Организация Объединенных Наций ECE/TRADE/C/CEFACT/2022/13

Экономический и Социальный Совет

Distr.: General
19 July 2022
Russian
Original: English

Европейская экономическая комиссия

Исполнительный комитет

Центр Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям

Двадцать восьмая сессия
Женева, 10–11 (первая половина дня) октября 2022 года
Пункт 5 d) предварительной повестки дня
Рекомендации и стандарты:
Материалы для имплементационной поддержки

Доклад по направлению eDATA, посвященный стандартам в области интернета вещей в целях упрощения процедур торговли

Представлен Бюро

Резюме

Интернет вещей (ИВ) облегчает торговлю, позволяя собирать трансграничную электронную информацию и обмениваться ею без вмешательства человека, что делает ее более безопасной, эффективной и экономичной. Учитывая широкое распространение ИВ, в настоящем докладе освещается роль, которую стандарты Центра Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям (СЕФАКТ ООН) могут играть в определении потоков данных и технологических потоков между устройствами ИВ, применяемыми различными сторонами в рамках международной цепочки поставок, а также то, как эти данные могут быть интегрированы в существующие процессы автоматизации цепочки поставок на интероперабельной основе. В докладе приведены примеры стандартов данных, технологических процессов и обмена информацией ИВ, а также определены потребности в данных для более широкого внедрения ИВ в приложениях, предусматривающих упрощение процедур торговли.

Документ ECE/TRADE/C/CEFACT/2022/13 представляется Бюро на двадцать восьмой сессии для принятия к сведению.

I. Введение

1. Интернет вещей (ИВ) — это сеть, которая соединяет уникально идентифицируемые «вещи» или устройства с Интернетом. Эти устройства обладают сенсорными возможностями и, потенциально, могут быть запрограммированы. Используя их уникальные идентификационные и сенсорные возможности, можно собирать информацию об этих устройствах и изменять их состояние.

2. Некоторые из ключевых характеристик экосистемы ИВ включают следующее:

- взаимосвязи с устройствами и между ними;
- уникально идентифицируемые устройства;
- сенсорные возможности;
- встроенный интеллект;
- коммуникационные возможности; и
- программируемость.

3. Эти экосистемы ИВ обладают потенциалом для создания новых приложений, способствующих трансграничной безбумажной торговле благодаря использованию подключенных устройств, которые чувствуют, собирают и обрабатывают данные, обмениваются ими и действуют на основе данных. Такие данные, как температура, влажность и местоположение, могут собираться с ИВ-устройств и использоваться в целом ряде приложений для решения различных задач — от обеспечения свежести продуктов в цепочке поставок до отслеживания местонахождения материальных средств и обнаружения неисправности оборудования в сфере логистики и транспорта.

4. ИВ-устройства также способны собирать и записывать данные в режиме реального времени и непрерывно, а также связывать эти данные с уникальными идентификаторами. Поэтому их можно использовать для отслеживания происхождения данных, относящихся к показаниям основных датчиков, даже когда эти данные используются программными приложениями для генерирования сложной производной информации. Эти данные, представленные в режиме реального времени, могут быть переданы в системы принятия решений, которые являются частью международной цепочки поставок, для дальнейших действий и автоматизации, как это задокументировано в Проекте использования смарт-контейнеров Центра Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям (СЕФАКТ ООН).

5. ИВ создает интересные возможности для упрощения процедур торговли, позволяя генерировать трансграничную электронную информацию и обмениваться ею без вмешательства человека, т. е. более безопасным, эффективным и экономичным способом. Системы ИВ также могут быть разработаны для обеспечения целостности данных о физическом состоянии таких предметов, как упаковка, транспортные средства и контейнеры.

6. В сочетании с другими развивающимися технологиями, такими как блокчейн, сети 5G, интерфейсы программирования приложений (ИПП) и облачные платформы, ИВ может оказать огромное влияние на тенденцию к значительной автоматизации международных цепочек поставок и облегчению трансграничной безбумажной торговли.

7. Во всем мире уже существует множество проектов, направленных на коренное преобразование цепочек поставок за счет операционной эффективности, обеспечиваемой ИВ для лучшего отслеживания материальных средств, управления запасами и упреждающего обслуживания оборудования. Интересный пример этого задокументирован в Проекте использования смарт-контейнеров СЕФАКТ ООН, в рамках которого рассматривается вопрос о том, как смарт-контейнеры (стандартизированные морские контейнеры, оснащенные датчиками) позволяют отслеживать и мониторить ситуацию «от двери до двери». Смарт-контейнеры способны обеспечить сквозную видимость и прозрачность всей цепочки поставок.

8. Учитывая широкое использование ИВ в целом спектре систем и его потенциал для улучшения существующих каналов связи и создания новых каналов, в настоящем документе делается попытка осветить роль стандартов и то, как СЕФАКТ ООН может внести вклад в разработку или расширение существующих технических спецификаций, чтобы максимально повысить ценность этой технологии для клиентов СЕФАКТ ООН.

9. Поэтому в данном документе основное внимание уделяется роли, которую стандарты СЕФАКТ ООН могут играть в определении потоков данных и технологических потоков между устройствами ИВ, применяемыми различными сторонами в рамках международной цепочки поставок, а также тому, как эти данные могут быть интегрированы в существующие процессы автоматизации цепочки поставок на интероперабельной основе.

II. Стандарты данных

10. ИВ может помочь понять смысл происходящего в физическом мире за счет сбора данных, полученных в результате физических перемещений и экологических изменений. Этот процесс начинается с того, что сенсорные устройства регистрируют физические перемещения людей, животных, автомобилей, посылок и т. д. и/или изменения окружающей среды, такие как температура и влажность. Затем эти необработанные данные передаются на шлюзовое устройство, которое преобразует их в формат данных, совместимый с протоколом Интернета (ПИ), и отправляет их на серверы, расположенные либо в помещениях, либо в облаке, для хранения и вычислений. После данные снова преобразуются в стандартный формат, чтобы их содержание можно было понять и использовать для получения оптимальных желаемых результатов.

11. Примером проекта ИВ, в котором была оптимально задействована и развернута библиотека ключевых компонентов СЕФАКТ ООН, как раз и является Проект использования смарт-контейнеров СЕФАКТ ООН. Этот проект служит важной составляющей разработки международных мультимодальных стандартов для поддержки будущего мировой торговли. Смарт-контейнер — это морской транспортный контейнер, оснащенный постоянно установленным смарт- устройством мониторинга. Смарт- устройство имеет набор датчиков, встроенных в контейнер, что позволяет ему измерять в реальном времени такую информацию, как местоположение, открытие и закрытие двери, вибрации, температура, влажность и другие поддающиеся измерению физические параметры среды, окружающей материальные средства внутри контейнера, а также сам контейнер. Он также обладает возможностями связи (используется для передачи измеренных данных в центр сбора) и может быть сопряжен с дополнительными удаленными датчиками для решения конкретных задач, относящихся к конкретной партии груза.

12. В рамках процесса моделирования данных Проект использования смарт-контейнеров добавил новые элементы в библиотеку ключевых компонентов (БКК) и справочную модель данных для мультимодальных перевозок (ММП) с целью регистрации:

- элементов и категорий данных, связанных с датчиками;
- элементов и категорий данных, относящихся к географической информации; и
- смежных элементов ММП, таких как груз и транспортное оборудование.

13. Тогда как смарт-контейнеры представляют собой интересный пример использования стандартов СЕФАКТ ООН в ИВ, по мере расширения использования ИВ на транспорте и в торговле открываются возможности для совершенствования модели данных ММП, чтобы лучше адаптироваться к меняющимся бизнес-требованиям, обусловленным растущим числом приложений ИВ.

III. Стандарты технологических процессов

14. Различные технологии могут сделать цепочки поставок более эффективными благодаря соответствующему обмену информацией на различных этапах цепочек поставок. ИВ — это одна из таких технологий, которая может обеспечить бесперебойный обмен данными с помощью многочисленных датчиков, предоставляя такую информацию, как атмосферные условия, температура, удары и вибрации, координаты ГПС и т. д. Эти данные, полученные с помощью ИВ-устройства, могут быть использованы в качестве исходных данных для программ, которые удаленно изменяют настройки, контролируют окружающую среду и обеспечивают необходимые условия для сохранения качества товаров. Они также могут быть использованы в качестве исходных данных для других процессов, например, для страховых выплат.

15. Существует множество возможностей для применения стандартов технологических процессов СЕФАКТ ООН, совместимых с ИВ, в целях повышения эффективности трансграничной безбумажной торговли. Одно из основных препятствий для плавного внедрения систем ИВ заключается в нежелании властей передавать контроль над своими данными и процессами общим платформам, находящимся за пределами их юрисдикции[1]. Чтобы преодолеть это нежелание, необходимо создать процессы, которые позволят надлежащим образом обмениваться записанными данными в трансграничном контексте и на различных платформах без нарушения норм конфиденциальности и регулирования.

16. Проект использования смарт-контейнеров является отличным примером того, как можно использовать ИВ в цепочке поставок. СЕФАКТ ООН разработал спецификации требований ведения деловых (СТДО) для смарт-контейнеров, которые являются первыми официальными стандартами, детализирующими элементы данных, используемые приложениями для смарт-контейнеров. Важно придерживаться этих стандартов, так как широкое внедрение смарт-контейнеров очень необходимо различным заинтересованным субъектов, а системы ИВ, основанные на стандартах, имеют больший потенциал для увеличения внедрения смарт-контейнеров. Стандартизация смарт-контейнеров важна, поскольку она позволит снизить затраты на развертывание и разработку ИВ-решений[2], которые необходимы с целью сокращения сроков транспортировки и рисков для всех сторон.

17. Стандарты бизнес-процессов модели «покупка — отгрузка — оплата» СЕФАКТ ООН[3] послужили эталоном для применения СТДО СЕФАКТ ООН[4]. Эта модель описывает основные стороны и процессы, задействованные в международной цепочке поставок, и устанавливает взаимосвязь между объектами данных, используемыми в различных частях цепочки поставок, начиная от транспортных контрактов и заканчивая договорами международной купли-продажи. Эти бизнес-процессы взаимосвязаны в рамках сферы охвата модели «покупка — отгрузка — оплата», которая включает в себя оперативный транспорт и логистику, контракты на коммерческие перевозки, пограничное оформление, нормативные и финансовые процессы и обеспечивает обмен информацией как внутри бизнес-доменов, так и между ними.

18. Модель «покупка — отгрузка — оплата» может применяться в любом регионе, отрасли или стране для разработки электронных документов с целью обмена данными в сфере транспорта и торговли, которые в дальнейшем интегрируются в программные решения для перевозчиков, агентов, трейдеров, таможни, экспедиторов и т. д. Модель

[1] UN/CEFACT, «White Paper: Technical Applications of Blockchain to UN/CEFACT Deliverables, version 2», (2019),URL: https://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain_TechApplication.pdf.

[2] UN/CEFACT, «Business Requirements Specification (BRS), Smart Containers», (2019).

[3] https://tfig.unece.org/contents/buy-ship-pay-model.htm.

[4] UN/CEFACT, «Buy-Ship-Pay Reference Data Model, Version 1», (2019). URL: https://www.unece.org/fileadmin/DAM/cefact/brs/BuyShipPay_BRS_v1.0.pdf.

также полезна для поддержки и наращивания внедрений «единого окна», поскольку она обеспечивает основу для гармонизации данных и для глобально согласованных спецификаций обмена данными в международной цепочке поставок. Системы ИВ могут еще больше расширить возможности модели «покупка — отгрузка — оплата» за счет использования существующих, установленных стандартов для процессов «покупка — отгрузка — оплата» и их дальнейшего развития в контексте совместимости с информацией, получаемой через системы ИВ.

19. Владельцами потоков данных, генерируемых устройствами ИВ, обычно являются конкретные платформы, операторы инфраструктуры или поставщики дополнительных услуг, а данные предоставляются через ИПП-платформы или на основе сообщений. Если в рамках стандартов технологических процессов «покупка — отгрузка — оплата» будут установлены стандарты управления данными, собранными с помощью ИВ, это будет способствовать значительному росту международной торговли за счет повышения своевременности, качества и объемов данных по линии цепочки поставок, а также увеличит масштабы внедрения модели «покупка — отгрузка — оплата».

20. Особое внимание следует уделить общим платформам, поскольку они позволят шире использовать преимущества инноваций благодаря обмену информацией и доступу к данным по требованию. СТДО или схемы спецификации требований (ССТ) должны быть структурированы таким образом, чтобы обеспечить обмен информацией через поддерживаемые соответствующей платформой веб-сайты, которые предлагают частный/публичный доступ с использованием таких протоколов, как HTTP, а также позволяют использовать внешние ИПП для добавления функциональности и доступа к данным[5]. Это позволит использовать информацию, полученную с помощью ИВ-устройств, для обеспечения эффективности, меньшего обращения к услугам посредников и снижения затрат.

21. Создание и соблюдение основанных на стандартах семантических моделей СЕФАКТ ООН может расширить сети между трейдерами и поддержать интеграцию на различных платформах. Разработка соответствующих СТДО и ССТ поможет добиться развертывания ИВ в более широких масштабах. Подобно тому, как было установлено соответствие между семантическими стандартами СЕФАКТ ООН и ЭДИФАКТ ООН[6] и XML, семантические стандарты СЕФАКТ ООН в идеале должны быть сопоставлены с синтаксисом, используемым в таких технологиях, как ИВ, блокчейн и ИПП, ориентированные на веб-платформы. Для управления потоками данных на более детальном уровне все большее значение будет приобретать моделирование детальной семантики процессов.

22. Более широкая интеграция ИВ с другими технологиями, такими как блокчейн и ИИ, может открыть интересные возможности для упрощения трансграничной безбумажной торговли. В поддержку этого можно рассмотреть следующие рекомендации по улучшению стандартов технологических процессов[7]:

- создание эталонной архитектуры для содействия полному пониманию спецификаций и новых технологий;
- пересмотр существующих моделей процессов для СТДО/ССТ, чтобы обеспечить совместимость данных на блокчейне (после регистрации данных от ИВ) с целью поддержки разрешенного доступа к порталам органов власти в разных странах, используя смарт-контракты для событий, начиная от выпуска партий грузов и заканчивая утверждением счетов-фактур;
- разработка более детальных моделей процессов, которые сфокусированы на жизненных циклах ключевых ресурсов в глобальных цепочках создания

[5] UN/CEFACT, «White Paper: Technical Applications of Blockchain to UN/CEFACT Deliverables, v.2», (2019).

[6] Правила Организации Объединенных Наций для электронного обмена данными в управлении, торговле и на транспорте.

[7] UN/CEFACT, «White Paper: Technical Applications of Blockchain to UN/CEFACT Deliverables, v.2», (2019).

стоимости. Эти ресурсы варьируются от таких элементов, как контракты и платежи, до партий грузов и контейнеров.

23. Стандарты должны быть разработаны для обеспечения последовательности, чтобы независимо от платформы, на которой размещена информация о ресурсе, при условии соблюдения стандартов заинтересованные субъекты могли интерпретировать данные одинаковым образом.

24. Возможности систем ИВ еще больше расширяются в сочетании с технологией блокчейн и стандартизированными данными.

25. Стандартизированные данные, собранные с помощью датчиков ИВ, могут храниться в цифровых реестрах третьих лиц (на основе технологии блокчейн), а также использоваться для отслеживания продукции в цепочках поставок. Это позволяет генерировать надежные данные для использования в различных приложениях, в частности, с целью подтверждения страны происхождения и количества отправленных грузов, выставления страховых претензий в связи с плохими условиями транспортировки и т. д.

26. Цифровые реестры используются в торговых процессах, в которых участвуют различные стороны, и, как следствие, приложения должны будут поддерживать обмен данными между различными цифровыми реестрами, что требует разработки стандартов для облегчения этого процесса. Например, в одной сквозной импортной транзакции в будущем может происходить обмен между столькими различными цифровыми реестрами, сколько имеется участников в этом процессе: один реестр электронного торгового финансирования может использоваться импортером, а другой — экспортером, причем каждым со своими банками, а затем каждый банк может использовать разные реестры для проверки лицензий и сертификации качества продукции. Затем страховые компании могут использовать различные цифровые реестры для проверки данных и обмена данными, а перевозчики/экспедиторы могут использовать свой реестр для управления товаросопроводительными документами. Кроме того, таможенная служба может использовать еще один реестр для проверки документов и для того, чтобы удостовериться в прошлой добросовестной практике экспортера и импортера.

27. Если будут созданы стандарты СЕФАКТ ООН, учитывающие ограничения, возникающие при использовании устройств ИВ и цифровых реестров, это позволит обеспечить обмен данными или интероперабельность между несколькими реестрами. В дальнейшем возможности ИВ также будут еще более улучшены, обеспечивая большую безопасность и конфиденциальность при управлении данными. Одним словом, технологические стандарты СЕФАКТ ООН могут быть полезны для поддержки более широкого внедрения ИВ путем установления стандартов, обеспечивающих семантическую интероперабельность между несколькими реестрами.

IV. Стандарты сообщений (обмена информацией)

28. Настоящий документ посвящен необходимости дальнейшей разработки документа СТДО для поддержки международных стандартов сообщений с целью эффективного обмена информацией, содержащейся в ИВ и цифровом реестре. Некоторые из наиболее уникальных характеристик этих данных сводятся к необходимости обмена относительно небольшими объемами данных (фрагментами) и/или большим количеством этих самых фрагментов данных. Например, необходимо создать согласованные структуры данных и сообщений, которые можно использовать для обмена данными такого типа в различных торговых моделях, таких как смарт-контейнеры, порталы для единовременного представления данных (ПЕПД) или модель «покупка — отгрузка — оплата». Документ СТДО должен включать стандартизированные элементы данных, позволяющие взаимодействие между платформами, а в случае регистрации данных с помощью устройств ИВ —полностью интегрированную систему обмена данными на основе использования общих ИПП, которые, в свою очередь, основаны на стандартах. Кроме того, данные, полученные с

помощью устройств ИВ, также должны соответствовать требованиям ССТ для отображения единиц данных, таких как местоположение, хозяйствующие субъекты или различные заинтересованные стороны.

29. Эффективный обмен данными важен для бесперебойного функционирования логистических цепочек поставок, поскольку в транзакциях участвует множество заинтересованных сторон, а сами цепочки поставок являются глобальными и разнообразными. Уже используется много смарт-контейнеров и устройств, но в настоящее время не существует глобальных стандартов для сбора и последовательной передачи массива данных, получаемых ИВ-устройствами в смарт-контейнерах.

30. СЕФАКТ ООН уже создал СТДО для смарт-контейнеров, которая является первым официальным стандартом, детализирующим элементы данных смарт-контейнера. Важно придерживаться этих стандартов, поскольку более широкое внедрение смарт-контейнеров крайне необходимо различным заинтересованным сторонам. В этом контексте использование устройств ИВ вместе со стандартами способствует более масштабному внедрению и гарантирует интероперабельность.

31. ИВ также может быть развернут в порталах для единовременного представления данных (ПЕПД), поскольку стандартизация потоков данных является важным элементом ПЕПД и обеспечивает основу для связи между правительствами и предприятиями в поддержку трансграничной торговли[8]. Основной целью любого ПЕПД является создание условий и содействие точному декларированию данных трансграничным регулирующим органам, которые будут использовать эти данные для таможенного оформления и управления рисками на границе. Успешная реализация ПЕПД зависит от использования обмена сообщениями/информацией в согласованном виде и формате, чтобы обе стороны транзакции могли читать и понимать данные благодаря семантической интероперабельности[9]. Традиционно такая семантическая интероперабельность основывается на общей эталонной модели данных для логического потока информации в трансграничной торговле.

32. Гармонизация данных важна для достижения целей ПЕПД, которые включают устранение избыточности, двусмысленности и дублирования данных, в связи с чем для эффективной реализации требуется отобразить требования, предъявляемые к данным, содержащимся в соответствующих документах, в преломлении к международным стандартам трансграничной торговли[10]. Стандартизированный обмен информацией, поддерживаемый развертыванием систем ИВ и блокчейн, которые используют стандартизированные данные, может помочь достичь целей ПЕПД, если он интегрирован в процессы, определенные в СТДО и ССТ. Такие документы, как разрешения, сертификаты и таможенные декларации, можно вести в цифровом виде после получения ключевых данных с помощью ИВ-устройств и хранить в блокчейне, чтобы обеспечить их неизменную целостность. Но для достижения этой цели необходимо создать соответствующие форматы обмена сообщениями и интерфейсы наряду со стандартизацией элементов данных с учетом необходимости обеспечения прозрачности и конфиденциальности пользователей в соответствии с Общим регламентом защиты данных Европейского союза (ОРЗД) и другими законодательными актами. Использование надежных систем ИВ вместе с разрешенными блокчейнами может обеспечить необходимую инфраструктуру для достижения целей ПЕПД.

33. В контексте модели «покупка — отгрузка — оплата» необходимо дальнейшее развитие для того, чтобы полностью реализовать ее потенциал и потенциал

[8] UN/CEFACT, «Recommendation No 37: Single Submission Portal», (ECE/TRADE/447) (2019). URL: http://www.unece.org/fileadmin/DAM/trade/Publications/ECE_TRADE_447E_CF-Rec37.pdf.

[9] Ibid.

[10] https://tfig.unece.org/contents/data-harmonization.htm.

развертывания ИВ. Стандарты необходимы для удовлетворения следующих потребностей, где существуют пробелы в существующей модели[11]:

- обеспечение большей наглядности и мониторинга в цепочке поставок посредством детального документирования и стандартизации изменений состояния, происходящих в объектах модели «покупка — отгрузка — оплата», для отслеживания потоков более подробных данных и их увязки с более глубокими событиями более высокого уровня;
- обеспечение здоровья и условий содержания животных посредством стандартов процессов и данных для обмена и использования соответствующих ИВ-данных (например, о температуре в вагонах для скота, состоянии гидратации животных и т. д.);
- обеспечение обнаружения и отслеживания функциональных элементов в сфере логистики и выполнения нормативных требований с помощью СТДО/ССТ, которые отражают использование данных ИВ (например, от устройств мониторинга, прикрепленных к товарам или контейнерам); и
- выявление новых возможностей в рамках модели «покупка — отгрузка — оплата» для процессов, использующих данные ИВ в конвейерах данных для нормативной отчетности, производства, планирования, управления материально-техническим обеспечением, финансирования заказов на поставку и государственных закупок.

34. Зачастую отсутствие прозрачности в обмене данными между различными заинтересованными сторонами в глобальной трансграничной торговле является проблемой для реализации всех преимуществ цифровых цепочек поставок. Технология блокчейн обеспечивает прозрачность и высокий уровень достоверности благодаря надежной регистрации и хранению данных с помощью криптографии. После получения данных ИВ из окружающего пространства контейнера можно получить другую информацию, такую как местоположение/позиционирование контейнера (также с помощью ИВ) и добавить ее к записи о грузе, зарегистрированной в блокчейне.

35. Интеграция данных, собранных с помощью ИВ во время транспортировки грузов на основе стандартов данных СТДО/ССТ, жизненно важна для повышения эффективности цепочек поставок и внедрения безбумажной трансграничной торговли. Дальнейшая стандартизация этих процессов в сочетании с записью данных на блокчейне обеспечит большую видимость и доступ к данным (через интероперабельность) для регулирующих органов на границе, тем самым позволяя им ускорить торговые процессы. Одним словом, транспонирование ИВ вместе с технологией блокчейн в стандарты данных СТДО и ССТ значительно повысит эффективность цифровых цепочек поставок, поскольку стандартизация позволит увеличить объем генерируемых и используемых данных. Это также будет способствовать улучшению аналитической обработки данных и совершенствованию принятия решений, позволяя системам искусственного интеллекта использовать стандартизированные данные из различных источников.

V. Вопросы кибербезопасности

36. ИВ относится к растущей цифровой сети связей, которые соединяют устройства и датчики для облегчения передачи данных через Интернет без внешнего вмешательства. В этой процветающей цифровой среде, когда передача данных с помощью технологий становится все более применимой во всем мире, международная торговля продолжает расширяться и пересекать юрисдикции. Цифровизация через ИВ начала трансформировать торговый ландшафт, особенно в трансграничном контексте.

[11] ЕЭК, «Программа работы СЕФАКТ ООН на 2019–2020 годы» (ECE/TRADE/C/CEFACT/2019/21) (2019 год).
URL: https://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/PoW_2019-2020_E.pdf.

ИВ поддерживает упрощение электронных торговых документов на основе автоматического сбора ключевых данных, что в сочетании с технологией блокчейн способно ускорить процедуры экспорта и импорта. Возможность отслеживать грузы с помощью ИВ уже повысила эффективность перевозок[12], а электронная аутентификация может облегчить процесс проверки онлайн-транзакций[13]. Как показывают действующие тенденции, переплетение Интернета и вычислительных устройств сегодня является неотъемлемой частью будущей экономической деятельности. По оценкам, только в 2020 году объем продаж в сфере электронной торговли в мире должен составить 26,7 трлн долл. США[14], при этом ожидается, что в 2022 году доля трансграничной электронной торговли достигнет 22 % от общего объема продаж в сфере электронной торговли (по сравнению с 15 % в 2016 году)[15]. Более того, согласно прогнозам, к 2030 году к Интернету будет подключено 500 млрд устройств[16], в то время как факторы уязвимости, связанные с развертыванием подключенных устройств, остаются практически не устраненными[17]. Проблемы совместимости и взаимодополняемости аппаратного и программного обеспечения (при отсутствии проектирования с учетом требований безопасности) могут усугубиться в связи с экспоненциальным ростом числа подключенных устройств ИВ по мере продвижения в будущее[18]. Поскольку предприятия часто работают в трансграничном контексте, чтобы снизить торговые издержки, торговые документы и данные циркулируют между многочисленными сетями, расположенными в разных юрисдикциях[19]. Это также усилило угрозы кибербезопасности, связанные с массовым появлением трансграничных потоков торговых данных[20].

[12] World Trade Organization, *World Trade Report 2018: The future of world trade: How digital technologies are transforming global and commerce*, (2018), pages 66–67 and 73. URL: https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf (дата обращения: 24 мая 2022 года).

[13] Maria Ptashkina, «Facilitation 2.0: E-Commerce and Trade in the Digital Age» (RTA Exchange, International Centre for Trade and Sustainable Development (ICTSD) and Inter-American Development Bank (IDB), 2018), p 9. URL: https://e15initiative.org/wp-content/uploads/2015/09/rta_exchange_-_ptashkina_-_facilitation_2.0_-_e-commerce_-_ptashkina_0.pdf (дата обращения: 24 мая 2022 года).

[14] United Nations Conference on Trade and Development (UNCTAD). «Global e-commerce jumps to $26.7 trillion, COVID-19 boosts online sales», (03 May 2021). URL: https://unctad.org/news/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-sales (дата обращения: 24 мая 2022 года).

[15] Statista.com, «Cross-border e-commerce as share of total e-commerce worldwide in 2016 and 2022», URL: https://www.statista.com/statistics/867991/cross-border-e-commerce-share-world/ (дата обращения: 24 мая 2022 года).

[16] CISCO, «At-a-Glance: Internet of Things: Connected Means Informed» (2016). URL: https://emarsonindia.com/wp-content/uploads/2020/02/Internet-of-Things.pdf (дата обращения: 6 марта 2020 года).

[17] EY, «Cybersecurity and the Internet of Things» (2015), pp. 10–11. URL: https://pdf4pro.com/amp/view/ey-cybersecurity-and-the-internet-of-things-567613.html (дата обращения: 24 мая 2022 года).

[18] World Economic Forum, «Global Risks Report 2020», *Insight Report, 15th Edition* (2020), p. 62. URL: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (дата обращения: 24 мая 2022 года); Siddiqui, F.M., M. Hagan & S. Sezer, «Embedded Policing and Policy Enforcement Approach for Future Secure IoT Technologies», *Living in the Internet of Things: Cybersecurity of the IoT —2018*, (conference paper). p. 5. URL: https://pureadmin.qub.ac.uk/ws/portalfiles/portal/153474397/Final_Paper_Submitted.pdf (дата обращения: 24 мая 2022 года).

[19] Economic and Social Commission for Asia and the Pacific (UNESCAP), «Mechanism for cross-border mutual recognition of trade-related data and documents in electronic form» (2019) Conference Room Paper for the Fifth Meeting of the Interim Intergovernmental Steering Group on Cross-border Paperless Trade Facilitation by the Legal and Technical Working Groups, p. 6. URL: https://www.unescap.org/sites/default/files/B1900234.pdf (дата обращения: 24 мая 2022 года).

[20] Joshua P. Meltzer, «Cybersecurity and digital trade: What role for international trade rules?», (Brookings Institution, 2019), p.2. URL: https://www.brookings.edu/wp-content/uploads/2019/11/Cybersecurity-and-digital-trade_final-11.20.pdf (дата обращения: 24 мая 2022 года).

37. Взаимосвязанные устройства ИВ могут обеспечить доступ к большим объемам данных в различных секторах, где существует серьезная возможность для злоупотреблений. Если экосистемы ИВ призваны способствовать развитию торговли, то их открытость, стабильность, безопасность и надежность должны стать обязательным условием их использования в международной торговле[21]. Учитывая, что рост международной торговли и растущая зависимость от ИВ будут только увеличиваться по своему масштабу и охвату, опасения бизнеса должны выходить за рамки потенциальных денежных потерь и включать репутационный ущерб.

38. Для целей настоящего доклада мы предполагаем, что разработка всеобъемлющего набора стандартов кибербезопасности через посредство сотрудничества государственного и частного секторов может способствовать безопасной трансграничной торговле.

A. Стандарты кибербезопасности: более широкие последствия

39. Угрозы кибербезопасности распространяются в условиях инновационного технологического роста; однако до сих пор не существует общепринятого определения того, что должны включать в себя стандарты кибербезопасности. Сегодня такие стандарты могут принимать форму законодательства, правил, принципов, руководящих положений, передовой практики, схем сертификации, технических спецификаций и/или других механизмов, разработанных государственными, частными и некоммерческими организациями[22].

40. Принятый в США Закон о конфиденциальности потребителей Калифорнии и Общий регламент Европейского союза о защите данных направлены на использование и сбор персональных данных (которые включают персональные данные, собираемые устройствами ИВ), а не конкретно на аспекты безопасности ИВ. Однако в период после 2017 года Сенат США представил и обсудил Закон об улучшении кибербезопасности ИВ, требующий от Национального института стандартов и технологии (НИСТ) предпринять конкретные шаги для повышения кибербезопасности устройств ИВ[23]. Аналогичным образом в 2018 году Европейская комиссия разработала систему добровольной сертификации кибербезопасности (на основе уровней гарантии), направленную на повышение доверия и безопасности устройств ИВ[24]. Эти нормативные подвижки усиливают необходимость внедрения кибербезопасности в качестве средства укрепления доверия в пределах экосистем ИВ, что, в свою очередь, повышает доверие в области международной торговли. Управление угрозами и снижение рисков требует разработки комплексной системы для формирования политики, которая может повлечь за собой широкую защиту механизмов взаимодействия между продуктами, процессами и технологиями с использованием наилучших видов практики обеспечения соответствия. Установление стандартов кибербезопасности имеет решающее значение для любого предприятия, если оно хочет процветать.

[21] Neha Mishra, «International Trade, Internet Governance and the Shaping of the Digital Economy» (UNESCAP, 2017) ARTNeT Working Paper Series No. 168. URL: https://www.unescap.org/sites/default/files/AWP%20No.%20168.pdf (дата обращения: 24 мая 2022 года).

[22] Brass, I., et al., «Standardising a Moving Target: The Development and Evolution of IoT Security Standards» (June 2018) *Living in the Internet of Things: Cybersecurity of the IoT – 2018*, Conference Paper, p. 2. URL: https://www.researchgate.net/publication/325436966_Standardising_a_Moving_Target_The_Development_and_Evolution_of_IoT_Security_Standards (дата обращения: 24 мая 2022 года).

[23] US Congress, «S.734 – Internet of Things Cybersecurity Improvement Act of 2019» 116th Congress (2019–2020). URL: https://www.congress.gov/bill/116th-congress/senate-bill/734 (дата обращения: 24 мая 2022 года).

[24] European Commission, «The EU cybersecurity certification framework». URL: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (дата обращения: 24 мая 2022 года).

41. Основополагающим для обеспечения кибербезопасности является определение формы и содержания ожидаемых результатов достижения безопасности. На начальном этапе может быть сложно разработать единый набор стандартов кибербезопасности для всех приложений ИВ в разных юрисдикциях[25]. Это неудивительно, учитывая, что у разработчиков стандартов есть свои приоритеты и критерии при оценке рисков кибербезопасности в экосистеме ИВ. Тем не менее принятие принципов «безопасности по замыслу» в качестве базового требования (т. е. интеграция функций безопасности в устройства ИВ на этапе проектирования[26]) может оказаться необходимым для решения насущных проблем интероперабельности.

42. Для разработки совокупности стандартов кибербезопасности важно сначала определить, какие компоненты должны быть безопасными[27]. Это устройство ИВ, система, процесс, организация, данные и/или люди в экосистеме ИВ? Определив эти компоненты, разработчики стандартов могут затем определить сферу применения своих собственных принципов «безопасности по замыслу» и решить, какие аспекты безопасности ИВ должны быть включены как часть их базовых/минимальных требований безопасности. Например, Национальный центр готовности к инцидентам и стратегии кибербезопасности (НЦИК) Японии рассматривает аспекты обеспечения безопасности систем ИВ на этапах проектирования, разработки и эксплуатации как часть своих принципов «безопасности по замыслу»[28]. Целостный подход к определению этих принципов необходим в свете далеко идущего и растущего влияния, которое экосистемы ИВ оказывают на упрощение процедур международной торговли в рамках цепочек поставок.

43. Глобальная разработка базовых требований безопасности все еще находится в зачаточном состоянии и таит в себе огромные возможности для определения протоколов превентивных и корректирующих действий. В существующей литературе отмечается все более сходящаяся тенденция к разработке набора минимальных спецификаций для безопасности ИВ в США и ЕС[29]; однако происходившая в последнее время и продолжающаяся разработка базовых требований выявляет несколько иную картину. В черновой версии своих основных базовых требований НИСТ уделяет больше внимания обеспечению безопасности ИВ на уровне устройств[30],

[25] Brass, I., et al. p.6.

[26] HM Government (UK), «Internet Safety Strategy—Green Paper 2017» (October 2017) p.11. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf (дата обращения: 24 мая 2022 года). Правительство Великобритании определенно склоняется к концепции принятия принципов «безопасности по замыслу», о чем свидетельствуют документ «Secure by Design: Improving the cyber security of consumer Internet of Things Report» («Безопасность по замыслу: отчет об улучшении кибербезопасности потребительского интернета вещей») и добровольный кодекс «Code of Practice for Consumer IoT Security»(«Свод правил безопасности потребительского ИВ»), опубликованные Министерством цифровых технологий, культуры, СМИ и спорта в 2018 году (хотя обе публикации были направлены на защиту интересов потребителей при использовании ИВ-устройств).

[27] Carr, M., et al., «Standards, Governance, and Policy Stream – Governance and Policy Cooperation on the Cyber Security of the Internet of Things» (PETRAS Internet of Things Research Hub, (27 March 2018) pp. 22–23. URL: https://discovery.ucl.ac.uk/id/eprint/10063234/1/Carr_Report_Global-governance-of-the-Internet-of-Things-Report-PDF.pdf (дата обращения: 24 мая 2022 года).

[28] Japan NISC, «General Framework for Secure IoT Systems» (26 August 2016), p. 1. URL: https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf (дата обращения: 24 мая 2022 года).

[29] Brass et al. (n. 12) p. 3. Авторы отметили некоторую повторяемость минимальных требований к безопасности ИВ в документах НИСТ, конкретно посвященных и конкретно не посвященных ИВ: на уровне устройств они могут включать раскрытие уязвимостей, возможность обновления и управление услуговым жизненным циклом. На уровне системы это может включать в себя аутентификацию, авторизацию, контроль доступа, управление криптографическими ключами и управление целостностью.

[30] NIST, «Considerations for a Core IoT Cybersecurity Capabilities Baseline», draft document (2019), pp. 5–9. URL: https://www.nist.gov/system/files/documents/2019/02/01/final_core_ IoT _cybersecurity_capabilities_baseline_considerations.pdf (дата обращения: 24 мая 2022 года). Минимальные требования безопасности на уровне устройства (которые НИСТ предлагает

в то время как Агентство кибербезопасности Европейского союза (АКЕС), наоборот, поддерживает принципы «безопасности по замыслу» и «конфиденциальности по замыслу» (защита данных) на протяжении всего жизненного цикла устройств ИВ и их экосистем[31]. Разработчикам систем ИВ также рекомендуется уделять приоритетное внимание мониторингу безопасности и анализу эффективности.

44. Разработка и внедрение стандартов ИВ сопряжены с трудностями. Технологии ИВ и технологии киберхакеров постоянно развиваются быстрыми темпами. В то же время разработка международных стандартов может занять годы. Например, разработка стандарта ИСО занимает в среднем три года с момента внесения первого предложения до окончательной публикации[32]. Это означает, что разработчикам стандартов постоянно приходится бороться за то, чтобы не отстать от быстро меняющейся сферы кибербезопасности. Другим следствием является то, что все большее число отраслевых ассоциаций стали разрабатывать свои собственные стандарты, чтобы заполнить образовавшуюся пустоту. В результате исполнители сталкиваются с трудностями при оценке и мониторинге разработки стандартов[33], и существует серьезный риск разработки дублирующих стандартов. Таким образом, хотя государственные институты, такие как АКЕС в Европе или НИСТ в США, могут выпускать полезные рекомендации, они могут оказаться недостаточными для обеспечения кибербезопасности ИВ, учитывая все более важную роль экосистем ИВ в упрощении процедур международной торговли.

45. Сотрудничество государственного и частного секторов в разработке стандартов кибербезопасности все чаще воспринимается как жизнеспособный вариант. Экосистема ИВ имеет широкий спектр областей применения. Поэтому может оказаться целесообразным, чтобы заинтересованные стороны в каждом секторе работали коллективно и разрабатывали конкретно отраслевые стандарты кибербезопасности ИВ на основе консенсуса[34]. Например, рекомендация Организации

включить в базовый уровень) включают физическую и логическую идентификацию устройства; обновление программного обеспечения и микропрограммного обеспечения внутри устройства; возможность безопасного изменения конфигурации устройства; возможность контролировать локальный и удаленный доступ к устройству; использование криптографии; и т. д. Учитывая сложность проверки принципов проектирования и вероятную высокую стоимость реализации, НИСТ предлагает исключить практику проектирования и конфигурирования устройства ИВ из базового уровня возможностей кибербезопасности ИВ. См. также NIST, «NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks» (2019), pp. 11–12. URL: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf (дата обращения: 24 мая 2022 года). НИСТ классифицирует риски кибербезопасности для устройств ИВ с точки зрения безопасности устройства, безопасности данных и конфиденциальности. Он также рассматривает прочие аспекты, имеющие решающее значение для снижения рисков, включая управление активами, выявление и устранение факторов уязвимости, управление доступом, обнаружение инцидентов, защиту данных, управление информационными потоками и многое другое. Некоторые из этих аспектов пересекаются с минимальными мерами безопасности, перечисленными в базовых рекомендациях АКЕС по безопасности (см. ниже).

[31] The European Union Agency for Network and Information Security (ENISA), «Baseline Security Recommendations for IoT in the context of critical information infrastructures» (November 2017), pp. 46–52. URL: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport (дата обращения: 24 мая 2022 года). АКЕС классифицирует базовые меры безопасности ИВ по трем направлениям: политика; организационные, кадровые и процессуальные меры; и технические меры. Некоторые из пересекающихся с НИСТ США меры безопасности включают управление активами, выявление и устранение факторов уязвимости и/или инцидентов безопасности, управление доступом, безопасное обновление программного обеспечения/ микропрограммного обеспечения, криптографию, защиту и обеспечение соответствия данных и т. д.

[32] ISO, «Developing Standards» https://www.iso.org/developing-standards.html (дата обращения: 24 мая 2022 года).

[33] Brass, I., et al. p.6.

[34] OECD, *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document* (OECD Publishing, Paris, 2015). URL: http://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm (дата обращения: 24 мая 2022 года).

экономического сотрудничества и развития (ОЭСР) по цифровой безопасности стимулирует координацию и сотрудничество между всеми заинтересованными сторонами (включая правительства и частный сектор), которые полагаются на «цифровую среду для всей или части своей экономической деятельности»[35]. Проводя параллельное сравнение с юридическим сектором, Международная ассоциация юристов (МАЮ), например, наладила диалог между различными заинтересованными сторонами в сфере юридической профессии с целью разработки рекомендованного списка видов передовой практики, призванного помочь юридическим фирмам защититься от угроз кибербезопасности[36]. В рамках этого процесса к разработке руководства по кибербезопасности, касающегося укрепления технологической инфраструктуры юридических фирм, организационных процессов и политики обучения персонала, были привлечены практикующие юристы, эксперты в области права, ИТ-специалисты и консультанты по кибербезопасности[37].

46. Для того чтобы экосистема ИВ играла ключевую роль в торговле, важно привлечь отраслевых экспертов и собрать вместе различные заинтересованные стороны (включая разработчиков ИВ, торговых экспертов и специалистов по кибербезопасности), призванные совместно определить, что и как необходимо обезопасить для дальнейшей активизации глобальной торговли.

B. Роль торговых соглашений и электронной торговли

47. Следует отметить, что лишь недавно в международные торговые соглашения были включены специальные главы, посвященные вопросам, связанным с электронной торговлей, как это задокументировано в публикации «Facilitation 2.0: E-Commerce and Trade in the Digital Age» («Упрощение 2.0: Электронные коммерческие операции и торговля в цифровую эпоху»). Эти вопросы включают ограничение потоков цифровых данных и проблемы кибербезопасности. В 2007 году Международный союз электросвязи (МСЭ) запустил Глобальную повестку дня по кибербезопасности в качестве основы для международного сотрудничества государств-членов с целью укрепления доверия и безопасности в контексте новейших технологий. Комиссия Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ) сыграла важную роль в упрощении процедур международной торговле путем модернизации правил глобальной торговли. Ее Типовой закон об электронных передаваемых записях (ТЗЭПЗ) зиждется на принципах функциональной эквивалентности и технологической нейтральности, лежащих в основе всех документов ЮНСИТРАЛ по электронной торговле. В перечне критериев для оценки общего стандарта надежности электронных передаваемых записей в главе III, статья 12, есть конкретная ссылка на «безопасность аппаратного и программного обеспечения». Это важно, поскольку безопасность аппаратного и программного обеспечения напрямую влияет на надежность метода, используемого странами для упрощения процедур трансграничной цифровой торговли, особенно когда данные берутся из экосистем ИВ.

48. Как правило, страны могут принять международные или основанные на консенсусе стандарты в качестве основы для торговых соглашений, чтобы поддержать «развитие глобально согласованных и наименее ограничивающих торговлю подходов к кибербезопасности»[38]. Однако стороны, заключающие соглашения, должны сначала договориться о том, какие стандарты кибербезопасности и/или инфраструктуру кибербезопасности каждая из них считает взаимоприемлемыми или эквивалентными в рамках своей нормативной/законодательной базы ИВ, а это очень часто является спорным вопросом. Кроме того, не стоит недооценивать напряженность, связанную с вопросами национальной безопасности и кибербезопасности, поскольку переплетение

[35] Ibid. p. 8.

[36] International Bar Association (IBA), «Cybersecurity Guidelines by the IBA's Presidential Task Force on Cybersecurity» (2018), p. 4. URL: https://dokumen.tips/documents/cybersecurity-guidelines-hspi-attacking-unsecured-wi-fi-connections-eg-public.html?page=1 (дата обращения: 24 мая 2022 года).

[37] Ibid, p. 6–21.

[38] https://www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right/.

многочисленных интересов требует тщательного рассмотрения и является довольно сложным балансированием. Продолжающиеся споры, связанные с международной торговлей и правом собственности на данные ИВ, применением международного права в цифровом пространстве, а также стремление сохранить государственный суверенитет будут и дальше создавать серьезные препятствия для разработки системы стандартов кибербезопасности на глобальном уровне.

VI. Заключение и предлагаемые направления дальнейшей работы СЕФАКТ ООН

49. Интернет вещей как технологию в ближайшем будущем ожидает взрывной рост с распространением систем связи, например, использующих технологию 5G. Учитывая этот контекст, СЕФАКТ ООН занимает идеальное положение для того, чтобы стимулировать разработку новых технических спецификаций для расширения использования ИВ в торговле и, в то же время, повысить способность существующих стандартов удовлетворять потребности развивающейся технологической среды.

A. Интероперабельность

50. Развитие ИВ привело к тому, что различные производители и разработчики приложений используют различные технологии, стандарты и протоколы связи для сбора информации и обмена ею. По мере расширения использования ИВ будет расти потребность в обеспечении интероперабельности, чтобы различные устройства и системы ИВ могли обмениваться информацией друг с другом.

51. Это та область, где СЕФАКТ ООН может сыграть важную роль в разработке и стимулировании использования стандартов данных для интероперабельности ИВ.

B. Обнаружение ресурсов

52. В контексте трансграничной торговли использование ИВ будет генерировать данные, которые могут быть получены в одной системе, обработаны в другой системе и сохранены в третьей системе, причем все они могут находиться в режиме онлайн и в различных юрисдикциях. Ключевые элементы, такие как информация об устройстве ИВ, используемом для сбора данных или событий, или элементы данных, собираемые как часть потока событий, должны быть доступны для обнаружения, чтобы обеспечить прозрачность и видимость всей цепочки поставок.

53. Как и в случае с технологией блокчейн, ИВ также представляет возможность для СЕФАКТ ООН сыграть важную роль в устранении этого пробела и разработать спецификации, которые позволят различным системам и платформам обнаруживать такие ресурсы, как идентифицирующая информация, информация о событиях и т. д.

C. Нормативно-правовая база

54. Динамичный характер угроз кибербезопасности требует проактивного подхода к устранению и снижению таких рисков. Недавняя тенденция на пути интеграции функций кибербезопасности в устройства и программное обеспечение ИВ с использованием принципов «безопасности по замыслу» — это шаг в правильном направлении. Принятие подхода, основанного на участии многих заинтересованных сторон, с постоянным диалогом между заинтересованными сторонами как в государственной, так и в частной сферах, имеет важное значение для определения оптимальной формы и содержания стандартов безопасности ИВ. Углубленное сотрудничество между организациями, устанавливающими стандарты ИВ, может эффективно способствовать разработке всеобъемлющего набора стандартов кибербезопасности для экосистем ИВ. В конечном счете, торговля и кибербезопасность — это два винтика в колесе ИВ. Снижение рисков

кибербезопасности в экосистемах ИВ за счет использования стандартов в значительной степени способствовало бы обеспечению безопасности международной торговли.

D. Потребности в данных для приложений, касающихся интернета вещей

55. В рамках Проекта использования смарт-контейнеров была усовершенствована БКК СЕФАКТ ООН путем добавления 120 новых элементов данных для поддержки применения устройств ИВ в контейнерах. Это только одно приложение ИВ, и поэтому есть возможности для сотрудничества с разработчиками приложений в других областях, чтобы выявить данные ИВ, которые требуют определения, но которые еще не включены в текущие стандарты СЕФАКТ ООН. Учитывая, что для систем ИВ характерна частая передача небольших массивов данных, может также возникнуть потребность в удовлетворении этой потребности в рамках усилий по стандартизации и гармонизации и дальнейшего развития СТДО/ССТ и БКК.

56. Сфера использования ИВ со временем будет только расти, а также будет все больше совместима в операционном отношении с другими развивающимися технологиями, такими как технология блокчейн, ИИ, технологии 5G и платформы ИПП. Поэтому СЕФАКТ ООН может сыграть значимую роль во взаимодействии с органами по стандартизации для устранения разрыва между существующими стандартами и всеми остальными параметрами, которые могут потребоваться для более широкого внедрения ИВ в приложениях, предусматривающих упрощение процедур торговле.