Организация Объединенных Наций ECE/CTCS/WP.6/2018/9

Экономический и Социальный Совет

Distr.: General
10 September 2018
Russian
Original: English

Европейская экономическая комиссия

Руководящий комитет по потенциалу и стандартам торговли

Рабочая группа по политике в области стандартизации и сотрудничества по вопросам нормативного регулирования

Двадцать восьмая сессия
Женева, 14–16 ноября 2018 года
Пункт 9 b) предварительной повестки дня
Международное сотрудничество в области нормативного регулирования:
Секторальные проекты

Проект предложения по общей системе регулирования в области кибербезопасности

Документ представлен секретариатом

Резюме

В настоящем документе содержится проект предложения по общей системе регулирования в области кибербезопасности, который представляется для обсуждения Рабочей группой.

Целью этого первого обсуждения является выяснение мнения делегатов о направленности предлагаемой общей системы регулирования. Если их мнение будет положительным, окончательное предложение будет представлено на ежегодной сессии Рабочей группы 6 в 2019 году.

Предлагаемое решение:

Рабочая группа положительно оценивает в целом подход общей системы регулирования, изложенный в настоящем проекте предложения.

Она поручает доработать данное предложение; а его доработку поручить Группе экспертов по системе регулирования и секретариату; более зрелый проект будет представлен на ежегодной сессии Рабочей группы 6 в 2019 году. Она также поручает секретариату продолжать докладывать о ходе осуществления этой инициативы.

GE.18-14944 (R) 170918 180918
1814944

I. Введение

1. На своей двадцать седьмой сессии Рабочая группа одобрила предложение о новой секторальной инициативе по кибербезопасности (решение 21, ECE/CTCS/WP.6/2017/2).

2. В соответствии с этим решением было налажено партнерство с Рабочей группой 17 Совета по оценке соответствия Международной электротехнической комиссии (МЭК) и Системой оценки соответствия электротехнического оборудования и компонентов (МЭКСЭ), которые активно поддерживают этот проект.

3. Были проведены обсуждения, и проекты предложений по общей системе регулирования в области кибербезопасности были представлены на двух совещаниях Группы экспертов по управлению рисками в системах нормативного регулирования (в марте 2018 года и в июле 2018 года).

4. Настоящий документ содержит первый проект общей системы регулирования в этом секторе.

II. Цели общей системы регулирования

5. Цель Секторальной инициативы по кибербезопасности заключается в поощрении сближения национальных технических регламентов, действующих в настоящее время или которые еще предстоит разработать, в этом секторе в целях создания общей системы, основанной на риск-ориентированном подходе и другой передовой международной практике. Это позволит снизить барьеры для торговли компонентами, оборудованием, услугами квалифицированных специалистов и сервисами, будет поощрять конкуренцию, расширит выбор на рынке и будет содействовать сокращению расходов. Это также повысит уровень защиты данных при оказании банковских, медицинских и других основных связанных с данными услуг и уровень надежности, бесперебойности и безопасности критических компонентов инфраструктуры, например электроэнергоснабжения, и других основных служб, которые являются опорой любой национальной экономики. Таким образом, это будет способствовать обеспечению общего благополучия и процветания граждан страны.

6. Если говорить более конкретно, то общая система регулирования будет содействовать:

- гармонизации законодательства в общемировом масштабе;
- принятию законодательства, соразмерного рискам, которые оно призвано устранять;
- обеспечению взаимного признания процедур и результатов испытаний и оценки испытательными лабораториями;
- стремлению к согласованным и сопоставимым процедурам оценки и осуществлению мер по обеспечению кибербезопасности.

III. Справочная информация

7. В эпоху цифровых технологий кибербезопасность является одной из важнейших составляющих экономической конкурентоспособности и безопасности большинства стран мира.

8. Обеспечение высокого уровня устойчивости к угрозам кибербезопасности во всем мире имеет первостепенное значение для обеспечения оказания основных услуг и завоевания доверия потребителей в эпоху цифровых технологий, а также для дальнейшего построения более безопасного, более инновационного, конкурентоспособного, устойчивого и богатого мира.

9. Киберугрозы представляют собой явление мирового масштаба, которое пересекает национальные, региональные и международные границы. Поэтому обеспечение кибербезопасности требует комплексного подхода на всех уровнях.

10. Для того чтобы быть эффективными, меры по обеспечению кибербезопасности на уровне предприятий и на национальном и международном уровнях должны опираться на результаты процесса системного управления рисками, осуществляемого с участием всех соответствующих заинтересованных сторон.

11. Базовые принципы кибербезопасности хорошо задокументированы в многочисленных международных стандартах, но страдают отсутствием широкой известности, глубокого понимания или тщательного применения. В качестве примера можно привести стандарты серии МЭК 62443 и серии международных стандартов Международной организации по стандартизации (ИСО)/МЭК 27000.

12. Существует путаница между потребностями кибер-физических систем, так называемых систем эксплуатационной технологии, такими как критическая инфраструктура и интеллектуальные системы, обусловленными необходимостью поддержания функционирования этих систем в реальном мире, и потребностями чисто информационных систем, так называемых систем информационной технологии, обусловленными необходимостью обеспечения защиты данных и безопасности их потоков в виртуальном мире.

13. Очевидно, что киберзащита технической системы требует общесистемного подхода. Очевидно, что необходимость применения риск-ориентированного подхода обусловлена следующими причинами:

- в любой системе некоторые элементы являются более ценными и более уязвимыми, чем другие, и нуждаются в более мощной и более дорогостоящей защите, в то время как в случае других элементов можно обойтись менее строгими и более дешевыми мерами защиты. Этот анализ должен носить риск-ориентированный характер.
- Необходимо установить баланс между уровнем защиты и стоимостью защиты.

14. Очевидно, что в рамках системного подхода могут использоваться как сильные, так и слабые формы защиты, что означает, что сильные и слабые формы подтверждения выполнения требований защиты также являются уместными.

15. Из этого следует, что целостный подход к кибербезопасности должен носить нейтральный с точки зрения оценки соответствия характер и допускать различные формы оценки соответствия – оценку соответствия первой стороной, второй стороной и третьей стороной – в соответствии с различными уровнями риска, определенными для различных элементов системы, подлежащих защите.

16. Поскольку киберугрозы могут носить национальный, региональный или международный характер, наиболее целесообразной является выработка международной передовой практики. Международные стандарты ИСО и МЭК все шире используются странами на региональном и национальном уровнях, либо полностью, без каких-либо изменений, либо частично, с дополнительными требованиями, содержащимися в национальных стандартах.

17. Страны используют стандарты в своих регламентах различным образом, в том числе:

- путем придания стандартам обязательного характера через принятие законодательного акта;
- путем превращения соблюдения стандартов в средство доказательства соблюдения основных требований, предусмотренных законодательством; в соответствии с этим подходом оборудование, компетенции людей, услуги, практика и процессы, которые соответствуют положениям стандартов, «считаются соответствующими» требованиям, установленным в регламентах.

18. Если в результате анализа рисков определяется, что надлежащей является оценка соответствия третьей стороной, тогда рекомендуется использовать передовую

международную практику и прибегнуть к услугам глобальной сертификации, как, например, предлагаемые МЭКСЭ, когда таковые доступны и являются надлежащими.

IV. Сфера применения Общих целей регулирования

19. Общие цели регулирования (ОЦР), изложенные в настоящем документе, были сформулированы в соответствии с Рекомендацией L Рабочей группы по политике в области стандартизации и сотрудничества по вопросам нормативного регулирования (Рабочая группа 6) Европейской экономической комиссии Организации Объединенных Наций (ECE/TRADE/378 – Рекомендации ЕЭК по политике в области стандартизации).

20. Эти ОЦР носят двоякий характер. С одной стороны, они могут использоваться в качестве модели для составления законодательных актов в странах, которые в настоящее время не имеют регламентов в этом секторе. С другой стороны, они могут использоваться для гармонизации существующего национального регламента с международно согласованной передовой практикой.

21. Эти ОЦР составлены с учетом международных стандартов и процедур оценки соответствия, разработанных МЭК и ИСО, и передовой практики оценки соответствия таким стандартам в рамках МЭКСЭ.

22. ОЦР формируют систематическую методологию определения надлежащего уровня требований и оценки соответствия на основе рисков.

23. ОЦР описывают требования к технологии систем, включая компоненты, продукты и оборудование, а также к компетенциям и квалификации лиц и к процессам управления, включая проектирование компонентов, интеграцию и реализацию, функционирование, обслуживание и модернизацию систем и т. д. (ОЦР – часть 4 настоящего документа).

24. Кибербезопасность можно обеспечивать с помощью целого набора разнообразных законных средств. В настоящем документе описывается систематическая методология системного подхода к кибербезопасности. Она отличается от других методологий тем, что в дополнение к моделированию технической системы, анализу рисков и анализу пробелов в требованиях она также предусматривает анализ потребностей в оценке соответствия. Она также является и должна быть гибкой методологией, поскольку должна быть применима к множеству различных технических систем.

25. Кроме того, настоящий документ основывается на подходе «жизненного цикла», который требует надлежащей инспекции, обслуживания, ремонта и модернизации технической системы. Такой подход гарантирует эффективную и действенную кибербезопасность во времени, по мере того как сама система развивается и меняется сам характер угроз.

26. Национальная система регулирования может сама использовать эту модель в отношении некоторых важнейших секторов и видов применения или требовать, чтобы коммерческие структуры в тех же или других секторах и видах применения использовали данную модель для убедительной демонстрации соблюдения. Оценка соответствия третьей стороной должна требоваться только тогда, когда это целесообразно, с учетом результатов анализа рисков.

27. Конвергенция к общей методологии, опирающейся на согласованные международные стандарты и передовую международную практику оценки соответствия, обладает рядом преимуществ. В частности, в тех случаях, когда оценка соответствия третьей стороны используется для демонстрации соответствия компонентов и технологий, компетенций и квалификации лиц, это облегчает признание данного соответствия в международной торговле и передвижение квалифицированных специалистов.

28. С другой стороны, существование или использование различающихся требований и процедур в тех секторах, которые функционируют в качестве подлинно

глобальных и комплексных сфер приложения, может само по себе представлять собой повышенный риск.

29. По этим причинам в тех случаях, когда требуется оценка соответствия третьей стороной, международно признанная система сертификации, такая как МЭКСЭ, имеет жизненно важное значение, для того чтобы уменьшить излишние издержки, связанные с дублированием инспекции, оценки, проверки квалификации и испытаний.

30. Один последний и существенный элемент настоящего документа касается надзора за рынком. Надзор за рынком необходим для контроля за правильным применением ОЦР промышленностью и повышения доверия к эффективности ОЦР. Будут определены общие руководящие принципы, призванные помочь национальным органам, определяющим и осуществляющим меры и процедуры, включая изъятие не отвечающих требованиям компонентов систем и товаров с национального рынка.

V. Общие цели регулирования

1. ОЦР – Часть 1: Методология достижения надлежащей кибербезопасности – общий обзор

31. Настоящая общая система регулирования описывает всеобъемлющую и систематическую методологию системного подхода к кибербезопасности. Эта типовая методология предусматривает пять шагов, которые затем периодически повторяются. Эти пять шагов заключаются в следующем:

- анализ и ранжирование рисков:
- требования – анализ пробелов в стандартах (часть 4 настоящего документа);
- анализ оценки соответствия согласно рейтингу рисков (часть 5 настоящего документа);
- применение – демонстрация соответствия;
- ОПО – обзор, пересмотр, обновление.

2. ОЦР – Часть 2: Методология определения соответствующих требований

32. Анализ пробелов: типовая матричная модель (см. приложение A) используется для определения точек, в которых необходимы требования к системе. Анализ различных систем в разных ситуациях приведет к определению различных потребностей в требованиях. Требования будут опираться на международные стандарты, такие как стандарты МЭК и ИСО (приведенные в части 4 и перечисленные в добавлении к настоящему документу), или, в их отсутствие, на региональные стандарты, или, наконец, на национальные стандарты. В случаях отсутствия стандартов требования должны опираться на признанные рынком передовую практику и процедуры.

33. Рекомендация R «Управление рисками в системах нормативного регулирования» Рабочей группы 6 ЕЭК должна использоваться органами нормативного регулирования для обеспечения согласованности и соразмерности между существующими рисками для кибербезопасности и соответствующими нормативными требованиями.

3. ОЦР – Часть 3: Методология определения соответствующих требований оценки соответствия

34. Анализ пробелов: типовая матричная модель (см. приложение A) используется для определения точек, в которых необходимы требования к системе. Метод определения того, какие требования являются надлежащими, описан в части 2 настоящего документа. Уровень оценки соответствия, который должен применяться к требованиям, будет определяться на основе оценки рисков, которая обеспечит ранжирование рисков по каждой точке общей матричной модели. Анализ различных систем в разных ситуациях приведет к различным рейтингам требований. Точкам с

высокими значениями в рейтинге будет присвоен более высокий уровень оценки соответствия, так же, как и точкам с высокой уязвимостью, в то время как точкам с более низкими значениями в рейтинге и с меньшей уязвимостью могут быть присвоены более низкие уровни оценки соответствия.

4. ОЦР – Часть 4: Требования для признания рынком

A. Требования к компонентам, продуктам и оборудованию

35. Требования к компонентам, продуктам и оборудованию, используемым в качестве элементов системы, будет опираться на международные стандарты, такие как стандарты МЭК и ИСО (приведенные в части 4 и перечисленные в добавлении к настоящему документу), или, в их отсутствие, на региональные стандарты, или, наконец, на национальные стандарты.

B. Требования к личным компетенциям

36. Требования к личным компетенциям будут опираться на международные стандарты, такие как стандарты МЭК и ИСО (приведенные в части 4 и перечисленные в добавлении к настоящему документу), или, в их отсутствие, на региональные стандарты, или, наконец, на национальные стандарты. В случаях отсутствия стандартов требования должны опираться на признанные рынком личные компетенции.

C. Требования к процессам

37. Требования к процессам будут опираться на международные стандарты, такие как стандарты МЭК и ИСО (приведенные в части 4 и перечисленные в добавлении к настоящему документу), или, в их отсутствие, на региональные стандарты, или, наконец, на национальные стандарты.

5. ОЦР – Часть 5: Справочный перечень международных стандартов, обеспечивающих презумпцию соответствия настоящей модели регулирования

38. Стандарты, обеспечивающие презумпцию соответствия требованиям части 4, перечислены в добавлении, главах A, B и C. Данный перечень стандартов должен обновляться с необходимой периодичностью в зависимости от выхода в свет международных стандартов МЭК или ИСО/МЭК, имеющих отношение к целям данной модели регулирования.

39. При условии надлежащего обзора оперативными и руководящими органами ЕЭК группа стран, внедряющая эту модель регулирования, сформирует группу по признанию стандартов ЕЭК, которая будет сама заниматься вопросами признания международных стандартов МЭК или ИСО/МЭК в качестве обеспечивающих презумпцию соответствия настоящей модели регулирования. Члены этой группы будут стремиться получить доступ ко всей работе МЭК по стандартизации (проекты, совещания), с тем чтобы обеспечить учет пожеланий регулирующих органов на раннем этапе разработки стандартов. После признания группой соответствующий стандарт будет включен в перечень, содержащийся в добавлении к настоящей модели регулирования. При наличии предыдущего варианта стандарта предыдущий вариант будет изъят из перечня в течение трех лет.

6. ОЦР – Часть 6: Требования к оценке соответствия

A. Определение применимых процедур оценки соответствия

40. Соблюдение ОЦР удостоверяется надлежащим инструментом оценки соответствия требованиям, определенным для конкретного применения, как это предусмотрено процессом, изложенным в части 1 настоящего документа.

41. В тех случаях, когда требуется оценка соответствия третьей стороны, соблюдение настоящих ОЦР удостоверяется с помощью международной системы сертификации, такой как система МЭКСЭ для прямого допуска на рынок товаров, лиц,

услуг и организаций, имеющих сертификацию МЭКСЭ. В альтернативном случае, когда законодательство страны не позволяет использования сертификатов МЭКСЭ, национальная сертификация соблюдения должна опираться на методику испытаний, инспекций и оценок МЭКСЭ.

B. Признание органов по оценке соответствия

42. Аккредитация органов по оценке соответствия и испытательных лабораторий должна соответствовать применимым международным стандартам ИСО/МЭК (см. добавление, раздел D.1). Орган по аккредитации должен быть членом Международного сотрудничества по аккредитации лабораторий/Международного форума по аккредитации. По крайней мере, один член группы оценщиков должен обладать компетенциями в области соответствующих требований к кибербезопасности (см., например, список признанных оценщиков МЭКСЭ).

43. Сертификаты должны соответствовать требованиям типа соответствующей системы, описанным в применимом стандарте ИСО/МЭК (см. добавление, раздел D.2).

44. Использование системы оценки соответствия МЭКСЭ МЭК обеспечивает презумпцию соответствия требованиям части 6.

7. ОЦР – Часть 7: Руководящий комитет ЕЭК по кибербезопасности

45. При условии надлежащего обзора оперативными и руководящими органами ЕЭК в целях мониторинга соблюдения ОЦР в странах, которые в качестве основы для своего национального законодательства использовали модель регулирования ЕЭК, и обновления модели регулирования с учетом их опыта должен быть сформирован Руководящий комитет ЕЭК по кибербезопасности, которые будет действовать под эгидой Рабочей группы 6 ЕЭК.

46. Руководящий комитет по кибербезопасности согласует свой устав и другие правила и процедуры, регулирующие его повседневную деятельность (например, процедуры голосования).

47. Руководящий комитет по кибербезопасности уведомляет членов Группы по признанию стандартов ЕЭК.

48. Члены Руководящего комитета по кибербезопасности, имеющие право голоса, являются представителями тех стран, которые внедрили данную модель регулирования. Наблюдателями, которые также приглашаются для участия в работе совещаний, являются: представители Совета управляющих по стандартизации МЭК, Совета по оценке соответствия МЭК, Технического комитета 65 МЭК, Объединенного технического комитета 1/СК27 ИСО/МЭК, МЭКСЭ, Системы сертификации стандартов, касающихся оборудования для использования во взрывоопасных средах МЭК, Консультативной группы ЕЭК по надзору за рынком.

8. ОЦР – Часть 8: Надзор за рынком

49. При условии надлежащего обзора оперативными и руководящими органами ЕЭК в целях мониторинга надлежащего соблюдения требований настоящей модели регулирования на рынке должна быть сформирована и действовать сеть экспертов по надзору за рынком в области кибербезопасности (см. добавление, раздел F.1).

50. Планирование процессов надзора за рынком должно опираться, в частности, на Рекомендацию S «Применение прогнозных инструментов управления рисками для целевого надзора за рынком» Рабочей группы 6 ЕЭК.

51. Что касается случаев критического несоблюдения, то должна быть создана международная система оповещения для информирования всех государств – членов ЕЭК ООН о недавно выявленных рисках.

Добавление

Перечень признанных стандартов и руководящих принципов, ведущихся ЕЭК, МЭК и ИСО

A.1. Базовые концепции и методология

1. Подлежит дальнейшей разработке.

A.2. Требования к конструкции компонентов системы

2. Подлежит дальнейшей разработке.

A.3. Производство оборудования

3. Подлежит дальнейшей разработке.

B.1. Требования к компетенциям персонала

4. Подлежит дальнейшей разработке.

D.1. Стандарты оценки соответствия

5. ISO/IEC 17065, ISO/IEC 17021, ISO/IEC 17024, ISO/IEC 17025.

D.2. Основные принципы сертификации продуктов

6. ISO/IEC 17067.

F.1. Руководящие принципы надзора за рынком

7. Руководящие принципы надзора за рынком разрабатываются настоящей Секторальной инициативой в сотрудничестве с Консультативной группой по надзору за рынком.

Приложение A

Пояснение типовой матричной модели

1. Типовая матричная модель (ТММ) представляет собой инструмент, используемый для моделирования технической системы и последующей увязки полученной модели с объектами соответствия (или вещами, которые фактически могут быть оценены на предмет соответствия требованиям). ТММ, как правило, представляется в виде матрицы, в которой система моделируется вертикально по левой стороне, а объекты соответствия указываются сверху.

2. На графическом изображении ТММ горизонтальные линии проводятся от элементов модели системы под всеми объектами соответствия. Аналогичным образом вертикальные линии проводятся вниз от объектов соответствия. Точки пересечения вертикальных и горизонтальных осей иллюстрируют возможность оценки соответствия требованиям, когда требования имеются в наличии.

3. ТММ может использоваться для определения того, что является важным для заданной технической системы, рассматриваемой через конкретную призму. Это позволит определить наиболее важные элементы и подэлементы, которые должны быть видимы через эту призму и которые, таким образом, должны присутствовать в модели системы. Когда кибербезопасность рассматривается через эту призму, систему можно смоделировать с помощью таких элементов, как технология или компоненты, взаимосоединения, вмешательства, зоны безопасности, тестирование на проникновение и т. д.

4. Требования могут касаться многих вещей в зависимости от того, чего мы пытаемся достичь. Как правило, требования выступают в форме передовой практики, компетенций, спецификаций, стандартов, определенного минимального или максимального результата стандартизированных тестов и т. д. Для выполнения этих требований, возможно, будет необходимо также располагать определенным типом или уровнем оборудования, ноу-хау, набором навыков, компетенциями, опытом и т. д.

5. Акт проведения оценки для выяснения того, удовлетворяются ли требования, является актом оценки соответствия требованию. Официальным термином является «оценка соответствия». Фактически существуют три возможных объекта соответствия. Речь идет о продуктах, людях (компетенции) и процессах.

6. Эти три объекта соответствия являются тремя базовыми объектами. Предлагались многие другие объекты соответствия, такие как услуги, данные, установки, проекты, органы или организация и системы. Однако на деле каждый из них является лишь одним или сочетанием нескольких из этих трех базовых объектов. Например, услуги являются по сути процессами, осуществляемыми людьми (обладающими надлежащими компетенциями), возможно, с использованием надлежащих продуктов или оборудования. И не более того. Таким образом, услуги уже охватываются тремя базовыми объектами соответствия и не нуждаются в выделении в особую категорию.

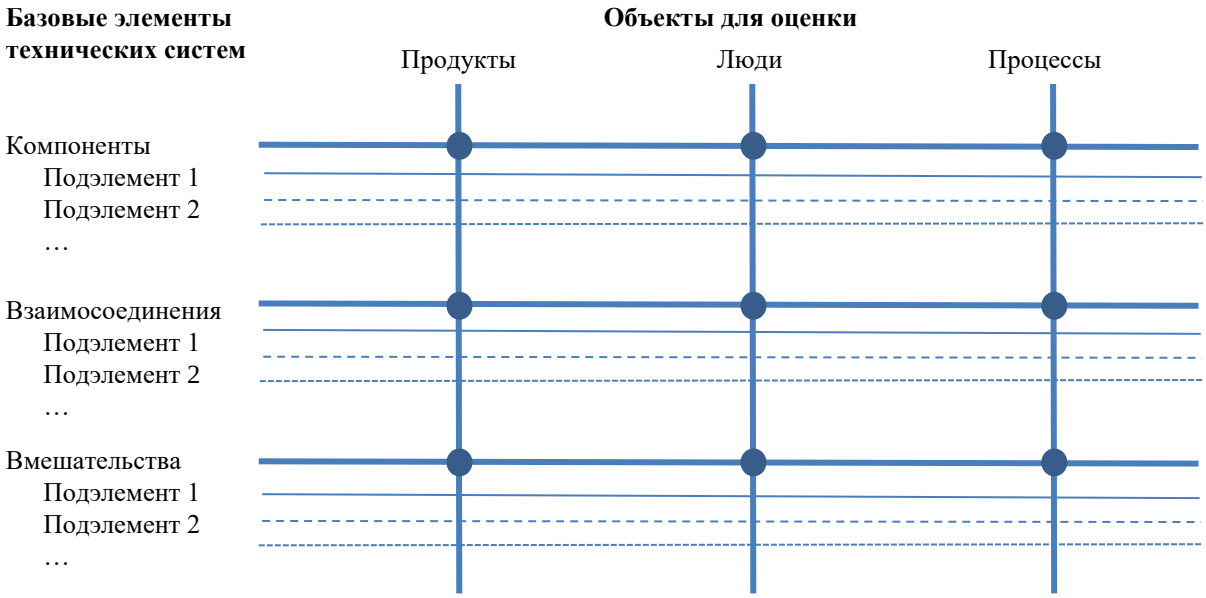
7. Вместе с тем, если какому-то сектору необходимо специфицировать более трех базовых объектов соответствия, тогда в конкретную ТММ следует включить дополнительный(е) объект(ы) соответствия.

8. Точки пересечения элементов модели системы и объектов соответствия находятся там, где могут применяться требования. Что представляют собой эти требования и имеются ли они в наличии, определит анализ пробелов.

9. Понимание системы и знание того, в чем заключается ее ценность и где находятся уязвимости, будет затем использоваться при оценке риска каждой из точек пересечения для определения того, какого рода оценка соответствия является необходимой применительно к требованиям в каждой точке. Высоко значимые или высоко уязвимые точки пересечения потребуют тщательной оценки соответствия, в то время как менее значимые или уязвимые точки пересечения потребуют менее строгой

оценки соответствия. Для обеспечения надлежащего использования должен быть доступен полный спектр вариантов оценки соответствия. Это означает оценку соответствия первой стороной, такой как заявление о соответствии изготовителя или поставщика; оценку соответствия второй стороной, такую как самооценка и внутренний аудит пользователем или владельцем системы; и оценку соответствия третьей стороны, например, тип испытания 1 (ISO/IEC 17067) или тип 5, полная сертификация соответствия, и т. д. Большинство регламентов должны быть нейтральными с точки зрения оценки соответствия и лишь специфицировать, что является надлежащим с учетом результатов анализа рисков.

10. Точки пересечения вертикальных и горизонтальных линий ТММ являются точками, в которых проводится оценка соответствия, а системным подходом является общая матрица требований и операций по оценке соответствия.



Типовая модель системного подхода к оценке соответствия (простейшая форма)

Что представляет собой техническая система?

11. Технические системы не являются природными системами, такими как биологические системы, как, например, система кровообращения, или экологическими системами, такими как погодная система, или небесными системами, такими как солнечная система, и т. д., а, скорее, созданными человеком системами.

12. Что общего между железнодорожными системами, облачными вычислениями, умной энергосистемой, автоматизированной системой управления технологическими процессами, атомной электростанцией, системой электроснабжения, нефтеперерабатывающим предприятием, газораспределительной системой, системой информации о здоровье населения, умными домами и т. д.?

13. Все они являются техническими системами.

14. Теперь, если считать, что техническая система представляет собой

- группу взаимодействующих, взаимосвязанных или взаимозависимых элементов, образующих служащее определенной задаче целое;
- и что эти элементы могут носить процедурный, физический и/или виртуальный характер;
- и что эти элементы могут быть компонентами, которые должны быть спроектированы и изготовлены или созданы;

- и что сама система будет спроектирована и построена (или системно интегрирована), и что элементы системы могут находиться в определенном физическом местонахождении или могут быть физически широко распределены;
- и что эти элементы нуждаются в периодическом пересмотре, обслуживании и/или обновлении/модернизации;
- и что некоторые из этих элементов передают и получают информации между собой;
- и что система определенным образом связана с миром за пределами самой системы либо физически, либо виртуально (например, через Интернет);
- и что вся система сама периодически или постоянно подвергается изменениям и усовершенствованиям благодаря вмешательствам, которые могут носить виртуальный, автоматизированный или человеческий характер;

тогда все технические системы являются весьма типическими.

15. Хотя технические системы являются весьма типическими, они также являются довольно сложными и запутанными. Поэтому в целях упрощения все технические системы можно рассматривать как состоящие из трех базовых элементов: компоненты, взаимосоединения и вмешательства.

16. Эти три элемента, как они перечислены, носят несколько хронологический характер в жизненном цикле системы, причем следуют один за другим. Например, сначала разрабатываются и создаются компоненты, затем системные интеграторы проектируют систему, выбирают компоненты и затем реализуют эту систему. Система затем управляется с помощью вмешательств. Каждый элемент следует за другим. Однако существует также много возвратов к началу цикла. Поскольку система стареет и развивается, необходимы новые и сменные компоненты, зачастую новые по своей конструкции и технологии, что, таким образом, означает возврат к этапу компонентов. Сама система может эволюционировать в результате появления новых и иных потребностей, требующих интеграции новых типов компонентов, концепций и технологий, что, таким образом, означает возврат к этапу взаимосоединений. И по мере развития и совершенствования практики эксплуатации во времени будут требоваться новые и иные типы вмешательств.

17. Компоненты: каждая техническая система имеет компоненты, которые являются физическими, но могут также быть виртуальными (такие как управляющие программы или данные и т. д.). Каждый компонент имеет свою цель и причину быть частью системы. Компоненты должны проектироваться с учетом их цели, а затем реализовываться (изготовляться, разрабатываться и т. д.). Компоненты иногда требуют ремонта, модернизации или замены. Иногда может проходить длительное время (интервал) между реализацией и интеграцией компонентов в систему (время хранения). Это время хранения необходимо контролировать для обеспечения работоспособности компонента и системы.

18. Взаимосоединения: речь идет о системной интеграции. То есть о том, как компоненты взаимодействуют, обмениваются информацией и работают вместе. Речь может идти о физических взаимосоединениях, таких как подвижные элементы производственной системы или поезда на рельсах, или линии электропередачи, или кабели, передающие сигналы управления. Речь может также идти о кабельных или беспроводных информационных потоках. Рельсовые пути, передающие провода и кабели – все они будут являться компонентами, но их функцией перемещения поездов, электроэнергии и сигналов является взаимосоединение.

19. Необходимо спроектировать интеграцию системы, и иногда взаимосоединения нуждаются в ремонте, модернизации или замене. В некоторых ситуациях взаимосоединения могут меняться динамично постоянно, как, например, в случае Интернета и умной электросети (при непрерывном появлении и исчезновении новых генерирующих мощностей и новых нагрузок в неконтролируемой среде собственной разработки).

20. Вмешательства: они могут быть человеческими, виртуальными или автоматическими. Вмешательства в основном связаны с функционированием системы на протяжении всего ее жизненного цикла и могут касаться передовой практики, процессов и процедур. Они также могут касаться услуг, предоставляемых своими силами или внешним источником, таких как услуги поставщика. Некоторые вмешательства могут быть автоматизированными, например автоматическое обновление антивирусного программного обеспечения/программного обеспечения защиты от взлома систем ИТ или автоматического квитирования установления связи и проверки виртуального сертификата входящих данных. Другие вмешательства являются повседневной, но важной практикой пользователей, как, например, регулярная смена паролей или сообщение и отмена утраченных ключей доступа или электронных удостоверений личности и т. д.

21. Эта концепция трех основных элементов служит типовым представлением системы весьма высокого уровня. Ниже в каждом из этих трех элементов всегда будут выделяться подэлементы, которые будут предоставлять более подробную информацию о системе. Многие подэлементы будут одинаковыми в разных системах, но их индивидуальное значение может существенно различаются в зависимости от системы. И некоторые системы будут иметь подэлементы, которые будут присущи только заданной системе. В зависимости от искомого уровня детализации может выделяться большое число подэлементов и даже подкатегории в рамках некоторых подэлементов.

Приложение B

Примеры типовой матричной модели, используемые в различных секторах применения

Промышленная автоматизация ГИМ в табличной форме

СИСТЕМА Действия	Кто	Общие составляющие	Объекты соответствия Продукты	Люди	Процессы
Компоненты					
Разработка компонентов системы	Производители компонентов Владельцы активов	62443-0-3 оценка пробелов 62443-1-1 концепции и модели терминологии 62443-1-2 мастер-глоссарий терминов и сокращений 62443-1-3 параметры соблюдения требований безопасности системы 62443-1-4. I пользовательские сценарии безопасности и жизненного цикла IACS ИСО/МЭК 15408 Общие критерии оценки безопасности информационных технологий ИСО/МЭК 27000 Обзор и словарь	МЭК 62443-4-2 Техническая безопасность Требования в отношении компонентов IACS		МЭК 62443-4-1 Разработка продукта Требования
Изготовление компонентов системы	Производители компонентов Владельцы активов		Конкретные технические стандарты на продукты с (функциональными и эксплуатационными) требованиями. (Конечная конструкционная защита устройство.)		
Взаимодействия					
Комплексирование систем с применением интегрирующих устройств	Проектировщики систем Владельцы активов				МЭК 62443-2-4 Требования в отношении IACS – поставщики решений
Осуществления/реализация системной интеграции	Сборщики систем Владельцы активов				??
Вмешательства					
Система управления безопасностью 1. Требования	Владелец активов Поставщик услуг				МЭК 62443-2-1 Система управления безопасностью IACS – Требования
2. Реализация					МЭК 62443-2-2 Система управления безопасностью IACS – Осуществление
3. Оценка рисков IACS					МЭК 62443-3-3 Требования к безопасности системы и уровни обеспечения безопасности
Архитектура безопасности	Владелец активов Поставщик услуг				МЭК 62443-3-2 Уровни обеспечения безопасности для зон и проверок
Операции по обеспечению безопасности	Владелец активов Поставщик услуг				?? ??
Решения по обеспечению безопасности	Владелец активов Поставщик услуг				МЭК 62443-3-1 Технологии обеспечения безопасности IACS
1. Реализация управления исправлениями	Владелец активов Поставщик услуг				МЭК 62443-2-3 Управление исправлениями в среде IACS