Организация Объединенных Наций ECE/CTCS/WP.6/2019/9

Экономический и Социальный Совет

Distr.: General
11 September 2019
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 девятая сессия
Женева, 20–22 ноября 2019 года
Пункт 10 b) предварительной повестки дня
Международное сотрудничество в области нормативного регулирования: Секторальные проекты

Доклад о ходе осуществления Секторальной инициативы в области кибербезопасности

Документ представлен секретариатом

Резюме

Настоящий документ содержит проект предложения по общей системе регулирования в области кибербезопасности, который представляется Рабочей группе для принятия решения.

Предлагаемое решение:

«Рабочая группа принимает предложение по общей системе регулирования, содержащееся в настоящем проекте предложения».

Она поручает опубликовать это предложение. Она также поручает секретариату продолжать докладывать о ходе осуществления этой Инициативы.

GE.19-15565 (R) 230919 260919
1915565

Просьба отправить на вторичную переработку

I. Введение

1. На своей двадцать седьмой ежегодной 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 совещаниях Группы экспертов по управлению рисками в системах нормативного регулирования в 2018 и 2019 годах.

4. В настоящем документе описывается систематическая методология системного подхода к кибербезопасности в рамках общей системы регулирования. Она отличается от других методологий тем, что в дополнение к моделированию технической системы, проведению анализа по выявлению рисков, оценке рисков и анализу пробелов в требованиях она также предусматривает анализ потребностей в области оценки соответствия и надзора за рынком. Она представляет собой гибкую методологию, применимую ко многим различным техническим системам в различных секторах экономики.

5. 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.

6. В настоящем документе излагаются основные элементы процессов регулирования, которые могут использоваться властями и директивными органами, особенно в тех секторах, где в настоящее время не существует никаких регламентов кибербезопасности. В нем определены стандарты, которые могут быть полезны для использования в качестве ссылок в нормативных документах. Это живой документ, который будет обновляться по мере изменения киберпространства.

II. Обоснование необходимости международного сотрудничества в области регулирования кибербезопасности

7. В эпоху цифровых технологий кибербезопасность является одной из важнейших составляющих экономической конкурентоспособности и стабильности для всех видов организаций.

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 выходит за рамки национальных, региональных и международных границ. Поэтому обеспечение кибербезопасности требует комплексного подхода на всех уровнях.

10. Поскольку киберугрозы могут носить национальный, региональный или международный характер, наиболее целесообразной представляется выработка международной передовой практики. Международные стандарты Международной организации по стандартизации (ИСО) и МЭК все чаще принимаются на вооружение странами в рамках их обязательств по выполнению целей Всемирной торговой организации в области технических барьеров в торговле (ТБТ ВТО) на региональном и национальном уровнях.

11. В большинстве случаев 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. Однако, возможно, что в некоторых случаях использование множественных и различных требований представляет собой способ снижения рисков и повышения безопасности (т. е. предотвращения распространения уязвимостей).

12. 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.

III. Цель ОЦР

13. Общие цели регулирования (ОЦР), изложенные в настоящем документе, были сформулированы в соответствии с Рекомендацией L и Рекомендацией R 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).

14. 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.

15. В документе описывается общая система регулирования, которую страны могут принять для достижения общих целей регулирования кибербезопасности. Этот документ можно использовать в качестве основы для:

- установления целей нормативного регулирования в области кибербезопасности;
- выявления и оценки рисков кибербезопасности;
- определения международных стандартов, которые могут использоваться в качестве основы для регламентов кибербезопасности;
- установления процедур оценки соответствия в области кибербезопасности; и
- осуществления процесса надзора за рынком.

16. Страны, желающие создать специальные оперативные транснациональные механизмы, могут использовать ОЦР в соответствии с процедурой, описанной в Рекомендации L, приложение C.

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

18. Применение общей системы 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; и

- стремлению к согласованным и сопоставимым процедурам оценки и осуществлению мер по обеспечению кибербезопасности.

19. Кроме того, применение этого документа будет способствовать сближению национальных технических регламентов, действующих в настоящее время или которые еще предстоит разработать, 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.

IV. Общие цели регулирования в области кибербезопасности

20. Система регулирования в области кибербезопасности нацелена на обеспечение общего благосостояния и процветания граждан страны посредством обеспечения:

a) защиты данных;

b) надежности;

c) стабильности функционирования;

d) технической безопасности; и

e) общей безопасности

важнейших элементов инфраструктуры, таких как системы электроснабжения, снабжения питьевой водой, очистки сточных вод, снабжения газом и топливом, банковского обслуживания, здравоохранения, транспорта и других основных услуг, как они определены или ограничены разделом V (Сфера охвата).

21. Регулирующие органы конкретных секторов могут использовать эти ОЦР для гармонизации регламентов на международном уровне в качестве основы для отраслевого законодательства в области кибербезопасности и минимизации любых особых требований, обоснованных специфическими национальными рисками.

22. Установление целей регулирования должно основываться на принципе, согласно которому нулевой риск не может быть достижимой целью регулирования. Определение приемлемого уровня риска и допустимого риска должно осуществляться согласно Рекомендации R.

V. Сфера применения Общих целей регулирования

23. Эти ОЦР заменяются существующими специальными режимами регулирования там, где они существуют или находятся в процессе разработки.

24. Продукты и процессы, охватываемые ОЦР, включают в себя:

- физические приложения, так называемые системы операционной технологии (ОТ), такие как критически важная инфраструктура и интеллектуальные системы, и процессы, обеспечивающие функционирование этих систем (как, например, охватываемые международными стандартами серии МЭК 62443); и
- информационные системы, так называемые системы информационной технологии (ИТ), с необходимостью защиты данных и их безопасной передачи (как, например, охватываемые международными стандартами серии ИСО/МЭК 27000).

25. ОЦР охватывают требования к технологии системы, включая:

a) данные, связь, компоненты, оборудование, прикладные программы и предоставление услуг;

b) компетентность и квалификацию лиц; и

c) управленческие процессы, включая:

i) проектирование компонентов; и

ii) интеграцию и реализацию, эксплуатацию, техническое обслуживание, модернизацию и т. д. систем.

26. Для идентификации всех компонентов технической системы следует использовать типовую матричную модель (приложение A).

VI. Выявление рисков кибербезопасности

27. Риски кибербезопасности – это инциденты или события, которые могут повлиять на выполнение целей кибербезопасности, определенных ранее в документе. Ясность при определении общих и специфических рисков помогает оценить риск и определить средства контроля для управления риском до приемлемого уровня.

28. Для выявления рисков кибербезопасности могут применяться следующие международные стандарты и другие системы кибербезопасности, включая:

- стандарты серии ИСО/МЭК 27000;
- стандарты серии МЭК 62443;
- стандарты серии ИСО 31000;
- Рамочная система v1.1 Национального института стандартов и технологий (НИСТ);
- Банк международных расчетов (БМР) – Базель 2/3, Операционный риск;
- Цели в области контроля за информационными и смежными технологиями – COBIT 5; и
- Открытый проект по безопасности веб-приложений – OWASP-Top10.

29. Очевидно, что киберзащита требует целостного, общесистемного подхода.

30. Типовая матричная модель (см. приложение A) может быть использована для определения точек, в которых следует проводить выявление рисков для кибербезопасности и проводить их оценку.

31. При выявлении рисков кибербезопасности следует учитывать следующие факторы (см. «модель нарушителя», приложение B, в которой описаны мотивы и потенциальные сценарии рисков кибербезопасности, которые могут возникнуть в рамках всей технической системы), а также следует учитывать приводимый ниже иллюстративный перечень:

- хакер-активист;
- киберпреступник;
- инсайдеры;
- кибершпионаж;
- кибертеррорист;
- кибервойна; и
- т. д.

Полный перечень факторов и их описание см. в приложении B (в настоящее время в стадии разработки).

32. Примеры рисков кибербезопасности и связанных с ними уязвимостей включают в себя:

i. потерю данных или несанкционированный доступ к ним, несоблюдение нормативных требований (например, Общего регламента защиты данных (ОРЗД) и других нормативных актов, касающихся данных);

ii. прекращение доступа или несанкционированный доступ к системам и приложениям;

iii. отказ или отсутствие поддержки унаследованных систем;

iv. потеря обслуживания/поддержки со стороны сторонних поставщиков;

v. перегрузка систем (сбой системы) в результате внешней атаки/ чрезмерного использования;

vi. случайное заражение вирусом;

vii. недостаточная компетентность для обслуживания унаследованных систем и разработки мер реагирования на текущие/будущие потребности; и

viii. недостаточные навыки руководства для понимания и разработки стратегии использования кибервозможностей (например, «облачных» технологий).

33. Регулирующие органы должны следить за эволюцией угроз кибербезопасности, поскольку прошлая история более не является всеобъемлющим предсказателем будущего.

VII. Оценка рисков кибербезопасности

34. По мере возможности следует проводить количественную оценку рисков кибербезопасности, с тем чтобы их можно было расставить по степени приоритетности и оценить с учетом уровня допустимого риска, как это описано в Рекомендации R.

35. Признается, что риск кибербезопасности невозможно устранить, и необходимо определить допустимый уровень риска.

VIII. Определение нормативных требований для устранения рисков кибербезопасности и соответствующие международные стандарты, предусматривающие презумпцию соответствия

36. При определении нормативных требований 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.

37. Основные принципы кибербезопасности хорошо документированы и постоянно обновляются в соответствии с современными международными стандартами, примерами которых являются стандарты серии МЭК 62443 и серия международных стандартов ИСО/МЭК 27000.

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

- путем включения ссылок на стандарты в законодательные акты; и
- 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.

39. Идентификация рисков и анализ различных систем в разных ситуациях приведут к определению различных потребностей в требованиях. Нормативные требования будут опираться на международные стандарты, такие как стандарты МЭК

и ИСО или, в их отсутствие, на региональные стандарты, или, наконец, на национальные стандарты. В отсутствие стандартов требования могут опираться на признанные рынком передовую практику и процедуры.

40. Примеры стандартов, которые могут быть использованы при установлении презумпции соответствия соответствующим нормативным требованиям, перечислены в настоящем документе. Перечень стандартов должен обновляться по мере необходимости в зависимости от результатов публикации международных стандартов МЭК или ИСО/МЭК, имеющих отношение к целям данной модели регулирования.

41. В отсутствие международных стандартов при разработке нормативных требований следует применять региональные стандарты или национальные стандарты.

Требования к компонентам, продуктам и оборудованию

42. Требования к компонентам, продуктам и оборудованию, используемым в качестве элементов системы, могут основываться на международных стандартах, таких как стандарты МЭК и ИСО, таких как:

i. МЭК 62443-1-1 изд. 2: Терминология, концепции и модели (в стадии разработки);

ii. МЭК 62443-2-1 изд. 2: Составление программы обеспечения защищенности системы управления и промышленной автоматики (в стадии разработки);

iii. МЭК 62443-2-3: Управление исправлениями в среде IACS (принят);

iv. МЭК 62443-2-4: Требования к программе безопасности для поставщиков услуг IACS (принят);

v. МЭК 62443-2-2: Уровни защиты IACS (в стадии разработки);

vi. МЭК 62443-3-2: Оценка рисков для безопасности и разработка системы (в стадии разработки);

vii. IECEE OD-2061: Программа промышленной кибербезопасности;

viii. МЭК 62443-4-1: Требования к безопасности жизненного цикла при разработке продукта (принят);

ix. МЭК 62443-3-3-3: Требования к безопасности системы и уровни безопасности (принят); и

x. МЭК 62443-4-2: Требования к технической безопасности компонентов IACS (в стадии разработки).

43. Всеобъемлющий перечень стандартов будет размещен на веб-сайте Инициативы.

44. Производство оборудования будет опираться на всеобъемлющий перечень стандартов, который будет размещен на веб-сайте Инициативы.

Требования к личностным компетенциям

45. Требования к личностным компетенциям будет основываться на имеющихся международных стандартах ИСО и МЭК в этой области, таких как:

- ИСО/МЭК 27021 изд. 1: Информационные технологии – Методы и средства обеспечения безопасности – Требования к компетенции специалистов систем менеджмента информационной безопасности.

Требования к процессам

46. Требования к процессам будут основываться на применимых международных стандартах, таких как стандарты МЭК и ИСО, например:

i. МЭК 62443-4-1: Требования к безопасности жизненного цикла при разработке продукта (принят);

ii. МЭК 62443-2-1: Составление программы безопасности IACS;

iii. МЭК 62443-2-2: Уровни защиты IACS (в стадии разработки);

iv. МЭК 62443-2-4: Требования к программе безопасности для поставщиков услуг IACS (принят); и

v. МЭК 62443-3-2: Оценка рисков для безопасности и разработка системы (в стадии разработки).

IX. Определение уровня оценки соответствия

47. 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 стороной используется для демонстрации соответствия компонентов и технологий, компетенций и квалификации лиц, это облегчает признание данного соответствия в международной торговле и передвижение квалифицированных специалистов.

48. Эти ОЦР составлены с учетом международных стандартов и процедур оценки соответствия, таких как разработанные МЭК и ИСО, и передовой практики оценки соответствия таким стандартам в рамках МЭКСЭ и СОКЭК.

49. Страны должны использовать систематическую методологию для определения надлежащего уровня оценки соответствия на основе рисков. 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.

50. Уровень оценки соответствия, который должен применяться к требованиям, будет определяться на основе оценки рисков, которая обеспечит ранжирование рисков по каждой точке общей матричной модели (приложение A). Анализ различных систем (см. примеры в приложении C) в различных ситуациях приведет к различным рейтингам рисков. 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.

51. 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.

52. Если в результате анализа рисков определяется, что надлежащей является оценка соответствия третьей стороной, тогда полезно использовать передовую международную практику и прибегнуть к услугам глобальной сертификации, как, например, предлагаемые МЭКСЭ и СОКЭК, когда таковые имеются и являются надлежащими.

Определение применимых процедур оценки соответствия

53. Соответствие продуктов/процессов в рамках регулирования в области кибербезопасносности будет удостоверяться надлежащим инструментом оценки соответствия требованиям, определенным для конкретного применения, как это предусмотрено процессом, изложенным в части VIII настоящего документа.

54. В тех случаях, когда требуется оценка соответствия третьей стороны, соблюдение настоящих ОЦР удостоверяется с помощью международной системы сертификации, такой как система МЭКСЭ и СОКЭК для прямого допуска на рынок продуктов, лиц, услуг и организаций, имеющих сертификацию МЭКСЭ или сертификацию СОКЭК. В альтернативном случае, когда законодательство страны не

позволяет использование сертификатов МЭКСЭ или сертификатов СОКЭК, регуляторам рекомендуется стремиться к национальной сертификации соблюдения, опирающейся на методику испытаний, инспекций и оценок МЭКСЭ или СОКЭК.

Признание органов по оценке соответствия

55. Квалификационная оценка органов по оценке соответствия и испытательных лабораторий должна соответствовать применимым международным стандартам ИСО/МЭК (см. ниже). Органы по аккредитации должны быть членами 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 и оценщиков СОКЭК).

56. Сертификаты должны соответствовать требованиям типа соответствующей системы, описанным в применимом стандарте ИСО/МЭК (см. ниже).

57. Использование систем оценки соответствия МЭК, таких как МЭКСЭ и СОКЭК, обеспечивает презумпцию соответствия требованиям части VIII. Другие системы могут быть сочтены в качестве справочных в одном из будущих изданий этих ОЦР, если они станут доступны и будут доведены до сведения Инициативы.

58. По этим причинам в тех случаях, когда требуется оценка соответствия третьей стороной, международно признанная система сертификации, такая как МЭКСЭ и СОКЭК, способна уменьшить излишние издержки, связанные с дублированием инспекции, оценки, проверки квалификации и испытаний.

Стандарты оценки соответствия

59. ИСО/МЭК 17065, ИСО/МЭК 17021, ИСО/МЭК 17024, ИСО/МЭК 17025, ИСО/МЭК 17040.

Основные принципы сертификации продукции

60. ИСО/МЭК 17067.

X. Установление процедур надзора за рынком

61. 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 продуктов с национального рынка.

62. 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.

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

64. 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.

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

65. При условии надлежащего обзора оперативными и руководящими органами ЕЭК в целях мониторинга соблюдения ОЦР в странах, которые в качестве основы для своего национального законодательства используют 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.

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

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

68. 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, соответствующих технических комитетов МЭК и ИСО, Систем по оценке соответствия МЭК и Консультативной группы ЕЭК по надзору за рынком. К участию в работе Руководящего комитета приглашаются консультанты, участвовавшие в ранее существовавших мероприятиях по регулированию кибербезопасности в качестве консультантов (например, руководство и секретариат РГ.29).

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.

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, на основе которых должна проводиться оценка соответствия, обычно выступают в форме передовой практики, компетенций, спецификаций, стандартов или же 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, системы и внешние факторы. 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.

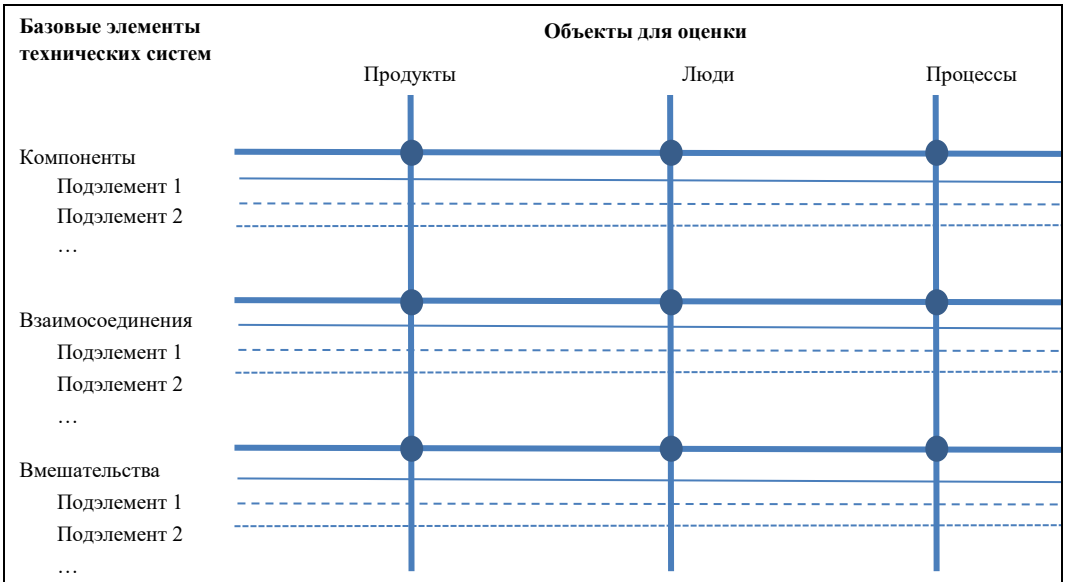
7. Вместе с тем, если какому-то сектору необходимо специфицировать более трех базовых объектов соответствия, тогда в конкретную ТММ следует включить дополнительный(е) объект(ы) соответствия.

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. Оценка риска должна проводиться в соответствии с описанием в части VII. Более значимые или более 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 стороной, например, тип испытания 1 (ИСО/МЭК 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 являются не 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. Общим между железнодорожными системами, облачными вычислениями, умной энергосистемой, автоматизированной системой управления технологическими процессами, атомной электростанцией, системой электроснабжения, нефтеперерабатывающим предприятием, газораспределительной системой, банковской и финансовой системой, системой информации о здоровье населения, умными домами и т. д. служит то, что все они являются техническими системами.

13. Считается, 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 информацию 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;

следовательно, все технические системы являются весьма типическими.

14. 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.

15. Эти три элемента, как они перечислены, носят несколько хронологический характер в жизненном цикле технической системы. 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, но может также быть 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, регламентов или стандартов во времени будут требоваться новые и иные типы вмешательств.

16. Компоненты: каждая техническая система имеет компоненты, которые являются физическими, но могут также быть и 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, совершенствоваться 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.

17. Взаимосоединения: речь идет о системной интеграции. То есть о том, как компоненты взаимодействуют, обмениваются информацией и работают вместе. Это может осуществляться через физические взаимосоединения, 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.

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

19. 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 носят повседневный характер, но могут включать в себя некоторую наилучшую практику пользователей, такую как, например, регулярная смена паролей или сообщение и отмена утраченных ключей доступа или электронных удостоверений личности и т. д.

20. 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 различаться в зависимости от системы. И некоторые системы будут иметь подэлементы, которые будут присущи только этой конкретной системе. В зависимости от искомого уровня детализации может выделяться большое число подэлементов и даже подкатегории в рамках некоторых подэлементов.

Приложение B

Модель противника

См. веб-сайт Инициативы (http://www.unece.org/tradewelcome/tradewp6/groups/cybersecurity.html, в настоящее время находится в стадии разработки).

Приложение C

Примеры типовой матричной модели, используемые в различных секторах применения

См. веб-сайт Инициативы (http://www.unece.org/tradewelcome/tradewp6/groups/cybersecurity.html, в настоящее время находится в стадии разработки).