Экономический и Социальный Совет

Distr.: General
24 February 2023
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Рабочая группа по автомобильному транспорту

Группа экспертов по введению в действие eCMR

Пятая сессия
Женева, 3–5 апреля 2023 года
Пункт 3 a) предварительной повестки дня
Программа работы:
Предлагаемые концепции и процессы будущей системы eCMR

Операционные процедуры, предусмотренные Дополнительным протоколом, касающимся eCMR: цифровая среда*

Представлено секретариатом и Группой экспертов

I. Справочная информация

1. На своей четвертой сессии Группа экспертов обсудила документ ECE/TRANS/SC.1/GE.22/2023/1, представила свои замечания и поручила секретариату пересмотреть его или подготовить на его основе новый документ для нынешней сессии с учетом обсуждений, проходивших в Группе. В этой связи секретариат подготовил документы ECE/TRANS/SC.1/GE.22/2023/3 и ECE/TRANS/SC.1/GE.22/2023/4. После того, как концепции и процессы будут согласованы, они сформируют основу высокоуровневой архитектуры будущей системы eCMR.

2. Группе экспертов предлагается обсудить официальные документы, подготовленные для нынешней сессии.

II. Операционные процедуры, предусмотренные Дополнительным протоколом, касающимся eCMR: цифровая среда

3. Дополнительный протокол, касающийся eCMR, а также цифровая среда накладывают ряд новых требований, которые участвующие стороны должны рассмотреть и согласовать, чтобы в отношении электронных накладных можно было найти международное и устойчивое решение. Следует напомнить, что данные концепции описывают не механизм распространения данных, содержащихся в

* Настоящий [документ] [доклад] был запланирован к выпуску после установленного срока в силу обстоятельств, не зависящих от представившей его стороны.

электронной накладной, а механизм валидации, благодаря которому электронная накладная с правовой точки зрения становится эквивалентом бумажной накладной. Именно в таком ключе необходимо обсудить и согласовать ряд процессов, обусловленных использованием цифровой среды.

A. Аутентификация пользователей

4. В Дополнительном протоколе, касающемся eCMR, говорится об установлении аутентичности накладной (статья 3). Однако в цифровом мире необходимо проводить различие между аутентификацией пользователей и установлением аутентичности электронной накладной (см. раздел «Электронные подписи» ниже).

5. Для того чтобы обеспечить доверие к системе и гарантировать ее взаимное признание всеми заинтересованными сторонами, при входе в систему пользователи должны проходить аутентификацию. Аутентификация пользователей автоматически означает принятие ими прав и обязанностей, предусмотренных Конвенцией КДПГ.

6. Таким образом, все пользователи перед работой в системе должны пройти аутентификацию с помощью различных средств, согласованных пользователями/сторонами на международном уровне (КВТ/SC.1) (список не является исчерпывающим):

a) национальная система аутентификации (электронные подписи и т. д.);

b) сторонние поставщики;

c) международная база данных пользователей.

7. Каждая договаривающаяся сторона должна объявить о механизмах аутентификации, используемых на ее территории, чтобы все заинтересованные стороны были надлежащим образом оповещены об официальных механизмах аутентификации, используемых в каждой стране. Каждый из таких национальных механизмов аутентификации будет генерировать для своих пользователей уникальный идентификационный номер (id).

8. Очевидно, что при создании электронной накладной весьма полезно знать уникальный национальный идентификатор каждого пользователя, так как это позволит сэкономить время и повысить удобство работы с системой для ее пользователей. Однако, когда число импортеров, экспортеров и перевозчиков, использующих систему, достигнет нескольких тысяч, узнать национальный идентификатор каждого пользователя будет практически невозможно. Возможно, понадобится разработать общие рекомендации по составлению международного списка идентификационных номеров, связанных с национальными идентификаторами, предоставляемыми механизмами аутентификации; эти рекомендации должны будут выполняться в рамках всех ИТ-решений на международном уровне, что будет способствовать дальнейшему упрощению работы с системой. Например:

Международная система идентификаторов	Национальный идентификатор, сгенерированный на основе механизма аутентификации
Страна – Идентификатор ИТ-решения – идентификационный номер	xxxxxx
SW – 03 – 00001	

B. Электронные подписи

9. В статье 3 Дополнительного протокола, касающегося eCMR, содержится прямая ссылка на использование электронных подписей для установления аутентичности электронных накладных, хотя в пункте 2 этой же статьи отмечается, что аутентичность электронной накладной может также устанавливаться с использованием любого другого метода электронной аутентификации, разрешенного законодательством соответствующей страны.

10. Электронные подписи — в случае согласования — будут облегчать следующие процедуры (список не является исчерпывающим):

- завершение оформления накладной сторонами в режиме онлайн;
- внесение оговорок перевозчиком и принятие отправителем;
- передача права распоряжаться грузом;
- изменение грузоотправителем сведений о грузополучателе или предоставление грузоотправителем инструкций;
- принятие получателем доставки груза с оговорками или без них;
- проверка груза таможенными органами и предоставление комментариев.

11. Международной Конвенции КДПГ об электронных подписях не существует. Однако существует ряд решений, которые могли бы способствовать упрощению процедур, обсуждение которых ведется в Группе. В частности:

a) Использование Типового закона ЮНСИТРАЛ об электронных подписях.

Цель Типового закона об электронных подписях (ТЗЭП) заключается в том, чтобы сделать возможным и облегчить использование электронных подписей посредством установления критериев технической надежности, определяющих эквивалентность электронных и собственноручных подписей. В этой связи ТЗЭП может помочь государствам в создании современных, согласованных и справедливых законодательных рамок для эффективного решения вопроса о правовом режиме электронных подписей и придания определенности их статусу. В основу ТЗЭП положены основополагающие принципы, общие для всех текстов ЮНСИТРАЛ, касающихся электронной торговли, а именно принципы недискриминации, технологической нейтральности и функциональной эквивалентности. В ТЗЭП устанавливаются критерии технической надежности, определяющие эквивалентность электронных и собственноручных подписей, а также базовые правила поведения, которые могут служить руководящими принципами для оценки обязанностей и сфер ответственности в отношениях между подписавшим лицом, доверяющей стороной и доверенными третьими сторонами, участвующими в процессе подписания. Наконец, в ТЗЭП содержатся положения, благоприятствующие признанию иностранных сертификатов и электронных подписей на основе принципа эквивалентности по существу, в соответствии с которым место происхождения иностранной подписи не принимается во внимание. К Типовому закону прилагается Руководство по принятию, в котором содержится справочная и пояснительная информация, призванная помочь государствам в подготовке необходимых законодательных положений, и которое может служить руководством для других пользователей текста.

b) Внесение поправок в Дополнительный протокол, касающийся eCMR

Включение в национальное законодательство типового закона ЮНСИТРАЛ об электронных подписях могло бы быть более эффективным способом создания международного и согласованного способа использования электронных подписей, особенно среди договаривающихся сторон Дополнительного протокола, касающегося eCMR. Однако, поскольку изменение национального законодательства может оказаться весьма длительным процессом, особенно в тех странах, где законы об электронных подписях уже существуют, но не

соответствуют типовому закону ЮНСИТРАЛ, и так как усилия Группы направлены на то, чтобы международное и устойчивое согласованное решение по электронным подписям появилось как можно скорее, временным решением может стать внесение изменений в Дополнительный протокол, касающийся eCMR. Включения в Дополнительный протокол, касающийся eCMR, нового общего положения, которое станет обязательным для всех договаривающихся сторон, будет достаточно для того, чтобы положить начало осуществлению операций eCMR. Возможную поправку можно сформулировать следующим образом: «*Заинтересованные стороны, выдающие электронные накладные, должны использовать электронные подписи, сгенерированные в соответствии с их национальным законодательством. Договаривающиеся стороны, связанные Дополнительным протоколом eCMR, принимают электронные подписи, сгенерированные другими договаривающимися сторонами*».

C. Решения в области информационных технологий (ИТ-решения)

12. Субъект, заинтересованный в использовании электронных накладных КДПГ, должен использовать для разработки того или иного электронного решения, позволяющего создавать электронные накладные, функциональные и технические спецификации, разработанные Группой экспертов и принятые Рабочей группой по автомобильному транспорту.

13. При разработке таких электронных решений следует придерживаться следующих принципов:

- Субъектами могут быть частные компании, занимающиеся информационными технологиями, перевозчики или экспедиторы, у которых есть возможность выделить деньги и время на разработку собственного решения, или же грузоотправители.
- Все организации могут по своему усмотрению выбрать любую технологию, при условии, что они придерживаются предоставленных им спецификаций, призванных обеспечить применение Конвенции КДПГ.
- Субъекты должны решить, взимать или не взимать плату за свои услуги.
- Поставщики ИТ-услуг не должны иметь доступ для чтения/изменения данных накладных КДПГ, генерируемых с помощью разработанной ими системы, когда эта система находится в открытом доступе. Если транспортная/экспедиторская компания сама разработала систему для обслуживания собственного бизнеса, то доступ к данным должен предоставляться в соответствии с правилами для перевозчиков/отправителей. Поставщики ИТ-услуг должны запрещать торговлю или обмен данными, генерируемыми на их платформе, с целью получения прибыли или в любых других целях, в том числе обусловленных соображениями конкуренции.

D. Национальный валидационный орган

14. Группа провела обсуждение вопроса о необходимости создания национального валидационного органа, по которому пока не удалось достичь договоренности. Основная функция такого органа будет заключаться в том, чтобы обеспечивать соблюдение спецификаций и применение Конвенции КДПГ. Данная идея, равно как и варианты создания других возможных органов, все еще находится на рассмотрении Группы.

15. Идея заключается в том, что национальный орган (национальные органы) должен (должны) официально назначаться правительствами для выполнения следующих обязательств/задач:

- Предоставление технических спецификаций, согласованных на уровне КВТ/SC.1, для разработки платформ, на базе которых создаются eCMR.

- Валидация электронных решений, разработанных на основе этих технических спецификаций (независимо от используемой технологии), и предоставление официального перечня ИТ-решений, одобренных для создания eCMR на территории соответствующей страны. Это также позволит защитить отправителей, перевозчиков и получателей от использования решений, не соответствующих Конвенции КДПГ и спецификациям eCMR, особенно в том, что касается судов, случаев повреждения грузов и т. д.
- Если не будет найдено других решений — выполнение функций резервного/безопасного хранилища всех записей, созданных различными поставщиками ИТ-услуг на соответствующей территории, для будущего использования судебными органами (этой же страны или других стран), а также в случаях банкротства поставщиков ИТ-услуг или технологических сбоев и т. д.
- Мониторинг использования связанных с eCMR услуг на соответствующей территории и сообщение о случаях нарушения/монополистической или олигополистической практики и т. д., противоречащих принципам работы eCMR.
- Временный/окончательный отзыв разрешения на создание eCMR с помощью ИТ-решений, замеченных в вышеупомянутых видах практики, с уведомлением всех заинтересованных сторон системы о факте временного/окончательного отзыва разрешения.

16. Национальный валидационный орган с таким мандатом создаст доверие к системе и обеспечит взаимное признание, необходимое для бесперебойного функционирования международной электронной системы. Правительству каждой страны следует решить, какой орган/какую организацию назначить для выполнения этих задач. Эти задачи могут выполнять различные палаты, национальная ассоциация автомобильного транспорта, новый орган и т. д. При этом правительство обязано официально объявить о создании соответствующего органа и о возложенных на него задачах и обязанностях. Следует отметить, что этот орган должен быть отличным от органа, осуществляющего аутентификацию пользователей (грузоотправителей, перевозчиков и грузополучателей), так как это является отдельной функцией.

E. Безопасное хранение данных

17. Безопасное хранение данных связано с функциями национального валидационного органа; однако данному аспекту следует уделить особое внимание, поскольку обеспечение безопасного хранения данных будет иметь решающее значение для формирования доверительной среды, необходимой для работы будущей системы eCMR.

18. Данные накладных КДПГ содержат информацию, составляющую коммерческую тайну, которая, с одной стороны, не подлежит распространению, а, с другой стороны, не должна концентрироваться в руках небольшого количества ИТ-компаний. В этой связи для обеспечения защиты данных, а соответственно и целостности системы, следует избегать монополистической или олигополистической практики. Однако в условиях свободного рынка, когда та или иная компания может объединиться с другой компанией из соседней страны, приобрести другую компанию из соседней страны или же просто открыть повсеместно филиалы, избежать такой практики практически невозможно. Скорее всего, Группа не сможет предложить какое-то одно решение вместо общих рекомендаций, поэтому такие проблемы необходимо будет решать на национальном уровне.

F. Кибербезопасность — Резервное копирование

19. С вышеуказанной темой и с формированием доверительной среды, в которой должно работать то или иное ИТ-решение, связан также вопрос кибербезопасности. Вопрос целостности данных тесно связан с доверием к системе. Будущая система

eCMR должна прежде всего обеспечивать строгую — не подлежащую изменению — сохранность информации о последовательности событий в соответствии с тем, в какой день и в какое время эти события произошли. Например, в рамках ИТ-решений частных компаний необходимо регулярно проводить резервное копирование данных. При этом необходимо четко разъяснить, где будут храниться эти резервные копии и т. д. Это послужит нескольким целям:

- по запросу можно будет проводить сравнение данных, чтобы удостовериться в представлении исходных данных;
- восстановление данных в случае технологического сбоя ИТ-решения;
- восстановление данных в случае банкротства поставщика ИТ-услуг;
- осуществление резервной процедуры.

20. Участвующие стороны должны соблюдать действующее законодательство в области кибербезопасности, конфиденциальности и т. д.

G. Осуществление резервной процедуры

21. В электронной среде сложно говорить о потере или отсутствии накладной, поскольку всегда есть возможность получить доступ к документу/онлайновым данным на исходной платформе, где эта накладная была создана.

22. В Дополнительном протоколе, касающемся eCMR, нет положения, определяющего резервную процедуру. Резервная процедура будет иметь первостепенное значение для работы будущей системы eCMR в тех случаях, когда по каким-либо причинам система перестанет работать в штатном режиме. Для признания и соблюдения резервной процедуры всеми договаривающимися сторонами требуется, чтобы она была юридически обязывающей процедурой, включенной в Протокол. Секретариат предлагает подготовить положение о включении резервной процедуры в Протокол.

23. Для целей резервной процедуры (в случае прерывания связи с Интернетом, ряда других технологических сбоев и т. д.) в момент заключения договора в режиме онлайн составляется электронный неизменяемый документ (в формате PDF, jpeg и т. д.), который будет автоматически отправлен на электронные адреса сторон накладной (грузоотправителя, перевозчика и, если это будет согласовано, грузополучателя). Этот документ должен иметь «электронную печать»/QR-код с указанием платформы, на которой он был создан, а также даты и места его создания. Возможно, формат этой «электронной печати»/QR-кода будет необходимо включить в технические спецификации системы для обеспечения их согласованности и, следовательно, признания всеми договаривающимися сторонами.

H. Дополнительные обязательства перевозчика при использовании электронных накладных (пункт 1 статьи 6 Дополнительного протокола, касающегося eCMR)

24. Это конкретное положение было буквально скопировано из Монреальской конвенции 1999 года, которая устанавливает ответственность авиакомпаний в случае смерти или телесного повреждения пассажиров, а также в случаях задержки, повреждения или утери багажа и груза. Она унифицировала все различные международные договорные режимы, регулирующие ответственность авиакомпаний, которые бессистемно развивались с 1929 года. Секретариат должен был выяснить, есть ли какая-либо информация о причинах включения пункта 1 статьи 6 в пояснительной записке к Протоколу, касающемуся eCMR.

25. В пункте 2 статьи 4 Монреальской конвенции говорится следующее:

26. Вместо авиагрузовой накладной могут использоваться любые другие средства, сохраняющие запись о предстоящей перевозке. Если используются такие другие

средства, перевозчик, по просьбе отправителя, выдает ему квитанцию на груз, позволяющую опознать груз и получить доступ к информации, содержащейся в записи, сохраняемой такими другими средствами.

27. Возможное объяснение того, почему статья 6 была включена в текст Протокола.

28. В документе TRANS/SC.1/2002/1 (стр. 4), который был представлен ЮНИДРУА (февраль 2002 года), упоминается конкретный пункт: «Этот пункт взят из статьи 4.2 Монреальской конвенции. Статья 4 предусматривает, что “вместо авиагрузовой накладной могут использоваться любые другие средства, сохраняющие запись о предстоящей перевозке”, однако во избежание “доминирования” электронных средств эта статья обязывает, тем не менее, перевозчика выдавать бумажную квитанцию о приеме груза». В этом же документе представлен вопросник, последний вопрос которого был посвящен этому конкретному положению, с тем чтобы выяснить у правительств, согласны ли они с его включением в Протокол.

29. В проекте 2003 года содержится статья 7 с заголовком «Право распоряжаться грузом». В этой статье говорится следующее: «1) В таких случаях, когда выдается электронная накладная, отправитель теряет право распоряжаться грузом, как только перевозчик передает ключ доступа получателю в соответствии со статьей 5». Кроме того, приводится также следующее примечание: «Поскольку электронная накладная выдается не более чем в одном экземпляре, требование о представлении первого экземпляра не применяется. Предоставление ключа, позволяющего вводить инструкции в накладную только лицу, имеющему право распоряжаться грузом, служит гарантией того, что только лицо, имеющее право распоряжаться грузом, будет уполномочено вводить инструкции в транспортную накладную».

III. Описание высокоуровневой архитектуры eCMR

30. Проведенные на сегодняшний день в Группе обсуждения являются основой для формирования описанной ниже высокоуровневой архитектуры будущей системы eCMR. Тысячи грузоотправителей, грузополучателей и перевозчиков должны определенным образом пользоваться услугами сотен частных ИТ-компаний, поставляющих ИТ-решения для eCMR на основе спецификаций ЕЭК ООН. Поскольку при этом будут использоваться пересмотренные (по результатам работы Группы) стандарты СЕФАКТ ООН, необходимо гарантировать операционную совместимость различных систем между собой. Функциональная совместимость — это характеристика системы, детали интерфейсов которой определены исчерпывающим образом для взаимодействия с другими системами, существующими или будущими, в том что касается имплементации или доступа, с обеспечением полной совместимости.

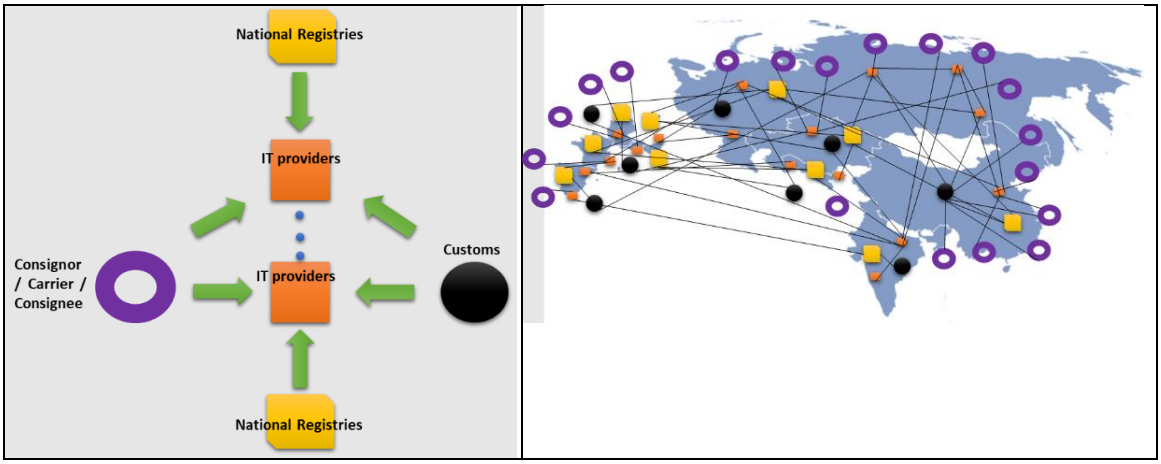
31. В основе ИТ-решений для eCMR будет лежать межмашинный обмен данными, инициируемый определенными событиями. Поэтому для облегчения подключения разных систем друг к другу необходимо четко определить интерфейсы взаимодействия между различными заинтересованными сторонами eCMR. Кроме того, в целях дополнительного облегчения такого подключения интерфейсы должны реализовываться на основе наиболее современных стандартов обмена данными, используемых по всему миру.

32. Однако даже при наличии надлежащих стандартов должно быть предусмотрено требование о необходимости проведения проекта по установлению подключения. Системы на основе ИТ-решений для eCMR должны разрабатываться и документально оформляться таким образом, чтобы облегчить установление подключения с различными сторонами, включая переход на новые версии. Простота подключения позволяет также минимизировать расходы на службу поддержки ИТ-решений в целях оказания содействия сторонам в подключении их собственных систем к ИТ-решениям для eCMR. Конфигурация ИТ-решений для eCMR должна быть настроена так, чтобы доступ к ним через Интернет был закрыт для всех адресов, кроме ограниченного перечня IP-адресов, соответствующих основным серверам заинтересованных сторон Протокола, касающегося eCMR, которые довели свои проекты по подключению до конца. Такой подход позволяет радикально снизить вероятность кибератак на

ИТ-решения для eCMR, способных в том числе вызывать такие последствия, как «отказ в обслуживании» и попытка «подменить» заинтересованную сторону eCMR (спуфинг).

33. С другой стороны, чтобы иметь доступ по требованию к информации системы eCMR, таможенные органы договаривающихся сторон должны иметь доступ (т. е., должны быть подключены) к сотням поставщиков ИТ-услуг.

Высокоуровневая архитектура будущей системы eCMR



Источник: Секретариат

34. С прикладной точки зрения можно выделить три типа пользователей:

- Нерегулярные пользователи: добавляют комментарии к электронной накладной с помощью ссылок определенного типа, отправляемых нерегулярным пользователям. С помощью этих ссылок нерегулярные пользователи смогут переходить на соответствующие веб-сайты. Однако остаются нерешенными вопросы, связанные с аутентификацией этих пользователей и их регистрацией для использования ИТ-решений на основе пройденной аутентификации. Тем не менее число нерегулярных пользователей должно измеряться сотнями тысяч.
- Профессиональные пользователи: нуждаются в интеграции собственных систем на базе ИТ-решений для обслуживания eCMR. Для получения доступа к тому или иному ИТ-решению должно быть предусмотрено несколько методов.
- Органы государственного управления: таможенные органы должны иметь доступ к сотням поставщиков ИТ-услуг.

35. Данный первоначальный проект высокоуровневой архитектуры предполагает осуществление следующих процессов:

- Национальный орган должен валидировать ИТ-решения, распространяемые на его территории, и доводить до сведения других договаривающихся сторон и участников рынка список валидированных решений (подлежит согласованию).
- Предусмотренные национальные механизмы аутентификации должны доводиться до сведения всех договаривающихся сторон. Любой пользователь системы (грузоотправитель, перевозчик, грузополучатель) должен проходить аутентификацию с помощью этих национальных механизмов аутентификации.
- ИТ-решения должны гарантировать, что доступ к соответствующим системам будет предоставляться только аутентифицированным пользователям.
- Перевозчики и грузоотправители из той или иной страны должны иметь возможность использовать ИТ-решения (частные или общедоступные), валидированные в их стране.
- Поставщики ИТ-решений должны обеспечить также безопасное хранение данных в национальном органе, осуществляющем валидацию ИТ-решений, или

же с помощью любого другого решения, выбранного правительством, при условии, что информация о выборе этого решения будет официально доведена до сведения всех договаривающихся сторон (подлежит согласованию).

- Поставщики ИТ-услуг должны обеспечивать возможность включать/принимать в качестве пользователей своих ИТ-решений грузополучателей, экспедиторов, субподрядных перевозчиков и последующих перевозчиков, которые работают за рубежом и прошли аутентификацию с помощью других национальных систем/механизмов аутентификации.
- Различные ИТ-решения из разных стран и регионов должны быть подключены/совместимы. На практике это означает, что если теоретически за один год работы системы eCMR наберется сто поставщиков ИТ-услуг, то для подключения и обеспечения совместимости всех ИТ-решений потребуется четыре тысячи девятьсот пятьдесят (4950) соединений. С практической точки зрения это означает достаточно затратные инвестиции со стороны поставщиков ИТ-решений.
- Кроме того, таможенные органы имеют право запросить данные конкретной накладной, относящейся к прибывающим на их границу транспортным средствам. Эти транспортные средства могут прибывать из любой точки и использовать любое ИТ-решение, валидированное в их стране. На практике это означает, что если на данный момент имеется 58 договаривающихся сторон КДПГ и если в конечном итоге будет найдено решение для введения в действие eCMR и все они ратифицируют Протокол, то 58 таможенных органов должны будут — если это будет разрешено, в первую очередь по соображениям безопасности — подключиться по крайней мере к 100 ИТ-решениям (теоретическое число). Это означает, что каждый таможенный орган, желающий получить доступ для считывания данных, должен выполнить в общей сложности 100 проектов по подключению, т. е. для всех таможенных органов всех договаривающихся сторон необходимо будет выполнить 5800 проектов по подключению.
- Для дорожной полиции и судебных органов в итоге будут действовать те же условия.
- Возникает вопрос о грузополучателях, поскольку именно грузополучатели обычно используют зарубежные ИТ-решения, т. е. ИТ-решения, отличные от тех, которыми пользуются грузоотправитель и перевозчик. Число подключений, необходимых грузополучателям, будет зависеть от количества их торговых партнеров, количества перевозчиков/экспедиторов, услугами которых они пользуются, и т. д. Кроме того, на налаживание таких подключений будет уходить не так много времени, как, например, в случае таможенных органов.
- На данный момент, по приблизительным подсчетам, каждый год оформляется более 600 млн накладных КДПГ. Это очень крупный рынок, и 100 поставщиков ИТ-услуг/ИТ-решений, о которых идет речь в нашем сценарии, это, скорее всего, пессимистичная оценка.
- Следует также отметить, что Организация Объединенных Наций прилагает усилия для обеспечения надлежащего и устойчивого функционирования eCMR с целью дальнейшего продвижения Конвенции КДПГ в других регионах (Африка, Латинская Америка), привлекая новые договаривающиеся стороны и облегчая автомобильные перевозки в других регионах. С практической точки зрения это означает, что в ближайшие годы можно ожидать резкого увеличения числа пользователей/заинтересованных сторон.

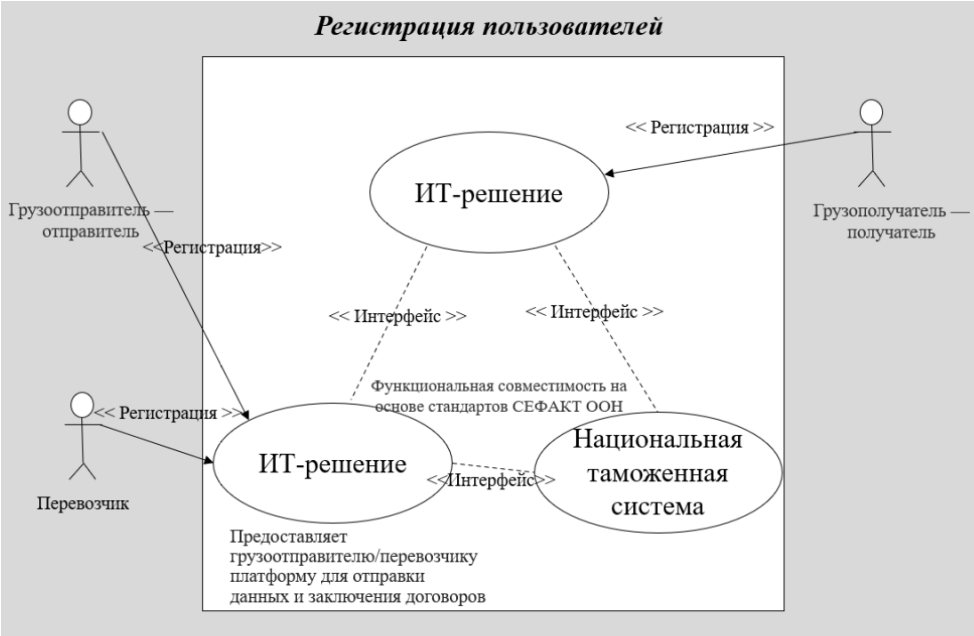
IV. Анализ вариантов использования (примерный перечень)

36. Анализ вариантов использования позволяет получить общее представление о взаимодействиях (вариантах использования), реализуемых между участниками/пользователями.

A. Аутентификация пользователей

Название	*Вариант использования для аутентификации пользователей с помощью национальных механизмов аутентификации*
Описание	Каждый пользователь должен проходить аутентификацию и подтверждать ее с помощью национальных механизмов аутентификации. При регистрации для работы с IT-решениями необходимо использовать доказательство аутентификации (уникальный код?).
Участники	Пользователи
Цели осуществления	Получить доступ к любому ИТ-решению и воспользоваться им могут только аутентифицированные пользователи.
Предварительные условия	Пользователь является авторизованным/ аутентифицированным пользователем.
Постусловия	Пользователю разрешен доступ к любому ИТ-решению.
Сценарий	**Аутентификация** ИТ-решения должны предоставлять возможность проверить, является ли информация, предоставленная пользователем, действительной и зарегистрированной в национальном механизме аутентификации.
Альтернативный сценарий	**Запасной сценарий** Если провести аутентификацию по какой-либо причине не удалось, пользователь будет проинформирован об этом. После этого пользователю необходимо будет исправить предоставленную информацию для успешного прохождения аутентификации.
Специальные требования	Информация о пользователе, необходимая для получения доступа к любому ИТ-решению eCMR

B. Регистрация пользователей



Название	*Регистрация пользователей в ИТ-решениях*
Описание	Для того чтобы иметь возможность отправлять, проверять и получать данные, каждый пользователь должен зарегистрироваться в выбранных им ИТ-решениях.
Участники	Грузоотправитель — отправитель, перевозчик, грузополучатель — получатель
Цели осуществления	–
Предварительные условия	Пользователь, регистрирующийся в любом ИТ-решении, должен сначала пройти аутентификацию с помощью национального механизма аутентификации, при этом для регистрации должен быть предоставлен уникальный идентификатор аутентификации.
Постусловия	Данные пользователя хранятся в ИТ-решении со статусом «авторизован».
Сценарий	Регистрация Для регистрации пользователей в системе используется двухфакторный механизм (адрес электронной почты и номер мобильного телефона), и пользователи уведомляются о результатах регистрации.
Альтернативный сценарий	Запасной сценарий Если регистрация по какой-либо причине не удалась, пользователь будет проинформирован об этом. После этого пользователю необходимо будет исправить предоставленную информацию для успешного прохождения регистрации.
Специальные требования	Пользователи смогут обновлять свою информацию в ИТ-решении и сохранять все относящиеся к их работе файлы, статистические данные и т. д.

C. Создание электронной накладной

Название	*Вариант использования для создания электронной накладной*
Описание	Грузоотправитель или перевозчик создают электронную накладную с помощью выбранного ИТ-решения, включая в нее всю необходимую информацию. Сторона, создающая электронную накладную, должна знать и использовать уникальные коды других партнеров. По согласованию с перевозчиком и грузоотправителем грузополучатель также должен быть проинформирован о создании новой электронной накладной.
Участники	Грузоотправитель, перевозчик
Цели осуществления	Все электронные накладные, выданные грузоотправителю или перевозчику, регистрируются в ИТ-решении.
Предварительные условия	Держатели договора перевозки должны быть аутентифицированы и зарегистрированы в ИТ-решении.
Постусловия	Информация о контракте сохраняется в ИТ-решении со статусом «выдано» или «используется».
Сценарий	**Создание** После того, как отправителем или перевозчиком будет инициировано создание электронной накладной, противоположная сторона получит электронное уведомление о создании новой электронной накладной с просьбой подтвердить ее, предоставив всю информацию, необходимую для накладной eCMR.
Альтернативный сценарий	**Запасной сценарий** В случае если накладную eCMR нельзя переслать IT-решению с помощью каких-либо электронных средств или веб-служб, никакие функциональные запасные варианты не предусмотрены, и та же информация может быть отправлена стороной, декларирующей накладную eCMR, сразу же, как только это станет возможным.
Специальные требования	–