Экономический и Социальный Совет

Distr.: General
4 August 2023
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Рабочая группа по автомобильному транспорту

Сто восемнадцатая сессия
Женева, 17–19 октября 2023 года
Пункт 2 c) iv) предварительной повестки дня
Документы по внутреннему транспорту:
Конвенция о договоре международной дорожной перевозки грузов
Группа экспертов по введению в действие Дополнительного протокола

Часть II доклада Группы экспертов по введению в действие eCMR: Операционные процедуры, предусмотренные Дополнительным протоколом, касающимся eCMR: цифровая среда

Представлено Группой экспертов

I. Справочная информация

1. Настоящий документ содержит часть II доклада GE.22 к сто восемнадцатой сессии SC.1. В его основу положен текст ECE/TRANS/SC.1/GE.22/2023/4/Rev.1 с пересмотренными положениями и конкретными замечаниями различных участников (с учетом опасений, сформулированных МСАТ и его членами), изложенными на шестой сессии GE.22, как это указано ниже.

2. SC.1 предлагается рассмотреть доклад Группы экспертов, состоящий из частей I, II, III и IV (ECE/TRANS/SC.1/2023/2–5), и принять по просьбе Группы экспертов (за исключением Ирана (Исламская Республика)) решение о продлении ее мандата согласно ее нынешнему кругу ведения и плану работы, с тем чтобы завершить выполнение ее задач и представить SC.1 доклад на ее сто девятнадцатой сессии в октябре 2023 года. МСАТ также просил учесть в контексте будущей деятельности GE.22 (в случае продления ее мандата) гибридное решение (т. е. возможность представления транспортным оператором или водителем данных e-CMR различными способами, с тем чтобы они могли быть прочитаны человеком).

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, с тем чтобы в отношении электронных накладных можно было найти международное и устойчивое решение. Следует напомнить, что данные концепции описывают не механизм распространения данных, содержащихся в 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.

Замечания, высказанные на шестой сессии MCAT и его объединениями ABADA, BGL и LAA по пункту 3 при поддержке Ирана (Исламская Республика): как КДПГ, так и eCMR имеют одинаковую юридическую силу, что и указано в статье 2.1 Протокола, поэтому нет никакой необходимости в создании нового механизма валидации, который может оказаться излишне громоздким и дорогостоящим для частного сектора и правительств.

ФИАТА, Ассоциация логистики Словакии и BIFA как представители части частного сектора, а также Правительство Швеции заявили о своем несогласии с замечаниями MCAT и его объединений, а также Правительства Ирана (Исламская Республика).

A. Аутентификация пользователей

Замечания, высказанные на шестой сессии MCAT и его объединениями ABADA, BGL и LAA по пунктам 4–8 при поддержке Ирана (Исламская Республика): Протокол eCMR требует только установления аутентичности накладной, но не аутентификации ее пользователей. В Конвенции КДПГ четко определены пользователи накладной, которыми являются отправитель, перевозчик и грузополучатель. Таможенные органы, полиция, пограничная служба, суды и другие государственные организации не являются пользователями по смыслу КДПГ/eCMR. Обычно они не требуют отдельной аутентификации, а используют доступ для того, чтобы иметь возможность прочитать накладную и отслеживать изменения, вносимые в нее пользователями. MCAT предложил гибридное решение, предполагающее необходимость отпечатать накладную КДПГ, о чем подробно говорится в его заявлении.

ФИАТА, Ассоциация логистики Словакии и BIFA как представители части частного сектора, а также Правительство Швеции заявили о своем несогласии с замечаниями MCAT и его объединений, а также Правительства Ирана (Исламская Республика).

GE.22 не согласна с позицией MCAT, его объединений и Правительства Ирана (Исламская Республика), поскольку она противоречит текущему мандату Группы, сути Протокола eCMR и ЦУР 12 и 13, касающимся ответственного потребления и производства, а также борьбы с изменением климата.

4. В Дополнительном протоколе, касающемся eCMR, говорится об установлении аутентичности накладной (статья 3). Однако с учетом мандата группы, который касается введения в действие eCMR и высокоуровневой архитектуры будущей системы eCMR, эксперты определили следующие два требования в отношении аутентификации:

a) аутентификация пользователей;

b) установление аутентичности накладной в ее окончательном виде.

5. Для того чтобы обеспечить доверие к системе и гарантировать ее признание всеми пользователями, необходимо проводить аутентификацию пользователей при входе в систему. Аутентификация пользователей автоматически означает принятие ими прав и обязанностей, предусмотренных Конвенцией КДПГ. В качестве пользователей Группа определила следующих лиц:

a) грузоотправитель/отправитель;

b) перевозчик/последующий перевозчик/экспедитор/субподрядчик;

c) грузополучатель/получатель;

d) таможенные органы;

e) полиция/пограничная служба;

f) суды и другие государственные учреждения.

6. В качестве механизмов аутентификации пользователей и электронных накладных следует применять те механизмы, которые уже используются или предусмотрены в национальном законодательстве Договаривающихся сторон Дополнительного протокола, касающегося eCMR.

7. Исходя из соображений транспарентности и эффективности каждая из Договаривающихся сторон Протокола eCMR, возможно, пожелает объявить о механизмах аутентификации, используемых на ее территории, с тем чтобы все заинтересованные стороны были надлежащим образом оповещены об официальных механизмах аутентификации, используемых в каждой стране. В каждом из таких национальных механизмов аутентификации для пользователей будет генерироваться уникальный идентификационный номер (id).

8. Очевидно, что при формировании 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. Вместе с тем, когда число импортеров, экспортеров и перевозчиков, использующих систему, достигнет нескольких тысяч, узнать национальный идентификатор каждого пользователя будет практически невозможно. Можно предложить разработать общие руководящие принципы составления 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. Если такие руководящие принципы будут согласованы, то каждый раз при регистрации в системе нового пользователя ИТ-решениями будут автоматически генерироваться уникальные единые номера. В дальнейшем пользователи смогут применять эти уникальные номера при работе со всеми сертифицированными решениями, позволяющими создавать электронные накладные. Такие руководящие принципы могут выглядеть, например, нижеследующим образом. Кроме того, Группа экспертов могла бы произвести оценку существующих решений по уникальным цифровым идентификаторам, если она получит соответствующий мандат в будущем.

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

B. Электронные подписи

Замечания, высказанные на шестой сессии МСАТ и его объединениями ABADA, BGL и LAA по пунктам 9–11 при поддержке Ирана (Исламская Республика): Согласно положениям Протокола eCMR нет никакой необходимости в установлении аутентичности любого из процессов, описанных в документе. Предлагаемая концепция не может навязывать согласованный подход или предусматривать использование Типового закона ЮНСИТРАЛ об электронных подписях в качестве основы для обеспечения такого согласования. Порядок использования электронных подписей и механизмов аутентификации регулируется на национальном уровне и может быть различным в разных странах.

ФИАТА, Ассоциация логистики Словакии и BIFA как представители части частного сектора, а также Правительство Швеции заявили о своем несогласии с замечаниями МСАТ и его объединений, а также Правительства Ирана (Исламская Республика).

9. В статье 3 Дополнительного протокола, касающегося eCMR, содержится прямое указание 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. При этом под электронными подписями или каким-либо другим используемым механизмом не подразумеваются имена пользователей и их пароли.

10. Электронные подписи или любой другой национальный механизм аутентификации будет использоваться для установления аутентичности следующих процедур (список не является исчерпывающим):

a) установление аутентичности накладной в ее окончательном виде, осуществляемое в режиме онлайн сторонами (грузоотправитель/перевозчик);

b) установление аутентичности сделанных перевозчиком оговорок при погрузке груза и его принятии грузоотправителем/отправителем;

c) установление аутентичности передачи права распоряжаться грузом. Одна из основных функций будущей системы eCMR будет заключаться в предоставлении сведений о том, кто именно имеет право распоряжаться грузом на определенных этапах перевозки, когда в подтверждение этого нет второго экземпляра бумажной накладной. Каждый раз при наступлении такого события (см. ECE/TRANS/SC.1/GE.22/2023/3) должно проводиться установление аутентичности;

d) установление аутентичности изменений в отношении грузополучателя/получателя, внесенных грузоотправителем/отправителем, или новых инструкций, выданных грузоотправителем/отправителем. Это событие напрямую связано с ответственностью перевозчика, поэтому необходимо удостовериться в том, кто дает новые инструкции;

e) установление аутентичности подтверждения принятия или непринятия доставки груза грузополучателем с оговорками или без них. Как указано в документе ECE/TRANS/SC.1/GE.22/2023/3, грузополучатель должен совершить два действия, связанных с получением груза, а именно: a) оформить подтверждение доставки и b) оформить подтверждение принятия или непринятия груза. Что касается первого документа, то грузополучатель уже прошел аутентификацию в системе. Что касается подтверждения принятия, то грузополучатель должен пройти аутентификацию, с тем чтобы получить возможность принять груз с оговорками или без оговорок либо не принимать его;

f) аутентификация таможенных органов, проверяющих груз и регистрирующих комментарии, или судебных органов, запрашивающих данные. Речь

идет о тех случаях, когда для получения доступа к каким-либо данным сотрудники таможни должны проходить аутентификацию; это зависит от схемы высокоуровневой архитектуры и от того, как в итоге будут устанавливаться подключения таможенных органов. Поскольку подход, предполагающий регистрацию и аутентификацию таможенных органов в системах сотен поставщиков ИТ-услуг по оформлению электронных накладных для получения возможности запрашивать информацию, представляется нерациональным, данная функция, скорее всего, специально применяться не будет.

11. Никакой международной конвенции об электронных подписях не существует. Вместе с тем в Группе обсуждается ряд решений, которые могли бы способствовать выработке согласованного подхода. В частности, Группа предлагает использовать Типовой закон Комиссии Организации Объединенных Наций по праву международной торговли (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. И 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 содействовать государствам в подготовке необходимых законодательных положений, и которое может служить руководством для других пользователей текста.

C. Решения в области информационных технологий

Замечания, высказанные на шестой сессии МСАТ и его объединениями ABADA, BGL и LAA по пунктам 12–14 при поддержке Ирана (Исламская Республика): Протокол e-CMR регулирует вопросы, относящиеся к международному частному праву. Положения Конвенции не предусматривают использования каких-либо конкретных функциональных и технических спецификаций. По этой причине не существует никаких правовых оснований ни для разработки таких функциональных и технических спецификаций Рабочей группой по автомобильному транспорту (SC.1) и их принятия Комитетом по внутреннему транспорту ЕЭК, ни для рассмотрения их в качестве обязательных. Кроме того, предлагаемый подход, предполагающий обязательное использование таких спецификаций, поставит под угрозу реализацию уже существующих решений. Даже если и потребуются функциональные и технические спецификации для генерации e-CMR, их следует разработать частному сектору и не следует навязывать ему в обязательном порядке. Что касается средств передачи данных, то частному сектору следует предоставить возможность выбора из ряда уже имеющихся у него ИТ-инструментов и

совместимых решений при условии соблюдения требований к оформлению электронной накладной. Согласование должно распространяться на наборы данных, с тем чтобы ими могли обмениваться различные субъекты. Одним из оптимальных примеров могут служить электронные накладные ЦИМ/СМГС для железнодорожных перевозок и e-AWB для грузовых авиаперевозок, которые уже внедрены и функционируют.

ФИАТА, Ассоциация логистики Словакии и BIFA как представители части частного сектора, а также Правительство Швеции заявили о своем несогласии с замечаниями МСАТ и его объединений, а также Правительства Ирана (Исламская Республика).

12. Субъект, заинтересованный в применении электронных накладных КДПГ, должен использовать для разработки того или иного электронного решения, позволяющего создавать электронные накладные при соблюдении Конвенции КДПГ и Дополнительного протокола к ней, функциональные и технические спецификации, принятые Комитетом по внутреннему транспорту ЕЭК на основе предложения Рабочей группы по автомобильному транспорту (SC.1).

13. Экспертам следует решить, будет ли применение функциональных и технических спецификаций носить обязательный характер. Разумеется, что разработка технических спецификаций может быть предусмотрена мандатом будущей новой группы экспертов по ИТ/технической группы экспертов. Вместе с тем в статье 5 Протокола указывается, что сторонам следует договориться о процедурах, т. е. явно подразумевается, что всем сторонам следует согласовать и использовать одни и те же процедуры, поскольку, если они договорятся о процедурах, но не будут их использовать, то желаемый результат достигнут не будет. Оба подхода имеют ряд преимуществ и недостатков. В частности:

a) если спецификации будут носить обязательный характер, то вне зависимости от конкретного используемого ИТ-решения пользователям будет известно следующее:

i) оформленная с их помощью электронная накладная *обладает такой же доказательной силой и влечет за собой такие же последствия, что и* бумажная *накладная* (пункт 2 статьи 2 Протокола);

ii) между Договаривающимися сторонами Протокола существует договоренность относительно *способа, посредством которого сторона, обладающая правами, возникающими на основании электронной накладной, в состоянии продемонстрировать наличие такого права*;

iii) между Договаривающимися сторонами Протокола существует договоренность относительно *процедур дополнения или изменения электронной накладной* и *подтверждения сохранения целостности электронной накладной*;

iv) таким образом, таможенные органы по маршруту следования будут признавать эту электронную накладную в качестве оригинала, а в любом из будущих судебных разбирательств суды будут признавать аутентичность электронной накладной, сформированной в соответствии с Конвенцией;

v) однако если придать спецификациям обязательный характер, то у государств появится еще одно обязательство — проводить сертификацию каждого ИТ-решения. В идеале правительство объявит национальный орган, который будет заниматься подтверждением соответствия этих ИТ-решений спецификациям. Другой, не столь идеальный подход, заключается в том, что в целях облегчения процесса сертификации будет создана центральная платформа для самосертификации (если ее созданием будет заниматься ООН, то понадобится проверка службами правового обеспечения), на которой сами пользователи будут заявлять о соответствии их ИТ-решений функциональным и техническим спецификациям. Для валидации

ИТ-решений также могут быть предусмотрены проверки соответствия. При этом сертифицированные пользователи уведомляются о том, что в случае какой-либо будущей выборочной проверки или, например, в случае возникновении проблем в судебных органах они могут лишиться своего сертификата, и принимают любые репутационные издержки, связанные с этим действием;

b) если спецификации не будут носить обязательный характер, то любой субъект сможет претендовать на оформление электронных накладных в соответствии с Конвенцией КДПГ. Любое существующее на сегодняшний день решение можно будет и впредь использовать в прежнем режиме. Это позволит упростить нынешнее положение дел, которое не является идеальным для использования электронных накладных ввиду того, что попросту невозможно понять, кто применяет Конвенцию, а кто нет:

i) в случае реализации гибридной модели, при которой одни ИТ-решения соответствуют спецификациям, а другие нет, на веб-сайтах решений будет необходимо разместить, по крайней мере, обязательное заявление о том, что то или иное решение «соответствует спецификациям ООН в отношении электронных накладных» либо «не соответствует спецификациям ООН в отношении электронных накладных»;

ii) благодаря этому соответствующая информация будет доводиться до пользователей, которые смогут осознать и решить, хотят они использовать ту или иную платформу или нет;

iii) таможенным органам будет еще сложнее, поскольку практически вся работа по созданию функциональных и технических спецификаций была направлена на то, чтобы государственные учреждения совместно признали эти решения, доверяли им и приступили к их использованию на международном уровне. В случае реализации гибридной модели таможенные органы будут вынуждены использовать только те ИТ-решения, которые соответствуют техническим спецификациям;

iv) если высокоуровневая архитектура в контексте подключения таможенных органов, будет реализована исходя из модели центральной платформы для установления подключений, то это дополнительно упростит ситуацию, поскольку в этом случае только сертифицированные ИТ-решения будут уполномочены подключаться к центральной платформе и предоставлять данные таможенным органам.

14. При разработке таких электронных решений следует придерживаться нижеприведенных принципов:

a) субъектами могут быть любые структуры, заинтересованные в разработке электронного решения, причем как частные, так и государственные организации;

b) субъекты могут по собственному усмотрению выбрать любую технологию при условии, что они придерживаются предоставленных им спецификаций, призванных обеспечить применение Конвенции КДПГ. Следует еще раз подчеркнуть, что в случае реализации модели на основе обязательных спецификаций ИТ-решения должны будут сертифицироваться национальным валидационным органом/центральной платформой и т. д.;

c) субъекты должны решить, будет ли взиматься плата за их услуги;

d) поставщики ИТ-услуг не должны иметь доступ для просмотра/изменения данных накладных КДПГ, оформляемых с помощью разработанной ими системы, когда эта система находится в открытом доступе, если только этого не требуется по причинам оперативного характера, причем с согласия пользователей системы. Если транспортная/экспедиторская компания сама разработала систему для обслуживания собственного бизнеса, то доступ к данным должен предоставляться этой компании 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

Замечания, высказанные на шестой сессии MCAT и его объединениями ABADA, BGL и LAA по пунктам 15–17 при поддержке Ирана (Исламская Республика): Нет никакой необходимости в учреждении национального органа по валидации для обеспечения соответствия функциональным и техническим спецификациям. На самом деле ни национальный валидационный орган, ни указанные спецификации в Протоколе e-CMR не предусмотрены. Кроме того, учреждение такого органа ляжет дополнительным бременем на плечи нынешних пользователей e-CMR, о чем уже говорилось выше. Такое предложение затронет и правительства, поскольку на них будет возложен ряд новых обязательств. На самом деле учреждение такого органа наряду с осуществлением прочих обременительных процедур (а именно с формированием платформы для создания eCMR, опубликованием перечня ИТ-решений, хранением данных, резервным копированием и т. д.) обусловлено потребностью в обеспечении соответствия функциональным и техническим спецификациям, разработанным соответствующими органами ЕЭК, и поэтому от данного предложения необходимо отказаться.

ФИАТА, Ассоциация логистики Словакии и BIFA как представители части частного сектора, а также Правительство Швеции заявили о своем несогласии с замечаниями MCAT и его объединений, а также Правительства Ирана (Исламская Республика).

15. 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. Однако если будет предложено использовать валидационный орган, то Группа предлагает согласовать процедуры валидации (проверки соответствия).

16. Основная идея состоит в том, что национальный орган (национальные органы) должен (должны) официально назначаться правительствами для выполнения следующих обязательств/задач:

a) предоставление технических спецификаций, согласованных на уровне КВТ/SC.1, для разработки платформ, на базе которых создаются eCMR;

b) утверждение электронных решений, разработанных на основе этих технических спецификаций (независимо от используемой технологии), и предоставление официального списка ИТ-решений, одобренных для создания eCMR на территории соответствующей страны (а также признанных Договаривающимися сторонами Протокола eCMR. (Замечание Ассоциации логистики Словакии и MCAT: на практике это реализовать нелегко.) Это также позволит защитить отправителей, перевозчиков и грузополучателей от использования решений, не соответствующих Конвенции КДПГ и спецификациям eCMR особенно в том, что касается судов, повреждения грузов и т. д.;

c) мониторинг использования связанных с eCMR услуг на соответствующей территории и уведомление о случаях нарушения/монополистической или олигополистической практики и т. д., противоречащих принципам работы eCMR;

d) временный/окончательный отзыв разрешения на создание eCMR с помощью ИТ-решений, замеченных в вышеупомянутых видах практики, с уведомлением всех пользователей системы о факте временного/окончательного отзыва разрешения.

17. Национальный валидационный орган с таким мандатом позволит создать доверие к системе и обеспечит его всеобщее 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, органы по аккредитации, какая-либо новая структура и т. д. При этом правительство обязано официально объявить о создании соответствующего органа и о возложенных на него задачах и обязанностях. Следует отметить, что речь не идет об органе, осуществляющем аутентификацию пользователей (грузоотправителей, перевозчиков и грузополучателей), поскольку это отдельная функция.

E. Безопасное хранение данных

Замечания, высказанные на шестой сессии МСАТ и его объединениями ABADA, BGL и LAA по пунктам 18–20 при поддержке Ирана (Исламская Республика): Поскольку в учреждении национального валидационного органа нет необходимости, это же касается и безопасного хранения данных. Необходимо произвести юридическую оценку для выяснения того, будет ли этот так называемый национальный валидационный орган иметь право хранить коммерческие данные в соответствии с положениями национального законодательства каждой из Сторон Протокола e-CMR. Если эти данные могут быть сохранены, то сроки их хранения также необходимо юридически оценить, так как они устанавливаются на национальном уровне. С учетом вышеизложенного согласованный подход навязан быть не может.

ФИАТА, Ассоциация логистики Словакии и BIFA как представители части частного сектора, а также Правительство Швеции заявили о своем несогласии с замечаниями МСАТ и его объединений, а также Правительства Ирана (Исламская Республика).

18. Безопасное хранение данных (т. е. «*оригинала электронной накладной с изменениями, перечисленными в хронологическом порядке*») имеет решающее значение для формирования доверительной среды, необходимой для использования будущей системы eCMR.

19. Данные накладных КДПГ содержат информацию, составляющую коммерческую тайну, которая, с одной стороны, не подлежит распространению, а, с другой стороны, не должна оказываться в руках небольшой группы 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 компании могут объединяться с компаниями из соседних стран, приобретать другие компании из соседних стран или же просто открывать повсеместно филиалы, избежать такой практики практически невозможно. Скорее всего, Группа не сможет предложить вместо общих рекомендаций какое-то одно решение, поэтому такие проблемы необходимо будет решать на национальном уровне.

20. Число лет безопасного хранения данных следует согласовать. Группа в предварительном порядке решила, что содержащиеся в eCMR сведения следует хранить в течение десяти лет после их передачи для использования в будущем любой государственной или частной организацией.

F. Кибербезопасность — Резервное копирование

Замечания, высказанные на шестой сессии МСАТ и его объединениями ABADA, BGL и LAA по пунктам 21–23 при поддержке Ирана (Исламская Республика): Поскольку в учреждении национального валидационного органа нет необходимости, это же касается и методов обеспечения кибербезопасности/резервного копирования. В том случае, если сторонам

договора перевозки все же необходимо повысить кибербезопасность или обеспечить резервное копирование данных, они вольны принимать решения по собственному усмотрению. Вопросы, связанные с кибербезопасностью и резервным копированием, регулируются на национальном уровне, поэтому вряд ли можно навязать согласованный подход.

ФИАТА, Ассоциация логистики Словакии и BIFA как представители части частного сектора, а также Правительство Швеции заявили о своем несогласии с замечаниями МСАТ и его объединений, а также Правительства Ирана (Исламской Республики).

21. С вышеуказанной темой и с формированием доверительной среды, в которой должно функционировать 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 сохранность (не подлежащей изменению) 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:

a) по запросу можно будет проводить сравнение данных, с тем чтобы удостовериться в представлении исходных данных;

b) восстановление данных в случае технологического сбоя в рамках ИТ-решения;

c) восстановление данных в случае банкротства поставщика ИТ-услуг;

d) осуществление резервной процедуры.

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

23. Протокол гласит (пункт 3 статьи 4), что: «п*роцедура, используемая для дополнения или изменения электронной накладной, должна давать возможность непосредственно выявлять любое дополнение или изменение в электронной накладной и сохранять сведения, которые в ней изначально содержались*». При этом в пункте 2 статьи 4 отмечается: «*Процедура, используемая для выдачи электронной накладной, обеспечивает целостность содержащихся в ней сведений с момента, когда она была впервые подготовлена в ее окончательной форме*». Таким образом, исходя из Протокола становится ясно, что в отношении безопасного хранения данных следует придерживаться подхода, основанного на использовании «*оригинала электронной накладной с изменениями, перечисленными в хронологическом порядке*», а не на подходе, основанном на использовании «*электронной накладной в ее окончательной форме после завершения рейса с изменениями, перечисленными в хронологическом порядке*». Очевидно, что в отличие от мировой практики бумажного документооборота, когда бумажная накладная в ее окончательном виде сдается на хранение после завершения перевозки со всеми печатями/подписями, в Протоколе предусмотрен подход, ориентированный на использование *электронной накладной в ее окончательной форме* в тот момент до начала поездки, когда грузоотправителем и перевозчиком была первоначально установлена ее аутентичность.

G. Осуществление резервной процедуры

Замечания, высказанные на шестой сессии MCAT и его объединениями ABADA, BGL и LAA по пунктам 24–26 при поддержке Ирана (Исламская Республика): Поскольку в учреждении национального валидационного органа нет необходимости, это же касается и осуществления резервных процедур. Эта концепция предлагает единое глобальное решение, согласно которому использование QR-кодов и уведомлений по электронной почте будет обозначено в качестве «обязательного», между тем как грузоотправители и перевозчики смогут самостоятельно договариваться о том, какие ИТ-решения, технологии и виды уведомления они будут использовать в соответствии с подпунктом f) пункта 2 статьи 5 Протокола e-CMR. Поэтому согласованный подход к осуществлению резервной процедуры навязать невозможно.

ФИАТА, Ассоциация логистики Словакии и BIFA как представители части частного сектора, а также Правительство Швеции заявили о своем несогласии с замечаниями MCAT и его объединений, а также Правительства Ирана (Исламская Республика).

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

25. В Дополнительном протоколе, касающемся eCMR, нет никаких положений, описывающих резервную процедуру. В то же время в подпункте 2 f) статьи 5 отмечается, что стороны должны достичь договоренности в отношении «*процедур возможной замены электронной накладной, выданной с помощью других средств*», что подразумевает наличие резервной процедуры. 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.

26. Весьма важно определить случаи, в которых необходима резервная процедура, а затем установить используемую резервную процедуру. В нижеследующей таблице сведены воедино различные случаи, когда может потребоваться резервная процедура, и предложена процедура, которой следует придерживаться.

Случаи, когда может потребоваться резервная процедура	**Резервная процедура, которой следует придерживаться**
Процессы, связанные с инициированием составления электронной накладной/оформлением электронной накладной в ее окончательном виде/установлением аутентичности электронной накладной в ее окончательном виде:	1. Использование бумажной накладной
a. Функциональный сбой или возникновение ошибок	a. Система должна отреагировать, предоставив инструкции по решению проблемы b. У пользователей должна быть возможность автоматически связаться с администратором системы для решения проблемы c. Использование другой системы/ИТ-решения
b. Отсутствие доступа из-за отключения интернета/электроэнергии	b. Использование бумажной накладной

Случаи, когда может потребоваться резервная процедура	Резервная процедура, которой следует придерживаться
В случае возникновения проблем по маршруту следования, например в случае отсутствия Интернета в том или ином пункте пересечения границы, неработающего устройства сотрудников полиции, отсутствия у грузополучателя доступа к Интернету для получения уникального кода (например, QR-кода, штрих-кода), отправляемого для завершения процесса оформления подтверждения доставки и т. д.	Когда была установлена аутентичность электронной накладной в ее окончательном виде: a. следует создать неизменяемый документ в формате pdf, который рассылается всем задействованным пользователям b. если указан номер мобильного телефона перевозчика, то на него отправляется QR-код, который необходимо сохранить в кошельке по аналогии с посадочными талонами c. если в рамках ИТ-решения предоставляется мобильное приложение, то вся информация с QR-кодом будет сохранена в мобильном приложении d. в момент начала рейса предварительную информацию для eCMR получают все таможни по маршруту следования и в пункте назначения, если эти таможни подключены к IT-решению и если перевозчик согласился включить маршрут, по которому он будет следовать (в случае необходимости всегда остается возможность его изменить по ходу выполнения рейса). Таможни смогут проводить анализ рисков задолго до прибытия грузового транспортного средства; в момент его прибытия эта информация уже будет храниться в их системе e. таможенным органам следует принимать бумажные накладные КДПГ f. грузополучателю следует предоставить возможность получать уникальный код как на свою электронную почту, так и на мобильный телефон с помощью механизма двухфакторной проверки

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

27. 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 Дополнительному протоколу, касающемуся eCMR.

28. В пункте 2 статьи 4 Монреальской конвенции говорится следующее: «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».

29. Это возможное объяснение причин, по которым статья 6 была включена в текст Дополнительного протокола, касающегося eCMR.

30. На странице 4 документа TRANS/SC.1/2002/1, 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 также представлен вопросник, последний пункт которого посвящен этому конкретному положению и содержит адресованный правительствам вопрос о том, согласны ли они с его включением в протокол.

31. В проекте 2003 года содержится статья 7, озаглавленная «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

Высокоуровневое описание системы eCMR

Замечания, высказанные на шестой сессии МСАТ и его объединениями ABADA, BGL и LAA по пунктам 33–40 при поддержке Ирана (Исламская Республика): В отличие от того, что предполагалось, процессы, предлагаемые высокоуровневой архитектурой, предполагают внесение ряда изменений в существующую практику. Если эти изменения вступят в силу, то нынешним пользователям eCMR придется перестраивать свою деловую практику, что повлечет за собой увеличение их расходов. В качестве альтернативы — с учетом высокой сложности этой концепции — нынешние пользователи eCMR могут пожелать и впредь использовать бумажные накладные. Вариант eCMR должен сохранить все преимущества бумажного формата, модернизировав систему посредством устранения необходимости в обработке документов и связанных с этим затрат. Задачу разработки реализуемых, индивидуальных и рентабельных решений в контексте eCMR следует возложить на частный сектор.

ФИАТА, Ассоциация логистики Словакии и BIFA как представители части частного сектора, а также Правительство Швеции заявили о своем несогласии с замечаниями МСАТ и его объединений, а также Правительства Ирана (Исламская Республика).

32. Как предусмотрено во вводной части документации по eCMR, конечной целью компьютеризации КДПГ является компьютеризация всего цикла использования накладной КДПГ с момента ее выдачи с отражением всех прав и обязанностей, предусмотренных Конвенцией, с тем чтобы в конечном итоге заменить существующую бумажную накладную КДПГ без изменения базовой концепции самой Конвенции.

33. Составители накладных eCMR — отправители/грузоотправители, перевозчики и при необходимости грузополучатели — смогут использовать любое сертифицированное ИТ-решение для оформления электронных накладных. Благодаря использованию стандартов данных Центра Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям (СЕФАКТ ООН), пересмотренных группой экспертов, будет гарантирована взаимная эксплуатационная совместимость всех электронных решений. Эти электронные решения, отвечающие спецификациям, согласованным на уровне ЕЭК, позволят обеспечить предоставление всех электронных услуг, необходимых для использования электронных накладных, включая все потребности, права, обязанности и процедуры, предусмотренные КДПГ. Именно благодаря этому электронная накладная сможет быть признана юридическим эквивалентом бумажной накладной.

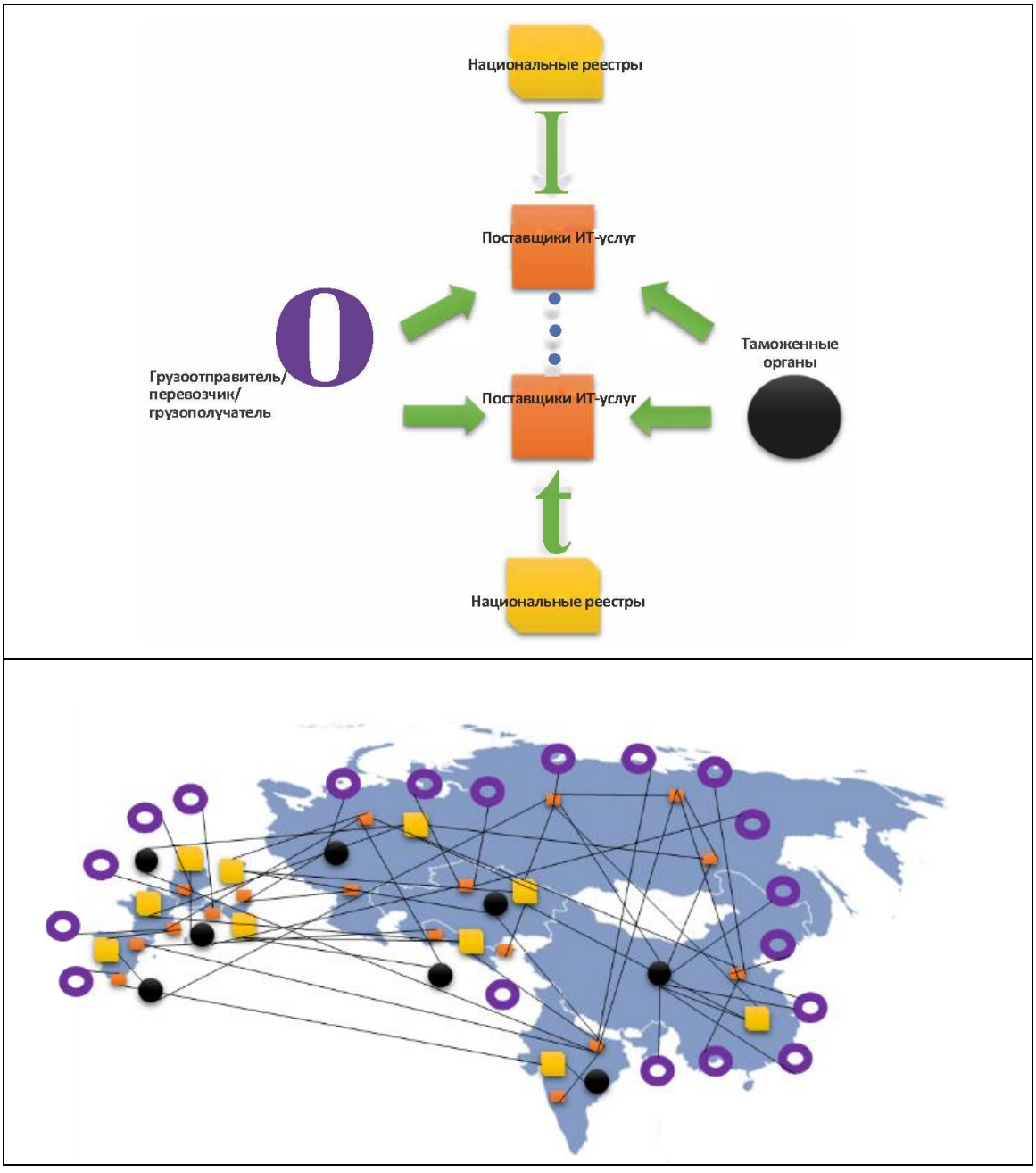
34. Проведенные в Группе обсуждения являются основой для формирования описанной ниже высокоуровневой архитектуры будущей системы eCMR. Следует осознавать, что в будущем тысячи грузоотправителей, грузополучателей и перевозчиков так или иначе должны будут использовать сотни ИТ-решений для eCMR, которые будут или не будут (необходимо будет принять соответствующее решение) функционировать на основе спецификаций ЕЭК ООН. Поскольку при этом будут использоваться пересмотренные (по результатам работы Группы) стандарты СЕФАКТ ООН, следует гарантировать эксплуатационную совместимость различных систем. Эксплуатационная совместимость — это характеристика системы, у которой детали интерфейсов определены исчерпывающим образом для обеспечения взаимодействия с другими системами (существующими или будущими) в контексте имплементации или доступа с обеспечением полной совместимости.

35. 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 пользователями eCMR. Кроме того, в целях дополнительного облегчения такого подключения интерфейсы должны реализовываться на основе наиболее современных стандартов обмена данными, используемых во всем мире.

36. Вместе с тем даже при наличии надлежащих стандартов должно быть предусмотрено требование о необходимости 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, в том числе при переходе на новые версии. Простота подключения позволяет также свести к минимуму расходы на службу поддержки ИТ-решений, оказывающую помощь сторонам в подключении их собственных систем к ИТ-решениям для eCMR.

37. С другой стороны, для того, чтобы в случае необходимости таможенные органы Договаривающихся сторон могли получить доступ к информации, содержащейся в eCMR, они должны иметь доступ (т. е. должны быть подключены) к системам сотен поставщиков ИТ-услуг.

Высокоуровневая архитектура будущей системы eCMR: вариант 1 (децентрализованный подход)



Источник: секретариат.

38. С прикладной точки зрения уместно выделить пользователей следующих трех типов:

a) нерегулярные пользователи: могут добавлять комментарии к электронной накладной, воспользовавшись ссылками определенного типа, отправляемыми нерегулярным пользователям. С помощью этих ссылок нерегулярные пользователи могут переходить на соответствующие веб-сайты. Вместе с тем остаются нерешенными вопросы, связанные с аутентификацией этих пользователей и их регистрацией для использования ИТ-решений на основе пройденной аутентификации. При этом число нерегулярных пользователей должно измеряться сотнями тысяч;

b) профессиональные пользователи: нуждаются в интеграции собственных систем с ИТ-решениями для eCMR. Для получения доступа к тому или иному ИТ-решению следует предусмотреть многочисленные методы.

c) органы государственного управления: таможенные органы должны иметь доступ к системам сотен поставщиков ИТ-услуг.

39. Настоящий первоначальный проект высокоуровневой архитектуры предполагает осуществление следующих процессов:

a) при наличии такой возможности или по согласованию между сторонами национальный орган должен утверждать ИТ-решения, предоставляемые на его территории, и доводить до сведения других Договаривающихся сторон и участников рынка список утвержденных решений (подлежит согласованию);

b) предусмотренные национальные механизмы аутентификации должны доводиться до сведения всех Договаривающихся сторон. Любому пользователю системы (грузоотправителю, перевозчику, грузополучателю) следует проходить аутентификацию с помощью этих национальных механизмов аутентификации;

c) ИТ-решения должны гарантировать, что доступ к соответствующим системам будет предоставляться только аутентифицированным пользователям;

d) перевозчикам и грузоотправителям из той или иной страны следует предоставить возможность использовать ИТ-решения (частные или общедоступные), утвержденные в их стране;

e) поставщикам ИТ-решений следует предоставить варианты безопасного хранения данных в безопасных хранилищах у пользователя или в среде третьей стороны, соответствующей требуемым стандартам безопасности;

f) поставщики ИТ-услуг должны обеспечить возможность включать/принимать в качестве пользователей своих ИТ-решений грузополучателей, экспедиторов, субподрядчиков и последующих перевозчиков, которые работают за рубежом и прошли аутентификацию с помощью других национальных систем/механизмов аутентификации;

g) различные ИТ-решения из разных стран и регионов должны быть подключены/совместимы между собой. 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;

h) кроме того, таможенные органы имеют право по запросу ознакомиться с данными конкретной накладной, относящейся к прибывающим на их границу транспортным средствам. Эти транспортные средства могут прибывать из любой точки и использовать любое ИТ-решение, утвержденное в их стране. Это значит, что если на данный момент насчитывается 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 просмотра данных, должен реализовать в общей сложности 100 проектов по подключению, т. е. для всех таможенных органов всех Договаривающихся сторон необходимо будет выполнить 5800 проектов по подключению;

i) такие же условия в итоге будут распространяться на дорожную полицию и судебные органы;

j) 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 числа их торговых партнеров, числа перевозчиков/экспедиторов, услугами которых они пользуются, и т. д. Кроме того, на установление этих подключений будет уходить не так много времени, как, например, в случае таможенных органов;

k) 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;

l) следует также отметить, что Организация Объединенных Наций прилагает усилия для обеспечения полноценного и устойчивого введения в действие eCMR с целью дальнейшего продвижения Конвенции КДПГ в других регионах (Африка, Латинская Америка), с тем чтобы привлечь новые Договаривающиеся стороны и облегчить автомобильные перевозки в других регионах. С практической точки зрения это означает, что в ближайшие годы можно ожидать резкого увеличения числа пользователей;

m) Другой подход, который необходимо обсудить, заключается в том, что вместо установления подключений всех со всеми (что требует значительных усилий, а также временных и финансовых затрат) можно предоставить возможность подключения к одной центральной платформе, которая будет играть роль мессенджера. У этой платформы должен быть доступ ко всем данным, и в зависимости от запрашиваемой информации она сможет извлекать и передавать данные, взаимодействуя с такими разнообразными ИТ-решениями и государственными органами, как таможня и полиция. Такой подход позволит значительно сократить временные и финансовые затраты на установление подключений, поскольку в этом случае каждая из сторон будет взаимодействовать только с одной центральной платформой.

Высокоуровневая архитектура будущей системы eCMR: вариант 2 (централизованный подход)