Организация Объединенных Наций ECE/CTCS/WP.6/2024/11

Экономический и Социальный Совет

Distr.: General
3 June 2024
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 (РГ.6)

Тридцать четвертая сессия
Женева, 26 (вторая половина дня) — 28 августа 2024 года
Пункт 6 предварительной повестки дня
Специальная группа специалистов по методам стандартизации и нормативного регулирования

Всеобъемлющие единые рамки регулирования для обеспечения соответствия нормативным требованиям продуктов и/или услуг со встроенными технологиями искусственного интеллекта или другими цифровыми технологиями

Документ представлен Председателем РГ.6*

Резюме

Обеспечение гармонизации и совместимости на международном уровне нормативных требований к продуктам со встроенными технологиями искусственного интеллекта (ИИ) или другими цифровыми технологиями является сложной задачей для регулирующих органов, но необходимо для достижения целей регулирования, а также избежания ненужных технических барьеров в торговле и многократных испытаний на соответствие.

Мандат

Программа работы Рабочей группы по политике в области стандартизации и сотрудничества по вопросам нормативного регулирования (РГ.6) на 2024 год предусматривает, что Рабочая группа стремится «содействовать дальнейшей горизонтальной координации деятельности своих подгрупп в отношении проблем регулирования, связанных с цифровизацией. Речь идет о таких темах, как кибербезопасность, конфиденциальность, искусственный интеллект и товары, опирающиеся на данные» (ECE/CTCS/2023/14, пункт 7).

* Настоящий документ представлен под ответственность Председателя РГ.6. Кроме того, он не редактировался профессиональным редактором.

Предлагаемое решение

«Государства-члены приняли к сведению Всеобъемлющие единые рамки регулирования для обеспечения соответствия нормативным требованиям продуктов и/или услуг со встроенными технологиями искусственного интеллекта или другими цифровыми технологиями (ECE/CTCS/WP.6/2024/11) и Декларацию о техническом регулировании продуктов со встроенными технологиями искусственного интеллекта (ECE/CTCS/WP.6/2024/12). Государства-члены призывают свои соответствующие учреждения и экспертов изучить эти два документа и доработать их в течение следующих шести месяцев с целью принятия Декларации и ее публикации для всеобщего сведения летом 2025 года».

1. Продукты и/или услуги, в которые встроены технологии искусственного интеллекта (ИИ) или другие цифровые технологии, используются в широких масштабах, однако они еще не имеют общепризнанных или общепринятых определений, а нормативно-правовые режимы их регулирования разнятся. Соответствующие стандарты, направленные на гармонизацию нормативных требований на международном уровне, в настоящее время находятся в процессе разработки. Функциональная безопасность и кибербезопасность таких продуктов являются важными элементами экономической конкурентоспособности и касающихся продукции нормативных положений. Однако технический прогресс и инновации опережают разработку стандартов и норм в отношении устойчивого развития данной отрасли и общества в целом.

2. Регулирование продукции зачастую осуществляется на основе разрозненного подхода, в то время как встроенные технологии носят скорее горизонтальный характер. В некоторых странах это может приводить к расхождениям между нормативными документами на национальном уровне и, соответственно, к различиям в толковании требований к системам ИИ или другим встроенным технологиям и их испытаниях.

3. Согласно *Рекомендации L Международная модель транснационального сотрудничества по вопросам нормативного регулирования на основе надлежащей практики нормативного регулирования*[1] РГ.6 Европейской экономической комиссии (ЕЭК), единые рамки регулирования (ЕРР) представляют собой добровольные рамки для сотрудничества по вопросам регулирования, которые облегчают доступ на рынки благодаря использованию надлежащей практики для повышения уровня гармонизации и заключения секторальных и/или касающихся конкретных продуктов соглашений между заинтересованными государствами — членами Организации Объединенных Наций.

4. ЕРР основываются на документе «Обеспечение соответствия нормативным требованиям продуктов со встроенными технологиями искусственного интеллекта или другими цифровыми технологиями» (ECE/CTCS/WP.6/2023/9), подготовленном в рамках РГ.6 для ежегодной сессии в ноябре 2023 года[2], при этом в них учтен «Промежуточный доклад по вопросу об управлении искусственным интеллектом на благо человечества», подготовленный Консультативным советом Организации Объединенных Наций по искусственному интеллекту в декабре 2023 года[3]. С этой точки зрения они способствуют использованию ИИ в качестве одного из потенциальных средств достижения всех 17 Целей в области устойчивого развития и обеспечения устойчивого развития во всех его трех аспектах — экологическом, экономическом и социальном.

5. Ввиду непрерывного развития технологий эти ЕРР потребуется, вероятно, регулярно пересматривать и, при необходимости, обновлять. В ссылках на этот документ рекомендуется четко указывать номер версии.

I. Сфера применения

6. В настоящих ЕРР предлагается общий подход к продуктам и/или услугам со встроенными системами ИИ или другими цифровыми технологиями в качестве основы для:

- постановки законных целей регулирования;
- выявления и оценки рисков;
- определения соответствующих международных стандартов для разработки нормативных документов;

[1] См. https://unece.org/DAM/trade/wp6/Recommendations/Recommendation_L_en.pdf.
[2] См. https://unece.org/sites/default/files/2023-10/ECE_CTCS_WP6_2023_09_E.pdf.
[3] См. https://www.un.org/en/ai-advisory-body.

- определения взаимно признаваемых процедур оценки соответствия;
- создания механизмов надзора за рынком и других механизмов обеспечения соблюдения.

7. ЕРР могут использоваться на национальном уровне существующими или будущими учреждениями для поощрения сближения национальных технических регламентов.

8. В настоящих ЕРР приводится описание общего подхода к продуктам и/или услугам со встроенными технологиями ИИ или другими цифровыми технологиями. Для демонстрации возможного применения ЕРР в разных секторах экономики предлагается разработать сценарии использования.

A. Термины и определения

9. Если в тексте не указано иное, используемая терминология основывается на определениях, содержащихся в приложении 1[4] к Соглашению Всемирной торговой организации (ВТО) по техническим барьерам в торговле (ТБТ) или в рекомендациях РГ.6. Терминология, связанная с продуктами и/или услугами, которые относятся к сфере применения настоящих ЕРР, включает следующие термины:

- система искусственного интеллекта (ИИ) — это техническая система, которая генерирует такие конечные результаты, как контент, прогнозы, рекомендации или решения для заданного набора определенных человеком целей (как, например, предусмотрено в стандарте Международной организации по стандартизации (ИСО)/Международной электротехнической комиссии (МЭК) 22989, Концепции и терминология ИИ)[5];
- генеративный искусственный интеллект (ГенИИ) — это система искусственного интеллекта, которая может генерировать данные в различных форматах, таких как изображения, видео, трехмерные модели или аудиофайлы. Такие системы могут быть встроены в устройства или предоставляться в формате программного обеспечения как услуги (SaaS);
- продукт и/или услуги со встроенными технологиями ИИ или другими цифровыми технологиями — это продукт и/или услуга со встроенной, обновляемой (дистанционно, в автономном режиме или другими способами) системой ИИ, или с интегрированным обновляемым программным обеспечением, или с комбинацией того и другого, которые имеют ту или иную степень автономности, управляют своей работой и способны принимать решения, влияющие на физическую или виртуальную среду таким образом, чтобы в целом способствовать достижению поставленных человеком целей.

10. Сфера применения настоящих ЕРР не распространяется на автономные колесные транспортные средства[6] и автономные системы вооружений[7]. Эти две категории устройств напрямую регулируются другими национальными или международными соглашениями. Тем не менее рекомендации, содержащиеся в настоящем документе, могут быть пригодны и для продуктов этих категорий.

[4] См. https://www.wto.org/english/docs_e/legal_e/17-tbt.pdf.

[5] См. https://www.iso.org/standard/74296.html.

[6] Самоуправляемые автомобили и автономные колесные транспортные средства относятся к сфере компетенции отдельных комитетов Организации Объединенных Наций. В отличие от автономных колесных транспортных средств, летательные и подводные аппараты, а также роботы входят в сферу применения настоящих ЕРР. См. https://unece.org/wp29-introduction.

[7] Развертывание автономных систем вооружений и продуктов и/или услуг оборонного назначения со встроенными системами ИИ и другими цифровыми технологиями относится к сфере национальных стратегий обороны и национальной безопасности и, следовательно, выходит за рамки сферы применения настоящих ЕРР.

II. Требования к продуктам и/или услугам

A. Цели регулирования и оценка уровня риска

11. При постановке целей в области регулирования следует исходить из того, что нулевой уровень риска недостижим. При определении приемлемого уровня риска и степени готовности идти на риск следует руководствоваться *Рекомендацией R* РГ.6 ЕЭК, *Управление рисками в системах регулирования*[8].

12. Некоторым продуктам со встроенными технологиями ИИ или другими цифровыми технологиями может быть изначально присущ высокий уровень риска, например, если существует вероятность прямого негативного воздействия на здоровье и безопасность людей или их основные права. Уровень риска, который может сказаться на вопросах безопасности, оценивается как умеренный (или средний). Система ИИ отличается низким уровнем риска, если в ней не используются персональные данные и/или она не влияет на человека. Правительствам необходимо будет проводить оценку рисков и выбирать надлежащие методы оценки соответствия.

13. В ситуациях, когда риск ошибки, связанной с системой ИИ, оценивается как высокий, к процессу принятия решений следует в максимально возможной степени привлекать человека. Системы ИИ не должны иметь возможность блокировать команды управления, отдаваемые человеком.

14. В некоторых секторах, где угроза для жизни и здоровья людей особенно велика, уровень опасности изначально выше. Например, некоторые виды медицинского оборудования в больницах оснащены сложными диагностическими системами со встроенным ИИ. Даже если такое медицинское оборудование может обеспечить принятие основанных на алгоритмах решений, с учетом вопросов ответственности и потенциального риска для пациентов предлагается, чтобы в процессе принятия решений по возможности участвовал человек. Обязательный контроль и вмешательство со стороны человека стоит предусмотреть и для некоторого промышленного оборудования, в работе которого участвуют люди и запрограммированные роботы под управлением систем ИИ.

15. Технологии, встроенные в продукты, зачастую с трудом поддаются оценке и определению реальных внутренних алгоритмов (например, неизвестны ни метод, ни логика, на основе которых достигаются определенные результаты). Это справедливо, возможно, даже в большей степени, и для продуктов со встроенными технологиями ИИ или другими цифровыми технологиями, поскольку из-за информации, полученной из других источников, сама система может отреагировать неожиданным образом. Этот элемент неизвестности в технологиях обычно компенсируется серией тщательно проработанных испытаний в разных условиях; однако их может быть недостаточно для выявления всех неизвестных особенностей системы, поэтому сохраняется определенный уровень остаточного риска. Регулирующие органы и дистрибьюторы таких продуктов должны гарантировать, что такие остаточные риски не превышают приемлемого уровня риска, и раскрывать информацию о них. В качестве примера можно привести соответствующие дополнительные рекомендации, разработанные Национальным институтом стандартов и технологий (НИСТ) и изложенные в документе «Механизм управления рисками, связанными с ИИ» (AI RMF1.0)[9].

B. Цели регулирования и воздействие на общество

16. Встроенная система проектируется таким образом, чтобы минимизировать смещенность в самой системе ИИ и в процессе принятия решений с помощью ИИ. При этом учитываются когнитивная предвзятость человека, смещенность данных и смещенность, возникающая в результате применения тех или иных инженерных

[8] См. https://unece.org/fileadmin/DAM/trade/wp6/Recommendations/Recommendation_R_en.pdf.
[9] См. https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf.

решений. Виды смещенности рассматриваются в документе ISO/IEC TR 24027 «Смещенность в системах ИИ и при принятии решений с помощью ИИ»[10].

17. Встроенная система проектируется таким образом, чтобы не происходила потеря свободы личности, ответственности или автономии человека.

18. Встроенная система не должна оказывать негативного влияния на психическое благополучие отдельных людей или общества в целом. С этой целью учитываются уязвимость детей и права детей в области образования, проживания, СМИ и геймификации/игр. Они перечислены в Конвенции Организации Объединенных Наций о правах ребенка (КПР ООН)[11] и рассматриваются более подробно в замечании общего порядка № 25 (2021) о правах детей в связи с цифровой средой[12].

19. Встроенная система не должна способствовать дальнейшему увеличению цифрового разрыва, о чем говорится в резолюции Организации Объединенных Наций на тему «Использование возможностей безопасных, защищенных и надежных систем искусственного интеллекта для устойчивого развития» (A/78/L.49)[13]. Следует обеспечивать полную функциональность продуктов со встроенными технологиями ИИ или другими цифровыми технологиями в странах с формирующейся рыночной экономикой. Кроме того, их следует разрабатывать таким образом, чтобы не создавать для стран с формирующейся рыночной экономикой барьеров в торговле этими товарами или в части выхода на их рынки.

C. Цели регулирования и вопросы, связанные с цифровизацией

20. Встроенная система должна проектироваться таким образом, чтобы быть надежной. Для этого необходимы гарантии от связанных с ИИ угроз безопасности, связанных с ИИ угроз конфиденциальности, непредсказуемости, непрозрачности и проблем, возникающих в процессе внедрения и использования систем ИИ. Они описываются в документе ISO/IEC TR24028 «Обзор надежности искусственного интеллекта»[14]. Отдельные вопросы, связанные с потерей данных или несанкционированным доступом к данным, рассматриваются в Общем регламенте Европейского союза (ЕС) по защите данных (ОРЗД)[15], Законе ЕС об ИИ[16] и других нормативных актах, касающихся данных.

21. Во встроенных системах следует предусмотреть надежную систему защиты от кибератак. В этих системах должны иметься механизмы, гарантирующие защиту от изменения исходных данных, изменения концепции, применения алгоритмов взлома вознаграждения и угрозы для безопасного исследования. Об этом говорится в документе ISO/IEC TR5469 «Функциональная безопасность и системы ИИ»[17]. См. другие примеры в документах НИСТ «Состязательное машинное обучение, таксономия и терминология атак и мероприятий по снижению риска» (NIST AI 100-2e2023)[18] и «Система кибербезопасности (СКБ) 2.0» (NIST CSWP.29)[19].

22. Кроме того, должны быть приняты меры, с тем чтобы встроенная технология не могла использоваться для незаконной деятельности (такой как несанкционированный или незаконный контроль или мониторинг, клевета или оскорбление).

[10] См. https://www.iso.org/standard/77607.html.
[11] См. https://www.unicef.org.uk/what-we-do/un-convention-child-rights/.
[12] См. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.
[13] См. http://www.undocs.org/A/78/L.49.
[14] См. https://www.iso.org/standard/77608.html.
[15] См. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[16] См. https://artificialintelligenceact.eu/.
[17] См. https://www.iso.org/standard/81283.html.
[18] См. https://csrc.nist.gov/pubs/ai/100/2/e2023/final.
[19] См. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

III. Связь с международными стандартами

23. Помимо стандартов, перечисленных в предыдущем разделе, для разработки и регулирования продуктов или услуг со встроенными технологиями ИИ или другими цифровыми технологиями может использоваться и ряд других стандартов.

24. Как указано в *Рекомендации D* РГ.6, *Ссылки на стандарты*, и дополнительно разъясняется в статье 2.4 Соглашения ВТО о ТБТ, «В том случае, если возникает потребность в технических регламентах, и существуют соответствующие международные стандарты или завершается их разработка, члены [ВТО] используют их или их соответствующие разделы в качестве основы для своих технических регламентов, за исключением случаев, когда подобные международные стандарты или их соответствующие разделы были бы неэффективными или неподходящими средствами для достижения поставленных законных целей, например, вследствие существенных климатических или географических факторов или существенных технических проблем».

25. К продуктам и/или услугам со встроенными технологиями ИИ или другими цифровыми технологиями могут быть применены следующие международные стандарты:

- серия стандартов ISO/IEC 42001, посвященных системам управления ИИ[20];
- серия стандартов ISO/IEC 23894:2023, посвященных ИИ: «Руководство по управлению рисками»[21];
- серия стандартов ISO/IEC TR 22100-5, посвященных последствиям машинного обучения ИИ[22];
- серия стандартов IEC 62443, посвященных промышленным системам автоматизации и управления (ПСАУ)[23];
- серия стандартов IEEE 7001-2021, посвященных прозрачности автономных систем[24];
- Рекомендация Совета по искусственному интеллекту Организации экономического сотрудничества и развития (ОЭСР) (OECD/LEGAL/0449)[25];
- Рекомендация об этических аспектах искусственного интеллекта, подготовленная Организацией Объединенных Наций по вопросам образования, науки и культуры (SHS/BIO/PI/2021/1)[26];
- публикация Всемирной организации здравоохранения (ВОЗ) под названием «Этика и управление искусственным интеллектом в здравоохранении: руководство по крупным мультимодальным моделям»[27].

26. Также необходимо принимать во внимание стандарты, посвященные защите прав потребителей и инклюзивности.

[20] См. https://www.iso.org/standard/81230.html.
[21] См. https://www.iso.org/standard/77304.html.
[22] См. https://www.iso.org/standard/80778.html.
[23] См. https://www.iec.ch/blog/understanding-iec-62443.
[24] См. https://ieeexplore.ieee.org/document/9726144.
[25] См. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjgxvXX3ICFAxVyVKQEHXRyBlUQFnoECBMQAQ&url=https%3A%2F%2Flegalinstruments.oecd.org%2Fapi%2Fprint%3Fids%3D648%26lang%3Den&usg=AOvVaw3bU62HpvCxeAcd6gxRGeJ6&opi=89978449.
[26] См. https://unesdoc.unesco.org/ark:/48223/pf0000381137.
[27] См. https://www.who.int/publications/i/item/9789240084759.

IV. Оценка соответствия

27. В настоящее время практика оценки соответствия на уровне нормативного регулирования основана на отраслевых предписаниях, в то время как обеспечение соответствия продуктов и/или услуг со встроенными технологиями ИИ или другими цифровыми технологиями носит горизонтальный характер и требует новых знаний. Для выявления и снижения рисков, а также выявления и устранения уязвимостей и киберугроз и повышения операционной устойчивости необходимы горизонтальное сотрудничество между регулирующими органами и междисциплинарный подход. В связи с этим нужно развивать горизонтальный потенциал в области нормативного регулирования, выходящий за рамки отраслевых мандатов, преодолевающий процедурную разрозненность мандатов, поддерживающий динамичность цифровых инноваций и способствующий реализации стратегий, необходимых цифровому рынку и направленных на обеспечение соблюдения нормативных требований.

28. Помимо проверки соответствия продукции, поднадзорной конкретным ведомствам, продукты со встроенными технологиями ИИ или другими цифровыми технологиями необходимо будет проверять на соответствие техническим параметрам, связанным с ИИ. Как отмечалось выше, риск заключается в том, что национальные ведомства могут выбрать разные подходы к ИИ применительно к продуктам, надзор за которыми традиционно относится к их сфере компетенции. В результате в пределах одной страны будет действовать несколько наборов требований к ИИ. Рекомендуется избегать такого подхода.

29. Строгость процедур оценки соответствия должна быть соразмерна рискам, связанным с несоответствием продукции.

30. В стандарт невозможно включить такое описание системы ИИ, чтобы соответствия стандартам было достаточно, чтобы считать соответствующий стандарту продукт безопасным. Даже если бы это было возможно, экономический оператор или орган по оценке соответствия не может заглянуть внутрь таких систем для их проверки. Кроме того, такие системы могут срабатывать случайным образом и вести себя по-разному в схожих условиях.

31. В целях минимизации рисков, связанных с той или иной системой ИИ, рамки регулирования для систем ИИ должны устанавливать требования к поставщику системы ИИ/другим заинтересованным сторонам на этапе ее разработки и требовать снижения остаточного риска системы ИИ до приемлемого уровня.

32. Традиционные процедуры оценки соответствия позволяют доказать, что система ИИ была разработана в условиях, нацеленных на снижение рисков, тогда как для демонстрации приемлемости уровня остаточного риска необходимо создать механизм проверки и оценки соответствия систем ИИ.

33. Такой механизм должен включать по крайней мере следующие процессы[28]:

- выявление всех возможных угроз и связанных с риском событий, которые могут материализоваться в процессе работы системы ИИ и причинить ущерб;
- составление перечня ситуаций/сценариев, в которых может оказаться та или иная система;
- выявление потенциальных угроз в каждом сценарии;
- оценка потенциальной серьезности угроз в сценариях и частоты их реализации;
- выбор сценариев для тестирования на основе уровня рисков: обеспечение охвата наиболее вероятных и наиболее опасных сценариев;
- моделирование/тестирования и оценка остаточного риска.

[28] См. «Key to ensuring continuous compliance: assessing the residual risks of AI systems/products with embedded software», Valentin Nikonov, 23–24 November 2023 WP.6 conference «How to target continuous compliance».

34. Как и в приведенных выше примерах с нормативным регулированием продукции, можно выделить три уровня риска: высокий, умеренный (или средний) и низкий. В случае продуктов с низким уровнем риска правительства могут рассмотреть возможность отказа от специального процесса оценки соответствия или, как максимум, требовать представления поставщиком декларации о соответствии. В случае продуктов с умеренным уровнем риска правительства могут рассмотреть возможность введения требования о представлении поставщиком декларации о соответствии. В случае продуктов с высоким уровнем риска правительства могут рассмотреть возможность проведения оценки соответствия независимой третьей стороной.

A. Декларация поставщика о соответствии

35. Декларация поставщика о соответствии может требоваться в случае продуктов или услуг со встроенными технологиями ИИ или другими цифровыми технологиями с умеренным риском, а в перспективе и в случае продуктов или услуг с низким риском.

36. В такой декларации должно быть указано, что поставщик признает важность принципов, которые изложены в разделе, посвященном требованиям к продукции, и что продукт или услуга соответствует применимым международным стандартам. Например, в декларации поставщика целесообразно дать ссылку на стандарт ISO/IEC TR5469, «Функциональная безопасность и системы ИИ»[29], а также на Рекомендацию Совета по искусственному интеллекту (OECD/LEGAL/0449) Организации экономического сотрудничества и развития (ОЭСР)[30].

B. Оценка соответствия третьей стороной

37. Для продуктов или услуг со встроенными технологиями ИИ или другими цифровыми технологиями, уровень риска в связи с которыми оценивается как высокий, наиболее предпочтительным вариантом будет, вероятно, проведение оценки соответствия третьей стороной. Применительно к техническим аспектам продукта или услуги, имеющим отношение к ИИ, такая оценка должна подтвердить, что они соответствуют принципам, которые изложены в разделе, посвященном требованиям к продукции, и что продукт или услуга соответствует применимым международным стандартам. В зависимости от типа продукции могут приводиться ссылки на разные стандарты. Например, в случае медицинского оборудования можно ссылаться на публикацию Всемирной организации здравоохранения (ВОЗ) «Этика и управление искусственным интеллектом в здравоохранении: руководство по крупным мультимодальным моделям»[31].

38. Принимая настоящие ЕРР, государственные учреждения дают свое согласие на проведение третьей стороной оценки соответствия связанных с ИИ аспектов продукта или услуги на основе принципов этих ЕРР. Такая оценка может проводиться как в рамках, так и за рамками уже существующих соглашений о взаимном признании. В обоих случаях в отношении аспектов, связанных с ИИ, необходимо будет ссылаться на принципы, содержащиеся в настоящих ЕРР.

[29] См. https://www.iso.org/standard/81283.html.

[30] См. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjgxvXX3ICFAxVyVKQEHXRyBlUQFnoECBMQAQ&url=https%3A%2F%2Flegalinstruments.oecd.org%2Fapi%2Fprint%3Fids%3D648%26lang%3Den&usg=AOvVaw3bU62HpvCxeAcd6gxRGeJ6&opi=89978449.

[31] См. https://www.who.int/publications/i/item/9789240084759.

V. Надзор за рынком

39. Одной из основных характеристик продуктов или услуг с встроенными технологиями ИИ или другими цифровыми технологиями, затрудняющей их нормативное регулирование, является возможность их подсоединения к удаленному серверу, который может осуществлять их регулярное обновление. Таким образом, трудность заключается в том, чтобы обеспечить постоянное соответствие этих продуктов нормативным требованиям после их поступления на рынок в условиях, когда могут отсутствовать возможности для физического отслеживания, инспектирования или верификации изменений в характеристиках продукта или услуги.

40. Органам надзора за рынком необходимо будет интегрировать в процесс своей работы методы обеспечения постоянного соответствия. Это будет включать проведение регулярных обязательных независимых аудитов продуктов или услуг, уже находящихся на рынке, на предмет соблюдения установленных правительством бинарных (соответствует/не соответствует) критериев и проверку на основе настоящих EPP их соответствия принципам и стандартам, которые изначально подлежали соблюдению для выхода на рынок. Такие аудиты будут иметь особенно большое значение для продуктов или услуг, риск в связи с которыми оценивается как высокий.

41. Продукты или услуги, которые более не соответствуют принципам и стандартам, подлежавшим соблюдению для выхода на рынок, должны быть незамедлительно отозваны и сняты с продажи. В случае критического несоответствия следует выпустить международное оповещение, чтобы поставить в известность другие страны.