, встроенная в архитектуру системы (SdB), может предусматривать добровольные либо обязательные

стандарты. Последние необходимы, если есть необходимость усилить основу кибербезопасности, что добавляет прозрачность и уверенность.

### **2.3 ИТ и ЭТ: различия в требованиях к безопасности информационно-технического и эксплуатационно-технического комплексов**

Традиционно, считается, что во всех вопросах, относящихся к категории кибербезопасности, специализируется информационно-технический (ИТ) отдел. Квалификации ИТ-отдела обычно достаточно, чтобы понимать угрозы и реагировать на них, понизить уязвимость и принять меры реагирования на атаки применительно к большинству корпоративных ИТ ресурсов. Обычно первоочередной задачей по ИТ-ресурсам является обеспечение конфиденциальности информации, содержащейся в информационных системах. Именно на предотвращении несанкционированного доступа к секретной информации и сосредоточивают усилия специалисты по информационной безопасности.

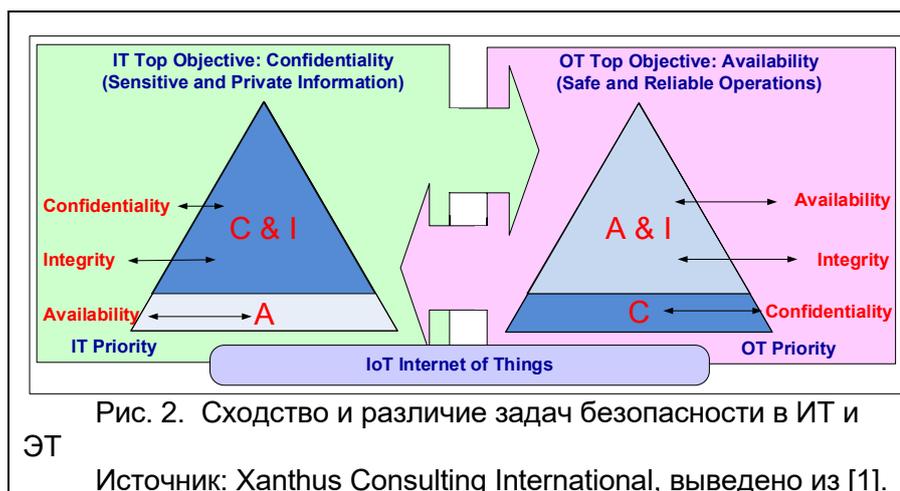
Однако в таких ЭТ, как, например, энергосистемы, эксплуатационно-техническая (ЭТ) составляющая важнее, потому что как намеренные, так и случайные инциденты, связанные с кибербезопасностью и отказом ИТ-ресурсов, могут привести к пагубным последствиям и для техники, поскольку энергосистемы сегодня являются *информационно-техническими системами*. Самые тяжелые последствия такого рода относятся к физической безопасности: неправильные действия в отношении ИТ-ресурсов, злонамеренные либо неумышленные, могут привести к повреждению оборудования, травме или даже смерти людей. Следующее по важности последствие — нарушение работы энергосистемы. На стадии проектирования энергосистем давно применяются весьма высокие требования к надежности их компонентов (выключателей, трансформаторов, ЛЭП). Однако сегодня проектирование сопряженных с ними ИТ-ресурсов требует такого же высокого уровня надежности.

Соответственно, как показано на рис. 2, важнейшими требованиями к ЭТ становятся доступность и достоверность данных (что именно важнее, доступность или достоверность, зависит от конкретных обстоятельств)<sup>11</sup>. Специалисты по эксплуатации энергосистем хорошо осведомлены в вопросах надежности и в силу этого зачастую лучше других ориентируются в том, насколько адекватной является та или иная реакция на инциденты безопасности, затрагивающие ИТ-ресурсы; сочетание их знаний с знаниями в области кибербезопасности ИТ позволяет определить, какие технические стратегии и методы эксплуатации «механической» части энергосистемы следует задействовать, чтобы свести к минимуму влияние этих инцидентов.

---

<sup>11</sup> Доступ и достоверность («целостность») данных стали предметом полемики о том, что из них важнее. Естественно, крайне нежелательно, чтобы злоумышленник имел полный доступ к какому-либо процессу. Но если в данных условиях нет возможности обеспечить достоверность данных о процессе, целесообразно перейти в безопасный режим офф-лайн до тех пор, пока результаты проверки не покажут, что данные достоверны, а несанкционированного вмешательства в процесс не было. В действительности, приоритетными считаются оба требования, и оба следует оперативно учитывать и балансировать (см. рис. 2).

При обеспечении безопасности ЭТ-комплекса возникают весьма специфические задачи. Например, высокая доступность ИТ и технических ресурсов (в данном случае понимаемая как эксплуатационная готовность) требует



проектных решений, отвечающих требованиям резервирования, высокой надежности и высокой эффективности. Требования к безопасности могут вызвать необходимость в изменениях конфигурации сетей и потоков информации вследствие применения периметров защиты, демилитаризованных зон и межсетевых экранов. Кроме того, процессы, происходящие на больших скоростях в режиме реального времени, которые связаны с взаимодействием двух самостоятельных узлов, автономной работой, чувствительностью ко времени и другими характеристиками, требуют решений по безопасности, отличных от типовых решений для ИТ.

В то же время, при проектировании должны приниматься во внимание ограничения, налагаемые эксплуатацией. Например, ограничения по ресурсам аппаратуры (времени, скорости обмена информацией, доступу к сети) могут повлиять на то, какие процедуры и технические средства обеспечения кибербезопасности можно будет применить. В частности, приемы сверхсложного шифрования или интернет-доступ к органам сертификации редко применимы к ресурсам ЭТ. Кроме того, на график технического обслуживания, обновления и модернизацию оборудования налагают ограничения эксплуатационные требования: вывести оборудование из эксплуатации для этих целей может быть разрешено только на короткое время весной или осенью.

Важный фактор, ограничивающий применение мер кибербезопасности, состоит в наличии большого количества устаревшей, но еще не выработавшей ресурс техники, модернизировать которую так, чтобы она допускала применение указанных мер киберзащиты, затруднительно. Следует учитывать и критическую важность эксплуатации энергосистем: средства обеспечения безопасности не должны затруднять работу эксплуатационного персонала, особенно в нештатных ситуациях. Иными словами, ситуации типа «разбить стекло при аварии» должны быть отражены в регламентах безопасности.

Еще одно существенное отличие ОЭ от обычных бизнес-операций — необходимость применения сетей и техники «интернета вещей» (Internet-of-Things, IoT), в частности, для взаимодействия с объектами потребителей для оперативного контроля и управления распределенными источниками электроэнергии (РИЭ) и обмена информацией с микропроцессорными счетчиками («умные электросчетчики»). Применение «интернета вещей» приводит к тому, что энергокомпании уже не могут полагаться исключительно на собственные интернет-сети, т.е. должны распространить действие средств кибербезопасности и на операции через сети общего пользования, где применяется известная всем техника связи.

Органы регулирования могут порекомендовать коммунальным предприятиям наладить совместную работу групп ИТ и ЭТ с целью разработки оптимального

согласованного подхода к кибербезопасности и отказоустойчивости и обсуждения требований к безопасности. По мере развития сотрудничества, специалисты этих групп могут перейти к совместным оценкам угроз, уязвимостей и последствий инцидентов, определить категории рисков и оптимальный порядок применения методики и приемов эксплуатации, приемлемых как для ИТ, так и для ЭТ. В таких оценках рекомендуется учитывать вышеописанный SbD-подход, но обязательно в сочетании с опытом специалистов как из ИТ, так и из ЭТ.

Также следует рассмотреть использование комплексного подхода, который позволит коммунальным предприятиям применять и совершенствовать междисциплинарные знания по безопасности ИТ- и ЭТ-комплексов. Сюда относятся, например, создание в компаниях так называемой «кибер-культуры» посредством учебных курсов по культуре и гигиене безопасности, специализированное обучение в области безопасности, а также общее обучение безопасности посредством тренингов, обмена информацией и практической отработки навыков. Решая, выполняет ли коммунальное предприятие требования кибербезопасности, регулирующие органы должны принимать во внимание и эти аспекты, а не только оценку риска.

## **2.4 Оценка риска, снижение риска,<sup>12</sup> процессы в жизненном цикле и оповещение о нарушениях**

Оценка риска, нейтрализация риска, систематическая актуализация процессов и оповещений об инцидентах в течение всего жизненного цикла системы — основа повышения уровня безопасности. Применяя требования, обусловленные основной деятельностью (финансовые, брендовые, эксплуатационные, общественные), и методики, предложенные в международных стандартах по ЭТ, организации могут определить подверженность риску безопасности в собственных системах.

В стратегии нейтрализации риска обязательно должны быть отражены эксплуатационные ограничения, в частности, ограничения, налагаемые ЭТ сетями. К ним относятся, в первую очередь, физическая защита технических ресурсов, безопасность персонала, а также ограничения, связанные с эффективностью и архитектурой сетей. Важно иметь в виду специфику энергокомпаний, заключающуюся в том, что обслуживание потребителей электроэнергии обеспечивается процессами в электрических сетях.

Стоимость киберфизических активов может составлять миллионы долларов, а их замена требует года и более. Важность предотвращения повреждения этих ресурсов с помощью мер безопасности невозможно переоценить. К поиску лучших средств снижения риска крайне важно привлекать специалистов соответствующего профиля, причем не как консультантов, а как членов коллектива, ответственного за кибербезопасность. Эта рекомендация относится ко всем подразделениям и группам компании, в том числе, инженерным подразделениям по средствам коммуникации и ЭТ, т.к. определение уязвимостей, а особенно реагирование на атаку и восстановление штатной эксплуатации требуют мобилизации всех наличных специалистов. Постоянное улучшение качества общей политики обеспечения безопасности, регламентов безопасности и соответствующих технических средств в течение всего жизненного цикла приобретает первоочередное значение. Регулярный анализ кибербезопасности, который проводится

---

<sup>12</sup> Риск определяется как совокупность последствий нежелательного явления и его вероятности. Оценку рисков проводят, чтобы выявить, оценить и ранжировать по приоритету риски, связанные с эксплуатацией и использованием информационных комплексов и затрагивающие организационные мероприятия, организационные ресурсы, отдельных лиц, сторонние организации и страну в целом.

Снижение риска определяется как действия, направленные на систематическое уменьшение объема ресурсов, которые может затронуть риск (т.е. имеющие целью снижение степени тяжести воздействия).

по проверочному сценарию, позволит коммунальным предприятиям вовремя обновить систему и внедрить новые меры снижения риска.

Рис. 3 иллюстрирует общий процесс управления рисками. Сложность состоит в том, как применить его отдельные аспекты при разработке плана обеспечения кибербезопасности конкретного ЭТ-комплекса. Типовой процесс не может удовлетворять всем требованиям, но дает представление о том, как, когда и в каких целях нормы и стандарты кибербезопасности могут использоваться для повышения отказоустойчивости и уровня безопасности ЭТ комплекса.

Органы регулирования могут поощрять проведение оценок риска с целью более полного понимания угроз и уязвимостей и определения вариантов снижения риска. Начинать оценку риска можно с рассмотрения большинства эксплуатационных процессов, а впоследствии сосредоточить внимание на детальной оценке угроз и уязвимостей в отдельных компонентах системы.

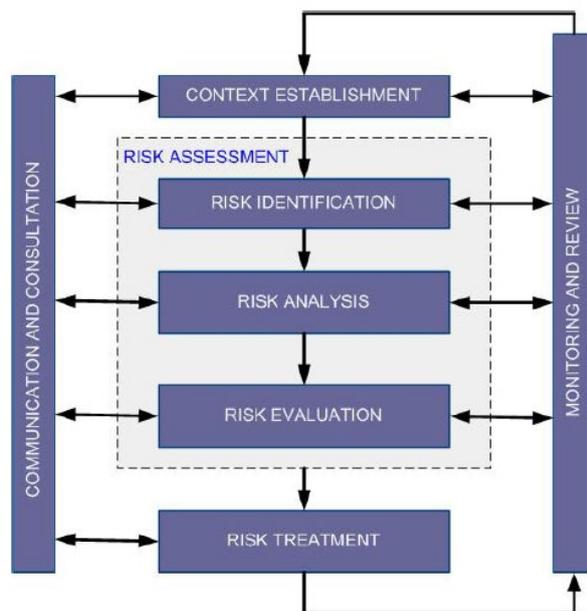


Рис. 3. Схема управления рисками.  
Источник: ISO/IEC 27005 (2018) [7].

Основные этапы оценки риска приведены ниже.

- Соберите общие требования, как внутренние, так и регуляторные, применимые к ЭТ-комплексу и определите последствия несоблюдения этих требований для безопасности, экономических показателей, эксплуатации.
- Выберите методику оценки риска, которая наиболее соответствует вашим организационным требованиям и ограничениям.
- Установите объем планируемой оценки риска в соответствии с границами систем, которые планируется проанализировать, с учетом не только элементов внутри этих границ, но и стыков с другими ЭТ и не ЭТ-системами.
- Выработайте понимание того, что угрозы могут быть связаны с техническим оборудованием, информацией, процессами, взаимодействиями, конфигурациями и другими ресурсами.
- Снижение риска предполагает взвешенный подход, основанный на разумном соотношении самого риска и затратами на его снижение до приемлемого уровня. Внутренняя политика безопасности определяет, какие риски считать приемлемыми.<sup>13</sup> Снижение риска может потребовать переоценки риска с целью подтверждения его приемлемости, особенно если в порядке мер, направленных на снижение риска, произведены многочисленные изменения.

<sup>13</sup> Расчет допустимого риска – центральная проблема, стоящая перед коммунальными предприятиями и органами регулирования. Целый ряд инструментов по оценке риска и моделей оценки технологической зрелости помогают коммунальным предприятиям оценить уровень своей рискоустойчивости, а органам регулирования получить достаточную информацию для проверки.

- Внедрите меры управления безопасностью в целях снижения выявленных рисков.
- Вслед за оценкой риска выберите и внедрите необходимые меры к его снижению.
- Определите меры контроля (например, конкретные процедуры, технологии, коммерческие продукты), которые будут использованы в каждом из видов контроля безопасности.
- Регулярно осуществляйте оперативный контроль над выбранными подходами и мерами, чтобы убедиться в их текущей эффективности и в том, что они не были подорваны вероятными атаками.

## 2.5 Стандарты и передовой опыт кибербезопасности в энергетике

Учитывая сложность оперативных процессов и широкий спектр ИТ-ресурсов в энергетике, следует заключить, что ни один нормативный документ по кибербезопасности не может охватить все требования к безопасности и меры управления, стратегии повышения отказоустойчивости и технические средства. В некоторых нормативных документах и руководствах содержатся общие требования к организационной безопасности, в других — подробные описания рекомендуемых средств обеспечения безопасности (они отвечают на вопрос «Что?»), есть и такие, в которых рассматриваются технологии реализации мер обеспечения кибербезопасности (они отвечают на вопрос «Как?»).

Несмотря на то, что множество разнообразных документов могут быть предоставлены национальными и международными организациями, включая NIST, Международной электротехнической комиссией (МЭК), Институтом инженеров по электротехнике и электронике (IEEE) и Североамериканской корпорацией обеспечения надежности электросетей (NERC), на рис. 4 ниже стандарты по кибербезопасности и передовому опыту организованы по категориям («Что» и «Как») и порядку обеспечения их применения.

### Cybersecurity Standards and Guidelines that Apply to Smart Energy Operational Environments

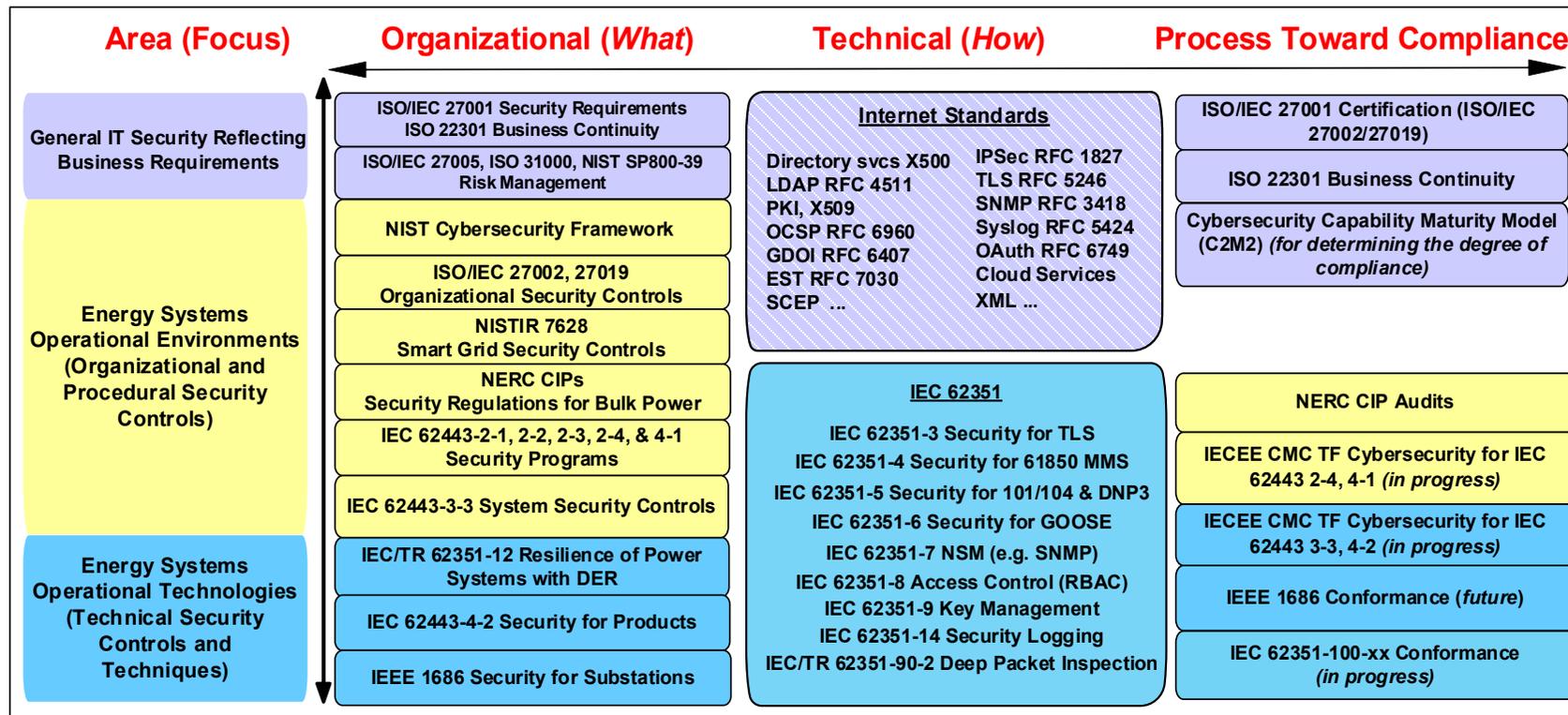


Рис. 4. Важнейшие стандарты и пособия Международной организации по стандартизации (МОС/ISO) и Международной электротехнической комиссии (МЭК/IEC).  
 Источник: Xanthus Consulting International.

Наиболее актуальные нормативные документы по кибербезопасности с общими требованиями категории «что?»

- ИСО/МЭК 27001 — аудит безопасности (общие положения на уровне информационного комплекса)
- ИСО/МЭК 27002 — уточнение мер управления, рассмотренных в ИСО/МЭК 27001
- ИСО/МЭК 27019 — разработана специально для промышленных систем контроля (ICS), оперативно-диспетчерского контроля и сбора данных (SCADA) (ЭТ)
- NIST — «Базовая структура кибербезопасности»
- Межведомственный отчет NIST (NISTIR) 7628. Пособие по безопасности «умных» электрических сетей
- НЕРК — «Защита критической инфраструктуры»
- МЭК 62443-2-1, 2-2, 2-3, 2-4, 4-1 — программы по безопасности
- МЭК 62443-3-3 — требования по системной безопасности
- МЭК 62443-4-2 — безопасность составляющих
- МЭК 62351-12 — отказоустойчивость систем с РИЭ
- IEEE 1686 — обеспечение безопасности подстанций

Нормативные документы технического уровня описывают унифицированные методики и технические средства, отвечающие на вопрос, «как» повысить уровень безопасности и отказоустойчивости ИТ-ресурсов. Сюда относится ряд стандартов по Интернету, в частности, стандарты МЭК серии 62351 по разным протоколам связи, а также управлению доступом на основе функций персонала, оперативному контролю сетей и систем, управлению ключами шифрования, журнальной регистрации, углубленной проверке пакетов.

Большинство этих нормативных документов привязаны (или планируется их привязка в будущем) к нормативам испытаний на соответствие требованиям и сертификации. Нормативы и указания по кибербезопасности описаны подробнее в Приложении.

Органы регулирования могут рекомендовать энергокомпаниям выбрать нормативные документы, которые наиболее применимы для оценки на разных уровнях собственно безопасности, а также регламентов и технических средств обеспечения безопасности.

В частности, органам регулирования целесообразно поощрять использование общих нормативов кибербезопасности, которые помогают лучше понять требования к безопасности и применять меры управления безопасностью надлежащим образом во всех областях. Кроме того, органы регулирования могут порекомендовать энергокомпаниям изучить нормативные документы технического уровня, чтобы точнее определить, какие из них целесообразно применять для удовлетворения конкретных требований к безопасности.

С другой стороны, органам регулирования полезно проанализировать инициативы и регламенты безопасности из разных источников, чтобы сформировать широкую

исходную позицию и гарантировать, что все средства обеспечения безопасности учтены в должной мере.

## **Регламенты кибербезопасности, которые органы регулирования могут рекомендовать коммунальным предприятиям в целях повышения их безопасности**

---

Ниже изложены подготовительные этапы, а в Приложении описаны некоторые нормативные документы, признанные международным сообществом, которые могли бы в дальнейшем внедрены органами регулирования.

### **3.1 Подготовительные этапы**

Органы регулирования могут предложить коммунальным предприятиям сделать некоторые шаги предварительного характера параллельно с разработкой официальных мер обеспечения кибербезопасности. К ним относятся:

- ознакомиться с нормативными документами по кибербезопасности, включая как международные, так и региональные или национальные;
- провести полную инвентаризацию ИТ-ресурсов, в т.ч., информационных систем, сетей, баз данных, «умных» электронных устройств, пунктов доступа и прочих «умных» устройств;
- определить, в каких ИТ- и ОТ-отделах или подразделениях уже введены меры безопасности, хотя бы частично, а также в каких эти вопросы даже не поднимались. Рассмотреть, среди прочего, управление учетными записями пользователей, информационные системы диспетчерского пульта, информационные системы и оборудование подстанций и пр.;
- начать контролировать состояние важнейших ИТ-ресурсов посредством извещений или сигнализации; визуализация состояния ИТ-ресурсов может быть весьма важна даже при отсутствии полной оценки риска;
- отделить эксплуатационные сети от корпоративных вычислительных сетей и, в любом случае, от Интернета: по возможности, предусмотреть физическое разделение; установить межсетевые экраны во всех точках доступа; организовать периметры безопасности вокруг подстанций и диспетчерских пультов с доступом только через межсетевые экраны.

Органы регулирования также могут находиться на этом (последнем в списке выше) этапе в процессе внедрения средств кибербезопасности. Важно отметить, что эти предварительные шаги потребуют развития стратегического сотрудничества. Органам регулирования рекомендуется создавать необходимые связи со всеми заинтересованными лицами. Заинтересованные лица могут принадлежать как к сторонним организациям (сотрудники профильного министерства, генеральные управляющие энергокомпаний), так и к самим органам регулирования. Их задача — оказывать содействие описанному интенсивному процессу. Важность средств кибербезопасности и большая трудоемкость их внедрения в органах регулирования и энергокомпаниях требуют долгосрочной поддержки и уверенности в правильном видении перспектив безопасности систем в эксплуатации. В частности, как только между органами регулирования и энергокомпаниями построены и укреплены отношения, позволяющие содействовать внедрению нормативов кибербезопасности, дальнейшие действия приведут к долгосрочным последствиям.

### 3.2 Порядок оценки рисков

Важной задачей коммунальных предприятий является обеспечение безопасности энергосистем на основе оценки риска. Оценка риска может дать целый спектр результатов, в частности, (1) проекты энергосистем, которые предусматривают оперативный контроль над энергооборудованием; (2) резервные меры, включая обнесение подстанций и других опасных объектов ограждениями с целью недопущения несанкционированного прохода; (3) четкие рабочие правила для штатных и нештатных ситуаций. Аналогичная оценка риска проводится для ИТ-ресурсов. Несмотря на то, что орган регулирования не может знать всех подробностей оценки риска, проведенной коммунальным предприятием, по причине конфиденциальности информации, он должен ознакомиться с результатами в достаточной мере, чтобы оценить готовность коммунального предприятия с точки зрения кибербезопасности, а также проверить соответствие тарифов (возмещение издержек) и капиталовложений.<sup>14</sup>

Оценку риска можно начинать незамедлительно после осуществления ряда предварительных шагов. Процесс оценки риска разделяется на основные этапы, перечисленные ниже.

- Выделить общие внутренние и регуляторные требования, относящиеся к ЭТ-комплексу и определить возможные последствия невыполнения этих требований (для безопасности, экономических показателей, эксплуатации и проч.). Общие требования отражают важнейшие критерии, которым должны соответствовать энергосистемы и имеющиеся в них ИТ-ресурсы.
  - Сформировать внутреннюю политику безопасности, которая определит приемлемые риски и установит порядок и меры контроля над неприемлемыми рисками.
- Разработать порядок оценки риска на основе передового опыта и проверенных на практике нормативных документов, определяющих базовые элементы кибербезопасности (например, на базе серии стандартов ИСО/МЭК 27000), чтобы с большой степенью вероятности выявить все риски.
  - Теоретически, в процессе оценки рисков выясняется, как снижение риска повлияет на финансовые и прочие показатели, а затем данное соотношение (т.е., степень влияния с одной стороны, и вероятность применения угрозы с другой) «уравновешивается» с издержками по снижению риска.
  - Однако на практике применяется целый ряд методик оценки рисков, приведенных в пособиях и нормативных документах. Некоторые методики в большей степени, чем остальные, имеют количественный характер, но в большинстве своем они предполагают, что специалисты по эксплуатации энергосистем и кибербезопасности совместно выявляют уязвимости, вероятные угрозы, возможные последствия, а также перспективные схемы, регламенты или технические средства нейтрализации, актуальные для их систем.

---

<sup>14</sup> «Руководство по оценке кибербезопасности для органов регулирования стран Черноморского региона» опубликовано в 2017 г. в рамках проекта НАРУК и ЮСАИД для органов регулирования и является простым инструментом проверки готовности в сфере кибербезопасности. Руководство предоставляет органам регулирования методику оценки уровня готовности коммунальных предприятий в сфере кибербезопасности и выявления недостатков. См. NARUC, *Evaluative Framework* («базовая структура оценки»).

Базовая структура оценки включает пять начальных этапов и 107 типовых вопросов, взятых из письменных опросов по кибербезопасности, которые проводились органами регулирования США. Вопросы охватывают 12 основных аспектов кибербезопасности и позволяют органам регулирования оценить уровень подготовки энергокомпаний в сфере кибербезопасности на основе их ответов.

- Провести оценки рисков по интересующим направлениям (например, по конкретному объекту), применяя методики, приведенные в пособиях по оценке риска, и учитывая информацию, полученную от компаний, и требования, выдвинутые органами регулирования. Оценивая риски, следует принимать во внимание рамки соответствующих объектов, а также их стыки с другими системами, как ЭТ, так и отличными от ЭТ.
  - Оценку риска можно проводить с разной глубиной детализации, например, по подстанции в целом, по части аппаратуры подстанции, по небольшому объекту или по крупной электростанции.
  - Некоторые риски, например, связанные с физической безопасностью персонала, могут не быть сопряжены с финансовыми показателями, тем не менее, должны быть отнесены к категории весьма важных.
  - Риски определенных категорий могут оказаться не столь значительными, чтобы применять к ним особые меры.
  - Большинство категорий рисков оценивается с целью уравновесить потенциальные последствия применения мер по снижению риска и вероятности угрозы с одной стороны, и издержек по снижению риска с другой. Зачастую одно средство снижения риска (например, отделение сетей управления от корпоративных сетей) позволяет свести к минимуму последствия множества рисков.
- Определить какие средства управления (процедуры, технические средства и даже продукты) могут или должны применяться по каждой категории риска.
  - Средства управления в разных средах могут различаться и основываться на разных нормативных документах.
  - Некоторые методы снижения риска являются сугубо техническими (например, резервные системы, проверка корректности данных, физическое разделение, оперативный контроль), другие относятся к сфере кибербезопасности (например, регулирование доступа, межсетевые экраны, сертификаты, шифрование).
  - Следует выявить ограничения каждого из возможных средств контроля над риском с учетом особенностей различных сред ЭТ, например, специфики подстанций (длительные периоды времени между возможностями корректировки работы системы) или РИЭ (недостаток знаний по безопасности на местах).
- Начать внедрение отдельных средств снижения рисков, выбранных в процессе оценки риска.
  - Некоторые типовые или особые средства снижения риска могут оказаться неприменимыми в системах на конкретных объектах так, как это предполагалось вначале; особенно часто это случается в устаревших системах. Например, устаревшие системы могут не поддерживать некоторые средства нейтрализации, в том числе, антивирусные программы или защищенные процедуры установления пакетов обновлений («заплат»).
  - В подобных случаях возникает необходимость поиска альтернативных методик, уже с учетом различий в функциональных возможностях систем и устройств в конкретной среде и на конкретном объекте (альтернативные методики могут быть предложены поставщиками или собственными специалистами, обладающими опытом работы с соответствующими средами).
  - Альтернативная методика может быть приемлема, потому что поставщик гарантирует конкретный уровень риска, а не просто предоставляет средства снижения риска согласно техническому заданию.

- Поставщик может также осуществить интеграцию своего комплекса с типовыми для энергокомпаний средствами нейтрализации рисков.
- Перепроверить результаты после того, как внедрение мер по снижению рисков завершено.
  - По мере реализации проекта убедиться в том, что внедряемые подходы к снижению риска применяются корректно и действительно обеспечивают ожидаемый эффект.
  - Объяснить, как применять новые меры. Это крайне важно для понимания того, каких результатов следует ожидать от новых мер и как оценивать их эффективность.
  - Использовать моделирование для оценки эффективности новых мер.
  - Определить, действительно ли внедренные меры помогли достаточно снизить риск. Если необходимо, провести повторную оценку риска.
  - Предусмотреть порядок обеспечения качества, например, аудит, который, по возможности, проводится сторонней группой специалистов.
- По завершении проекта, организовать оперативный контроль (мониторинг) всех регламентов и технических средств безопасности, проверяя, по-прежнему ли средства снижения рисков дают желаемый результат, или же новые направления атак, которые могут возникнуть в будущем, способны обойти эти средства.
  - Во всех случаях сведения о нарушениях безопасности, выявленных в ходе оперативного контроля, следует сообщать в центральную группу реагирования на нарушения безопасности (CERT) или в группу реагирования на инциденты, связанные с кибербезопасностью (CSIRT).
- Убедиться в том, что центральная группа имеет все возможности и способна фильтровать и давать оценку событиям безопасности (либо череде таких событий).

### 3.3 Последующий переход на регламенты и типовые технические средства безопасности

Процесс оценки рисков включает формирование регламентов и определение технических средств безопасности. В идеале они должны иметь исчерпывающий и внутренне согласованный характер. Однако, поскольку устаревшее оборудование не всегда допускает применение новых технических средств, а также в силу отсутствия типовых технических средств, комплексы снижения рисков сначала разрабатываются на временной или неунифицированной основе. В подобных случаях следует постепенно переходить к единым регламентам и типовым техническим средствам безопасности.

## Выводы

---

Органам регулирования следует помнить, что потребность в обеспечении требований кибербезопасности и отказоустойчивости в энергетике будет возрастать. В частности, органам регулирования потребуется поощрять либо требовать (в зависимости от того, являются ли стандарты добровольными или обязательными) от руководства коммунальных предприятий разработки комплексной внутренней политики, порядка, регламентов и технических средств безопасности с учетом отказоустойчивости, обеспечения встроенной в архитектуру безопасности (SbD), эксплуатационных требований, управления рисками, а также применения нормативных документов и руководств по кибербезопасности. Меры безопасности дадут результат только тогда,

когда руководство энергокомпаний по-настоящему осознает их важность и распространит свое отношение на все нижележащие уровни. В организации должна повсеместно сформироваться и распространиться культура безопасности, во всё большей степени опирающаяся на требования органов регулирования и действующее законодательство.

Не следует разрабатывать регламенты кибербезопасности с нуля. Органы регулирования могут (и должны) исходить из существующих нормативных документов и пособий по кибербезопасности. Решая вопросы инвестирования (и возмещения затрат), коммунальные предприятия (и, соответственно, органы регулирования) должны сделать упор на безопасность и отказоустойчивость системы. Прежде, чем утверждать нормативные документы и требовать их соблюдения, их следует проанализировать и понять. В новых стандартах должны быть отражены организационные и управленческие аспекты, вплоть до возможных финансовых последствий от их внедрения.

Как и все другие компоненты кибербезопасности, оценка риска, стандарты и иные предупредительные меры должны постоянно обновляться. Организаторы кибератак способны менять свои методы гораздо быстрее, чем органы регулирования могут реагировать на них, поэтому, чтобы решить эту проблему, от стандарта потребуются определенная гибкость. Стандарты не статичны: органы регулирования вместе с коммунальными предприятиями должны постоянно соотносить их с реальной ситуацией и применять новые методы для решения проблем безопасности.

Независимо от того, какие стандарты используются, а также добровольны они или обязательны, все большее значение для органов регулирования будут приобретать безопасность и отказоустойчивость, встроенные в архитектуру системы (SdB, security-by-design). Подобный подход позволит коммунальным предприятиям обеспечить доступные услуги и качество, которое заслуживают и ждут потребители. Стратегии, руководящие принципы и системы должны быть ориентированы на проверенный передовой опыт и открыты усовершенствованиям, которые учитывают эволюцию стандартов и технологий.

В Приложение к настоящему документу дана дополнительная информация о ряде международно-признанных стандартов кибербезопасности. Органы регулирования могут применить предложенные подходы вместо того, чтобы изобретать новые, и адаптировать эти подходы в соответствии со спецификой своих стран (например, применение добровольных или обязательных стандартов).

## Приложение. Стандарты и передовой опыт в сфере кибербезопасности

---

В Приложении приведено описание ряда ключевых действующих стандартов и мер кибербезопасности, сгруппированных по категориям «что?» и «как?», а также методов, позволяющих обеспечить их применение. По мере накопления органами регулирования необходимых знаний и привлечения коммунальных предприятий и других государственных организаций к совместной работе, направленной на обеспечение эффективных мер кибербезопасности, они могут опираться на накопленный опыт и существующие стандарты. Вместо попыток разработать стандарты с нуля, регулирующим органом имеет смысл адаптировать действующие стандарты, которые уже доказали свою практичность.

Органам регулирования важно иметь представление об основных причинах, обуславливающих необходимость стандартов, о критериях введения добровольных либо обязательных стандартов в соответствии с местной спецификой, а также мерах, предпринимаемых (или не предпринимаемых) коммунальными предприятиями их стран. Сотрудничество органов регулирования, коммунальных предприятий и других ключевых организаций ведет к усилению мер кибербезопасности в энергетике, что укрепляет безопасность и отказоустойчивость электрической сети.

Ниже дан краткий обзор ключевых аспектов следующих базовых стандартов кибербезопасности:

- Раздел А.1 Базовая структура кибербезопасности NIST
- Раздел А.2 Стандарты ИСО/МЭК серии 27000
- Раздел А.3 Стандарты НЕРК по защите важнейших объектов инфраструктуры
- Раздел А.4 Пособие по кибербезопасности в «умных» электрических сетях NISTIR 7628
- Раздел А.5 Стандарты серии МЭК 62443 на промышленные средства автоматизации<sup>15</sup>
- Раздел А.6 Стандарты серии МЭК 62351 по кибербезопасности «умных» электрических сетей<sup>16</sup>

Поскольку единственной, «самой лучшей» модели эффективного регулирования энергетики не существует, предлагаемые ниже базовые стандарты кибербезопасности следует рассматривать в контексте целей и условий каждой конкретной страны. Авторы настоящего пособия подготовили краткий обзор тех стандартов кибербезопасности, в отношении которых у них накоплен большой опыт, в надежде, что представленная ими информация поможет регулирующим органам осуществить дальнейшие шаги и возглавить работу по обеспечению кибербезопасности энергетики своих стран.

### А.1 NIST Базовая структура кибербезопасности<sup>17</sup>

Базовая структура кибербезопасности NIST — важный первый этап, который должны пройти специалисты по ИТ в целях анализа и улучшения своего ИТ-комплекса. Соответствующий документ используется органами регулирования по всему миру, так как в нем дана общая классификация результатов применения мер кибербезопасности, а также методика оценки и управления этими результатами. Данную методику могут использовать самые разные предприятия и организации, поскольку она позволяет действовать на опережение в сфере управления рисками и кибербезопасности.

---

<sup>15</sup> IEC. “Search results for ‘62443.’”

<sup>16</sup> IEC. “IEC 62351:2020 SER Series.”

<sup>17</sup> NIST, *Framework*.

Как показано на рис. 5, базовая структура NIST содержит общие функции — идентификацию, защиту, обнаружение, реагирование и восстановление. Эти пять функций применимы как к управлению рисками в сфере кибербезопасности, так и в любой другой сфере. Детализация в каждой категории позволят установить конкретные задачи кибербезопасности в организации — ИТ, физическая защита, персонал и т.п. — с привязкой к основной деятельности.

Подкатегории позволяют глубже понять базовую структуру, или «ядро» (Framework Core). Сто восемь подкатегорий — это положения, ориентированные на результаты и содержащие рекомендации по формированию и совершенствованию программы кибербезопасности. Поскольку подкатегории не предписывают, как именно достигать этих результатов, базовая структура, внедряемая в конкретной организации, может быть модифицирована под ее нужды и исходить из рисков, типичных для данной организации.

Из рис. 6 видно, что базовая структура (его «ядро») проста для понимания и выполняет функцию посредника, обеспечивая взаимодействие между многопрофильными коллективами на основе простого, без лишних технических терминов, языка. Базовая структура состоит из трех основных частей — функций, категорий и подкатегорий.

Базовая структура NIST позволяет сформировать общий язык и систематизированную методику для управления рисками кибербезопасности. «Ядро» базовой структуры включает меры, которые должны предусматриваться в любой программе кибербезопасности и которые, однако, могут быть адаптированы так, чтобы удовлетворять специфическим запросам организации. Таким образом, базовая структура дополняет, а не заменяет программу кибербезопасности и методику управления рисками, которые приняты в организации. Также, структура направляет продвижение важных решений по контролю над рисками по всем уровням — от высшего руководства компании до руководителей бизнес- и операционных подразделений и далее, до уровня непосредственной эксплуатации и внедрения.



Рис. 5. NIST Базовая структура повышения кибербезопасности критической архитектура.

Источник: NIST, “Cybersecurity Framework,” [16].

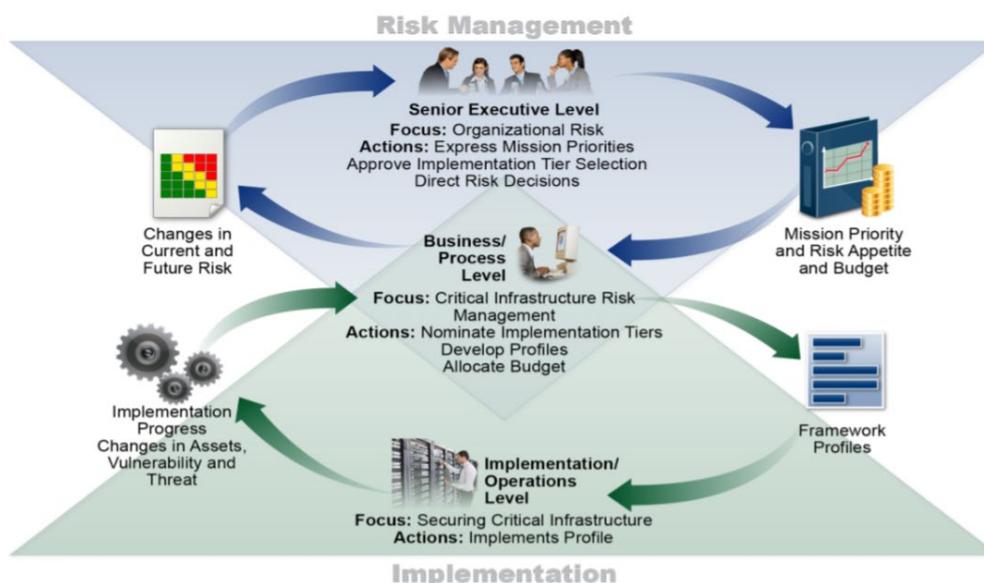


Рис. 6. Схема процесса управления рисками на всех уровнях организации (NIST)  
Источник: NIST, *Framework*, [15].

## A.2 Стандарты ИСО/МЭК серии 27000<sup>18</sup>

Стандарты ИСО/МЭК серии 27000 охватывают широкий круг требований по кибербезопасности (см. рис. 7). Стандарты нормируют политику и регламент кибербезопасности, которые должны быть внедрены на предприятии.

Наиболее актуальными для «умных» электросетей являются стандарты ИСО/МЭК 27001, 27002 и ИСО/МЭК 27019. В данных стандартах приведены общие организационные и процедурные требования к кибербезопасности, в том числе, требования к оценке риска, безопасности персонала и информационной безопасности. ИСО/МЭК 27001 имеет общий характер и может применяться в организациях любого типа. ИСО/МЭК 27002 относится к промышленным организациям. Дополнительные требования к организациям в области энергетики, а также обеспечение соответствия и порядок сертификации приведены в стандарте ИСО/МЭК 27019.

<sup>18</sup> *Information technology - Security techniques - Information security management systems*

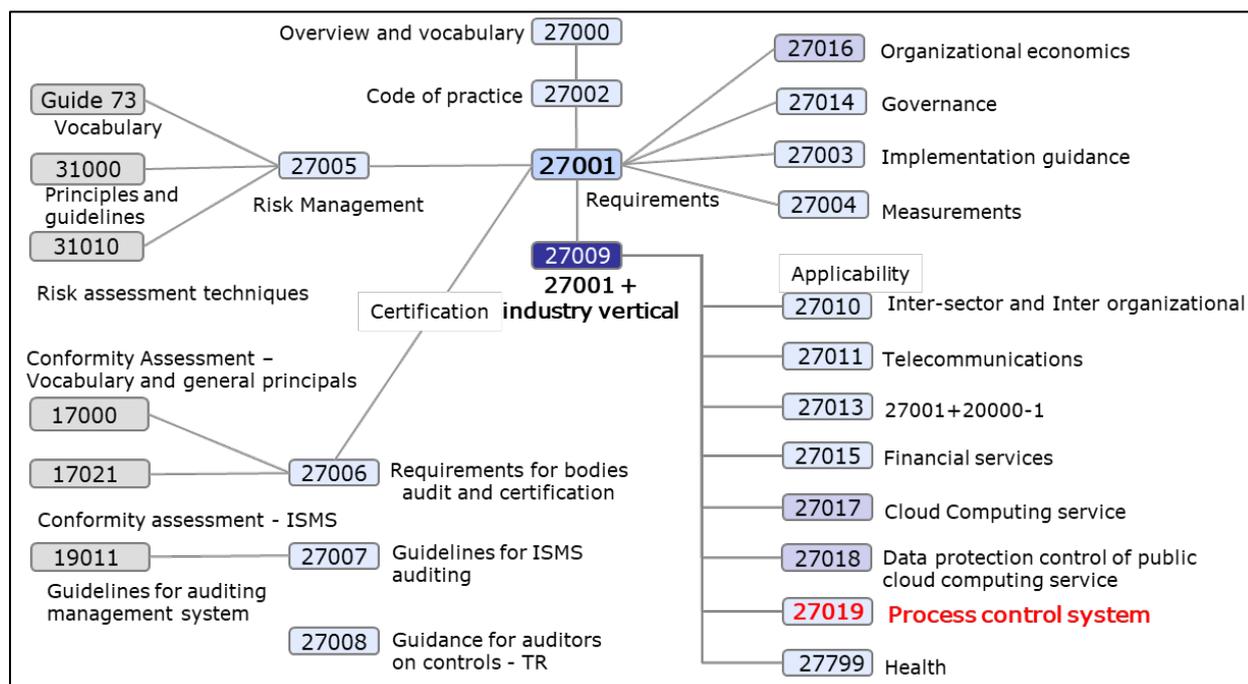


Рис. 7. Стандарты серии ИСО/МЭК 27000, в частности, 27019 по АСУ ТП  
Источник: ISO/IEC 27000 series, [8].

## A.2.1 Серия стандартов ИСО/МЭК 27001

ISO/IEC Стандарт ИСО/МЭК 27001 признан во всем мире. Он устанавливает требования к внедрению систем управления информационной безопасностью (СУИБ). ИСО определяет СУИБ как «системный подход к контролю над секретной информацией компании, обеспечивающий ее сохранность. Система включает персонал, процессы, и ИТ-комплексы и действует посредством применения процесса управления рисками».<sup>19</sup> Стандарт указывает, как следует определять задачи системы безопасности и риски, ставящие эти задачи под угрозу. Организация реагирует на выявленные риски согласно установленному плану. Важным элементом такого плана является выбор конкретных мер контроля из тех мер, которые предлагаются в стандартах ИСО/МЭК 27002 и отраслевых стандартах серии ИСО/МЭК 27002.

Серия стандартов ИСО/МЭК 27001 в последние годы активно развивалась и в настоящее время включает около 40 стандартов. Рис. 8 представляет сведения о наиболее актуальных для наших целей стандартах серии ИСО/МЭК 27001.

ИСО/МЭК 27001 (и другие стандарты серии 27000) помогают создать базу для аудита и сертификации СУИБ независимыми сторонними специалистами. Организации могут привлекать независимых специалистов для сертификации своих СУИБ на соответствие ИСО/МЭК 27001. Сторонние специалисты, в свою очередь, должны быть аккредитованы национальным органом аккредитации.

Серия стандартов СУИБ включает ряд взаимосвязанных нормативных документов, которые уже опубликованы либо разрабатываются в настоящее время. Серия состоит из нескольких структурных компонентов, включающих:

- требования к СУИБ (ИСО/МЭК 27001);

<sup>19</sup> <https://www.iso.org/isoiec-27001-information-security.html>

- требования к сертифицирующим организациям (ИСО/МЭК 27006), которые осуществляют сертификацию на соответствие ИСО/МЭК 27001;
- дополнительные требования по внедрению СУИБ в конкретных отраслях (ИСО/МЭК 27009).

В прочих документах содержатся рекомендации, затрагивающие различные аспекты внедрения СУИБ, как в плане процесса общего характера, так и с учетом отраслевой специфики.

Связи между стандартами СУИБ приведены ниже на рис. 8.

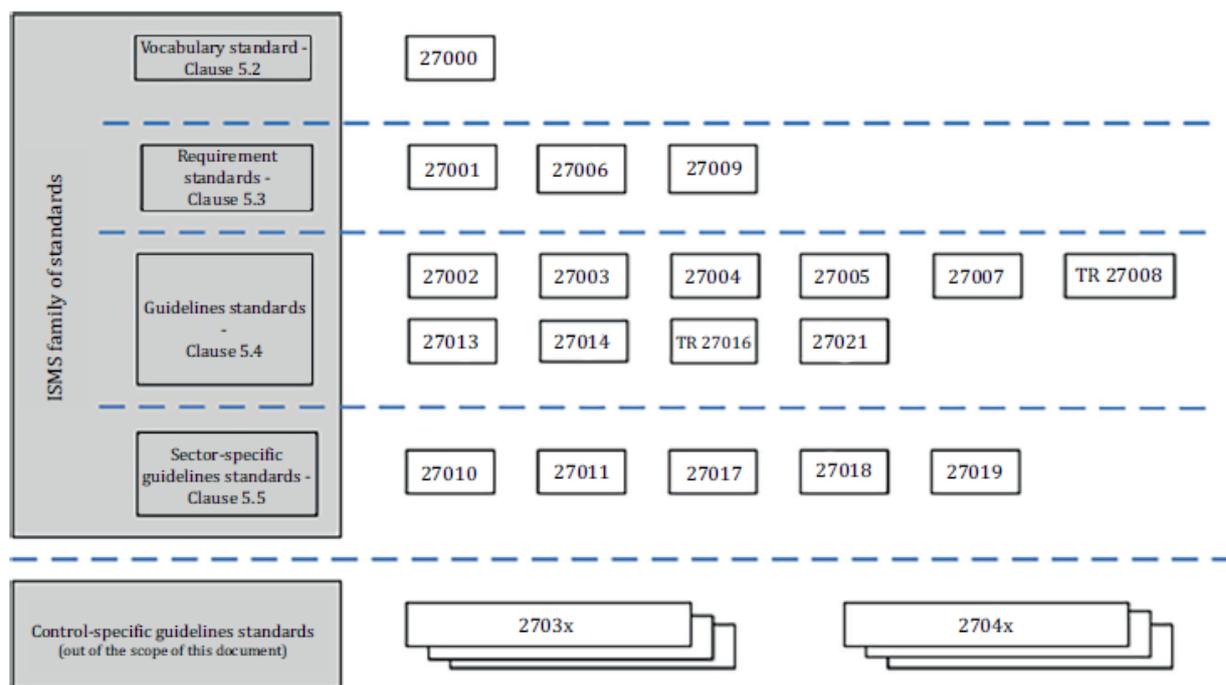


Рис. 8. ISMS Family of Standards Relationships

Источник: (ISO/IEC 27000:2018), [9].

## A.2.2 ИСО-МЭК 27002:2013<sup>20</sup>

Стандарт ИСО/МЭК 27002 представляет собой свод практических правил, которые затрагивают цели информационной безопасности, касающиеся снижения рисков, воздействующих, например, на конфиденциальность, целостность и доступность информации.

Меры управления безопасностью согласно ИСО/МЭК 27001 относятся к следующим основным категориям:

- организационные аспекты информационной безопасности;
- безопасность, связанная с персоналом;
- управление активами (киберфизическими ресурсами);
- управление доступом;
- криптография;
- физическая защита и защита от воздействия окружающей среды;

<sup>20</sup> ISO, *Code of Practice*.

- безопасность эксплуатации;
- безопасность связи;
- приобретение, разработка и эксплуатация информационных систем;
- отношения с поставщиками;
- менеджмент инцидентов информационной безопасности;
- соответствие (нормативам).

### **A.2.3 ИСО-МЭК 27019:2017<sup>21</sup>**

В стандарте ИСО/МЭК даны методические указания по контролю над информационной безопасностью на основе стандарта ИСО/МЭК 27002 в отношении АСУ ТП в энергетике. Цель ИСО/МЭК 27019 — дополнить серию стандартов ИСО/МЭК 27002 в части, относящейся к АСУ ТП и автоматизации. В энергетике данный стандарт позволяет внедрить унифицированную систему менеджмента информационной безопасностью (СУИБ), соответствующую ИСО/МЭК 27001, от руководства до эксплуатации.

Область применения стандарта ИСО/МЭК 27019 — АСУ ТП, используемые в энергетике для управления и контроля производства, передачи, хранения и распределения электроэнергии, газа и тепловой энергии в сочетании с управлением вспомогательными процессами. В частности, действие стандарта распространяется на следующие системы, программное обеспечение и компоненты:

- централизованное и распределенное управление технологическими процессами, оперативный контроль и средства автоматизации, а также информационные системы, используемые для функционирования упомянутых систем, например, программаторы и устройства параметрирования.
- цифровые контроллеры и звенья систем автоматики, например, контрольно-измерительные приборы, устройства нижнего уровня и программируемые логические контроллеры (ПЛК), в т.ч., элементы цифровых датчиков и исполнительных устройств;
- все остальные вспомогательные информационные системы, используемые в домене управления технологическими процессами, например, для дополнительных задач визуализации данных, а также в целях управления, оперативного контроля, архивного хранения данных, ведения документации;
- технические средства связи в целом, используемые в домене управления технологическими процессами, например, сети, телеметрия, устройства телемеханики и средства дистанционного управления;
- цифровые счетчики и измерительные приборы, например, для измерения потребления электроэнергии, производства электроэнергии, уровня выбросов в атмосферу;
- цифровые системы защиты и безопасности, например, релейная защита и аварийная защита на базе ПЛК;
- распределенные части будущих «умных сетей»;
- всё программное и микропрограммное обеспечение, а также прикладные программы, установленные на вышеупомянутых системах.

---

<sup>21</sup> ISO, *Energy Utility Industry*.

## А.3 НЕРК Защита объектов критической инфраструктуры (CIP)<sup>22</sup>

### А.3.1 Основные факты

На начальном этапе деятельности НЕРК/NERC (Североамериканская корпорация обеспечения надежности электросетей) участие в ней для предприятий электроэнергетики в Северной Америке было добровольным. НЕРК поощрял энергокомпании, управляющие крупными и сложными энергосистемами, организовывать управление и техническое обслуживание системных ресурсов таким образом, чтобы это способствовало повышению надежности энергосистемы в целом. В рамках добровольного участия были разработаны правила эксплуатации, руководства и нормативные документы, направленные на то, чтобы задачи повышения надежности решались энергокомпаниями на приемлемом уровне. Поскольку сбои в надежности энергосистем не прекращались, и к ним добавились новые, постоянно растущие угрозы в отношении критических компонентов инфраструктуры, были предприняты усилия по созданию органа регулирования («Закон США об энергетической политике» 2005 г.), который заявил о необходимости создания Организации по надежности в электроэнергетике (ЭРО). Такой организации предоставлялось право и вменялось в обязанность разработать и добиваться соблюдения стандартов, обеспечивающих надежность крупных энергосистем.

Представителем ЭРО по Северной Америке является НЕРК. НЕРК отвечает за работу с региональными отделениями по внедрению и обеспечению соблюдения стандартов надежности. Хотя стандарты НЕРК по защите важнейших объектов инфраструктуры были введены уже более 15 лет назад, мы рассмотрим лишь действующие на сегодня редакции этих стандартов (версии 5 и 6), см рис. 9.

Версия 5 – 6	Наименование стандарта
CIP-002-5.1	Классификация киберсистем больших энергетических систем (БЭС)
CIP-003-6	Средства управления безопасностью
CIP-004-6	Персонал и обучение
CIP-005-5	Электронные периметры безопасности
CIP-006-6	Физическая защита киберсистем БЭС
CIP-007-6	Управление безопасностью систем
CIP-008-5*	Отчетность по инцидентам и планирование реагирования
CIP-009-6	Планы восстановления киберсистем БЭС
CIP-010-2	Управление изменениями в конфигурации и оценка уязвимости
CIP-011-2	Защита информации

Рис. 9. Действующие стандарты НЕРК по защите объектов критической инфраструктуры (сочетание версий 5 и 6).

Источник: NERC [14].

В качестве вводной информации и с целью выявления некоторых достоинств данных стандартов, ниже обсуждаются их отдельные аспекты, которые следует учитывать при ознакомлении со стандартами этой группы.

<sup>22</sup> NERC, “CIP Standards.”

### **А.3.2 Стандарт, разработанный специалистами отрасли для отрасли**

Как и все стандарты NERC, стандарты по защите КИ разработаны согласно непосредственным рекомендациям представителей электроэнергетики. В 2003 г. ряд владельцев и менеджеров энергокомпаний установили, что кибербезопасность, точнее, ее отсутствие, сопряжена с существенным риском надежности электроснабжения. Предполагалось, что риск этого типа будет закономерно расти по мере того, как в энергосистемах расширяется использование ИТ-ресурсов, в частности, АСУ ТП. Одновременно с этим наблюдались еще две тенденции —увеличение числа межсистемных связей и доступности ЭТ-систем, а также повышение внимания злоумышленников к АСУ ТП. По этой причине энергокомпании начали разрабатывать отраслевой стандарт по кибербезопасности.

Процесс разработки стандарта сложен и трудоемок и требует учета следующих важных аспектов: проекты стандартов должны разрабатывать проектные группы, включающие представителей заинтересованных сторон-представителей электроэнергетической отрасли; процесс разработки должен быть открытым и гласным; при внесении изменений в проект стандарта необходимо предусмотреть неоднократные периоды, во время которых представители отрасли могут высказать свое мнение; наконец, что важнее всего, в голосовании за или против утверждения проекта стандарта должна принимать участие вся отрасль. Такой подход позволяет организациям, которые будут вынуждены соблюдать стандарт после его утверждения, высказывать свое мнение в течение всего процесса разработки стандарта и убедиться в том, что их мнение дошло до адресатов и принято во внимание.

### **А.3.3 Физические и кибер-угрозы стабильности электрических сетей**

В 2009 г. Министерство энергетики США выпустило совместный отчет, в котором были отражены основные угрозы электроэнергетике. В основном, речь шла о мощных, но крайне редких (почти никогда не случающихся) явлениях, которые, если все-таки происходят, обладают столь сильным воздействием, что для ликвидации их последствий могут потребоваться усилия всей отрасли. Одним из возможных сценариев такого явления была одновременная атака на физические объекты энергосистемы и кибератака на нее. По общему мнению, стандарты CIP следует внедрять так, чтобы снизить немедленное и долгосрочное воздействие атаки этого типа. Многие специалисты, хотя бы немного знакомые со стандартами CIP, знают, что их требования относятся и к кибербезопасности. Однако следует также отметить, что стандарт CIP-006 охватывает меры физической защиты ИТ-ресурсов крупных электроэнергетических систем, а CIP-014 — меры физической защиты важнейших объектов электропередачи.

### **А.3.4 Требования к традиционным ИТ-ресурсам и ЭТ-ресурсам**

Как упоминалось выше, стандарты защиты критической архитектуры NERC являются многопрофильными, в том смысле, что их положения относятся как к физическим угрозам, так и к киберугрозам. Следует также отметить, что сфера действия этих стандартов не ограничена традиционными ресурсами ИТ или разделяемыми устройствами межсистемных связей. Напротив, в стандартах даны достаточно детализированные перечни мер, которые должны быть предприняты в отношении ресурсов ИТ и ЭТ и от которых существенно зависит надежность энергосистемы всей страны. Положения стандартов указывают, что должны сделать энергокомпании, но не предписывают, как именно они должны выполнить эти требования. Соответственно, энергокомпаниям оставлена свобода в выборе подходов и технических решений, которые они могут применить, чтобы удовлетворить требованиям стандартов.

### А.3.5 Выводы

С момента своей первой публикации, стандарты защиты критической инфраструктуры (CIP) постоянно совершенствуются. Страна, заинтересованная в их применении, может воспользоваться последними редакциями данных стандартов, отражающими многолетний опыт их внедрения. Действующие редакции стандартов отличаются следующими достоинствами:

- **Разработка стандартов осуществлялась при непосредственном участии представителей отрасли.** Стандарты для сложных в эксплуатации систем, таких как электроэнергетическая система, должны разрабатываться представителями отрасли и для целей отрасли.
- **Соблюдение обеспечивается материальной заинтересованностью.** Внедрение стандартов экономически эффективно для предприятий.
- **Ресурсы, подпадающие под действие стандартов, определяет само предприятие по заданным критериям.** Попытка применить все возможные меры и средства ко всем компонентам системы, что довольно типично, приводит к провалу. Успешная программа делает правильный выбор, на каких объектах внедрять стандарт и к каким ИТ-ресурсам его применять.
- **Системный подход к классификации ресурсов и определению, насколько к ним применимы требования.** Обеспечение безопасности единичного устройства не всегда возможно; более эффективным является обеспечение безопасности системы в целом по мере необходимости.
- **Низкая, средняя и высокая степени применимости требований.** Такое разграничение позволяет выбирать меры и средства обеспечения безопасности экономно, в соответствии с рисками для электроэнергетической системы.
- **Стандарты имеют недирективный характер.** Стандарты указывают, что должно быть достигнуто, но не уточняют, как именно, оставляя предприятиям свободу действий и позволяя строить и реализовывать программу, которая наиболее подходит к конкретным условиям.

**Рекомендации организациям, планирующим внедрить стандарты защиты критической инфраструктуры (CIP) NERC.** Органам регулирования, рассматривающим возможность внедрения стандартов CIP для решения своих задач, предлагаются следующие рекомендации, которые помогут успеху внедрения стандартов.

- Назначить общегосударственный руководящий орган (пример — рассмотренные выше ЭРО). Необходима руководящая структура, которая будет обрабатывать обзоры энергокомпаний и возможный аудит стандартов.
- Внести изменения в Приложение CIP-002-5.1a, отражающие специфику вашей энергосистемы, с целью обеспечения надлежащего уровня защиты (высокого, среднего или низкого) ресурсов разных уровней<sup>23</sup>.
- Пересмотреть термины и определения NERC, использованные в стандартах CIP, и, при необходимости, внести изменения, обеспечивающие их понимание и эффективное применение как органами регулирования, так и энергокомпаниями.
- Применять «смещенное» поэтапное внедрение, в первую очередь, по ресурсам диспетчерских пультов, чье воздействие может сказаться на обширных территориях. Разработать план внедрения стандартов, в котором предусмотреть первоочередное внедрение на объектах, связанных с высокой степенью риска, последующее — на участках с более низкой степенью риска.

---

<sup>23</sup> NERC, CIP-002-5.1a.

- В ходе внедрения стандартов предусмотреть достаточно продолжительные периоды времени для сбора отзывов энергокомпаний. Разрешить энергокомпаниям равного ранга до проведения официального аудита выполнять перекрестную оценку программ в режиме, позволяющем делать выводы и совершенствовать программы.
- Проинструктировать аудиторов или инспекторов о том, что чем более совершенной системой внутренних мер и средств обеспечения безопасности обладает организация, тем больше нарушений стандарта она может выявить самостоятельно. Подобная ситуация ни в коем случае не должна считаться проблемой. Напротив, органы регулирования должны предусмотреть надлежащие меры поощрения правильного поведения в этом смысле.
- Требования данных стандартов являются базовыми, их превышение поощряется. Выполнение требований стандартов следует рассматривать как неизбежные расходы осуществления основной деятельности и поощрять предприятия к их перевыполнению.
- Соблюсти формальные предписания стандартов проще, чем не допустить реальных нарушений безопасности и снижения надежности. Программа, построенная на основе планов и общей политики, без реальных элементов кибербезопасности, не позволит выполнить требования стандартов и не обеспечит должного уровня кибербезопасности.

### А.3.6 Четыре основных вопроса

Модель защиты критической инфраструктуры НЕРК предлагает национальным органам регулирования четыре основополагающих принципа, которые позволят внедрить действенные стандарты.

- 1) **Определить, какие ресурсы критической инфраструктуры подпадают под действие стандарта.** Категории ресурсов определены в требовании 1 CIP-002, критерии ранжирования конкретных видов воздействия — в приложении 1. Пороговые значения критериев, приведенных в приложении 1, следует изменить в соответствии со спецификой энергосистемы конкретной страны или региона.
- 2) **Определить, какие требования актуальны.** Стандарты с CIP-003 по CIP-014 содержат требования к владельцам ресурсов по внедрению и менеджменту программы обеспечения безопасности. За годы внедрения данных стандартов на тысячах объектов по всей Северной Америке, образовалось множество организаций и консультационных фирм, которые могут разработать надежные программы защиты, обеспечить сертифицированный инструктаж всего личного состава и тем самым обеспечить способность персонала обслуживать программу защиты критической инфраструктуры.
- 3) **Определить, как будет проводиться оценка соблюдения стандартов.** За многолетний период, в который проводились добровольные самооценки, перекрестные оценки и официальные аудиты региональными органами, накоплен большой массив знаний и учебных программ, которыми могут воспользоваться органы регулирования других стран. Также, подготовлен большой контингент консультантов, обученных аудиту программ защиты критической инфраструктуры.
- 4) **Определить, кто и каким образом будет обеспечивать соблюдение стандартов.** Это — важная составляющая, которая имеет свою специфику в каждой из стран. Определять ее следует так, чтобы обеспечить успешное

внедрение и, в качестве дополнительного стимула, иметь надлежащий уровень надзорного органа.

## A.4 NISTIR 7628 Пособие по кибербезопасности в «умных» электрических сетях

### A.4.1 NISTIR 7628 Средства обеспечения кибербезопасности

The Документ NISTIR 7628 содержит набор указаний, направленных в первую очередь на обеспечение кибербезопасности «умных» электросетей и входящих в их состав аппаратных и программных компонентов. По сфере применения NISTIR 7628 сходен со стандартом ИСО/МЭК 27019, за исключением того, что его положения относятся исключительно к «умным» электрическим сетям. В документе дано общее описание около 300 мер и средств обеспечения кибербезопасности, сходных с мерами и средствами, приведенными в других документах NIST, в частности, по базовой структуре NIST (см. рис. 10).

Шифр	Группы требований NIST по безопасности в «умных» электрических сетях
SG.AC	Управление доступом
SG.AT	Осведомленность и обучение
SG.AU	Аудит и отчетность
SG.CA	Оценка безопасности и авторизация
SG.CM	Управление конфигурацией системы
SG.CP	Бесперебойность эксплуатации
SG.IA	Идентификация и аутентификация
SG.ID	Управление информацией и документацией
SG.IR	Реагирование на инциденты безопасности
SG.MA	Разработка и эксплуатация информационной системы «умной» электрической сети
SG.MP	Защита носителей информации
SG.PE	Физическая защита и защита от воздействия окружающей среды
SG.PL	Планирование
SG.PM	Управление программой по безопасности
SG.PS	Безопасность персонала
SG.RA	Управление и оценка риска
SG.SA	Приобретение информационных систем и услуг для «умных» электрических сетей
SG.SC	Защита информационных систем и систем связи «умных» электрических сетей
SG.SI	Информационные системы «умных» электрических сетей и целостность информации в них

Рис. 10. Группа стандартов NISTIR 7628 по безопасности «умных» электрических сетей

Источник: выведено из данных Xanthus Consulting International [17].

### A.4.2 NISTIR 7628 Эталонная логическая модель кибербезопасности

Меры и средства обеспечения кибербезопасности, приведенные в пособии NISTIR 7628, выходят за рамки общих требований. В документе описана эталонная, высокого уровня

модель логических стыков между элементами, которые разделены на 22 категории. Категории логических стыков характеризуются требованиями к связи и межсистемными ограничениями внутри доменов «умной» электрической сети и между ними. К ним относятся: эксплуатация, рыночные операции, системы поддержки, объекты потребителей, РИЭ и прочее полевое оборудование. По каждой из категорий логических стыков определены и вкратце описаны соответствующие общие требования по безопасности. На рис. 11 показана эталонная логическая модель высокого уровня («диаграмма спагетти»), которая демонстрирует категории требований к связи и ограничения, характерные для «умных» электросетей.

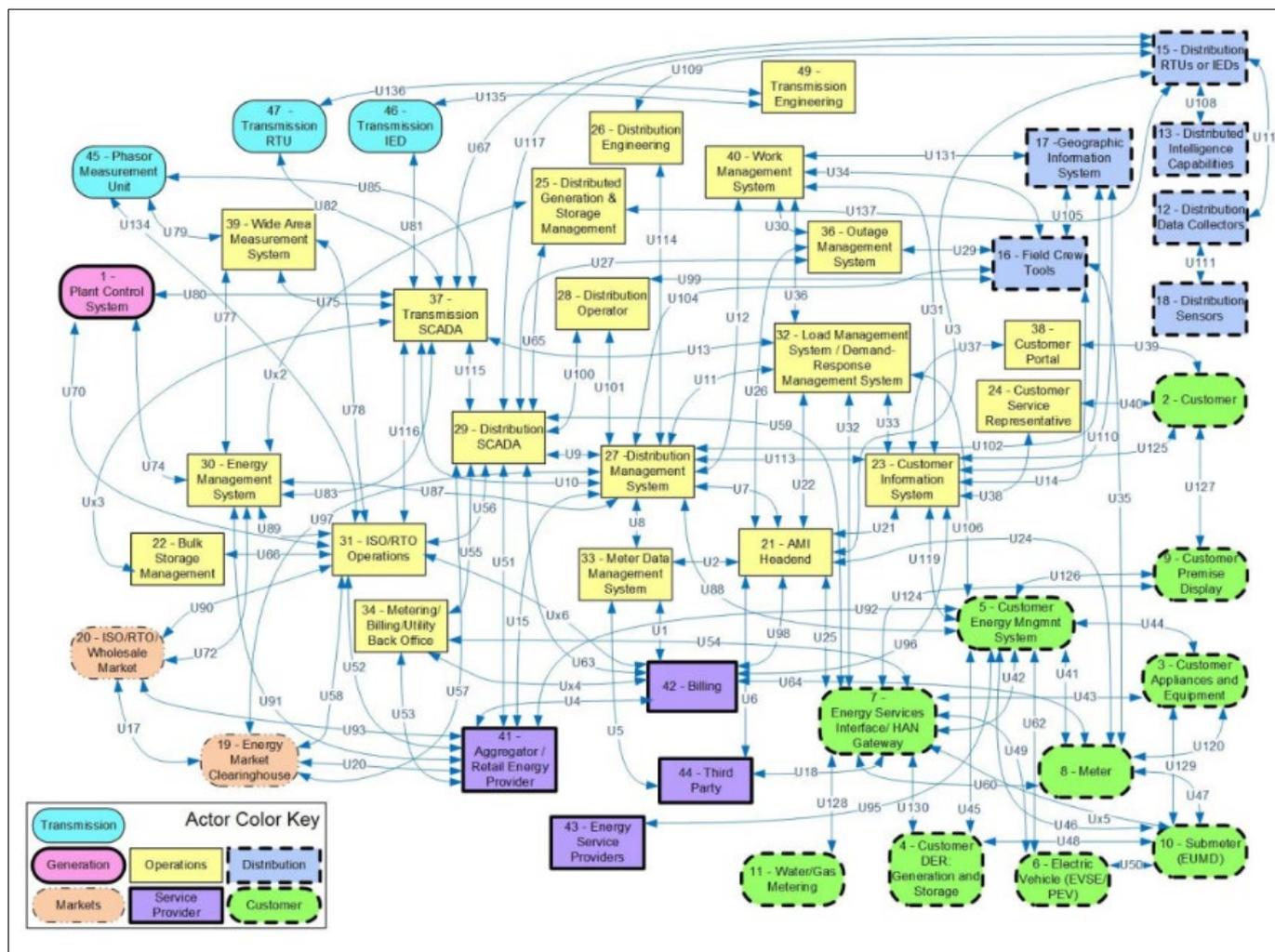


Рис. 11. Эталонная логическая модель с пересекающимися связями («спагетти») NIST IR 7628

Источник: NISTIR 7628, [17].

## **А.5 МЭК 62443 Стандарты на промышленные средства автоматизации<sup>24</sup>**

### **А.5.1 МЭК 62443 Основные факты**

Международные стандарты серии МЭК 62443 задают структуру требований к безопасности. Они разработаны совместно Международной электротехнической комиссией (МЭК) и комитетом Международной организации по автоматизации (ISA99) и содержат требования к безопасности систем промышленной автоматизации и управления (IACS) как в организационной, так и в технической части. Хотя стандарт относится, в первую очередь, к промышленной автоматике в целом, большинство требований по кибербезопасности применимы и к энергетике и включают более подробные требования по эксплуатации киберфизических систем, чем стандарты ИСО/МЭК серии 27000. Например, в стандартах этой серии подробно изложены требования по управлению пакетами обновлений («патч-менеджмент»), конкретные требования по безопасности систем и элементов применительно к разным уровням безопасности. Организационные требования по безопасности «умных» электрических сетей приведены в стандартах МЭК 62443-2-2, 2-3, 2-4 и 4-1, технические — в стандартах МЭК 62443-3-3 и 4-2. В стандарте МЭК 62443-2-1 изложены требования к владельцам ресурсов АСУ ТП, дополняющие ИСО 27001 в части мер и средств безопасности, специфических для данной сферы. Дополнительные требования к структуре управления безопасностью «умных» электрических сетей даны также в стандарте ИСО 27019.

Как уже отмечалось, технические требования по безопасности систем промышленной автоматизации и управления, а также их элементов, классифицированы по уровням безопасности. В комплекте сопутствующих документов определены требования по безопасности, предназначенные не только для операторов средств безопасности и их интеграторов, но также для изготовителей.

### **А.5.2 МЭК 62443 Основные факты**

Как показано на рис. 12, требования стандарта разделены на четыре группы следующего содержания:

- общие определения и измеряемые характеристики;
- требования к организации безопасности (соотносятся к СУИБ, положениями ИСО 27001, а также к процессам, внедренным у изготовителей и поставщиков средств безопасности).
- Технические требования и методика обеспечения безопасности на общесистемном уровне.
- Требования к безопасности производственного цикла компонентов системы и требования к безопасности компонентов системы на техническом уровне.

---

<sup>24</sup> IEC. "Search results for '62443.'"

General	Policies and Procedures	System	Component
1-1 Terminology, concepts and models IS 2009	2-1 Requirements for an IACS security management system Ed.2.0 Profile of ISO 27001 / 27002 CD 2Q18 <span>Cert</span> <span>Procedural</span>	3-1 Security technologies for IACS TR 2009	4-1 Product development requirements IS 1Q18 <span>Cert</span> <span>Procedural</span>
1-2 Master glossary of terms and abbreviations In Progress	2-2 IACS protection levels NP 3Q18 <span>Procedural</span>	3-2 Security risk assessment and system design CDV 1Q/18 <span>Cert</span> <span>Functional</span>	4-2 Technical security requirements for IACS products FDIS 2Q18 <span>Cert</span> <span>Functional</span>
1-3 System security compliance metrics Rejected	2-3 Patch management in the IACS environment TR 2Q15 <span>Procedural</span>	3-3 System security requirements and security levels IS 08/2013 <span>Cert</span> <span>Functional</span>	
1-4 IACS Security Life Cycle and Use Cases Planned	2-4 Requirements for IACS solution suppliers IS 08/2015 <span>Cert</span> <span>Procedural</span>		
Definitions and Metrics	Requirements for Organizations	Requirements for Systems	Requirements for Components

IS 2015 = Status    Cert = Certification relevance    Procedural / Functional = Scope  
 \*DC: Draft for Comment    \*IS: International Standard    \*NP: New Proposal  
 \*CDV: Committee Draft for Vote    \*FDIS: Final Draft International Standard    \*TR: Technical Report

Рис. 12. IEC 62443 Серия стандартов безопасности в промышленности МЭК 62443. Обзор.

Источник. ISA99.org, [5] Xanthus Consulting International, личная переписка.

Figure 13 показано соответствие разделов стандартов серии МЭК 62433 различным функциям производственным. Оператор системы эксплуатирует систему автоматизации и управления, которая интегрирована системным интегратором и в которой использованы комплектующие, предоставленные поставщиком.

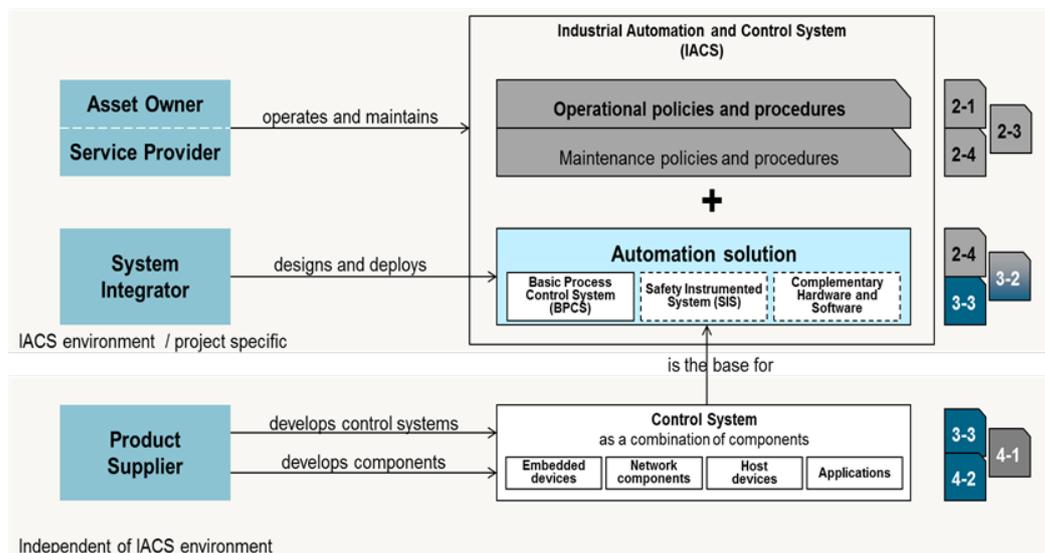


Рис. 13. Разделы стандартов серии МЭК 62443 согласно функциям.

Источник: Разработано ISA99 для уточнения IEC 62443-2-4 Ed1.1: 2017, [5] Xanthus Consulting International, личная переписка.

Согласно методике, описанной в МЭК 62443-3-2, структура сложной системы автоматизации разбита на зоны, между которыми связь и обмен информацией осуществляется по особым «трактам» (каналам), которые, в частности, привязаны к протоколу связи между двумя зонами в логической сети. Далее, в стандарте определены

также уровни безопасности, коррелирующие с эффективностью потенциального злоумышленника, как показано на рис. 14. Чтобы достичь заданного уровня безопасности, должны быть выполнены соответствующие требования. В стандарте МЭК 62443-3-3 определены требования к безопасности системы. При этом целесообразно сосредоточить внимание на отдельных аспектах безопасности, а не на всей системе в целом. Требования к безопасности, установленные стандартом МЭК 62443-3-3, помогают убедиться в том, что все значимые аспекты безопасности учтены при разработке.

В разделе 3-3 стандарта МЭК 62443 определены семь фундаментальных требований (FR) по категориям: идентификация и аутентификация (FR1), контроль использования (FR2), целостность системы, конфиденциальность данных (FR4), ограничение потока данных (FR5), своевременное реагирование на события (FR6), доступ к ресурсам (FR7).

Каждому базовому требованию соответствует ряд конкретных технических требований по безопасности, также расширенные требования для конкретных уровней безопасности. С учетом специфики безопасности связи, особый интерес представляют уровни безопасности трактов, соединяющих разные зоны.

### А.5.3 МЭК 62443 Уровни безопасности

В стандарте МЭК 62443-3-2 определены четыре уровня безопасности (уровень безопасности 1, 2, 3 и 4), соответствующие эффективности потенциального злоумышленника, как показано на рис. 14. Чтобы достичь заданного уровня безопасности, следует выполнить установленные для этого уровня требования и, возможно, расширенные требования. Стандартом предусмотрено, что удовлетворить требование безопасности можно либо непосредственно, либо с помощью компенсационной контрмеры.

4 Security Level (SL)	
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Рис. 14. Уровни безопасности в стандарте МЭК 62443

Источник: IEC 62443-3-2 [3], Xanthus Consulting International, личная переписка.

Введение понятия компенсационной контрмеры позволяет достигнуть определенного уровня безопасности, даже если некоторые требования невозможно реализовать непосредственно, например, когда отдельные компоненты системы не выполняют требуемые технические функции. Данный подход особенно важен для автоматизированных промышленных систем управления и контроля, находящихся в эксплуатации (brownfield installations), т.к. позволяет и далее эксплуатировать установленное оборудование.

Уровень безопасности зоны или тракта (тракт связывает зоны) можно рассматривать как вектор уровней безопасности из семи элементов (см. также приложение А стандарта МЭК 62443-3-3). Элементы вектора приписывают уровень безопасности каждому из фундаментальных требований. Таким образом можно определить конкретный уровень безопасности каждого из требований. Например, если конфиденциальность не входит в число задач безопасности в данной зоне, компонент уровня безопасности, соответствующий требованию «конфиденциальность данных», может иметь уровень 1 или вовсе не иметь уровня безопасности, но при этом по другим

фундаментальным требованиям (например, «идентификация и аутентификация» или «целостность системы») может быть необходим уровень 3. Таким образом, полученный в результате вектор уровня безопасности зоны будет иметь вид «уровень безопасности=(3,3,3,1,2,1,3)» или «уровень безопасности =(2,2,2,0,1,1,0)».

МЭК 62443 / ISA-99			
Общие	Правила и регламенты	Системы	Компоненты системы
1-1. Техника, понятия и модели	2-1. Организация системы безопасности IACS	3-1. Технические средства безопасности IACS	4-1. Требования к разработке продукции
1-2. Словарь терминов и сокращений	2-2. Применение системы безопасности IACS	3-2. Уровни обеспечения безопасности для зон и связующих трактов	4-2. Технические требования к безопасности изделий IACS
1-3. Показатели соответствия системы требованиям безопасности	2-3. Управление пакетами исправлений и обновлений в среде IACS	3-3. Требования к безопасности системы и уровни безопасности	Требования к обеспечению безопасности компонентов системы
Определения и показатели	2-4. Сертификация политики и практики поставщиков IACS	Требования к безопасным системам	
	Требования к организации безопасности и процессам владельцев станций и поставщиков		
		Функциональные требования	Процессы или регламенты

Рис. 15. Серия стандартов кибербезопасности МЭК 62443 комитета ISA-99.  
Источник: ISA99.org, [3], Xanthus Consulting International, личная переписка.

## А.6 Серия стандартов МЭК 62351 по кибербезопасности «умных» электрических сетей<sup>25</sup>

### А.6.1 МЭК 62351 Обзор

Серия стандартов МЭК 62351<sup>26</sup> устанавливает требования к техническим средствам кибербезопасности при обмене информацией по протоколам связи, предусмотренным в ТК 57 МЭК, в частности, в сериях МЭК 60870-5, МЭК 60870-6, МЭК 61850, МЭК 61970 и МЭК 61968. Как показано на рис. 16, однозначного соответствия между стандартами связи ТК 57 МЭК и стандартами по безопасности МЭК 62351 не существует. Дело в том, что стандарты связи на разных уровнях опираются на одни и те же базовые стандарты. Испытания на соответствие этим стандартам включены в серию МЭК 62351-100-хх.

<sup>25</sup> IEC. "IEC 62351:2020 SER Series."

<sup>26</sup> Более подробная информация в открытом доступе на веб-сайте:  
<http://iectc57.ucaiug.org/wg15public/default.aspx>

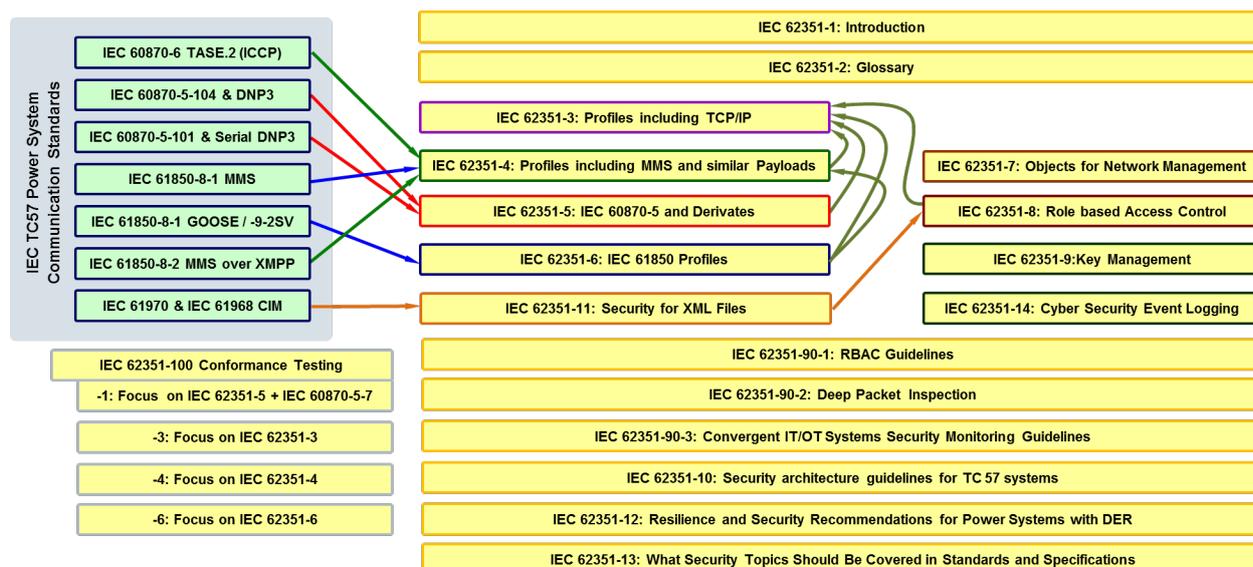


Рис. 16. Серия стандартов МЭК 62351 по кибербезопасности.

Источник: Xanthus Consulting International.

## А.6.2 МЭК 62351 Стандарты кибербезопасности связи

В серию стандартов по кибербезопасности МЭК 62351 входят следующие разделы, относящиеся к системам связи.

- Технические спецификации МЭК/ТТ 62351-1:2007. Введение. Первая часть стандарта включает общие положения по обеспечению безопасности при эксплуатации энергосистем и вводные сведения о стандартах по безопасности серии МЭК 62351.
- МЭК/ТТ 62351-2:2008. Словарь терминов. Содержит термины и сокращения, используемые в стандартах серии МЭК 62351. Определения, по мере возможности, согласованы с определениями в действующих стандартах в области связи и безопасности, с учетом того, что термины по безопасности широко применяются не только в энергетике, но и в других отраслях. Термины и определения находятся в свободном доступе на сайте МЭК: <http://std.iec.ch/terms/terms.nsf/ByPub?OpenView&Count=-1&RestrictToCategory=IEC%2062351-2>
- МЭК 62351-3:2014. Безопасность коммуникационных сетей и систем, включая протокол контроля над передачей данных и интернет-протокола TCP/IP. Этот стандарт безопасности затрагивает протоколы, охваченные в следующих нормативных документах:
  - МЭК 60870-6 (Telecontrol Application Service element [TASE.2] / Inter-control Center Communication Protocol [ICCP])
  - МЭК 60870-5 часть 104
  - IEEE 1815 (Distributed Network Protocol 3 [DNP 3]) по сетям TCP/IP
  - МЭК 61850 по сетям TCP/IP
- МЭК 62351-4. Безопасность данных и коммуникаций. Протоколы, включая Manufacturing Message Specification (MMS) и аналогичные пакеты. Стандарт охватывает протоколы, указанные в следующих нормативных документах:
  - МЭК 60870-6 (TASE.2 / ICCP) с применением Manufacturing Message Specification (MMS)
  - МЭК 61850-8-1 с применением протокола MMS объектов «данных»

- МЭК 61850-8-2 с применением XSD XML, соотнесенного с объектами «данных» MMS
- МЭК 62351-5. Безопасность данных и коммуникаций. Безопасность IEC 60870-5 и производных (например, DNP3). Данный стандарт охватывает последовательные и сетевые протоколы, указанные в следующих нормативных документах:
  - МЭК 60870-5-7 (сведения по безопасности для МЭК 60870-5-101 и 104)
  - IEEE 1815 (DNP3)
- МЭК 62351-6. Безопасность данных и коммуникаций. Безопасность для одноранговых протоколов согласно МЭК 61850. Стандарт охватывает протоколы, соответствующие:
  - МЭК 61850, не работающие по протоколам TCP/IP – общее объектно-ориентированное событие на подстанции (generic object-oriented substation event/GOOSE) и выборочное значение (sampled value/SV).

### **А.6.3 МЭК 62351 Дополнительные стандарты по кибербезопасности и технические отчеты**

Дополнительные стандарты по кибербезопасности и технические отчеты МЭК 62351 охватывают дополнительные перечисленные ниже области.

- «МЭК 62351-7. Управление сетями и системами (network and system management/NSM) информационной инфраструктуры». Стандарт определяет абстрактные объекты данных NSM для эксплуатационной среды энергосистем с учетом того, какая информация необходима для максимально надежного управления информационной инфраструктурой, с помощью которой осуществляется управление энергосистемой. Разработано соответствие информационным базам управления (MIB) стандарта SNMP (Simple Network Management Protocol), предоставленное в виде компонентов программного кода.
- «МЭК 62351-8. Контроль над доступом согласно функциям для системы управления энергосистемой» (Role-Based Access Control/RBAC). Назначение стандарта:
  - ввести концепцию авторизации «субъект-функции-права» (аналог «пользователь-функции-полномочия» согласно Национальному институту стандартизации США и Международному комитету по стандартам информационных технологий (ANSI INCITS) 359-2004;
  - распространить управление доступом согласно функциям (role-based access control/RBAC) на всю иерархию управления энергосистемой;
  - обеспечить эксплуатационную совместимость в условиях разных производителей энергетического оборудования;
  - стандарт МЭК 61850-90-19 развивает требования к RBAC, приведенные в МЭК 61850.
- «МЭК 62351-9. Управление ключами кибербезопасности». Стандарт предписывает порядок генерации, распределения, отзыва и обращения с цифровыми сертификатами и ключами шифрования, предназначенными для защиты данных и обмена ими. В частности, устанавливается порядок обращения с несимметричными ключами (например, закрытыми ключами и сертификатами X.509) и симметричными ключами (например, ключами сеансов).
- «МЭК Технический отчет 62351-10. Архитектура безопасности». Документ представляет собой технический отчет, в котором даны указания по архитектуре безопасности энергосистем, основанные на основных мерах и средствах

обеспечения безопасности, т.е. связанных с безопасностью элементов и функциях, и их взаимодействии.

- «МЭК 62351-11. Безопасность для документов XML». Определяет требования к безопасности при обмене XML-документами, которые используются для МЭК 61970 и некоторых других видов обмена информацией по МЭК 61850.
- «МЭК 62351-12. Отказоустойчивость энергосистем с системами РИЭ». Включает рекомендации по отказоустойчивости применительно к техническим и эксплуатационным стратегиям, а также техническим средствам кибербезопасности, применяемым в системах распределенных источников энергии (РИЭ). Технический отчет охватывает требования к отказоустойчивости, относящиеся к множеству различных заинтересованных сторон в таких распределенных киберфизических устройствах производства и накопления энергии. Его целью является обеспечение безопасности, надежности, качества электроэнергии и других аспектов эксплуатации энергосистем, более конкретно, содержащих в большом количестве системы РИЭ.
- «МЭК 62351-13. Какие проблемы безопасности должны быть учтены в стандартах и технических спецификациях». Данный документ призван помочь разработчикам стандартов решать вопросы кибербезопасности на уровне, соответствующем разрабатываемому стандарту. Дан перечень проблем безопасности, которые рекомендуется охватить в стандартах и технических спецификациях для использования в электроэнергетике.
- «МЭК 62351-14. Регистрация событий кибербезопасности». В данной части серии МЭК 62351 подробно описаны технические аспекты использования журналов безопасности: передача информации, наполнение и семантика.

#### **А.6.4 МЭК 62351 Технические требования к проверке на соответствие стандартам**

Дополнительные стандарты по кибербезопасности и технические отчеты МЭК 62351 охватывают дополнительные перечисленные ниже области.

- «МЭК 62351-7. Управление сетями и системами (network and system management/NSM) информационной инфраструктуры». Стандарт определяет абстрактные объекты данных NSM для эксплуатационной среды энергосистем с учетом того, какая информация необходима для максимально надежного управления информационной инфраструктурой, с помощью которой осуществляется управление энергосистемой. Разработано соответствие информационным базам управления (MIB) стандарта SNMP (Simple Network Management Protocol), предоставленное в виде компонентов программного кода.
- «МЭК 62351-8. Контроль над доступом согласно функциям для системы управления энергосистемой» (Role-Based Access Control/RBAC). Назначение стандарта:
  - ввести концепцию авторизации «субъект-функции-права» (аналог «пользователь-функции-полномочия» согласно Национальному институту стандартизации США и Международному комитету по стандартам информационных технологий (ANSI INCITS) 359-2004;
  - распространить управление доступом согласно функциям (role-based access control/RBAC) на всю иерархию управления энергосистемой;
  - обеспечить эксплуатационную совместимость в условиях разных производителей энергетического оборудования;

- стандарт МЭК 61850-90-19 развивает требования к RBAC, приведенные в МЭК 61850.
- «МЭК 62351-9. Управление ключами кибербезопасности». Стандарт предписывает порядок генерации, распределения, отзыва и обращения с цифровыми сертификатами и ключами шифрования, предназначенными для защиты данных и обмена ими. В частности, устанавливается порядок обращения с несимметричными ключами (например, закрытыми ключами и сертификатами X.509) и симметричными ключами (например, ключами сеансов).
- «МЭК Технический отчет 62351-10. Архитектура безопасности». Документ представляет собой технический отчет, в котором даны указания по архитектуре безопасности энергосистем, основанные на основных мерах и средствах обеспечения безопасности, т.е. связанных с безопасностью элементов и функциях, и их взаимодействии.
- «МЭК 62351-11. Безопасность для документов XML». Определяет требования к безопасности при обмене XML-документами, которые используются для МЭК 61970 и некоторых других видов обмена информацией по МЭК 61850.
- «МЭК 62351-12. Отказоустойчивость энергосистем с системами РИЭ». Включает рекомендации по отказоустойчивости применительно к техническим и эксплуатационным стратегиям, а также техническим средствам кибербезопасности, применяемым в системах распределенных источников энергии (РИЭ). Технический отчет охватывает требования к отказоустойчивости, относящиеся к множеству различных заинтересованных сторон в таких распределенных киберфизических устройствах производства и накопления энергии. Его целью является обеспечение безопасности, надежности, качества электроэнергии и других аспектов эксплуатации энергосистем, более конкретно, содержащих в большом количестве системы РИЭ.
- «МЭК 62351-13. Какие проблемы безопасности должны быть учтены в стандартах и технических спецификациях». Данный документ призван помочь разработчикам стандартов решать вопросы кибербезопасности на уровне, соответствующем разрабатываемому стандарту. Дан перечень проблем безопасности, которые рекомендуется охватить в стандартах и технических спецификациях для использования в электроэнергетике.
- «МЭК 62351-14. Регистрация событий кибербезопасности». В данной части серии МЭК 62351 подробно описаны технические аспекты использования журналов безопасности: передача информации, наполнение и семантика.

#### **5.1.1 А.6.4. МЭК 62351 Технические требования к проверке на соответствие стандартам**

Технические требования (ТТ) к проверке на соответствие стандартам кибербезопасности МЭК 62351 находятся на этапах планирования и разработки. К ним относятся следующие:

- Часть 100-1. Проверка соответствия требованиям Части 5. В разработке (в качестве технических требований [ТТ]).
- Часть 100-3. Проверка соответствия требованиям Части 3. В разработке (в качестве ТТ).
- Часть 100-4. MMS (случаи применения общего базового теста (common test cases)); предложение по новому разделу работ (NWIP) для ТТ.
- Часть 100-6-1. 61850-8-1/9-2. Часть 100-6-2. ICCP. Часть 100-6-3. 61850-8-2. Проверка соответствия требованиям МЭК 61850: NWIP для ТТ (только 100-6-1).

- Часть 100-7. Проверка соответствия требованиям в управлении сетью. Начните с описания в 90-3, в котором говорится о том, что следует (и что не следует) включать в проверку соответствия требованиям.
- Часть 100-8-1. RBAC; Часть 100-8-2. RBAC для 61850 в 90-19 (по включении в международные стандарты или в технические требования — возможно, также 62351-8-1 или 61850-xx).
- Часть 100-9. Проверка соответствия требованиям по управлению ключами. См. в PICS (Protocol Implementation Conformance Statement) о сертификатах подлинности, отзыве и управлении сертификатами, а также о расширениях GDOI (Group Domain of Interpretation).
- Часть 100-14. Проверка соответствия требованиям по регистрации событий.

## Литература

---

- [1] ENEL. “Enel Cyber Security Risk Management,” Presentation by Yuri Rassega, slide 38, October 2018, personal communication.
- [2] IEC (International Electrotechnical Commission). “WG15 Public Site.” IECTC57. IEC. Last modified 2016. <http://iectc57.ucaiug.org/wg15public/default.aspx>
- [3] IEC. “Search results for ‘62443.’” Webstore. IEC. Accessed February 13, 2020. <https://webstore.iec.ch/searchform&q=62443>
- [4] IEC. “IEC 62351:2020 SER Series.” Webstore. IEC. Published January 10, 2020. <https://webstore.iec.ch/publication/6912>
- [5] International Society of Automation (ISA). ISA99, Industrial Automation and Control Systems Security, <https://www.isa.org/isa99/>
- [6] ISO (International Organization for Standardization). Information Technology—Security Techniques—Code of Practice for Information Security Controls. ISO/IEC 27002. Paris: ISO, 2013. <https://www.iso.org/standard/54533.html>
- [7] ISO. Information technology — Security techniques — Information security risk management. ISO/IEC 27005:2018 <https://www.iso.org/standard/75281.html>
- [8] ISO. Information Technology—Security Techniques—Information Security Controls for the Energy Utility Industry. ISO/IEC 27019. Paris: ISO, 2017. <https://www.iso.org/standard/68091.html>
- [9] ISO. Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary. ISO/IEC 27000. Paris: ISO, 2018. <https://www.iso.org/standard/73906.html>
- [10] Lewis, James. Economic Impact of Cybercrime: No Slowing Down. Santa Clara, CA: McAfee and the Center for Strategic and International Studies, 2018. [https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1ldhuHd&utm\\_source=Press&utm\\_campaign=bb9303ae70-EMAIL\\_CAMPAIGN\\_2018\\_02\\_21&utm\\_medium=email&utm\\_term=0\\_7623d157be-bb9303ae70-1940938](https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1ldhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-1940938)
- [11] Morgan, Steve. “Cyber Crime Costs Projected to Reach \$2 Trillion by 2019.” Forbes. Last modified January 17, 2016. <https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/> - 5bd5bcc43a91
- [12] NARUC (National Association of Regulatory Utility Commissioners). Cybersecurity Evaluative Framework for Black Sea Regulators. NARUC, 2017. <https://pubs.naruc.org/pub.cfm?id=E20048B4-155D-0A36-3117-F2F0A7A692F4>
- [13] NERC (North American Electric Reliability Corporation). CIP-002-5.1a—Cyber Security—BES Cyber System Categorization. NERC, 2013. <https://www.nerc.com/pa/Stand/ReliabilityStandards/CIP-002-5.1a.pdf>.
- [14] NERC. “CIP Standards.” Standards. NERC. Accessed February 13, 2020. <https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>
- [15] NIST (National Institute of Standards and Technology). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. NIST, 2018. <https://doi.org/10.6028/NIST.CSWP.04162018>.

- [16] NIST. "Cybersecurity Framework." NIST. Accessed February 13, 2020. <https://www.nist.gov/cyberframework>.
- [17] NISTIR 7628 Revision1: *Guidelines for Smart Grid Cybersecurity*. NIST, 2014. <https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final>
- [18] OWASP Foundation. "Security by Design Principles." OWASP Foundation Wiki. OWASP Foundation. Last modified August 3, 2016, 12:35. [https://wiki.owasp.org/index.php/Security\\_by\\_Design\\_Principles](https://wiki.owasp.org/index.php/Security_by_Design_Principles)
- [19] Ragazzi, Elena, Alberto Stefanini, Daniele Benintendi, Ugo Finardi, and Dennis K. Holstein. *Evaluating the Prudence of Cybersecurity Investments: Guidelines for Energy Regulators*. NARUC, 2020.

*По всем вопросам, относящимся к настоящему документу,  
просим обращаться к Эрин Хаммель ([ehammel@naruc.org](mailto:ehammel@naruc.org)).*

**National Association of Regulatory Utility Commissioners (NARUC)**  
1101 Vermont Ave NW, Suite 200  
Washington, DC 20005 USA  
Tel: +1-202-898-2210  
[www.naruc.org](http://www.naruc.org)