Distr.: General
12 August 2021
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Рабочая группа по таможенным вопросам, связанным с транспортом

Группа экспертов по концептуальным и техническим аспектам компьютеризации процедуры МДП

Вторая сессия
Женева, 25–28 мая 2021 года
Пункт 6 d) предварительной повестки дня
Концептуальная, функциональная и техническая документация eTIR — версия 4.3
Технические спецификации eTIR

Технические спецификации eTIR

Оглавление

I. Мандат

1. Комитет по внутреннему транспорту на своей восемьдесят второй сессии (23–28 февраля 2020 года) одобрил (ECE/TRANS/294, пункт 84[1]) учреждение Группы экспертов по концептуальным и техническим аспектам компьютеризации процедуры МДП (WP.30/GE.1) и ее круг ведения[2] (ECE/TRANS/WP.30/2019/9 и ECE/TRANS/WP.30/2019/9/Corr.1) в ожидании утверждения Исполнительным комитетом Европейской экономической комиссии (ЕЭК) Организации Объединенных Наций (Исполком). Исполком на своем дистанционном неофициальном совещании членов Исполнительного комитета (20 мая 2020 года) одобрил учреждение Группы экспертов по концептуальным и техническим аспектам компьютеризации процедуры МДП (WP.30/GE.1) на период до 2022 года на основе круга ведения, содержащегося в документе ECE/TRANS/WP.30/2019/9 и Corr.1, как указано в документе ECE/TRANS/294 (ECE/EX/2020/L.2, пункт 5 b))[3].

2. Кругом ведения Группы предусматривается, что Группе следует сосредоточить свою работу на подготовке новой версии спецификаций eTIR в ожидании официального учреждения технического органа по осуществлению (ТОО). В частности, в соответствии с просьбой WP.30 Группе следует: a) подготовить новую версию технических спецификаций процедуры eTIR и поправки к ним с целью обеспечить их соответствие функциональным спецификациям процедуры eTIR; b) подготовить новую версию функциональных спецификаций процедуры eTIR и поправки к ним с целью обеспечить их соответствие концептуальным спецификациям процедуры eTIR; c) подготовить поправки к концептуальным спецификациям процедуры eTIR.

3. В этом документе представлены имеющиеся на данный момент части технических спецификаций eTIR: общее введение, международная система eTIR, безопасность системы eTIR и несколько приложений.

II. Общее введение

A. Цель

4. Цель технических спецификаций eTIR заключается в преобразовании функциональных спецификаций eTIR в соответствующие технические требования, компоненты архитектуры, руководящие принципы, процедуры и подробные описания всех сообщений, которыми обмениваются между собой международная система eTIR и соответствующие заинтересованные стороны eTIR.

5. Настоящий документ касается всех заинтересованных сторон eTIR (таможенных органов, гарантийных цепей и держателей), которым необходимо подключить свои информационные системы к международной системе eTIR. Все аспекты этих спецификаций должны рассматриваться как обязательные, если не указано иное.

6. Основная цель настоящего документа двоякая: определить технические аспекты международной системы eTIR и однозначно определить, каким образом осуществляется обмен информацией между международной системой eTIR и соответствующими заинтересованными сторонами eTIR.

[1] Решение Комитета по внутреннему транспорту, пункт 84 / ECE/TRANS/294, URL: www.unece.org/fileadmin/DAM/trans/doc/2020/itc/ECE-TRANS-294r.pdf.

[2] Круг ведения недавно созданной Группы, утвержденный Комитетом по внутреннему транспорту и Исполнительным комитетом (Исполком) ЕЭК.

[3] Решение Исполкома ECE/EX/2020/L.2 / пункт 5 b), URL: www.unece.org/fileadmin/DAM/commission/EXCOM/Agenda/2020/Remote_informal_mtg_20_05_2020/Item_4_ECE_EX_2020_L.2_ITC_Sub_bodies_E.pdf.

B. Сфера охвата

7. Настоящий документ состоит из пяти частей: настоящее общее введение, международная система eTIR, связь между заинтересованными сторонами eTIR и международной системой eTIR, процедуры технического обеспечения, а также приложения и добавления. В данном разделе определяется сфера охвата и содержание этих частей.

1. Международная система eTIR

8. Международная система eTIR является краеугольным камнем процедуры eTIR, поскольку она получает и регистрирует информацию, которой она обменивается с таможенными органами, гарантийными цепями и, возможно, держателями. Международная система eTIR разрабатывается, поддерживается, размещается и управляется под эгидой ЕЭК[4].

9. Эта часть начинается с определения трех принципов, которые были выбраны в целях управления деятельностью по развитию международной системы eTIR, обоснованию данного выбора и связанных с ним последствий. Далее в ней подробно описывается общая архитектура системы eTIR[5] и детальная архитектура международной системы eTIR, включая ее компоненты и интерфейсы. В ней также подробно излагаются технические требования к международной системе eTIR, т. е. ряд аспектов, которые непосредственно не связаны с ее функциями, но которые, тем не менее, столь же важны для обеспечения надлежащей работы этой системы. Кроме того, в ней описываются процедуры разработки, включая различные руководящие принципы, а также перечень соответствующих сред и связанных с ними процедур, имеющих целью разъяснить методы, используемые ЕЭК для разработки и поддержания международной системы eTIR. И наконец, последний раздел посвящен техническим требованиям, связанным с информационной безопасностью, и содержит детальное описание модели безопасности системы eTIR.

2. Связь между заинтересованными сторонами eTIR и международной системой eTIR

10. В системе eTIR информационные системы заинтересованных сторон eTIR обмениваются информацией с международной системой eTIR.

11. В этой части подробно описываются технические требования к интерфейсам между информационными системами, а также некоторые аспекты, которым должны следовать информационные системы заинтересованных сторон eTIR. Далее в ней описываются веб-услуги, оказываемые международной системой eTIR, и технические детали, необходимые для их использования. В ней также детально излагаются архитектурные и дизайнерские принципы реализации сообщений, которыми обмениваются соответствующие заинтересованные стороны в контексте процедуры eTIR, и приводятся все технические детали. И наконец, в ней разъясняются проекты по обеспечению взаимосвязи, которые должны быть введены в действие соответствующими заинтересованными сторонами eTIR в целях подключения их информационных систем к международной системе eTIR.

3. Технические резервные процедуры

12. В этой части подробно описываются технические аспекты резервных процедур, которые уже детально описаны в функциональных спецификациях eTIR и которые необходимо соблюдать в случае возникновения проблемы с одним или несколькими компонентами системы eTIR.

[4] В соответствии с пунктом 1 статьи 11 приложения 11 к Конвенции МДП.

[5] См. определение «системы eTIR» в разделе I.F.

4. Приложения и добавления

13. В этой заключительной части представлен технический глоссарий и подробная система записи, используемая в случае архитектурных диаграмм. В ней также представлена соответствующая система анализа в целях определения потребностей в части потенциала и масштабируемости международной системы eTIR. И наконец, в ней содержатся сведения о структуре и соглашениях, используемых для XSD-файлов, а также о списках кодов, используемых в различных атрибутах сообщений eTIR.

C. Целевая аудитория

14. Настоящий документ подготовлен для отделов и специалистов ИТ соответствующих заинтересованных сторон eTIR, желающих использовать процедуру eTIR. В частности, настоящий документ содержит всю информацию, которая требуется соответствующим заинтересованным сторонам eTIR для подключения своих информационных систем к международной системе eTIR.

D. Предварительные условия

15. С этим документом следует ознакомиться после изучения других документов, посвященных спецификациям eTIR, а именно: введения, концепций eTIR и функциональных спецификаций eTIR. Кроме того, следует иметь в виду, что, хотя в настоящем документе и повторяются некоторые ключевые термины и соображения, тем не менее важное значение имеет хорошее понимание Конвенции МДП, и в частности приложения 11 к ней.

16. Предполагается также, что читатели хорошо разбираются в концепциях и терминах ИТ, используемых в этом документе, прежде всего в области разработки программного обеспечения. Они также должны знать, как работают веб-сервисы, и быть знакомы с протоколом SOAP и языком разметки XML.

E. Применимые документы

17. Для того чтобы помочь читателю найти дополнительную информацию, в нижеследующей таблице перечислены и описаны все документы, которые следует использовать вместе с настоящим документом.

Таблица 1
Применимые документы

Название	*Описание*	*Версия или дата*
Справочник МДП	Этот документ содержит полный текст Конвенции МДП, включая приложения к ней (за исключением приложения 11).	2018 год
Сводный текст правовой базы eTIR	В приложении I к докладу о работе семьдесят второй сессии AC.2 содержится подробная информация о принятых изменениях к Конвенции МДП и текст нового приложения 11, в котором описывается процедура eTIR.	17 февраля 2020 года
Введение в концептуальную, функциональную и техническую документацию eTIR	Настоящий документ знакомит читателя с концептуальной, функциональной и технической документацией по процедуре eTIR.	4.3a

Название	*Описание*	*Версия или дата*
Концепции eTIR	В этом документе содержится описание подхода и основных концепций, используемых для поддержки бизнес-логики и реализации международной системы eTIR.	4.3a
Функциональные спецификации eTIR	Целью данного документа является воплощение концепций eTIR в соответствующие спецификации, которые позволяли бы разработчикам программного обеспечения, а также разработчикам сообщений совершенствовать систему eTIR.	4.3a

F. Определения

18. В следующей таблице приведены определения некоторых ключевых терминов, используемых в настоящем документе.

Таблица 2
Определение ключевых терминов

Термин	*Определение*
Сопроводительный документ	Распечатанный документ, составленный таможенной системой в электронном виде после принятия декларации в соответствии с руководящими принципами, содержащимися в технических спецификациях eTIR. Сопроводительный документ может использоваться для регистрации инцидентов по маршруту следования и заменяет собой протокол в соответствии со статьей 25 Конвенции МДП, а также для резервной процедуры.
Участник	См. «Заинтересованная сторона eTIR».
Предварительные данные об изменениях	Данные, представленные компетентным органам страны, в которой запрашивается изменение данных декларации в соответствии со спецификациями eTIR в связи с намерением держателя изменить данные декларации.
Предварительные данные МДП	Данные, представленные компетентным органам страны отправления в соответствии со спецификациями eTIR в связи с намерением держателя поместить груз под процедуру eTIR.
Таможня места отправления	Любая таможня Договаривающейся стороны, в которой начинается перевозка груза или части груза в режиме МДП.
Таможня места назначения	Любая таможня Договаривающейся стороны, в которой завершается перевозка груза или части груза в режиме МДП.
Таможня места въезда	Любое таможенное отделение Договаривающейся стороны, через которую дорожное транспортное средство, состав транспортных средств или контейнер въезжает в данную Договаривающуюся сторону или выезжает из нее в процессе перевозки.
Таможня места выезда	Любая таможня Договаривающейся стороны, через которую дорожное транспортное средство, состав транспортных средств или контейнер въезжает в данную Договаривающуюся

Термин	*Определение*
	сторону или выезжает из нее в процессе перевозки в режиме МДП.
Таможенный союз	Таможенный или экономический союз состоит из двух или более государств-членов и образует единую таможенную территорию в контексте процедуры eTIR при условии, что эти государства-члены являются Договаривающимися сторонами Конвенции МДП и применяют приложение 11.
Система таможенного союза	Центральная информационная система таможенного союза, объединяющая национальные таможенные системы его государств-членов.
Декларация	Акт, посредством которого держатель книжки МДП либо его/ее представитель сообщает в соответствии со спецификациями eTIR о своем намерении поместить груз под процедуру eTIR. С момента принятия декларации компетентными органами — на основе предварительных данных МДП или предварительных данных об изменениях — и передачи данных декларации в международную систему eTIR она представляет собой юридический эквивалент принятой книжки МДП.
Данные декларации	Предварительные данные МДП и предварительные данные об изменениях, которые были приняты компетентными органами.
Электронная гарантия	В контексте процедуры eTIR — электронная версия гарантии, описанная в Конвенции МДП и представленная книжкой МДП в рамках процедуры МДП.
Международная система eTIR	Информационно-коммуникационная технологическая (ИКТ) система, разработанная для обмена электронной информацией между участниками процедуры eTIR.
Процедура eTIR	Процедура МДП, осуществляемая посредством электронного обмена данными, которая служит функциональным эквивалентом книжки МДП. В случае применения положений Конвенции МДП используется процедура eTIR, которая определена в приложении 11.
Служба поддержки eTIR	Одна из функций ЕЭК заключается в оказании заинтересованным сторонам eTIR содействия в подключении их информационных систем к международной системе eTIR.
Спецификации eTIR	Концептуальные, функциональные и технические спецификации процедуры eTIR, принятые или измененные в соответствии с положениями статьи 5 приложения 11.
Заинтересованная сторона eTIR	Субъект, который является частью системы eTIR и пользуется процедурой eTIR, описанной в приложении 11 к Конвенции МДП. Заинтересованная сторона eTIR использует свои информационные системы в качестве части системы eTIR и может быть любым из следующих субъектов: • ЕЭК с международной системой eTIR; • гарантийные цепи с их информационными системами; • таможенные органы с их информационными системами; • держатели с их информационными системами.

Термин	*Определение*
Система eTIR	Контингент всех заинтересованных сторон eTIR вместе с их информационными системами, которые применяют процедуру eTIR, описанную в приложении 11 к Конвенции МДП.
Держатель	В контексте процедуры eTIR держатели книжек МДП больше не держат книжку МДП, так как цель как раз и состоит в том, чтобы заменить бумажную книжку МДП электронной гарантией. Однако в контексте процедуры eTIR термин «держатель» сохраняется и представляет собой то же лицо, которое указано в пункте o) статьи 1 Конвенции МДП.
Национальная таможенная система	Центральная информационная система таможенных органов соответствующей договаривающейся стороны Конвенции МДП. В контексте приложения 11 эта система должна быть подключена к международной системе eTIR.
Предварительная декларация	Данные, отправленные владельцем в соответствующую таможню до предъявления дорожного транспортного средства, состава транспортных средств или контейнера. Это могут быть предварительные данные МДП, предварительные данные об изменениях или отмена ранее отправленных предварительных данных МДП или предварительных данных об изменениях.
Механизм запроса	Набор сообщений, которые могут использоваться заинтересованными сторонами eTIR (I5/I6 в случае таможенных органов и E5/E6 в случае гарантийных цепей) для получения информации, хранящейся в международной системе eTIR, связанной с электронной гарантией, ее держателем и операциями МДП.
Технический орган по осуществлению	Технический орган по осуществлению занимается мониторингом технических и функциональных аспектов осуществления процедуры eTIR, а также координирует обмен информацией по вопросам, входящим в его компетенцию, и содействует его развитию.

G. Сокращения

19. В следующей таблице описаны все сокращения, используемые в настоящем документе. Определения некоторых из этих терминов и выражений можно найти в техническом глоссарии, содержащемся в приложениях к настоящему документу.

Таблица 3
Сокращения

Сокращение	*Описание*
AC.2	Административный комитет Конвенции МДП 1975 года
API	Интерфейс программирования приложений
BGP	Протокол пограничной маршрутизации
CA	Сертификационный орган
CD	Процесс непрерывного развертывания
CI	Процесс непрерывной интеграции

Сокращение	*Описание*
CL	Перечень кодов
CPU	Центральный процессор
DBMS	Система управления базой данных
DMR	Запрос о ведении данных
DOD	Критерии готовности
ЕЭК	Европейская экономическая комиссия Организации Объединенных Наций
ЭДИФАКТ	Электронный обмен информацией в области управления, торговли и транспорта
Гб	Гигабайт
HDD	Жесткий диск
IDS	Система обнаружения сетевых атак
IPS	Система предотвращения вторжений
ИД	Идентификатор
IDE	Интегрированная среда разработки
ИТ	Информационная технология
МБДМДП	Международный банк данных МДП
ИСО	Международная организация по стандартизации
ITIL	Библиотека инфраструктуры информационных технологий
Кб	Килобайт
KMS	Система управления базой знаний
Мб	Мегабайт
MTO	Максимально допустимый период сбоя
MTTR	Среднее время восстановления
OSS	Программное обеспечение с открытым исходным кодом
OWASP	Открытый проект по безопасности веб-приложений
ПКИ	Инфраструктура сертификации открытых ключей
ПРД	Продукция
PRINCE2	Проекты в контролируемой среде 2
RAID	Избыточный массив из независимых дисков
SAN	Совместная сеть хранения данных
SSD	Твердотельный накопитель
SIT	Система интеграционного тестирования
SLA	Соглашение об уровне обслуживания
SOP	Стандартный технологический регламент

Сокращение	*Описание*
SPOF	Единая точка отказа
Тб	Терабайт
TCO	Совокупная стоимость владения
TIB	Технический орган по осуществлению
ИСМДП	Исполнительный Комитет МДП
TOGAF	Базовая архитектура открытых групп
WSDL	Язык описания программных веб-служб
ППТ	Приемочное пользовательское тестирование
ПИ	Пользовательский интерфейс
ООН	Организация Объединенных Наций
UPS	Источник бесперебойного электропитания
ВСВ	Всемирное скоординированное время
UTF	Универсальный формат преобразования набора символов
VCS	Контроль и управление версиями
ВТамО	Всемирная таможенная организация
XML	Расширяемый язык разметки
XSD	Определение схемы XML

H. Доступность

20. Настоящий документ доступен на веб-сайте ЕЭК и на веб-сайте[6], посвященном системе eTIR, на которых читатель может в любое время ознакомиться с самыми последними версиями всех документов, касающихся системы eTIR, включая все технические руководства, используемые в контексте проектов по подключению.

III. Международная система eTIR

21. В данной части описываются все технические аспекты международной системы eTIR и содержится необходимая информация, позволяющая читателю понять, каким образом эта система реализуется на практике, как она управляется, где размещается и каким образом она обслуживается, а также как она должна работать с технической точки зрения.

22. Уровень детализации зависит от описанных здесь аспектов, притом что изложить здесь все технические детали не представляется возможным по следующим двум причинам:

- поскольку этот документ является общедоступным, некоторые технические детали преднамеренно не упоминаются по соображениям безопасности. Хотя ЕЭК признает, что обеспечение безопасности посредством утаивания[7] некоторых данных не должно являться единственной существующей мерой безопасности, она, тем не менее, не желает разглашать слишком большой объем

[6] См. www.etir.org/documentation.
[7] См. www.etir.org/documentation.

информации, которая может быть использована в ущерб безопасности системы eTIR. Договаривающиеся стороны, желающие узнать больше об этих дополнительных деталях, могут связаться с Секретарем МДП в целях организации ознакомительной поездки в штаб-квартиру ЕЭК;

- некоторые аспекты, связанные с используемыми программными или аппаратными продуктами, рамочными программами или библиотеками, а также с соответствующими аспектами реализации на практике, подвергаются регулярным изменениям вследствие быстрого технического прогресса. ЕЭК должна иметь возможность гибкого подхода к регулированию этих аспектов, позволяющего принимать во внимание изменение технических требований (например, в части пропускной способности, масштабируемости и эффективности) без необходимости представлять обновленную версию технических спецификаций.

23. Учитывая тот факт, что некоторые технические детали не упоминаются в настоящем документе, ЕЭК хотела бы сохранить транспарентность и продемонстрировать договаривающимся сторонам свой профессионализм, подробно изложив методы своей работы, свои руководящие принципы и свои процедуры разработки.

A. Руководящие принципы

1. Введение

24. Принципы, изложенные в этом разделе, определяют базовые общие правила и фундаментальные ценности, которыми необходимо будет руководствоваться в процессе принятия решений по техническим аспектам международной системы eTIR (например, в вопросах разработки, размещения, управления, эксплуатации и т. д.). Подход к определению этих трех принципов строится на основе метода отображения принципов архитектуры, детально изложенного в стандарте TOGAF[8].

2. Принцип 1: Информационная безопасность

a) Формулировка

25. Информация, хранящаяся в международной системе eTIR, считается конфиденциальной и доступной в любое время только уполномоченным заинтересованным сторонам с помощью сообщений eTIR, которые должны быть аутентифицированы и защищены.

b) Обоснование

26. В статьях 7 и 8 приложения 11 к Конвенции МДП установлены требования к удостоверению подлинности и целостности данных.

27. В статьях 11 и 12 приложения 11 к Конвенции МДП установлены требования в отношении доступности и целостности данных.

c) Последствия

28. Следует обеспечить конфиденциальность, целостность, доступность и невозможность отказа от информации (данные в процессе транзита), обмениваемой между международной системой eTIR и заинтересованными сторонами eTIR и регистрируемой в международной системе eTIR (хранимые данные).

29. Информация, которая является предметом обмена и которая регистрируется в международной системе eTIR, классифицируется как конфиденциальная информация в соответствии с положениями бюллетеня Генерального секретаря, озаглавленного

[8] См. TOGAF ® Standard v9.2: pubs.opengroup.org/architecture/togaf9-doc/arch/chap20.html.

«Конфиденциальность, классификация и использование информации»[9], а также в соответствии с политикой и мерами в этой области.

3. Принцип 2: Высокий уровень надежности и качества

a) Формулировка

30. Международная система eTIR разрабатывается и поддерживается в соответствии с высокими стандартами надежности и качества, притом что эти стандарты должны постоянно пересматриваться и совершенствоваться.

b) Обоснование

31. Высокая надежность позволяет свести к минимуму затраты на разработку, эксплуатацию и обслуживание международной системы eTIR.

32. Высокая надежность позволяет свести к минимуму ресурсы, которые необходимы заинтересованным сторонам eTIR для разработки, эксплуатации и поддержания взаимосвязи между их информационными системами и международной системой eTIR.

c) Последствия

33. Для разработки, эксплуатации и обслуживания международной системы eTIR следует использовать проверенные передовые методы, применяемые в сфере информационных технологий.

34. Необходимо регулярно оценивать возникающие тенденции в сфере информационных технологий для поиска путей постоянного совершенствования разработки, эксплуатации и обслуживания международной системы eTIR.

4. Принцип 3: Простота подключения для заинтересованных сторон eTIR

a) Формулировка

35. Международная система eTIR должна разрабатываться и документально оформляться таким образом, чтобы облегчить взаимодействие между заинтересованными сторонами eTIR, включая переход на новые версии.

b) Обоснование

36. Простота подключения позволяет свести к минимуму ресурсы, которые необходимы заинтересованным сторонам eTIR для разработки, эксплуатации и поддержания взаимосвязи между их информационными системами и международной системой eTIR.

37. Простота подключения позволяет свести к минимуму расходы на работу служб поддержки eTIR в целях оказания содействия договаривающимся сторонам в подключении их национальных таможенных систем к международной системе eTIR.

c) Последствия

38. Международная система eTIR, ее интерфейсы и документация должны, по мере возможности, разрабатываться с использованием всемирно известных стандартов.

39. В дополнение к спецификациям eTIR следует готовить необходимую документацию, которая должна служить руководством и помогать заинтересованным сторонам eTIR в их проектах по налаживанию взаимосвязи.

40. Благодаря накопленному опыту и полученным отзывам в связи с оказанием помощи заинтересованным сторонам в реализации их проектов по обеспечению взаимосвязи, следует предусмотреть дополнительные улучшения в целях постоянного

[9] См. undocs.org/st/sgb/2007/6.

совершенствования документации и системы помощи, оказываемой службой поддержки eTIR.

B. Общая архитектура системы eTIR

1. Введение

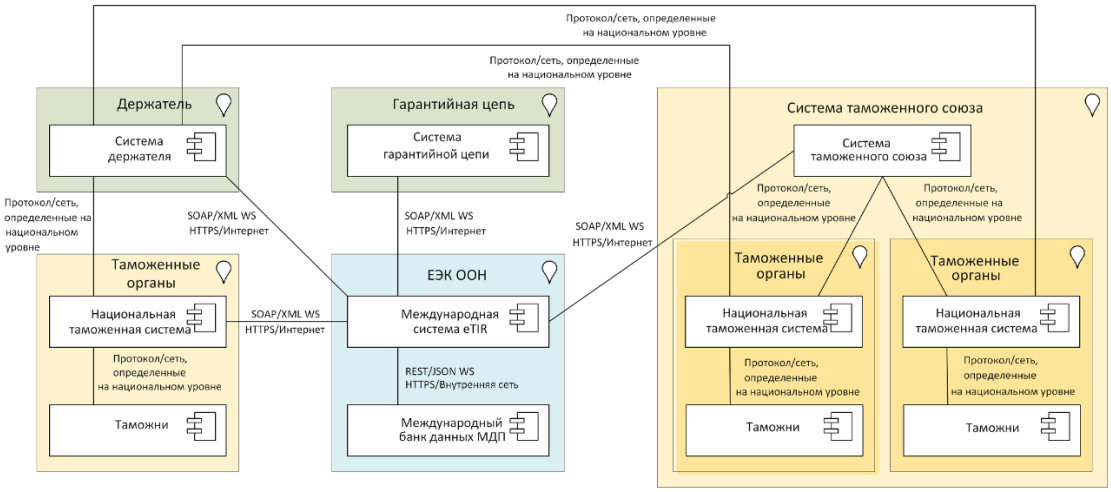
41. В данном разделе представлена общая техническая архитектура системы eTIR и, в частности, взаимодействие между информационными системами различных участников процедуры eTIR. Она также дает более детальное представление об информационных системах каждого участника, включая интерфейсы и сообщения, которыми он обменивается.

42. Диаграммы в этом разделе соответствуют символам языка «ArchiMate»[10], которые описаны в приложении IV.A к настоящему документу.

2. Обзор

43. Система eTIR состоит из взаимосвязанных информационных систем различных сторон, участвующих в процедуре eTIR: таможенных органов, держателей, гарантийных цепей и ЕЭК. Общая техническая архитектура, представленная на рисунке ниже, показывает взаимосвязь между информационными системами всех участников, в том числе таможенных союзов. Они могли бы воспользоваться преимуществами информационных систем и взаимосвязей, которые уже созданы в рамках таможенного союза[11].

Рисунок I
Общая техническая архитектура системы eTIR



44. В следующих разделах представлена более подробная информация об информационных системах каждого участника, в частности о его интерфейсах и сообщениях, которыми он обменивается. Во избежание повторов интерфейсы между двумя информационными системами детально описаны только в разделе, посвященном тому участнику, который инициирует большинство транзакций.

3. Таможенные органы

45. Таможенные органы используют информационные системы для управления таможенными процедурами, такими как импорт, экспорт и транзит. Проект и архитектура этих информационных систем разрабатывается на самостоятельной основе каждым таможенным органом, и поэтому у разных договаривающихся сторон

[10] ArchiMate® 3.0.1 Спецификация. См.: pubs.opengroup.org/architecture/archimate3-doc/.

[11] Как предлагается в пояснительной записке к пункту 2 статьи 3 приложения 11 к Конвенции МДП.

они могут сильно отличаться. Предполагается, что все таможенные отделения связаны с центральной информационной системой таможенных органов, называемой далее «национальная таможенная система».

46. В целях надлежащего осуществления положений приложения 11 к Конвенции МДП и адаптации своих информационных систем к процедуре eTIR таможенные органы должны подключить свою национальную таможенную систему к международной системе eTIR. В контексте процедуры eTIR основными участниками со стороны таможенных органов являются таможенные служащие (находящиеся в таможенных органах), которые производят таможенное оформление перевозок МДП. Хотя необходимо, чтобы все таможенные органы, уполномоченные оформлять перевозки МДП по процедуре eTIR, были подключены к национальной таможенной системе, способ этого подключения определяется каждым таможенным органом. Аналогичным образом, пользовательские интерфейсы, используемые таможенными служащими для работы режиме eTIR, разрабатываются и внедряются в практику каждым таможенным органом.

Рисунок II
Взаимодействие между национальной таможенной системой и таможнями

47. Таможенные служащие обмениваются информацией через свою национальную таможенную систему с международной системой eTIR, используя следующие сообщения, которые позволяют:

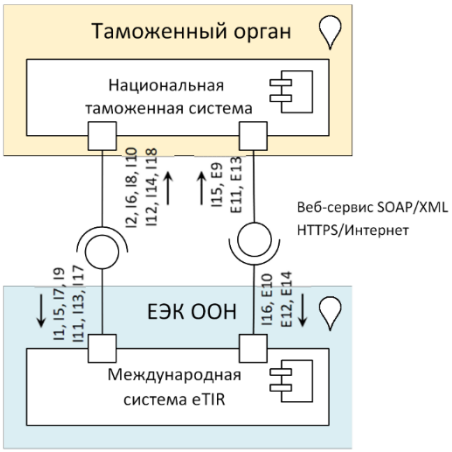
- принять гарантию, выданную на ту или иную перевозку МДП, используя запросное сообщение «I1 — Принятие гарантии» и соответствующее ответное сообщение «I2 — Результаты принятия»;
- запросить всю информацию, связанную с существующей гарантией, используя запросное сообщение «I5 — Запрос на гарантию» и соответствующее ответное сообщение «I6 — Результаты запроса»;
- зарегистрировать данные декларации перевозки МДП, используя запросное сообщение «I7 — Дата регистрации декларации» и соответствующее ответное сообщение «I8 — Результаты даты регистрации декларации»;
- начать операцию МДП применительно к данной перевозке МДП, используя запросное сообщение «I9 — Начало операции МДП» и соответствующее ответное сообщение «I10 — Результаты начала операции»;
- прекратить операцию МДП применительно к данной перевозке МДП, используя запросное сообщение «I11 — Прекращение операции МДП» и соответствующее ответное сообщение «I12 — Результаты прекращения»;
- завершить операцию МДП применительно к данной перевозке МДП, используя запросное сообщение «I13 — Завершение операции МДП» и соответствующее ответное сообщение «I14 — Результаты завершения»;
- отказать в начале операции МДП применительно к данной перевозке МДП, используя запросное сообщение «I17 — Отказ начать операцию МДП» и соответствующее ответное сообщение МДП «I18 — Результаты отказа начать операцию МДП».

48. Кроме того, международная система eTIR может уведомлять национальную таможенную систему о конкретных событиях, связанных с той или иной перевозкой МДП, используя запросное сообщение «I15 — Уведомление таможни» и соответствующее ответное сообщение «I16 — Подтверждение уведомления».

49. В завершение международная система eTIR может направлять информацию со стороны держателя, относящуюся к предварительным данным МДП и предварительным данным об изменениях[12], соответствующим таможенным органам, используя следующие сообщения, которые позволяют:

- получать предварительные данные МДП, отправленные держателем через международную систему eTIR, используя запросное сообщение «E9 — Предварительные данные МДП» и соответствующее ответное сообщение «E10 — Результаты проверки предварительных данных МДП»;
- получать предварительные данные о внесении изменений, отправленные держателем через международную систему eTIR, используя запросное сообщение «E11 — Предварительные данные об изменениях» и соответствующее ответное сообщение «E12 — Результаты проверки предварительных данных об изменениях»;
- получать сообщение об отмене ранее отправленных предварительных данных МДП или предварительных данных о внесении изменений, используя запросное сообщение «E13 — Отмена предварительных данных» и соответствующее ответное сообщение «E14 — Результаты отмены предварительных данных».

Рисунок III
Взаимодействие между национальной таможенной системой и международной системой eTIR



50. Эти сообщения (I1, I2, I5, I6, I7, I8, I9, I10, I11, I12, I13, I14, I15, I16, I17, I18, E9, E10, E11, E12, E13 и E14) передаются по протоколу HTTPS через Интернет с помощью веб-сервисов SOAP, а передаваемые данные форматируются на языке разметки XML.

4. Таможенные союзы

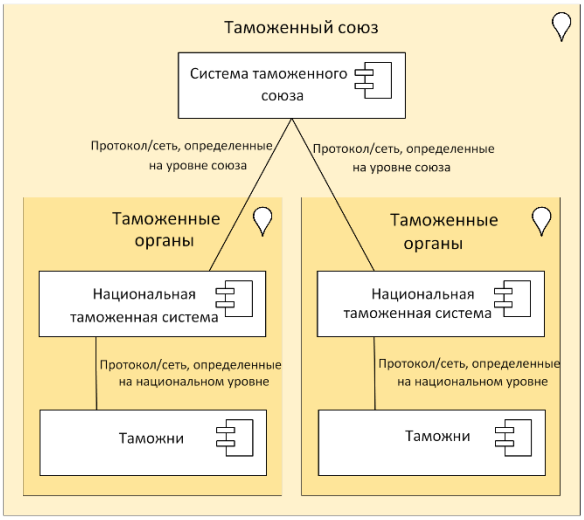
51. Таможенные союзы могут создать центральную систему таможенных союзов в целях содействия обмену информацией между национальными таможенными системами своих государств-членов. Проект и архитектура этих центральных систем таможенных союзов разрабатывается на самостоятельной основе таможенными союзами, поэтому у разных таможенных союзов они могут сильно отличаться.

52. В целях надлежащего осуществления положений приложения 11 к Конвенции МДП и адаптации своих информационных систем к процедуре eTIR государства — члены таможенного союза могут, при желании, подключить свои национальные таможенные системы к международной системе eTIR через свою систему таможенных

[12] В соответствии с пунктами 2 и 3 статьи 6 приложения 11 к Конвенции МДП.

союзов. В этом случае система таможенных союзов направляет сообщения соответствующим получателям и может также действовать в качестве своего рода преобразователя, если сообщения, которыми обмениваются между собой система таможенного союза и национальная таможенная система, не соответствуют спецификациям eTIR.

Рисунок IV
Взаимодействие между системой таможенного союза и национальными таможенными системами



53. Что касается остальной части настоящего документа мы будем считать, если не указано иное, что интерфейс между международной системой eTIR и системой таможенного союза является таким же, как и между международной системой eTIR и национальной таможенной системой.

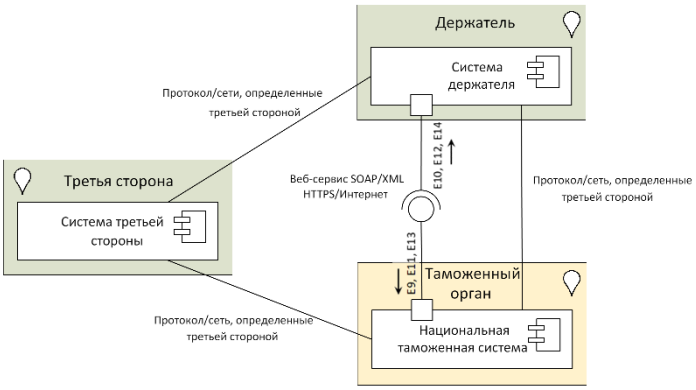
5. Держатели

54. Держатели обязаны представить в таможню места отправления предварительные данные МДП о перевозке МДП, которую они хотят инициировать. Держатель всегда может отменить ранее отправленные предварительные данные МДП и повторно отправить новые предварительные данные МДП. После принятия декларации таможней места отправления держатель может направить «предварительные данные о внесении изменений» следующей таможне места въезда или выезда, с просьбой внести в декларацию требуемые изменения. После этого держатель может отменить ранее направленные предварительные данные о внесении изменений, если они еще не были приняты таможенной службой.

55. Представление такой информации таможенным органам может осуществляться несколькими электронными способами: с веб-портала, управляемого таможенными органами, с использованием веб-сервисов в соответствии со спецификациями eTIR, с веб-портала, управляемого третьим лицом, и т. д. Каждый таможенный орган обнародует полный перечень способов представления такой информации[13]. Все эти электронные средства должны представлять информацию, необходимую в соответствующих сообщениях eTIR: E9, E11 и E13.

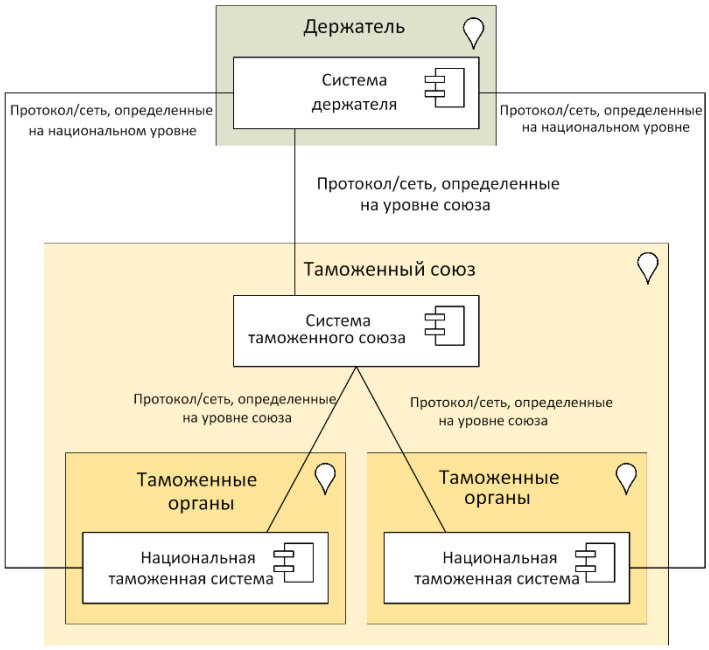
[13] В соответствии с пунктом 4 статьи 6 приложения 11 к Конвенции МДП.

Рисунок V
Возможные взаимодействия между системой держателя и национальной тамо-женной системой



56. В случае таможенных союзов аналогичный подход существует и в случае держателей, которые подают данные предварительной декларации в соответствующие таможенные органы государств-членов, входящих в данный таможенный союз. В дополнение к средствам, которые уже подробно описаны в предыдущем пункте, может быть также предусмотрен дополнительный портал, который создается на уровне таможенного союза.

Рисунок VI
Взаимодействие между системой держателя и системами таможенного союза

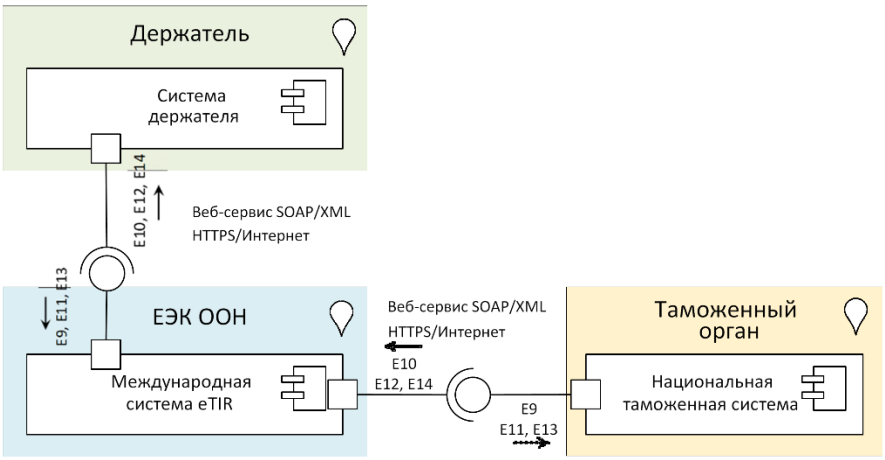


57. Наконец, держатели всегда имеют возможность подать данные предварительной декларации в соответствующие таможенные органы через международную систему eTIR[14], используя следующие сообщения, которые позволяют это сделать:

[14] В соответствии с пунктами 2 и 3 статьи 6 приложения 11 к Конвенции МДП.

- отправить предварительные данные МДП в таможню места отправления по линии международной системы eTIR, используя запросное сообщение «E9 — Предварительные данные МДП» и соответствующее ответное сообщение «E10 — Результаты предварительных данных МДП»;
- отправить предварительные данные об изменениях в соответствующий таможенный орган по линии международной системы eTIR, используя запросное сообщение «E11 — Предварительные данные об изменениях» и соответствующее ответное сообщение «E12 — Результаты проверки предварительных данных об изменениях»;
- отправить в соответствующий таможенный орган через международную систему eTIR уведомление об отмене ранее направленных предварительных данных МДП или предварительные данные об изменениях, используя запросное сообщение «E13 — Отмена предварительных данных» и соответствующее ответное сообщение «E14 — Результаты отмены предварительных данных».

Рисунок VII
Взаимодействие между системой держателя и национальной таможенной системой по линии международной системы eTIR



58. Эти сообщения (E9, E10, E11, E12, E13 и E14) передаются по протоколу HTTPS через Интернет с помощью веб-сервисов SOAP, а передаваемые данные форматируются на языке разметки XML.

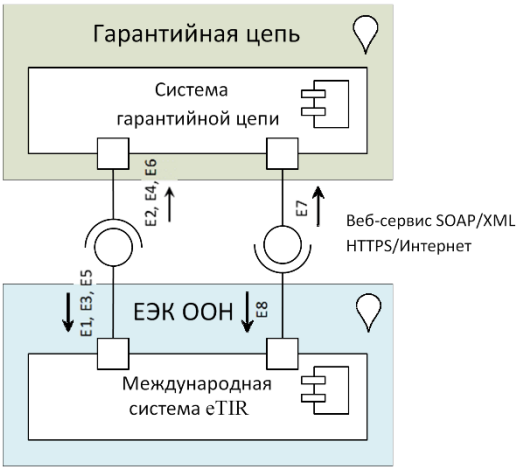
6. Гарантийные цепи

59. Гарантийные цепи управляют информационными системами, используемыми для управления системой электронных гарантий и обмена требуемыми данными с международной системой eTIR, используя следующие сообщения:

- зарегистрировать новую гарантию, используя запросное сообщение «E1 — Регистрация гарантии» и соответствующее ответное сообщение «E2 — Результаты регистрации»;
- отменить существующую гарантию, используя запросное сообщение «E3 — Отмена гарантии» и соответствующее ответное сообщение «E4 — Результаты отмены»;
- запросить всю информацию, связанную с существующей гарантией, используя запросное сообщение «E5 — Запрос в отношении гарантии» и соответствующее ответное сообщение «E6 — Результаты запроса»;

- получать уведомления международной системы eTIR о конкретных событиях, связанных с существующей гарантией, используя запросное сообщение «E7 — Уведомление гарантийной цепи» и соответствующее ответное сообщение «E8 — Подтверждение уведомления».

Рисунок VIII
Взаимодействие между системой гарантийной цепи и международной системой eTIR



60. Эти сообщения (E1, E2, E3, E4, E5, E6, E7 и E8) передаются по протоколу HTTPS через Интернет с помощью веб-сервисов SOAP, а передаваемые данные форматируются на языке разметки XML.

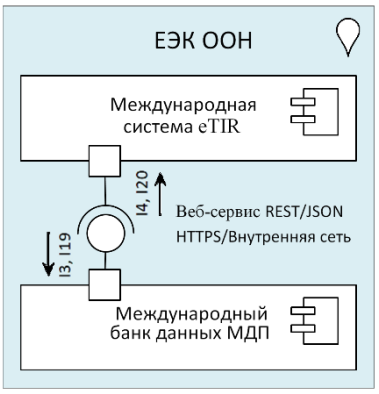
7. Европейская экономическая комиссия Организации Объединенных Наций

61. ЕЭК управляет двумя информационными системами: международной системой eTIR и Международным банком данных МДП (МБДМДП). Международная система eTIR является краеугольным камнем системы eTIR, и ее основная роль заключается в получении, проверке, регистрации и направлении данных, которыми обмениваются различные участники во время перевозки МДП в соответствии с процедурой eTIR. МБДМДП представляет собой информационную систему, которая относится к компетенции ИСМДП, притом что его основные функции в контексте системы eTIR заключаются в организации перечня уполномоченных держателей книжек МДП, а также перечня утвержденных таможенных органов, ответственных за осуществление операций МДП.

62. В контексте обработки информации, получаемой в сообщениях eTIR, международная система eTIR запрашивает МБДМДП (когда это применимо) с целью:

- проверить разрешение держателя, используя запросное сообщение «I3 — Получение информации о держателе» и соответствующее ответное сообщение «I4 — Информация о держателе»;
- проверить наличие таможен, используя запросное сообщение «I19 — Проверка таможен» и соответствующее ответное сообщение «I20 — Валидация таможен».

Рисунок IX
Взаимодействие между международной системой eTIR и МБДМДП



63. Эти сообщения (I3, I4, I19 и I20) передаются с использованием протокола HTTPS по защищенной сети центра обработки данных, в котором размещены обе информационные системы, с использованием веб-услуг RESTful, а соответствующие данные передаются в формате JSON.

C. Детальная архитектура международной системы eTIR

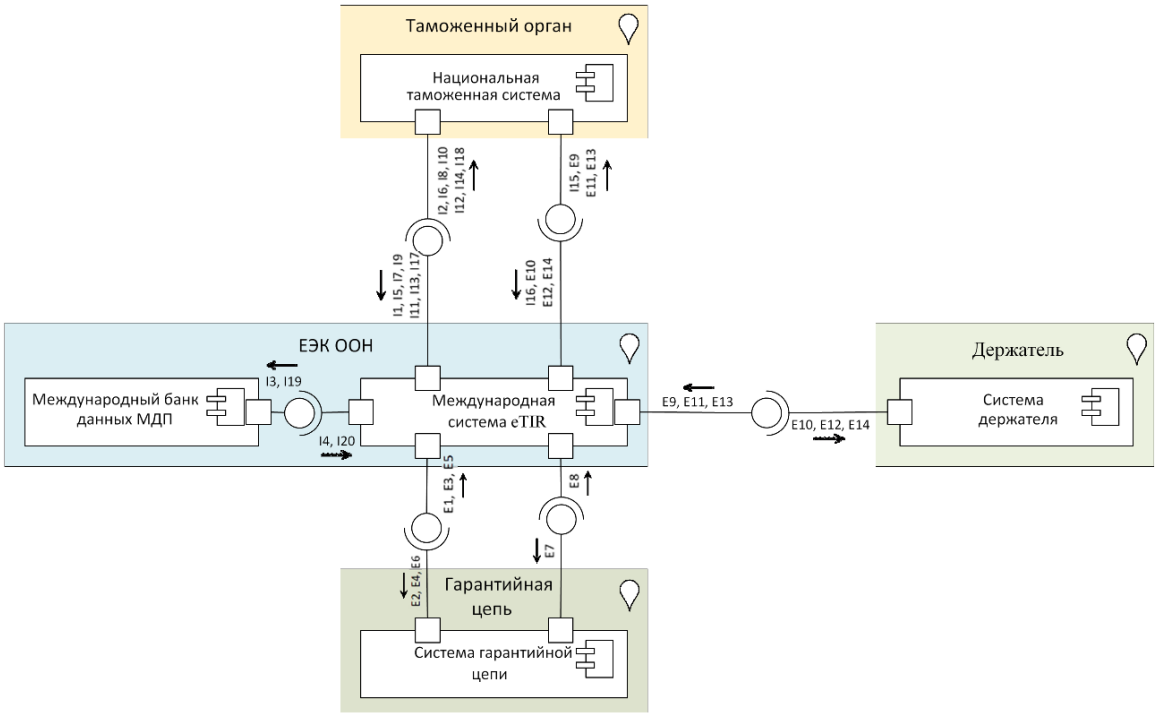
1. Введение

64. В данном разделе описываются программные и аппаратные аспекты архитектуры международной системы eTIR. Для того чтобы сохранить непредвзятость вне зависимости от технологий, в этом разделе не представлена информация о продуктах, инфраструктурных компонентах или библиотеках, используемых для выполнения функций, необходимых для работы соответствующих компонентов. Фактически, по мере быстрого развития технологий ЕЭК будет постоянно отслеживать имеющиеся варианты и вносить соответствующие изменения по своему усмотрению, с тем чтобы компоненты международной системы eTIR могли и впредь выполнять свои функции и надлежащим образом поддаваться масштабированию с течением времени в соответствии с требованиями к производительности и эксплуатационным характеристикам (см. следующий раздел, посвященный техническим требованиям).

2. Взаимодействие с субъектами eTIR

65. Интерфейсы, сопрягающие международную систему eTIR и другие заинтересованные стороны eTIR, уже подробно описаны в предыдущем разделе. На следующем рисунке они все обобщены с указанием кодов сообщений и потока информации.

Рисунок X
Интерфейсы международной системы eTIR



3. Места хранения данных

66. Сообщения обрабатываются международной системой eTIR, и их части регистрируются в трех различных местах хранения данных:

- все входящие и исходящие сообщения полностью регистрируются в **журналах eTIR** в целях сохранения данных, которые необходимы для того, чтобы исключить возможность отказа и предоставления информации, которая может быть запрошена договаривающимися сторонами;
- данные, извлеченные из сообщений, регистрируются в **базе данных eTIR** в целях их использования механизмом запросов и в статистических целях;
- если в сообщения встроены «вложенные документы» и «свидетельства о допуске» (что может быть в случае сообщений E6, E9, I6, I7 и I15), то они извлекаются и сохраняются в виде файлов в отдельной централизованной и защищенной файловой системе под названием «**Документы eTIR**».

4. Архитектура программного обеспечения

67. Международная система eTIR строится на следующих программных компонентах:

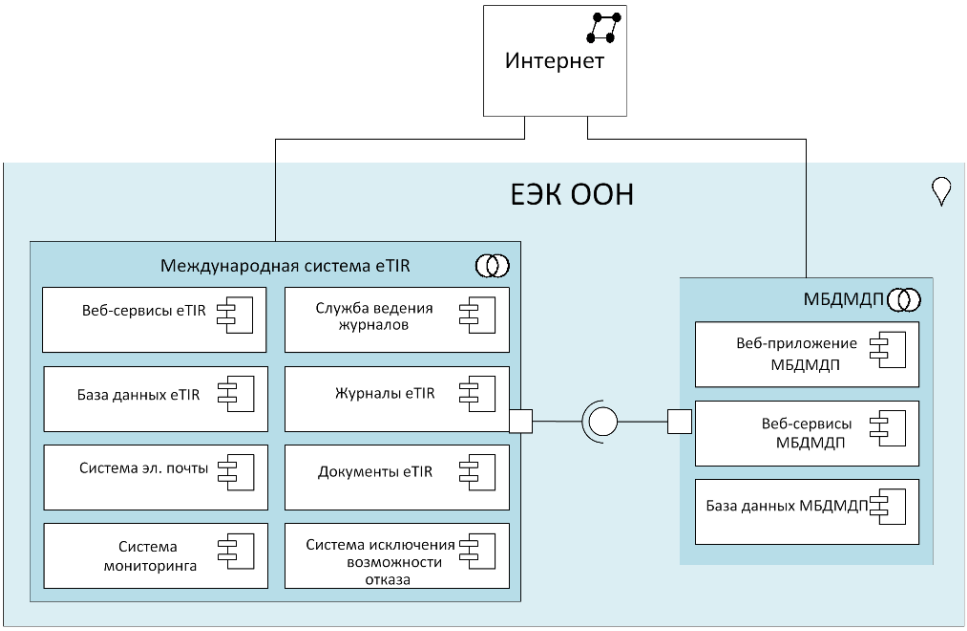
- основным компонентом международной системы, в которой принимаются, проверяются, обрабатываются, регистрируются и отправляются сообщения, являются **веб-сервисы eTIR;**
- **служба ведения журналов** используется для регистрации всех сообщений, отправляемых и получаемых международной системой eTIR, а также всей информации, регистрируемой другими программными компонентами, инфраструктурными компонентами и библиотеками.

68. Международная система eTIR также строится на следующих системах:

- **система электронной почты** используется для отправки электронных сообщений заинтересованным сторонам eTIR в особых случаях, главным образом во время аварийных процедур;
- **система мониторинга** используется для наблюдения за ресурсами и производительностью виртуальных серверов, а также за доступностью и производительностью услуг международной системы eTIR;
- **система исключения возможности отказа** предназначена для извлечения данных, хранящихся в журналах eTIR, их индексирования и выполнения функции пользовательского интерфейса, доступного только для ИТ-администраторов из ЕЭК. Этот пользовательский интерфейс позволяет выходить на журналы с целью найти конкретное сообщение (используя уникальный «Идентификатор сообщения») в виде парных запросных/ответных сообщений, а также предоставить всю информацию, необходимую договаривающимся сторонам для целей проверки[15].

69. На следующей диаграмме представлена архитектура программного обеспечения международной системы eTIR. Интерфейсы, которые открыты и просматриваются международной системой eTIR, не представлены, поскольку они уже перечислены и описаны в разделах выше.

Рисунок XI
Архитектура программного обеспечения международной системы eTIR



70. Технические требования к программным компонентам международной системы eTIR перечислены в следующем разделе. Программные компоненты МБДМДП перечислены в информационных целях, поскольку они находятся под управлением ЕЭК и относятся к компетенции ИСМДП.

5. Системная архитектура

71. Структура Организации Объединенных Наций, которая размещает на своих серверах международную систему eTIR (здесь и далее хостинговая структура), имеет свой собственный частный центр хранения и обработки данных, который находится в комплексе Организации Объединенных Наций и поэтому пользуется привилегиями и иммунитетами, закрепленными в Уставе Организации Объединенных Наций[16] и более

[15] В соответствии с пунктом 3 статьи 12 приложения 11 к Конвенции МДП.
[16] См. www.un.org/en/charter-united-nations/.

подробно изложенными в Конвенции о привилегиях и иммунитетах Организации Объединенных Наций[17].

72. Хостинговая структура использует соответствующую ферму виртуальных серверов для передачи в пользование нужных виртуальных серверов, которые образуют различные системные компоненты международной системы eTIR, притом что каждый узел соответствует отдельному виртуальному серверу. В ближайшем будущем ЕЭК рассмотрит вопрос об использовании контейнеров и системы управления контейнерами с целью обеспечить дальнейшее масштабирование требований международной системы eTIR в условиях сохранения расходов на хостинг на приемлемом уровне.

73. Международная система eTIR разрабатывается и реализуется на практике таким образом, чтобы ограничить наличие единых точек отказа (SPOF) с целью обеспечить достижение поставленных перед ней задач в части доступности (как подробно описано в следующем разделе). Такая архитектура также позволяет принимать нужные меры в отношении соответствующих компонентов системы, не прибегая к приостановке работы международной системы eTIR. Это особенно важно в случае выполнения регулярных работ по техническому обслуживанию, таких как замена дефектных аппаратных частей, обновление программных компонентов и устранение уязвимости в системе безопасности.

74. Международная система eTIR строится на следующих системных компонентах (их технические требования перечислены в следующем разделе):

- основным компонентом международной системы, в которой принимаются, проверяются, обрабатываются, регистрируются и отправляются сообщения, являются **веб-сервисы eTIR.** Он состоит из нескольких узлов коммуникационных веб-серверов, на которых сообщения распределяются с помощью соответствующего балансировщика нагрузки;
- **база данных eTIR** является основным хранилищем и состоит из кластерной системы управления базами данных (СУБД), использующей несколько виртуальных серверных узлов и высокопроизводительного дискового хранилища;
- **журналы eTIR** представляют собой хранилище, в которое ежедневно передаются журналы, и состоят из виртуального сервера с достаточным дисковым пространством для хранения всей занесенной информации;
- **документы eTIR** представляют собой хранилище, в которое передаются прилагаемые документы и которое состоит из виртуального сервера с достаточным дисковым пространством для хранения всех документов.

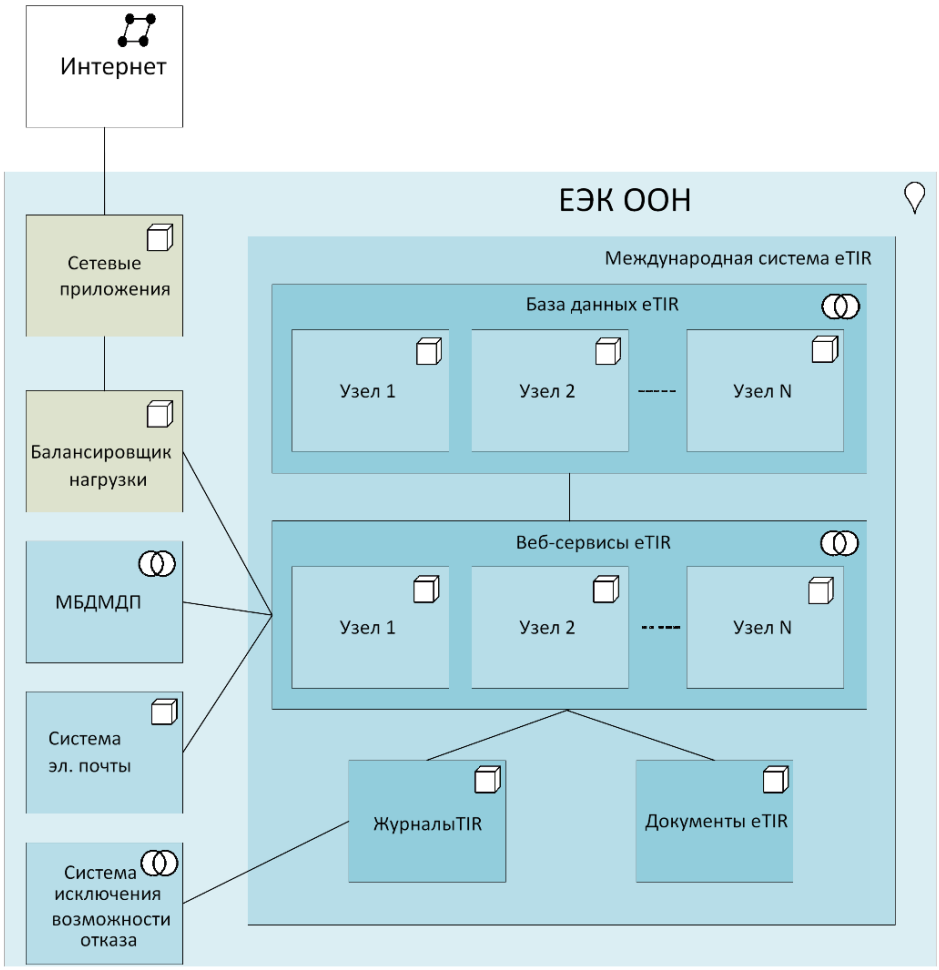
75. Международная система eTIR строится на следующих компонентах внешних систем:

- **МБДМДП**, который имеет собственную системную архитектуру, позволяющую ему обеспечивать достижение своих целей в части доступности. В случае недоступности МБДМДП международная система eTIR переходит в режим обхода отказа, который описан ниже в настоящем документе;
- **система электронной почты** предоставляется хостинговой структурой и состоит из виртуального сервера, используемого только для отправки электронных сообщений. В международной системе eTIR эта внешняя система используется главным образом в случае аварийных процедур;
- **система исключения возможности отказа** представляет собой внешнюю систему административного управления, которая непосредственно не требуется для надлежащей работы международной системы eTIR и, как следствие, состоит только из одного виртуального сервера.

[17] См. treaties.un.org/doc/Treaties/1946/12/19461214%2010-17%20PM/Ch_III_1p.pdf.

76. На следующей диаграмме представлена системная архитектура международной системы eTIR.

Рисунок XII
Системная архитектура международной системы eTIR



77. В следующем примере мы хотели бы проиллюстрировать обычный обмен информацией между соответствующими компонентами системы. Входящее сообщение, отправленное через Интернет какой-либо заинтересованной стороной eTIR, сначала поступает на сетевые устройства (BGP-маршрутизатор и сетевое устройство защиты) хостинговой структуры. Затем сообщение передается в систему балансировки нагрузки, которая направляет его на соответствующий узел веб-служб eTIR (коммуникационный веб-сервер), который проверяет и обрабатывает сообщение. Затем этот веб-сервер хранит соответствующие данные в базе данных eTIR, в журналах eTIR и, в случае применимости, в документах eTIR. В завершение тот же самый веб-сервер готовит ответное сообщение и отправляет его обратно заинтересованной стороне eTIR, которая изначально отправила запросное сообщение. Для наглядности на этой диаграмме не показаны дополнительные системы, связанные с маршрутизацией и безопасностью сети (маршрутизаторы, коммутаторы, межсетевые экраны, системы обнаружения вторжения (СОВ), системы обработки информации (СОИ) и т. д.).

D. Технические требования

1. Введение

78. В настоящем разделе описаны технические (или нефункциональные) требования, которым должна отвечать международная система eTIR. Технические

требования определяют критерии, которые могут быть использованы для оценки того, насколько эффективно системой осуществляются операции и выполняются ее функции. Эти критерии по своему значению не уступают функциональным требованиям и определяют архитектуру и принципы проектирования системы.

79. В каждом из нижеследующих подразделов описываются требования, связанные с определенным нефункциональным критерием. Требования могут быть качественными (например, исходный код должен версионироваться в Git) и/или количественными (например, международная система eTIR должна быть доступна 24 часа в сутки, 365 дней в году). Для удобства каждому требованию присвоен уникальный идентификатор.

80. Для оценки выполнения количественных требований необходимо осуществлять сбор значений по показателям. В том случае, если эти значения могут быть раскрыты без ущерба для обеспечения безопасности, их можно будет периодически передавать в ТОО в целях информирования.

81. Учитывая тот факт, что в основе системы eTIR лежит обмен сообщениями с использованием веб-сервисов и что разработка пользовательского интерфейса для международной системы eTIR не запланирована (за исключением внутренних целей, связанных с ее администрированием), следующие критерии не являются применимыми и описываться не будут: доступность представления информации, совместимость и удобство использования.

82. ЕЭК будет периодически проводить оценку по ряду количественных целевых показателей и представлять ТОО доклад о ней, а также предложения по устранению возможных недостатков и по дальнейшему улучшению целевых показателей. В дальнейшем ТОО будет принимать решение относительно реализации этих предложений или рекомендовать их применение АС.2.

83. Наконец, в тех случаях, когда упоминаются продукты, программное обеспечение, программные платформы и библиотеки, используемые для выполнения требований, ЕЭК оставляет за собой право изменить свой выбор на более позднем этапе (если это не повлечет за собой никаких финансовых затрат) с целью получения дополнительных выгод для системы eTIR. Информация об этом новом выборе будет доведена до сведения ТОО, и последующая версия спецификаций eTIR будет соответствующим образом обновлена.

2. Готовность к работе

84. Готовность международной системы eTIR к работе представляет собой состояние, когда авторизованные пользователи (ЕЭК и все подключенные к ней заинтересованные стороны eTIR) имеют полный доступ к этой системе и могут ею пользоваться.

85. Готовность международной системы eTIR к работе будет иметь решающее значение для надлежащего функционирования всей системы eTIR с самого начала и станет еще актуальнее, когда количество перевозок МДП, осуществляемых в соответствии с процедурой eTIR, увеличится. В нижеследующих таблицах описываются как качественные, так и количественные аспекты требований, касающихся готовности к работе. Некоторые из них будут включены в соглашение об уровне обслуживания (СУО), которое будет подписано с поставщиком хостинговых услуг Организации Объединенных Наций (далее — «хостинговая организация»), выбранным для хостинга международной системы eTIR.

Таблица 4
Качественные требования, касающиеся готовности к работе

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
AV.1	Обычные операции по обслуживанию программного обеспечения и системных компонентов международной системы eTIR осуществляются в транспарентном режиме при поддержании готовности сервиса к работе.	Международная система eTIR проектируется таким образом, чтобы можно было избежать возникновения единичных отказов (SPOF) благодаря использованию нескольких внешних веб-серверов для распределения рабочей нагрузки, кластеризации баз данных, дублирования компонентов приложений, и, возможно, благодаря использованию высокодоступных прокси-серверов и механизма управления контейнерами.

Таблица 5
Количественные требования, касающиеся готовности к работе

Идентификатор	*Описание*	*Каким образом достичь целевого показателя*	*Значение целевого показателя*
AV.2	Общая эксплуатационная готовность международной системы eTIR	Организация хостинга международной системы eTIR внутри организации системы ООН, которая предлагает обеспечение такого уровня эксплуатационной готовности, и его включение в СУО.	Круглосуточно, ежедневно в течение всего года
AV.3	Процентная доля времени продуктивной эксплуатации международной системы eTIR	Обычные операции по обслуживанию программного обеспечения и системных компонентов международной системы eTIR осуществляются в транспарентном режиме при поддержании готовности сервиса к работе. Быстрое выявление и решение связанных с системой проблем за счет использования СОПов и механизма эскалации.	Более 99 % (т. е. максимальное время простоя за год не должно превышать 3 суток 15 часов 39 минут 29 секунд)
AV.4	Максимальная продолжительность простоя международной системы eTIR в случае серьезной проблемы	Параметры мониторинга служб, программных компонентов и виртуальных серверов настраиваются и согласовываются с хостинг-провайдером. Процедуры разрабатываются и согласовываются в рамках СУО.	4 часа в будние дни и круглосуточно в выходные дни (на каждый случай)

86. После того как международная система eTIR будет введена в эксплуатацию, по итогам анализа собранных значений параметров и отзывов заинтересованных сторон eTIR ЕЭК или ТОО, возможно, пожелают сделать предложения относительно улучшения значений целевых показателей, связанных с требованиями AV.3 и AV.4, в целях повышения готовности сервиса к работе. В этом случае ЕЭК представит ТОО предложение по улучшению вышеупомянутых значений целевых показателей вместе с возможными последствиями для бюджета.

3. Резервное копирование

87. Резервное копирование — это создание копии касающихся eTIR данных, хранящейся в отдельном защищенном месте с целью возможности ее использования для восстановления данных в случае какого-либо события, связанного с их потерей.

88. Для обеспечения выполнения требований во всех местах хранения данных (т. е. базы данных eTIR, журналов eTIR и документов eTIR) будет осуществляться их резервное копирование. Указанные в нижеследующей таблице требования будут включены в СУО, которое будет подписано с хостинговой организацией.

Таблица 6
Требования, касающиеся резервного копирования

Идентификатор	*Описание*	*Каким образом достичь целевого показателя*	*Значение целевого показателя*
BK.1	Частота резервного копирования данных eTIR	Резервное копирование информации, хранящейся в базе данных eTIR, журналах eTIR и документах eTIR, осуществляется два раза в сутки, и резервные копии этих данные хранятся в защищенном месте.	Каждые 12 часов
BK.2	Максимальное время, необходимое для восстановления данных из резервных копий в результате события, связанного с потерей данных	Процедуры резервного копирования разрабатываются и согласовываются в рамках СУО с хостинг-провайдером. Регулярное проведение тест-проверок.	Каждые 6 часов

89. После введения международной системы eTIR в эксплуатацию ЕЭК или ТОО, возможно, пожелают сделать предложения относительно улучшения значений целевых показателей, связанных с требованиями BK.1 и BK.2. В этом случае ЕЭК представит ТОО предложение по улучшению вышеупомянутых значений целевых показателей вместе с возможными последствиями для бюджета.

4. Пропускная способность и масштабируемость

90. В целом существуют два аспекта, которые необходимо учитывать в контексте управления пропускной способностью: скорость обработки информации системой (т. е. ее способность обрабатывать входящие сообщения и отправлять ответы) и хранение различных видов полученной информации. Масштабируемость международной системы eTIR представляет собой ее способность справляться с увеличением объема работы за счет введения в систему дополнительных ресурсов.

91. В нижеследующей таблице указаны числовые значения, которые основаны на анализе, проведенном для определения потребностей с точки зрения пропускной способности и масштабируемости международной системы eTIR и включенном в приложение V.C. Как отмечается в выводах этого анализа, качество оценок и прогнозов относительно скорости обработки информации и объема данных зависит от качества различных допущений, лежащих в их основе. Поскольку международная система eTIR пока еще не введена в эксплуатацию, фактических данных для этого анализа не существует. По этой причине международную систему eTIR следует проектировать с учетом требований, касающихся пропускной способности и масштабируемости, только на первые два года, поскольку имеется высокая вероятность того, что реальные данные внесут коррективы в ряд допущений, что приведет к изменению результатов расчетов и прогнозов на последующие годы.

Таблица 7
Требования, касающиеся пропускной способности и масштабируемости

Идентификатор	*Описание*	*Каким образом достичь целевого показателя*	*Значение целевого показателя*
CP.1	Максимальное количество обрабатываемых сообщений	Определенный компонент помещает входящие сообщения в очередь. Затем сообщения из очереди извлекаются несколькими внешними веб-серверами и обрабатываются в соответствии с пороговыми значениями времени ожидания.	2021 год: 12 сообщений в минуту 2022 год: 78 сообщений в минуту 2023 год: 270 сообщений в минуту 2024 год: 570 сообщений в минуту 2025 год: 1200 сообщений в минуту
CP.2	Максимальный объем памяти, выделенной для журналов eTIR	Журналы eTIR сохраняются непосредственно на внешних веб-серверах. Ежедневно они перемещаются в центральное защищенное место, в котором будет достаточно памяти для их агрегированного хранения.	2021 год: 371 Гбайт в год 2022 год: 1,2 Тбайт в год 2023 год: 4,9 Тбайт в год 2024 год: 17,1 Тбайт в год 2025 год: 36,1 Тбайт в год
CP.3	Максимальный объем памяти, выделенной для базы данных eTIR	В зависимости от фактических полученных данных и регулярных измерений параметров производительности только самые последние данные (например, за последние шесть месяцев) можно будет хранить в кластерной базе данных (при этом более старые данные будут регулярно выгружаться во вторичную базу данных) для обеспечения того, чтобы размеры основной базы данных не оказывали негативного влияния на ее производительность.	2021 год: 1,4 Гбайт в год 2022 год: 4,3 Гбайт в год 2023 год: 17,9 Гбайт в год 2024 год: 62,6 Гбайт в год 2025 год: 133,3 Гбайт в год
CP.4	Максимальный объем памяти, выделенной для документов eTIR	Документы eTIR будут храниться не в базе данных, а в центральной (защищенной) файловой системе, имеющей достаточно дискового пространства для хранения всех документов.	2021 год: 100 Гбайт в год 2022 год: 315 Гбайт в год 2023 год: 1,3 Тбайт в год 2024 год: 4,6 Тбайт в год 2025 год: 9,8 Тбайт в год

92. Как указано в выводах анализа, представленного в приложении V.C, через шесть месяцев после введения международной системы eTIR в эксплуатацию ЕЭК проведет аналогичный анализ с целью представить ТОО пересмотр вышеупомянутых значений целевых показателей вместе с возможным предложением по бюджету.

5. Управление настройками

93. Управление настройками — это процесс, который позволяет отслеживать все отдельные элементы конфигурации международной системы eTIR. Элемент настроек — это ИТ-актив или комбинация ИТ-активов, которые могут зависеть от других ИТ-процессов и/или быть связанными с ними (например, исходный код, файлы настроек, процедуры, внутренняя документация и т. д.).

94. Надлежащий ряд мер и процедур, связанных с управлением настройками, является единственным эффективным и обеспечивающим устойчивость способом разработки и обслуживания такой крупной информационной системы, как

международная система eTIR, и ЕЭК будет обеспечивать надлежащее выполнение следующих технических требований.

Таблица 8
Требования, касающиеся управления настройками

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
CM.1	Исходный код всех модулей международной системы eTIR должен версионироваться с использованием системы управления версиями (СУВ) для обеспечения эффективного управления данным активом.	Исходный код всех модулей международной системы eTIR версионируется с помощью Git и его хостинг осуществляется в помещениях системы ООН.
CM.2	Все изменения, связанные с базой данных eTIR, должны версионироваться с использованием СУВ для обеспечения эффективного управления данным активом.	Все изменения, связанные с базой данных eTIR, версионируются с использованием технологий Liquibase и Git, и их хостинг осуществляется в помещениях системы ООН.
CM.3	Все активы, связанные с документацией системы eTIR, должны версионироваться с использованием СУВ для обеспечения эффективного управления этими активами.	Все активы, связанные с документацией системы eTIR, версионируются с использованием различных СУВ в зависимости от их характера, и их хостинг осуществляется в помещениях системы ООН.
CM.4	Все активы, связанные с внутренней документацией системы eTIR, должны версионироваться и должны быть доступны для ЕЭК благодаря использованию программного обеспечения для коллективной работы в целях эффективного обмена знаниями и повышения производительности.	Все активы, связанные с внутренней документацией системы eTIR, версионируются и доступны для ЕЭК благодаря системе управления базой знаний (СУБЗ), которая действует в качестве защищенной и версионированной платформы для коллективной работы и хостинг которой осуществляется в помещениях системы ООН.
CM.5	Все сообщения об ошибках, запросы на предоставление функций и другие события регистрируются, анализируются и в конечном итоге обрабатываются с помощью системы отслеживания проблем для обеспечения того, чтобы вопросы, поднимаемые всеми заинтересованными сторонами eTIR, должным образом оценивались и рассматривались согласно соответствующему уровню приоритетности.	Все сообщения об ошибках, запросы на предоставление функций и другие события регистрируются, анализируются и в конечном итоге обрабатываются с помощью системы отслеживания проблем, хостинг которой осуществляется в помещениях системы ООН.

6. Хранение данных

95. Хранение данных определяет политику в отношении непрерывного управления данными и записями для выполнения юридических и бизнес-требований, касающихся архивирования данных, в частности требований, перечисленных в приложении 11. В следующей таблице перечислены требования к международной системе eTIR, касающиеся хранения данных.

Таблица 9
Требования, касающиеся хранения данных

Идентификатор	*Описание*	*Каким образом достичь целевого показателя*	*Значение целевого показателя*
RE.1	Доступность информации, хранящейся в международной системе eTIR.	Ежедневно создается резервная копия информации, хранящейся в базе данных eTIR, журналах eTIR и документах eTIR, и дополнительные копии создаются и хранятся на ленточных накопителях, размещенных в отдельном защищенном месте, устойчивом к воздействию большинства стихийных бедствий.	10 лет[18]
RE.2	Извлечение информации, запрашиваемой договаривающимися сторонами для целей проверки[19].	Процедуры извлечения информации разрабатываются и согласовываются в рамках СУО с хостинг-провайдером.	На извлечение информации отводится не более трех дней

7. Послеаварийное восстановление

96. Послеаварийное восстановление включает в себя комплекс стратегий, инструментов и процедур, позволяющих восстановить или продолжить функционирование международной системы eTIR после стихийного бедствия или антропогенной катастрофы. Основное внимание при этом уделяется ИТ или технологическим системам, поддерживающим критически важные рабочие функции, и поэтому послеаварийное восстановление может рассматриваться как особая разновидность плана повышения устойчивости функционирования.

97. Обычно послеаварийное восстановление предполагает отсутствие возможности для восстановления первичного узла (по крайней мере в течение некоторого времени) и представляет собой набор необходимых процессов, позволяющих восстановить сервисы на базе вторичного узла. В рамках версии 4.3 спецификаций eTIR предполагается, что для целей аварийного восстановления будет использоваться только узел типа «теплый узел» — главным образом по финансовым соображениям.

98. «Теплый узел» содержит оборудование и каналы передачи данных, необходимые для быстрого налаживания операций. Такое оборудование, как правило, имеет предустановленную конфигурацию и готово к установке приложений, необходимых для поддержки работы организации. Однако, поскольку этот вторичный узел должен использоваться в случае недоступности из-за аварии основного узла, то на серверах «теплого узла» должны быть установлены и настроены все компоненты программного обеспечения. Кроме того, оперативные данные с первичных узлов реплицируются на вторичных узлах такого типа не в режиме реального времени, а лишь через определенные промежутки времени.

99. Последствия аварии весьма существенны, поскольку она приводит к выведению международной системы eTIR из строя на необычайно продолжительный срок (обычно превышающий одни сутки). Вместе с тем вероятность возникновения такой аварии крайне низка. Возникающий в результате этого риск является незначительным в контексте версии 4.3 спецификаций eTIR, поскольку количество перевозок МДП с использованием процедуры eTIR на начальном этапе будет небольшим и оно будет увеличиваться постепенно — по мере того как новые договаривающиеся стороны будут подключать свои национальные таможенные системы к международной

[18] Согласно пункту 1 статьи 12 приложения 11 к Конвенции МДП.
[19] Согласно пункту 3 статьи 12 приложения 11 к Конвенции МДП.

системой eTIR. Кроме того, в качестве мер по снижению такого риска выступают резервные процедуры, описанные в функциональных спецификациях eTIR.

100. В следующей таблице перечислены требования к международной системе eTIR, касающиеся послеаварийного восстановления.

Таблица 10
Требования, касающиеся послеаварийного восстановления

Идентификатор	*Описание*	*Каким образом достичь целевого показателя*	*Значение целевого показателя*
DR.1	Целевой показатель по времени восстановления (RTO)[20] международной системы eTIR после аварии	Разрабатывается план послеаварийного восстановления со всеми процедурами, подробно описывающими восстановление международной системы eTIR, и проводятся регулярные тест-проверки этого плана.	48 часов
DR.2	Целевая точка восстановления (RPO)[21] международной системы eTIR после аварии	Копии данных, связанных с eTIR, на регулярной основе и в защищенном режиме передаются в «теплый узел». Выполняются тест-проверки по восстановлению работы.	4 часа

101. После введения международной системы eTIR в эксплуатацию ЕЭК или ТОО, возможно, пожелают сделать предложения относительно улучшения значений целевых показателей, связанных с требованиями DR.1 и DR.2. В этом случае ЕЭК представит ТОО предложение по улучшению вышеупомянутых значений целевых показателей вместе с возможными последствиями для бюджета.

8. Устойчивость к сбоям

102. Устойчивость к сбоям — это свойство, позволяющее системе продолжать нормальную работу в случае отказа (или одного или нескольких сбоев внутри) некоторых из ее компонентов. В архитектуре и инфраструктуре современных информационных систем учитываются обычные технические отказы компонентов, в частности жестких дисков, сетевых подключений, перебоев с электропитанием, что может обеспечить уровень устойчивости к сбоям, который является транспарентным для конечных пользователей.

103. Требования, перечисленные в нижеследующей таблице, обеспечивают первый уровень перехода в режим нейтрализации неисправности, для активации которого не обязательны какие-либо действия заинтересованных сторон eTIR. Эти требования в основном выполняются за счет базовой инфраструктуры и будут включены в СУО, которое будет подписано с хостинговой организацией.

Таблица 11
Требования, касающиеся устойчивости к сбоям

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
FT.1	Эффективное реагирование на сбои в работе физического сервера, которые могут быть связаны с тем или иным элементом оборудования (ЦП, память,	Инфраструктура, выстроенная на основе пула виртуальных серверов и опирающаяся на несколько физических серверов, обеспечивающих возможность «горячей» замены виртуальных

[20] RTO — это время, в течение которого может быть восстановлена работа ИТ-сервиса в случае аварии.

[21] RPO — это максимальный целевой период, данные (транзакции) за который могут быть потеряны ИТ-сервисом в случае сбоя в работе.

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
	материнская плата, жесткий диск, сетевая карта и т. д.), во избежание нарушения готовности международной системы eTIR к работе.	устройств для смягчения последствий таких сбоев. Архитектура, основанная на работе вычислительного кластера во избежание возникновения единичных отказов.
FT.2	Эффективное реагирование на сбои в работе оборудования, используемого в местах хранения данных (HDD, SSD), во избежание нарушения готовности международной системы eTIR к работе.	Инфраструктура, выстроенная на основе SAN и использующая резервированную схему для дисковых накопителей (RAID). Архитектура, основанная на работе вычислительного кластера во избежание возникновения единичных отказов.
FT.3	Эффективное реагирование на разрыв подключения к Интернету во избежание нарушения готовности международной системы eTIR к работе.	Двойное подключение к Интернету с помощью двух разных провайдеров.
FT.4	Эффективное реагирование на перебои с электропитанием во избежание нарушения готовности международной системы eTIR к работе.	Блоки источников бесперебойного питания (ИБП) и аварийные топливные генераторы для обеспечения электропитания центра обработки и хранения данных с запасом топлива, достаточным для того, чтобы без дозаправки дождаться восстановления электропитания.

9. Интернационализация и локализация

104. Интернационализация и локализация — это средства адаптации компьютерного программного обеспечения с учетом различных языков, региональных особенностей и технических требований того или иного целевого вычислительного узла. Интернационализация — это процесс такой разработки программного приложения, которая позволяет осуществлять его адаптацию для различных языков и регионов без внесения каких-либо инженерных изменений. Локализация — это процесс адаптации интернационализированного программного обеспечения для конкретного региона или языка путем перевода текстовой информации и добавления локальных компонентов.

105. Поскольку в международной системе eTIR пользовательский интерфейс отсутствует, действие требований в отношении интернационализации ограничивается только сообщениями eTIR и способом хранения данных в различных местах хранения данных. Для сокращения связанных с локализацией потребностей был принят ряд мер:

- для большинства атрибутов в сообщениях eTIR используются перечни кодов. В них подробно описываются все возможные коды, которые может содержать атрибут, что облегчает передачу информации от одной системы к другой, поскольку во всех системах используется один и тот же набор перечней кодов. Кроме того, такой подход позволяет избежать необходимости в переводе значений, которые в этом случае не нуждаются в локализации;
- для выражения числовых данных используются фиксированные шаблоны, которые четко определены в Определении схемы XML сообщений eTIR. Такой подход позволяет исключить любую возможную неоднозначность, связанную с разделителями разрядов десятков и тысяч;
- даты также выражаются с использованием определенных шаблонов, содержащих либо только дату, либо дату и время, включая разницу со всемирным скоординированным временем (UTC);
- использование текстовых полей сводится к минимуму, и они чаще всего задействованы для представления текстовых данных, которые обычно не подлежат переводу, например идентификаторов, имен собственных и адресов.

Ряд текстовых полей используются для хранения предложений на заданном языке, и для определения языка их содержимого может использоваться субатрибут «Язык, в кодированном виде».

106. В нижеследующей таблице перечислены требования, касающиеся интернационализации и локализации.

Таблица 12
Требования, касающиеся интернационализации и локализации

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
IL.1	Сообщения eTIR должны позволять обработку текстовых значений на английском, русском и французском языках.	Набор символов сообщений eTIR, обмен которыми осуществляется в SOAP/XML, соответствует стандарту UTF-8; тип контента — «application/soap+xml».
IL.2	База данных eTIR должна обеспечивать возможность хранения текстовых значений (из сообщений eTIR) на английском, русском и французском языках.	Набор символов базы данных eTIR соответствует стандарту UTF-8.
IL.3	Журналы eTIR должны обеспечивать возможность хранения всех получаемых сообщений eTIR целиком.	Набор символов файлов, хранящихся в журналах eTIR, соответствует стандарту UTF-8.
IL.4	Документы eTIR должны обеспечивать возможность хранения прилагаемых документов, составленных на различных языках, помимо английского, русского и французского.	Набор символов файлов, хранящихся в документах eTIR, соответствует стандарту UTF-8.
IL.5	Язык текстовых значений, содержащихся в сообщениях eTIR, должен быть идентифицируемым.	Текстовые значения характеризуются субатрибутом «Language, coded» («Язык, в кодированном виде»), в отношении которого используется перечень кодов для указания названия языка.

10. Функциональная совместимость

107. 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.

108. В основе системы eTIR лежит межмашинная передача данных, инициируемая определенными событиями. Поэтому для облегчения подключения разных систем друг к другу интерфейсы взаимодействия между различными заинтересованными сторонами eTIR должны быть четко определены. Кроме того, в целях дополнительного облегчения такого подключения интерфейсы должны быть реализованы на основе широко известных всемирных стандартов.

Таблица 13
Требования, касающиеся функциональной совместимости

Идентификатор	*Описание и цели*	*Каким образом выполнить требование*
IT.1	Для облегчения установления подключения между международной системой eTIR и информационными системами других заинтересованных сторон	Модель данных eTIR полностью согласуется с моделью данных Всемирной таможенной организации (ВТамО). Для непрерывной адаптации модели данных ВТамО к потребностям

Идентификатор	*Описание и цели*	*Каким образом выполнить требование*
	eTIR модель данных eTIR должна согласовываться с широко известной моделью данных, используемой по всему миру.	процедуры eTIR ЕЭК направляет запросы о ведении данных (ЗВД).
IT.2	Формат и технические спецификации сообщений eTIR соответствуют строгим предписаниям для обеспечения функциональной совместимости обмена электронными сообщениями между информационными системами.	Характеристики сообщений eTIR соответствуют предписаниям ВТамО, касающимся XML. Кроме того, проводятся автоматизированные тесты для проверки соответствия по этому аспекту.
IT.3	Информация, обмен которой осуществляется в сообщениях eTIR, является максимально стандартизированной для облегчения ее обработки всеми заинтересованными сторонами eTIR.	В атрибутах сообщений eTIR в максимальной степени используются перечни кодов из широко известных стандартов (UN/EDIFACT и ISO).
IT.4	Заинтересованные стороны eTIR должны иметь достаточно времени, для того чтобы осуществлять переход на следующую версию спецификаций eTIR, продолжая при этом использовать текущую версию спецификаций eTIR.	Международная система eTIR сможет получать, обрабатывать и отправлять сообщения eTIR с использованием двух версий спецификаций eTIR: текущей и последующей, которую всем заинтересованным сторонам eTIR будет предложено внедрить в течение определенного периода времени, отведенного на осуществление перехода, подробно описываемого в процессах управления релизами.

11. Удобство обслуживания

109. Под удобством обслуживания понимают то, насколько легко можно осуществлять обслуживание продукта, направленное, в частности, на исправление дефектов[22], удовлетворение новых требований, облегчение последующего обслуживания и адаптацию к изменяющимся условиями эксплуатации.

110. Типичная ошибка разработки программного обеспечения и управления программным обеспечением заключается в недооценке необходимости постоянно инвестировать приемлемый объем финансовых средств на поддержание и обновление информационной системы во избежание чрезмерных финансовых затрат, связанных с ее полным перепроектированием по причине отсутствия должного обслуживания на протяжении многих лет.

111. Кроме того, в ИТ-индустрии отмечается, что на этапе обслуживания информационной системы формируется значительная доля связанной с ней совокупной стоимости владения (ССВ): обычно от 50 % до 80 %. Данный факт подчеркивает важность принятия необходимых превентивных мер для удерживания расходов на обслуживание информационной системы на приемлемом уровне при обеспечении соблюдения всех требований, касающихся удобства обслуживания.

112. В частности, следует принимать меры к тому, чтобы не допускать накопления «технического долга». «Технический долг» — это концепция разработки программного обеспечения, отражающая неявные издержки дополнительной доработки программного обеспечения в результате принятия ненадлежащего решения, которые могут принести пользу в краткосрочной перспективе, а в долгосрочной перспективе приведут к увеличению стоимости обслуживания. Как и в случае

[22] См. определение понятия «дефект» в техническом глоссарии.

денежного долга, непогашение технического долга может привести к накоплению «процентов», еще более затрудняющих имплементацию изменений в будущем.

113. В нижеследующей таблице перечислены требования, касающиеся удобства обслуживания.

Таблица 14
Требования, касающиеся удобства обслуживания

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
MT.1	Следует избегать накопления «технического долга» в отношении языков программирования, программных платформ и библиотек, используемых для создания международной системы eTIR.	Последние стабильно работающие версии базовых языков программирования, программных платформ и библиотек, используемых для создания международной системы eTIR, регулярно пересматриваются, и планирование их обновлений или модернизации осуществляется на регулярной основе. Кроме того, периодически проводится обзор новых тенденций и принимаются необходимые меры для перехода на использование более оптимальных решений, до того как тот или иной компонент устареет.
MT.2	Следует избегать накопления «технического долга» в отношении исходного кода международной системы eTIR.	Для измерения индекса удобства поддержки исходного кода используется инструмент статического анализа кода, и уменьшению количества проблем, выявленных с помощью этого инструмента, регулярно уделяется внимание. Кроме того, регулярно проводится работа по реорганизации кода в целях снижения *программной энтропии*[23] исходного кода.
MT.3	Сохранение базы знаний для надлежащего обслуживания и совершенствования международной системы eTIR.	Внутренняя документация международной системы eTIR управляется с помощью СУБЗ, которая действует как защищенная и версионированная платформа для совместной работы между членами ЕЭК. Одна из ролей ИТ-координатора заключается в том, чтобы обеспечить надлежащий уровень подготовки документации (включая СОПы) и ее постоянное обновление в СУБЗ с целью снижения рисков, сопряженных с текучестью кадров и ключевого персонала[24].

12. Производительность

114. Производительность — это показатель, позволяющий оценить максимальные или оптимальные возможности аппаратного, программного, системного или технического процесса для выполнения той или иной задачи. В случае международной системы eTIR требования распространяются на характеристики, касающиеся времени ожидания ответа и скорости обработки информации.

115. Требования к международной системе eTIR, касающиеся скорости обработки информации, уже были подробно описаны в разделе, посвященном пропускной способности, где представлены показатели CP.1 и CP.2. Требования, касающиеся времени ожидания ответа, подробно представлены в нижеследующей таблице, посвященной количественным требованиям, а дополнительные требования, связанные с производительностью, перечислены в таблице ниже, посвященной качественным требованиям.

[23] См. определение в техническом глоссарии.

[24] Риск, сопряженный с ключевым персоналом: риск, который несет организация, эффективность деятельности которой в значительной степени зависит от одного лица.

Таблица 15
Количественные требования, касающиеся производительности

Идентификатор	*Описание*	*Каким образом достичь целевого показателя*	*Значение целевого показателя*
PE.1	Среднее время ожидания ответа, содержащего короткие сообщения (до 10 КБ), измеряемое отправителем от момента отправки запроса до получения ответного сообщения.	Международная система eTIR спроектирована надлежащим образом, и в ней отсутствуют какие-либо логические или технические «узкие места», которые могут представлять собой проблему для производительности. Все операции, связанные с управлением базой данных eTIR, записью информации в журналы eTIR и подключением к МБДМДП, оптимизированы.	1 секунда
PE.2	Максимальное время ожидания ответа, содержащего короткие сообщения (до 10 КБ), измеряемое отправителем от момента отправки запроса до получения ответного сообщения.	Обеспечение достаточного количества узлов, для того чтобы компоненты программного обеспечения веб-сервисов eTIR могли обрабатывать все запросы. Обеспечение достаточного количества узлов, для того чтобы база данных eTIR могла обрабатывать все запросы.	10 секунд
PE.3	Максимальное время ожидания ответа, измеряемое отправителем от момента отправки запроса до получения ответного сообщения.	Установленный максимальный размер сообщений eTIR составляет 20 Мб. Подключение международной системы eTIR к Интернету характеризуется высокой пропускной способностью (более 100 мегабит в секунду).	Установленное значение времени ожидания составляет 60 секунд

Таблица 16
Качественные требования, касающиеся производительности

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
PE.4	Следует проводить мониторинг показателей производительности международной системы eTIR с целью выявления любых возможных проблем.	Значения показателей, связанных с производительностью, регистрируются на разных ключевых этапах во время получения запроса, его обработки, формирования и отправки ответного сообщения. Проводится мониторинг этих показателей, чтобы в случае превышения определенных пороговых значений обратить на это внимание ЕЭК для проведения анализа.
PE.5	Показатели эффективности международной системы eTIR остаются стабильными или улучшаются с течением времени.	Инструмент нагрузочного тестирования для выполнения автоматизированных нагрузочных испытаний используется в ходе интеграции в международную систему eTIR новых решений, чтобы удостовериться в том, что это не приведет к заметному снижению производительности.

13. Надежность

116. Надежность — это способность информационной системы справляться с ошибками во время выполнения цикла, а также распознавать ошибки при вводе данных. Кроме того, надежность включает в себя комплекс практических мер, принимаемых для обеспечения реализации целей, касающихся качества. Обеспечение максимальной надежности международной системы eTIR лежит в основе второго руководящего принципа, которого придерживается ЕЭК.

117. Для реализации этой цели и обеспечения высокого общего качества международной системы eTIR применяются следующие превентивные меры:

- в ЕЭК разработаны руководящие принципы, касающиеся следующих аспектов международной системы eTIR: разработка, развертывание, эксплуатация и техническое обслуживание. Эти руководящие принципы формируют общий свод правил и практики, направленный на обеспечение предсказуемых, высококачественных результатов;
- существуют строгие процедуры версионирования для обеспечения того, чтобы все изменения, внесенные в исходный код международной системы eTIR, а также в структуру и содержимое базы данных eTIR можно было проследить до запроса, введенного в систему отслеживания проблем;
- для снижения вероятности того, что в исходный код будут включены нежелательные побочные эффекты (дефекты), и для обеспечения соблюдения руководящих принципов по кодированию осуществляются ревизии кода;
- все изменения в исходном коде (связанные либо с добавлением функций, либо с исправлением дефектов) сопровождаются проведением соответствующих автоматизированных тест-проверок с целью убедиться в том, что в исходный код не были внесены регрессионные ошибки;
- исходный код регулярно проверяется инструментом статического анализа для определения ряда показателей, связанных с удобством обслуживания, надежностью, безопасностью, покрытием и дублированием кода. Проблемы, выявляемые с помощью этого инструмента, рассматриваются ЕЭК для реализации ранее поставленных целей в области качества (границы качества);
- для обеспечения высокого уровня надежности и качества конвейер непрерывной интеграции в автоматическом режиме выполняет ряд операций в процессе разработки международной системы eTIR.

118. Кроме того, помимо превентивных мер, для выявления проблем и их скорейшего решения используются следующие меры реагирования:

- система мониторинга позволяет постоянно отслеживать несколько индикаторов и показателей, связанных с программным обеспечением и системными компонентами международной системы eTIR, для выявления любых проблем и выдачи соответствующих предупреждений в целях их быстрого решения (в зависимости от уровня серьезности).

119. В нижеследующей таблице перечислены требования, касающиеся надежности.

Таблица 17
Количественные требования, касающиеся надежности

Идентификатор	*Описание*	*Каким образом достичь целевого показателя*	*Значение целевого показателя*
RL.1	Количество оставшихся проблем наибольшего уровня серьезности, обнаруженных инструментом статического анализа.	Регулярная проверка исходного кода с использованием инструмента статического анализа и решение в приоритетном порядке любых проблем наивысшего уровня серьезности.	0 (все проблемы такого рода должны быть решены)

Идентификатор	*Описание*	*Каким образом достичь целевого показателя*	*Значение целевого показателя*
RL.2	Количество оставшихся проблем нормального уровня серьезности, обнаруженных инструментом статического анализа.	Включение проверки исходного кода с помощью инструмента статического анализа в конвейер непрерывной интеграции для обеспечения быстрой обратной связи и улучшения методов работы.	Менее 150
RL.3	Процентная доля функционального исходного кода, охваченного автоматизированными тест-проверками (покрытие кода).	Проведение ревизий кода и наличие рекомендаций по его разработке гарантируют, что любые изменения исходного кода будут сопровождаться проведением необходимого количеством автоматизированных тест-проверок.	Более 60 %
RL.4	Процентная доля дублирующего исходного кода (дублирование кода).	Регулярная ревизия кода с целью предотвращения его дублирования.	Менее 3 %

120. В целях постоянного повышения общего качества исходного кода международной системы eTIR ЕЭК будет регулярно пересматривать и ограничивать значения целевых показателей в отношении количественных требований, касающихся надежности, которые перечислены в вышеприведенной таблице.

Таблица 18
Качественные требования, касающиеся надежности

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
RL.5	Все изменения вносятся в исходный код таким образом, чтобы снизить вероятность возникновения проблем.	При разработке международной системы eTIR ЕЭК придерживается конкретных руководящих принципов и методов передовой практики. Автоматизированные тест-проверки позволяют незамедлительно выявлять любые внесенные регрессионные ошибки. Операции подтверждения, которые не вписываются в определенные границы качества, отбраковываются.
RL.6	Внесение в исходный код любых изменений сопряжено с требованием об обеспечении надлежащей трассируемости.	СУВ, используемая для исходного кода, и система отслеживания проблем связаны между собой. В СУВ можно найти проблему, связанную с конкретной операцией подтверждения, при этом все такие операции должны содержать ссылку на ту или иную проблему.

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
RL.7	Исключение из процедур разработки как можно большего числа избыточных, ручных и подверженных возникновению ошибок задач.	Создание конвейера непрерывной интеграции, освобождающего ИТ-специалистов от выполнения рутинных задач и позволяющего им быстро получать отзывы о качестве изменений, вносимых ими в исходный код.

14. Возможность повторного использования

121. Повторное использование — это использование в процессе разработки программного продукта тех или иных форм существующих активов. Такие активы являются целевыми или побочными продуктами, созданными в ходе цикла разработки средств программного обеспечения, и они включают в себя код, программные компоненты, пакеты программ для тестирования, проектные решения и документацию.

122. Основная цель повторного использования заключается в том, чтобы избежать необходимости «заново изобретать колесо». Благодаря использованию современной инженерии разработки программного обеспечения и объектно-ориентированных языков программирования повторное использование существующих программных компонентов не представляет трудностей. Кроме того, такой подход актуален не только в случае компонентов программного обеспечения, но и в случае методов и программных платформ, поскольку разработка этих стандартных подходов сопряжена с задействованием обширного опыта и передовой практики. Ниже приводятся примеры повторного использования, связанные с разработкой системы eTIR:

- управление проектами: Секретариатом ООН была выбрана методология управления проектами PRINCE2® (PRojects IN Controlled Environments), и ЕЭК адаптировала этот метод для его использования в управлении собственными проектами;
- архитектура корпоративных приложений: Для решения архитектурных задач в ЕЭК используются несколько аспектов платформы TOGAF® (The Open Group Architecture Framework);
- разработка программного обеспечения: Для разработки и поддержания международной системы eTIR ЕЭК придерживается гибкой методологии разработки (Agile methodology) и использует ряд практических подходов DevOps (системной инженерии);
- управление услугами: Для своих процедур, связанных со службой поддержки eTIR, и для взаимодействия с подразделением ООН, осуществляющим хостинг международной системы eTIR, ЕЭК использует ряд аспектов библиотеки ITIL® (Information Technology Infrastructure Library);
- осведомленность в вопросах безопасности: Для получения информации о последних угрозах в области безопасности и о передовом опыте ЕЭК использует несколько аспектов OWASP® (Open Web Application Security Project).

123. В большинстве случаев следует отдавать предпочтение выбору элемента, пригодного для повторного использования, а не разрабатывать его самостоятельно. Если объем функциональных возможностей существующего элемента соответствует поставленным требованиям, то его повторное использование, как правило, позволяет сэкономить время и деньги. Что касается программных компонентов или продуктов, то речь может идти либо о программном обеспечении с открытым исходным кодом (ПО с ОИК), либо о каком-либо проприетарном программном обеспечении. В процессе принятия решений следует учитывать следующие аспекты: ССВ (включая обучение и поддержку), зрелость и устойчивость решения, его преимущества и недостатки.

124. В нижеследующей таблице указано требование, касающееся повторного использования.

Таблица 19
Требование, касающееся повторного использования

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
RU.1	Повторное использование существующих методов, программных платформ, программного обеспечения и системных компонентов для экономии времени и достижения более высокого качества результата.	В случае появления нового требования или в ходе регулярной оценки повторно используемых в настоящее время элементов ЕЭК занимается поиском существующих опций и, применяя свой подход к принятию решений, выбирает наилучший вариант.

15. Безопасность

125. Все аспекты, связанные с безопасностью и соответствующими техническими требованиями к международной системе eTIR, будут описаны позднее в отдельной части документа, озаглавленной «Безопасность системы eTIR».

E. Процессы разработки

1. Введение

126. В настоящем разделе описываются процессы, которые используют эксперты ЕЭК по информационным технологиям (ИТ) (здесь и далее «эксперты по ИТ») для разработки международной системы eTIR с целью дать Договаривающимся Сторонам Конвенции МДП и другим заинтересованным сторонам eTIR четкое представление об этих аспектах. Прозрачность этих процессов позволяет также всем заинтересованным сторонам eTIR выходить со своими предложениями по их совершенствованию, конечной целью которых является создание в долгосрочной перспективе более эффективной и действенной системы eTIR.

2. Общие руководящие принципы

127. Эксперты по ИТ уделили должное время для подготовки, обсуждения и принятия собственных внутренних руководящих принципов, связанных со всеми аспектами разработки и обслуживания международной системы eTIR. В основу разработки данных рекомендаций положены передовые виды практики в области информационных технологий и опыт, накопленный специалистами в этой области. Тем не менее они отнюдь не являются чем-то незыблемым, поэтому эксперты по ИТ будут и впредь постоянно изыскивать возможности их совершенствования. Это особенно важно в такой сфере знаний, как информационно-коммуникационные технологии, которая развивается столь быстрыми темпами.

128. В процессе подготовки и уточнении руководящих указаний, а также во всех нормотворческих процессах эксперты по ИТ руководствуются тремя руководящими принципами, подробно изложенными в начале настоящего документа.

129. В ходе принятия того или иного технического решения по любому аспекту, связанному с международной системой eTIR, эксперты по ИТ следуют обычной передовой практике, сложившейся в процессе принятия решений. Время, необходимое для изучения и анализа новых тенденций, подходов и возможных продуктов, уже запланировано. Затем необходимо будет сформулировать возможные варианты и составить перечень их соответствующих преимуществ и недостатков, после чего можно будет принимать решение на предмет выбора наилучшего варианта. Принятые решения оформляются документально вместе с обоснованием, которое подтверждает правомерность такого выбора, с целью обеспечить надлежащую организационную преемственность.

130. И наконец, в процессе принятия решений эксперты по ИТ также признают и учитывают принцип Парето[25], позволяющий найти оптимальное решение, которое в свою очередь позволяет обеспечить большинство преимуществ за минимально возможный период времени. Этот принцип обычно подтверждается в тех случаях, когда он применяется в процессе разработки программного обеспечения, и приобретает даже еще большую актуальность в трудных экономических условиях, когда требуется обеспечить разумное расходование средств.

3. Методология разработки

131. Успешное создание такой крупной информационной системы, как международная система eTIR, предполагает необходимость надлежащего соблюдения методологии соответствующего проекта в области ИТ. В короткой — хотя и интенсивной — истории ИТ было предложено и проверено несколько парадигм и моделей (например, «водопадный тип процесса разработки», «V-модель», разработка упрощенной версии, поэтапное внедрение в практику, гибкие методы управления и т. д.). В 2001 году благодаря появлению нескольких новых гибких методологий (например, методики экстремального программирования и проведения планерок) после принятия манифеста гибкой разработки программного обеспечения[26] и его двенадцати принципов в этой сфере был сделан существенный прорыв. С тех пор многие ИТ-проекты были реализованы на практике с использованием гибких методологий, которые дают наибольшие шансы на успех в таких сложных начинаниях.

132. При разработке международной системы eTIR ЕЭК решила следовать гибкой методологии, близкой к концепциям «планерок» и «канбан». Этот подход направлен на достижение следующих целей: разработка ценного и работающего программного обеспечения, умение быстро реагировать на изменения, обеспечение высокого уровня качества и прежде всего удовлетворение потребностей выгодополучателей.

133. Вся работа, которую необходимо было проделать, разбивается на задачи (здесь и далее называемые «проблемами») и сохраняется в списке под названием «невыполненная работа по eTIR». Разработка осуществляется в течение нескольких недель методом итерации. В начале каждого этапа итерации эксперты по ИТ выбирают из невыполненной работы по eTIR набор проблем с целью определить накопившиеся недоработки по программному обеспечению в процессе итерации. На этом этапе итерации выполняются работы по внедрению, тестированию и документальному оформлению результатов по этим выбранным видам работы, которые затем еще раз рассматриваются в конце данного этапа итерации с целью определить окончательный цикл итерации (поскольку ряд не до конца решенных вопросов из этого цикла можно удалить). По завершении последнего этапа, на котором производится окончательная проверка качества итерации, полученный результат этого процесса может рассматриваться в качестве потенциально готовой версии.

[25] См. en.wikipedia.org/wiki/Pareto_principle.
[26] См. agilemanifesto.org.

Рисунок XIII
Разработка методом итерации

134. Принимая во внимание тот факт, что международная система eTIR должна быть разработана один раз, после чего она должна работать и поддерживаться надлежащим образом бесконечно долго, ЕЭК также приняла решение перенять некоторые виды практики в рамках интеграции процессов разработки и эксплуатации ПО (известной под названием «DevOps»), имеющие целью предотвратить проблемы, которые могут возникнуть при переходе от этапа разработки данного проекта к этапу его реализации. Эти виды практики (которые более подробно описаны ниже) включают следующее: инвестирование в автоматизированное тестирование, акцент в работе на непрерывную интеграцию, анализ телеметрических параметров и критический разбор случаев сбоя в работе.

4. Руководящие принципы разработки

135. Основополагающим элементом руководящих принципов разработки является стандартное руководство по кодированию и обширная литература по ИТ по этой тематике[27]. Основой всего спектра технологий, используемых в международной системе eTIR, является язык «Java», притом что для эффективного программирования на этом языке эксперты по ИТ используют современную и известную интегрированную среду разработки (IDE) и опорную инфраструктуру. Данная среда IDE также позволяет включать в нее некоторые из руководящих принципов разработки (доступ к системе контроля версий (VCS), инструмент статического анализа кода, правила форматирования кода).

136. В качестве VCS международной системы eTIR эксперты по ИТ используют систему «Гит» и следуют в этом случае обычной передовой практике, связанной с этим продуктом. Модификации, вносимые в исходную программу, регулярно фиксируются и переносятся в центральное хранилище в целях совместного использования всеми разработчиками и предотвращения потери результатов своей работы в случае отказа соответствующей рабочей станции. Крупные разработки, как правило, выполняются на отдельных ветвях программного кода. В конечном итоге, в целях обеспечения высокого качества каждого вклада в работу внесение изменений в исходную программу в центральное хранилище предполагает необходимость предварительных шагов (подробно описанных в следующих разделах).

5. Руководство по ведению журнала

137. Служба ведения журналов международной системы eTIR имеет очень важное значение, поскольку она обеспечивает наличие данных, необходимых для работы системы исключения возможности отказа и подготовки показателей, необходимых для

[27] В частности, со стороны его авторов: Кента Бека, Мартина Фаулера и Роберта К. Мартина.

мониторинга глобального состояния системы. Как поясняется в практике работы системы «DevOps», эти показатели (или телеметрические параметры) являются единственным способом для экспертов по ИТ контролировать работу международной системы eTIR и получать оповещения о любой возникающей проблеме и, таким образом, быть в состоянии эффективно устранять ее, прежде чем с ней свяжутся конечные пользователи.

138. Служба ведения журнала генерирует несколько файлов, каждый из которых выполняет свою функцию. Каждая запись в журнале регистрации сопровождается информацией с указанием даты и времени ее поступления и потенциальной серьезности:

- **сообщения eTIR**: все содержимое входящих и исходящих сообщений сохраняется в файле для хранения всех потоков связи между международной системой eTIR и подключенными к ней информационными системами. Эти данные затем используются системой исключения возможности отказа и могут быть получены по запросу Договаривающихся Сторон Конвенции МДП;
- **база данных**: все запросы в направлении баз данных eTIR сохраняются в файле наряду со временем, которое потребовалось для реагирования на эти запросы. Это позволяет непрерывно измерять режим выполнения этих запросов и выдавать специалистам по ИТ соответствующие показатели, позволяющие им выявлять и устранять потенциальные «узкие места», а также более эффективно планировать будущие требования к масштабируемости;
- **МБДМДП**: все запросы в направлении интерфейса с Международным банком данных МДП (МБДМДП) сохраняются в файле наряду со временем, которое потребовалось для реагирования на эти запросы. Это позволяет непрерывно измерять режим реагирования на эти запросы и выдавать специалистам по ИТ соответствующие показатели, позволяющие им дополнительно оптимизировать работу данного интерфейса;
- **приложение**: все события, отраженные в модуле веб-сервисов eTIR, сохраняются в соответствующем файле, предназначенном для хранения всей последовательности событий, которая используется системой мониторинга для оповещения о любой серьезной проблеме, возникшей в международной системе eTIR, в режиме реального времени. Эти данные также используются для выяснения какой-либо прошлой проблемы для определения основной причины ее возникновения.

6. Руководство по тестированию

139. Тесты являются одним из важнейших компонентов разработки программного обеспечения. Прошлая работа в области ИТ однозначно указывает на то, что без должного внимания, уделяемого этому аспекту, вероятность провала проектов в области программного обеспечения существенно повышается. Тесты могут выполняться как вручную, так и автоматически. В случае ручного выполнения специалист, который проводит испытание, выполняет ряд операций по взаимодействию с информационной системой, подлежащей проверке, и сравнивает полученные фактические результаты с ожидаемыми. Если они совпадают, то считается, что результат тестирования положительный, а если нет, то отрицательный. Ручные тесты — это наиболее очевидное действие, которое специалист по программному обеспечению может незамедлительно применить к вновь разрабатываемому программному продукту с целью проверить, работает ли он так, как ожидается. Однако самым большим недостатком ручных тестов является то, что они зависят от человека, который их выполняет, что отнюдь не являются экономически эффективными и могут привести к ошибкам. Кроме того, они проверяют только состояние системы на момент выполнения той или иной операции, и, как следствие, их результат (положительный/отрицательный) теряет свою актуальность при изменении условий (в случае обновления исходной программы, настроек в условиях операционной среды и т. д.).

140. В настоящее время в современной практике, применимой в области технологии разработки программного обеспечения, признается, что для обеспечения высокой надежности и качества разрабатываемой информационной системы ручных испытаний уже недостаточно. Как поясняется в случае соответствующих видов практики, присущей системе «DevOps», в настоящее время тесты, проводимые в связи с возникновением конкретных частых событий (при изменении соответствующих условий, как упоминалось выше), должны быть автоматизированы с целью гарантировать отказ от необходимости возвращения системы в прежнее состояние. Действительно, в случае реализации новых возможностей или устранения дефектов в исходной программе инженеры-программисты всегда рискуют привнести нежелательные побочные последствия (например, дефекты). Для решения этой проблемы, присущей процессу разработки программного обеспечения, необходимо ввести в практику автоматизированные тесты, позволяющие проверять изменения, вносимые в исходную программу. Важно помнить, что время, затраченное на внедрение в практику автоматизированных тестов, окупится всегда. Действительно, когда система автоматизированных тестов отсутствует, количество дефектов будет гораздо большим, притом что времени, необходимого для их выявления и устранения, также придется затратить гораздо больше по сравнению с временем, необходимым для реализации автоматизированных тестов. Кроме того, регулярные проблемы, возникающие в случае тех или иных систем по причине присущих им дефектов, могут разочаровать пользователей и существенно подорвать репутацию той организации, которая отвечает за работу данной системы.

141. В настоящее время существует несколько типов автоматизированных тестов, которые обладают своими собственными характеристиками, дополняющими друг друга:

- **модульные тесты**: тесты, разработанные в целях проверки соответствия данного программного обеспечения (известного как «модуль») своему дизайну и предусмотренному алгоритму поведения. В объектно-ориентированных языках программирования, таких как «Java», единичный модуль зачастую представляет собой целый интерфейс, например класс, но может представлять собой и отдельный метод. Цель модульного тестирования состоит в том, чтобы изолировать каждую часть программы и убедиться в том, что все эти отдельные части работают правильно. Модульный тест предусматривает строгий письменный регламент, которому должна соответствовать данная часть программного кода. Модульные тесты, как правило, можно быстро разработать и затем выполнить;

- **комплексные тесты**: тесты, разработанные в целях проверки совмещенных программных модулей и их тестирования в качестве отдельной группы. Комплексное тестирование проводится в целях оценки соответствия той или иной системы заданным функциональным требованиям. Оно проводится после модульного тестирования и перед проверкой на подтверждение соответствия требованиям. В случае комплексного тестирования в качестве входных параметров используют те модули, которые подвергались модульному тестированию, группируют их в более крупные совокупности данных, подвергают их комплексным тестам, определенным в плане комплексного тестирования, и в итоге получают на выходе комплексную систему, готовую к проведению проверки на подтверждение соответствия требованиям;

- **тесты на эффективность работы**: тесты, разработанные в целях проверки соответствия данной системы программного обеспечения требованиям к эффективности работы. Эта совокупность тестов также включает в себя тесты, разработанные для моделирования заданной нагрузки (большое количество запросов), на которую рассчитано данное программное обеспечение. Этот тип тестов имеет важное значение в плане проверки того, что с течением времени эффективность программного обеспечения не снижается, прежде всего в случае добавления новых функций;

- **тесты на валидацию**: тесты, разработанные для проверки соответствия системы программного обеспечения ее спецификациям и ее предполагаемому

назначению. Обычно эти тесты являются наиболее сложными и дорогостоящими в плане реализации и поддержания, так как они предполагают моделирование соответствующих действий, выполняемых конечными пользователями на пользовательском интерфейсе (ПИ) данной системы. В конкретном контексте международной системы eTIR пользовательского интерфейса нет, поскольку обмен данными с информационными системами других участников eTIR с использованием сообщений eTIR осуществляется автоматически. Этот подход позволяет очень легко и эффективно выполнять проверки, так как после каждого сообщения с запросом на проведение теста система направляет обратно ответное сообщение, которое можно подтвердить с целью убедиться в том, что система ведет себя так, как ожидается;

- **тесты на соответствие**: они аналогичны тестам на подтверждение; в контексте системы eTIR этот тип включает также необходимые тесты, позволяющие убедиться в том, что репрезентативный набор моделируемых перевозок МДП регулируется надлежащим образом путем отправки и получения в определенной последовательности соответствующих сообщений eTIR, которые проверяются на предмет подтверждения всех сценариев. Эти тесты могут быть также сосредоточены на проверке информационной системы какой-либо одной заинтересованной стороны eTIR или включать в себя несколько таких тестов, позволяющих более точно воспроизвести реальные перевозки МДП в соответствии с процедурой eTIR.

142. В процессе разработки автоматизированных тестов специалистам по программному обеспечению также необходимо убедиться в том, что в большинстве (а то и во всех) случаях соответствующие строки исходной программы проверены и подтверждены. В частности, специалистам по программному обеспечению необходимо убедиться в том, что все пути доступа в исходной программе охвачены соответствующими тестами (эту практику и связанные с ней показатели называют «покрытием ветвей»). В дополнение к соответствующему «охвату программного кода», специалисты по программному обеспечению также должны убедиться в том, что аргументы, подтверждающие программный код, являются актуальными и исчерпывающими, в противном случае тесты не достигают своей цели.

143. Как было описано выше, обеспечение хорошего охвата программного кода является единственным устойчивым способом разработки и поддержания информационной системы, поэтому эксперты по ИТ включили эту цель и соответствующие виды практики в процессы разработки. В связи с реализацией на практике какой-либо новой функции и в порядке достижения цели в части охвата программного кода необходимо разработать нужное количество модульных тестов и тестов на подтверждение достоверности. Когда дефект исправлен, необходимо разработать еще один или несколько тестов, позволяющих предотвратить повторное возникновение той же проблемы.

7. Статический анализ программного кода

144. Статический анализ программного кода заключается в автоматической проверке качества исходной программы без его фактического прогона. Этот анализ проводится с помощью соответствующего средства, в которое загружаются правила и передовые виды практики программирования, которые в большинстве случаев определяются на протяжении многих лет мировым сообществом экспертов по ИТ. Статический анализ программного кода — это один из очень эффективных способов проведения первой проверки качества исходной программы и отличное дополнение к специализированным ручным проверкам кода, которые выполняются экспертами по ИТ на исходной программе.

145. Признавая полезность этого вида автоматизированного инструмента, эксперты по ИТ также признают необходимость совместного пересмотра применимости некоторых правил с учетом специфики международной системы eTIR. Как следствие, эксперты по ИТ устанавливают правила и их строгость таким образом, чтобы они наилучшим образом соответствовали этой специфике.

146. Статический анализ всей исходной программы международной системы eTIR проводится регулярно; к тому же эксперты по ИТ также выигрывают от интеграции этой возможности, заложенной в интегрированной среде разработки, которую они используют для программирования, в результате чего они незамедлительно видят реакцию на качество составленного ими программного кода.

147. Целью в данном случае является постепенное повышение качества исходной программы и поддержание его на очень высоком уровне на протяжении всего жизненного цикла. Это повышает удобство обслуживания и надежность исходной программы и, в конечном счете, экономит время экспертов по ИТ, что позволяет повысить эффективность их работы. Эта задача выполняется в два этапа: постепенное повышение качества исходной программы и поддержание его на высоком уровне.

148. На первом этапе эксперты по ИТ ставят в инструменте статического анализа программного кода низкокачественные шлюзы[28] и исправляют столько проблем, сколько необходимо для решения этих задач. Как только эти низкоуровневые задачи решены, их уровень постепенно поднимается, и эксперты по ИТ продолжают работать над устранением других проблем в порядке достижения новых целей. После того как качественные показатели достигнут уровня, который, по мнению экспертов по ИТ[29], является достаточным (в том числе с учетом принципа Парето), можно приступать ко второму этапу.

149. На втором этапе цель этой работы заключается в дальнейшем совершенствовании и поддержке международной системы eTIR посредством дальнейшего повышения качественных показателей шлюзов с целью добиться соблюдения всех требований, предъявляемых к качеству. В случае несоблюдения одного из параметров качества после обновления исходной программы можно принять дополнительные меры в виде направления соответствующего уведомления специалистам по ИТ, с тем чтобы они незамедлительно разобрались с этой проблемой в целях ее устранения.

8. Магистральная система непрерывной интеграции (CI)

150. В случае разработки программного обеспечения под непрерывной интеграцией (CI) понимается слияние рабочих копий в общую основную ветвь разработки несколько раз в день. Эта практика не нова (она получила начало в 1990 году) и постоянно совершенствовалась и расширялась, в результате чего она приобрела черты существующей практики «DevOps», известной как непрерывная интеграция и непрерывное развертывание (CD) или CI/CD. Эксперты по ИТ решили пока сосредоточить свою работу сначала на CI, а после того как будет достигнут соответствующий уровень доработки, они, возможно, рассмотрят вопрос и о переходе на практику CD, которая предполагает необходимость надежной опорной основы.

151. В настоящее время определение CI отражает автоматизацию всех этапов, связанных с интеграцией и проверкой изменений в исходной программе того или иного программного обеспечения. CI позволяет разработчикам программного обеспечения получить быстрый ответ по поводу качества программного кода, который они посылают в VCS, выполняя все автоматизированные тесты на базе вновь скомпонованной и развернутой версии программного обеспечения, содержащей последние модификации, внесенные в VCS. CI освобождает разработчиков программного обеспечения от рутинных, предрасположенных к ошибкам задач, связанных со сборкой, тестированием и развертыванием новой версии программного обеспечения, что позволяет им сосредоточиться на тех областях, в которых они могут проявить себя лучше всего: создавать соответствующие функциональные возможности для клиентов.

[28] Качественный показатель шлюза — это своего рода количественная цель, которая устанавливается по определенному критерию (например, «менее 10 критических проблем», «более 40 % исходной программы, охваченной тестами»).

[29] Как это детально закреплено в требованиях к надежности международной системы eTIR.

152. Эксперты по ИТ создали этот информационный канал CI, представляющий собой специализированное программное средство, которое определяет и конфигурирует несколько действий, выполняемых в виде последовательных автоматизированных этапов. Эти этапы выполняются каждый раз, когда один из экспертов по ИТ обновляет программный код в VCS. Эти этапы предусматривают следующее:

a) **компоновка**: магистральная система CI обнаруживает, что в VCS была произведена фиксация соответствующего изменения, после чего она извлекает самую последнюю версию исходной программы и собирает новые компоненты программного обеспечения, которые подверглись этому воздействию в результате изменения программного кода;

b) **первый этап тестирования**: после этого выполняются автоматизированные модульные и интеграционные тесты на только что созданных программных компонентах с целью проверить, что в результате изменения кода возвращение системы в прежнее состояние не требуется;

c) **развертывание в среде SIT**[30]: только что созданные программные компоненты развертываются в среде SIT в качестве полнофункционального варианта международной системы eTIR;

d) **второй этап тестирования**: далее выполняются автоматизированные тесты на новом варианте международной системы eTIR в порядке дальнейшей проверки на самом высоком уровне с целью убедиться в том, что в результате изменения программного кода возвращение системы в прежнее состояние не требуется.

153. Если во время одного из этапов происходит сбой (например, даже в случае непрохождения всего лишь одного теста), магистральная система CI останавливается и специалистам по ИТ направляется уведомление о сбое на их платформе для совместной работы. Для того чтобы обеспечить быструю обратную связь с экспертом по ИТ, который вносит изменения в систему VCS, время выполнения всех этапов не должно превышать 30 минут. Эта магистральная система CI сочетает в себе несколько самых передовых видов практики, описанных выше, и представляет собой отличный способ обеспечить высокую надежность международной системы eTIR и повысить производительность труда экспертов по ИТ.

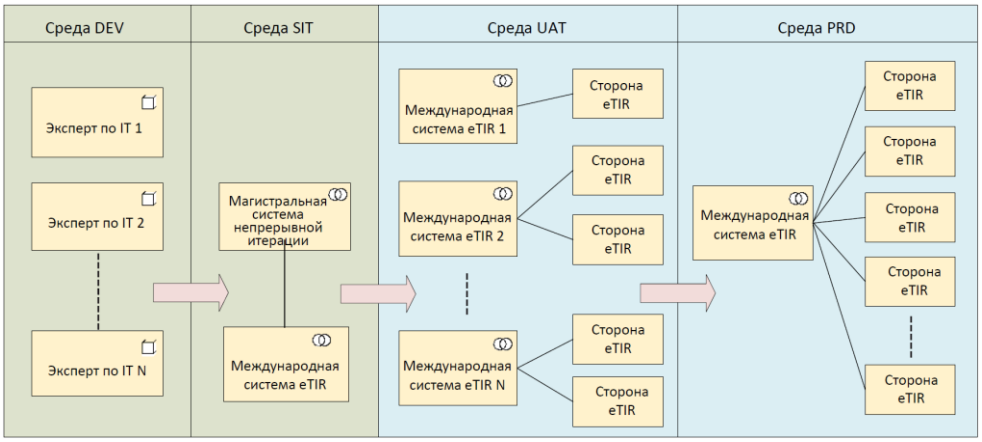
9. Операционные среды

154. Следуя современному передовому опыту, накопленному в отрасли информационных технологий, эксперты по ИТ создали и скомпоновали четыре различные операционные среды в порядке дальнейшего развития и поддержания международной системы eTIR в наиболее благоприятных условиях. Одна из проблем в управлении несколькими операционными средами заключается в необходимости ограничить количество расхождений между каждой из них во избежание сбоев, связанных с конкретной средой. Для ограничения вероятности возникновения таких сбоев все эксперты по ИТ устанавливают и соблюдают специальные процедуры разработки.

155. На рисунке ниже показаны различные операционные среды, которые затем описываются в следующих пунктах.

[30] Системное интеграционное тестирование (SIT), дополнительную информацию см. в следующем разделе.

Рисунок XIV
Операционные среды международной системы eTIR



156. **Среда разработки (DEV)**: каждый эксперт по ИТ имеет свою рабочую станцию, на которой он может разрабатывать и проверять локальную копию международной системы eTIR, не вмешиваясь в работу других. После подготовки и проверки внесенного изменения в программный код специалист по ИТ фиксирует его в VCS, где его можно автоматически развернуть и протестировать магистральной системой CI в среде SIT.

157. **Среда системного интеграционного тестирования (SIT)**: эта внутренняя операционная среда используется магистральной системой CI как временное местоположение, где компонуются, развертываются и автоматически тестируются новые версии международной системы eTIR. После подтверждения соответствующего пакета изменений программного кода в этой среде, эксперты по ИТ могут принять решение о создании и внедрении последней версии международной системы eTIR в среду UAT.

158. **Среда проверки приемлемости для пользователей (UAT)**: эта среда доступна заинтересованным сторонам eTIR для проведения тестов в контексте их проектов по подключению к системе. На данный момент доступно несколько копий международной системы eTIR, притом что каждый заинтересованный участник eTIR получает доступ к одной или нескольким из этих копий. Проверки соответствия международной системы eTIR и информационных систем участников eTIR также проводятся в среде UAT. После обстоятельного тестирования соответствующей версии международной системы eTIR в среде UAT ее можно перенести в среду PRD.

159. **Производственная среда (PRD)**: эта среда является уникальной копией международной системы eTIR, которая доступна только тем заинтересованным сторонам eTIR, которые завершили свой проект по подключению к системе. Эта «живая» среда является единственной, которая используется для осуществления перевозок МДП в соответствии с процедурой eTIR.

10. Руководство по базе данных

160. Для регистрации информации, получаемой в сообщениях eTIR, база данных eTIR использует соответствующую систему управления базой данных (СУБД). Этот компонент является ядром международной системы eTIR, поэтому к его разработке и обслуживанию следует подходить с максимальной тщательностью.

161. Эта структура базы данных eTIR была унаследована от пилотных проектов eTIR, однако эксперты по ИТ выявили несколько возможностей для усовершенствования и оптимизации, которые планируется внедрять на постепенной основе. Для отслеживания, компоновки и применения изменений схемы (структуры) базы данных эксперты по ИТ используют специализированный инструмент под названием «Liquibase». Кроме того, эта библиотека позволяет управлять изменениями, которые вносятся в основные и справочные данные, хранящиеся в БД.

162. В контексте системы eTIR «основные и справочные данные» означают данные о заинтересованных сторонах, ролях и данных, используемых для классификации или группирования данных, обрабатываемых и хранящихся в сообщениях eTIR (например, идентификационные данные участников eTIR, коды стран, виды гарантий, классификация грузов и т. д.). Эти данные меняются в редких случаях и предполагают необходимость кропотливой работы.

163. Использование этого инструмента также позволяет легко проверить изменения, которые были внесены в различные копии базы данных eTIR, имеющиеся во всех средах, перечисленных в предыдущем разделе. Это важно для того, чтобы последние изменения, внесенные в схему или в основные и справочные данные, последовательно применялись во всех средах после выполнения соответствующих процедур управления системой выпуска.

11. Реагирование на проблемы

164. Одним из важнейших аспектов принятой гибкой методологии является должным образом определенное и эффективное реагирование на возникающие проблемы. В этом контексте проблема может представлять собой запрос на какую-либо функцию, запрос на внесение соответствующего изменения или отчет о выявленном дефекте. Все изменения в модели данных eTIR, в исходной программе или в документации международной системы eTIR сначала должны регистрироваться в системе отслеживания проблем на уровне ЕЭК. Это необходимо для обеспечения правильной прослеживаемости всех изменений и позволяет убедиться в том, что в систему внесены только санкционированные изменения.

165. При входе в систему отслеживания проблем специалист по ИТ принимает все меры с целью обеспечить документальное оформление всех необходимых деталей, с тем чтобы любой другой специалист по ИТ мог разобраться в том, что нужно сделать. Это также является одним из необходимых предварительных условий обеспечения надлежащей организационной преемственности, позволяющей исключить неблагоприятные последствия потенциальной текучести кадров в ЕЭК.

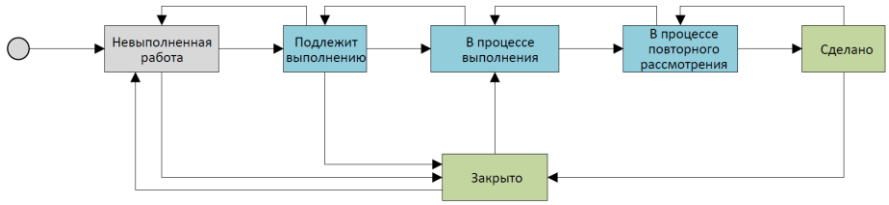
166. Эксперты по ИТ согласовали ряд мероприятий, которые должны выполняться на различных этапах жизненного цикла любой проблемы, прежде чем ее можно будет считать окончательно решенной. В названии этих этапов указывают разный статус проблем. Это — «критерий готовности», который определяется следующим образом:

- **Критерий готовности (DOD)**: случай, когда все условия или критерии принятия[31], которым должна удовлетворять данная проблема, выполнены. Цель в этом случае заключается в обеспечении надлежащего уровня качества и надежности системы в любой момент времени. С точки зрения предотвращения проявления дефектов в среде PRD время, затраченное на все эти мероприятия, всегда окупается. Меньшее количество дефектов дает возможность не нервничать и не тратить время на поиск и устранение неисправностей и позволяет не допустить ухудшения репутации ЕЭК.

167. Новой возникшей проблеме присваивают статус «невыполненная работа», указывающий на ее принадлежность к невыполненной работе по eTIR, а также соответствующий приоритет. Проблемы — это своего рода комплекс элементарных работ, которые поручаются специалистам по ИТ координатором ИТ в тот момент, когда они отбираются из числа накопившихся недоработок в процессе итерации. На следующем рисунке показан жизненный цикл проблем с различным статусом, который может быть присвоен той или иной проблеме, и нижеследующий список с их описанием.

[31] Условия и критерии принятия определены ниже в данном разделе.

Рисунок XV
Жизненный цикл проблемы



- **невыполненная работа**: данная проблема была идентифицирована и зарегистрирована в системе отслеживания проблем, но еще не выбрана в целях ее решения;
- **подлежит выполнению**: данная проблема был выбрана в целях ее решения в процессе итерации и передана эксперту по ИТ, которому необходимо выполнить шаги, предусмотренные этапом DOD «подлежит выполнению» (см. ниже);
- **в процессе выполнения**: данная проблема находится на стадии решения экспертом по ИТ, которому необходимо выполнить все шаги, предусмотренные этапом DOD «в процессе выполнения»;
- **в процессе повторного рассмотрения**: данная проблема находится на стадии рассмотрения другим экспертом по ИТ в целях проверки некоторых аспектов, связанных с обеспечением качества, путем выполнения всех шагов, связанных с этапом «в процессе повторного рассмотрения», которые предусмотрены DOD;
- **сделано**: проблема устранена (решена и рассмотрена повторно) и будет окончательно подтверждена экспертами по ИТ в ходе регулярных совещаний, на которых будут окончательно закрыты все поставленные вопросы, касающиеся среды PRD;
- **закрыто**: проблема либо решена (после этапа «сделано»), либо закрывается, так как она не подлежит исправлению, либо считается, что она дублирует другую проблему (после этапа «невыполненная работа» или «подлежит выполнению»).

168. Критерий DOD описывает следующие основные цели и критерии приемлемости на вышеупомянутых этапах:

- **подлежит выполнению**: проблема достаточно детализирована и подкреплена в достаточной степени справочной информацией, что дает возможность ее понять любому другому эксперту по ИТ; кроме того, сделана предварительная оценка необходимого времени;
- **в процессе выполнения**: необходимые изменения полностью внесены во все соответствующие ИТ-ресурсы (модель данных eTIR, исходная программа, документация). Все требования к качеству и надежности удовлетворены (включая проверки, выполняемые магистральной системой CI и инструментом статического анализа), и все применимые рекомендации выполнены;
- **в процессе повторного рассмотрения**: результаты выполнения задач на этапе «в процессе выполнения» проверяются другим экспертом по ИТ. В частности, проверяется охват тестированием обновленной исходной программы.

12. Руководство по документации

169. ЕЭК ведет три вида документации, связанной с международной системой eTIR. Первый тип соответствует спецификациям eTIR, в случае которых процедуры внесения поправок описаны в статье 5 Приложения 11 к Конвенции МДП.

170. Второй тип соответствует внутренней документации, которая необходима ЕЭК для надлежащей разработки, эксплуатации и обслуживания международной системы eTIR. Эта документация готовится и обновляется экспертами по ИТ из ЕЭК и регулируется в защищенной системе СУБЗ, которая предлагает возможности

поддержки версий в целях надлежащего обеспечения организационной преемственности. Внутренняя документация содержит, конфиденциальную информацию, касающуюся в частности:

- разработки: руководства, техническая документация, обучение, документация заинтересованных сторон, соответствующие стандартные операционные процедуры (СОП) и прочее;
- управления: группа административного сопровождения, протоколы совещаний, соответствующие СОПы и т. д.;
- операций: связь с договаривающимися сторонами, операционные среды, служба поддержки eTIR, соответствующие СОПы и т. д.

171. Третий тип соответствует документации, которая готовится ЕЭК для заинтересованных сторон eTIR в целях подключения их информационных систем к международной системе eTIR. Эти документы размещены на специальном веб-сайте eTIR[32] для ознакомления заинтересованных сторон eTIR. Эти документы готовятся в дополнение к спецификациям eTIR с целью содействовать реализации проектов по подключению к системе и налаживании обратной связи в процессе их реализации. Они служат для ЕЭК в какой-то мере одним из способов, позволяющих постоянно уточнять различные аспекты системы eTIR на более частой и гибкой основе. Все эти документы всегда полностью соответствуют Приложению 11 и той версии спецификаций eTIR, которая положена в их основу.

13. Управление версиями

172. ЕЭК управляет исходной программой международной системы eTIR и изменениями, которые вносятся в схему и «основные и справочные данные» базы данных eTIR с помощью VCS. ЕЭК выбрала систему «Гит» в качестве своей VCS и использует внутреннюю и защищённую платформу в качестве центрального «Гит-хранилища».

173. Эксперты по ИТ следуют обычным видам передовой практики IT-отрасли, связанным с системой «Гит», и особенно с «DevOps». В частности, эксперты по ИТ должны часто фиксировать и «проталкивать» свой программный код в центральное «Гит-хранилище» после выполнения ими всех тестов на локальном уровне с целью убедиться в том, что это не приведет к сбою в работе магистральной системы CI. Каждая фиксация должна содержать изменения, связанные только с одной проблемой, а в комментарии к фиксации следует четко указывать, к какой проблеме она относится, и описывать суть этих изменений.

174. Соответствующие ветви создаются и используются в нескольких случаях. Во-первых, их может создать специалист по ИТ, которому необходимо работать над сложной функцией, которую невозможно сразу же зафиксировать на основной ветви. После того как данная функция завершена и протестирована, эта ветвь подсоединяется к основной ветви. Во-вторых, каждый раз при выпуске версии международной системы eTIR в среде PRD создается соответствующая ветвь в соответствии с руководящими принципами управления версиями. При развертывании новой версии международной системы eTIR в среде UAT или в среде PRD создаются также соответствующие метки.

175. Что касается номера версии международной системы eTIR, то ЕЭК выбрала подход, который предполагает использование следующих трех номеров:

- **основной номер версии**: он увеличивается, когда происходит критическое изменение на уровне ППИ, которое позволяет заинтересованным сторонам eTIR подключиться к международной системе eTIR. Он также может быть увеличен в том случае, когда в международную систему eTIR вносятся существенные изменения в отсутствие изменений на уровне ППИ;

[32] См. etir.org/documentation.

- **второстепенный номер версии**: он увеличивается в любом ином случае, кроме тех, которые влияют на основные номера пакета исправлений. При увеличении основного номера версии второстепенный номер версии устанавливается на 0;
- **номер версии пакета исправлений**: используется только в том случае, когда один или несколько пакетов исправлений должны быть развернуты на уровне версии, которая уже развернута в среде PRD, что обусловлено желанием не создавать новую версию международной системы eTIR.

176. Основной и второстепенный номера версий, а также номер версии пакета исправлений, если он существует, всегда обновляются одновременно на всех программных компонентах международной системы eTIR и отражают ее номер версии по форме XX.YY.ZZ, где XX — большой, YY — малый номера версий и ZZ — номер версии пакетов исправлений (игнорируется, если он равен 0). Ниже приведены два примера номера версии для международной системы eTIR:

- **международная система eTIR 4.15**, где 4 — основной номер версии, а 15 — второстепенный номер версии (частый случай);
- **международная система eTIR 4.15.1**, где 4 — основной номер версии, 15 — второстепенный номер версии и 1 — номер версии пакета исправлений (редкий случай).

14. Управление версиями

177. Управление версиями — это процесс управления, планирования, диспетчеризации и контроля над созданием программного обеспечения в рамках различных этапов и сред, включая тестирование и развертывание версий программного обеспечения. В контексте международной системы eTIR речь идет о процессе, отраженном на следующем рисунке и описанном в разъяснении следующих этапов.

Рисунок XVI
Процесс управления версиями

a) **определить невыполненную работу в процессе итерации**: из невыполненной работы по eTIR эксперты по ИТ выбирают те проблемы, над которыми следует работать в процессе итерации, и определяют номер версии нового выпуска. Каждый выпуск имеет свой собственный уникальный номер версии, который является обязательным, если выпуск должен быть развернут в среде UAT или PRD;

b) **проанализировать невыполненную работу в процессе итерации**: эксперты по ИТ проверяют проблемы, которые считаются «решенными», и изменяют либо продолжительность итерации, либо список проблем, подлежащих решению в случае данной версии. В конце этого процесса все проблемы должны быть решены, проверены и оформлены документально, а качественные параметры шлюза переведены в среду SIT. Сопроводительные записки с объяснением изменений, внесенных этой новой версией, должны быть подготовлены;

c) **развернуть в среде UAT**: заинтересованные стороны eTIR, работающие над копиями международной системы eTIR, информируются о предстоящем развертывании новой системы. Затем новую версию развертывают во всех копиях международной системы eTIR, а соответствующие базы данных eTIR перезагружают. Сопроводительные записки доводят до сведения заинтересованных сторон eTIR;

d) **протестировать в среде UAT**: новую развернутую копию затем проверяют заинтересованные стороны eTIR в течение определенного периода времени, согласованного всеми сторонами. Эксперты по ИТ выясняют, требуется ли новое проведение тестов на соответствие или нет. Любая выявленная проблема подлежит передаче в службу поддержки eTIR для регистрации и отнесения к соответствующей категории. В случае выявления одной или нескольких блокирующих или существенных проблем, их либо устраняют, либо текущий выпуск аннулируют и готовят новый выпуск, в котором в качестве приоритета указывают проблему(ы), подлежащую(ие) устранению. Если эти проблемы устранены, то до подтверждения обновленного выпуска его необходимо развернуть в среде UAT и протестировать заново всеми заинтересованными сторонами eTIR в течение определенного периода времени. Второстепенные проблемы можно включить в категорию невыполненных работ eTIR в целях их устранения в последующем выпуске;

e) **развернуть в среде PRD**: если по истечении установленного периода тестирования в среде UAT не было сообщено о каких-либо существенных проблемах, то этот выпуск можно планировать для развертывания в производственной среде после надлежащего информирования заинтересованных сторон eTIR. После развертывания в этой конечной среде служба поддержки eTIR активно отслеживает телеметрические параметры с целью убедиться в том, что все работает правильно.

178. Впоследствии, если в производственной среде будет выявлена какая-либо проблема, то в этом случае возможны три варианта:

a) **проблема в блокировке**: эксперты по ИТ возвращают систему на предыдущую версию PRD и соответствующим образом информируют все заинтересованные стороны eTIR;

b) **проблема по существу**: эксперты по ИТ быстро готовят соответствующий пакет исправлений, выполняют все необходимые тесты в среде SIT и развертывают его в среде PRD в целях устранения данной проблемы. Все заинтересованные стороны eTIR информируются соответствующим образом;

c) **проблема носит второстепенный характер**: эту проблему регистрируют и вносят в категорию невыполненных работ eTIR для фиксации в последующем выпуске.

F. Процессы обслуживания

1. Введение

179. В данном разделе описываются процессы, которым следуют эксперты по ИТ из ЕЭК в порядке поддержки и обслуживания международной системы eTIR в целях обеспечения ее правильной работы, надлежащего устранения неполадок, а также прогнозирования и предотвращения возможных проблем в будущем. В этом разделе также описывается процедура, которой должны следовать заинтересованные стороны eTIR в случае сообщения о какой-либо проблеме, и содержится информация о внутренних мерах, принимаемых в целях ее устранения.

2. Непрерывное совершенствование

180. Один из основополагающих принципов практики «DevOps» заключается в применении подхода, в основу которого положен принцип непрерывного совершенствования. Это означает, что ни один из созданных продуктов (программное обеспечение, процессы, документация и т. д.) не является окончательным, так как их всегда можно улучшить. Это особенно актуально в том случае, если поднимается

какой-либо вопрос (дефект системы, недостаток процесса, пропуск или неточность в документации), который всегда следует рассматривать как возможность для улучшения. Этот принцип аналогичен принципу, используемому в цикле Деминга или в концепции ПОПД[33].

181. Этот подход свидетельствует о том, что эксперты по ИТ признают важность постоянного использования возможности извлечения уроков из возникших проблем с целью предотвратить повторное возникновение таких же проблем в будущем (или, по крайней мере, снизить вероятность их повторения в дальнейшем в результате принятия соответствующих мер). В этой связи важно потратить время на определение первопричины возникшей проблемы, с тем чтобы суметь полностью ее устранить и, по возможности, улучшить или оптимизировать соответствующие процессы. Этот подход также применяется в процессах разработки, однако он особенно важен в процессах технического обслуживания, так как их основные цели — это урегулирование и предотвращение проблем. Основные процессы, упомянутые выше, показаны на следующем рисунке. Они также поясняются в нижеследующих разделах.

Рисунок XVII
Процесс непрерывного совершенствования

3. Реагирование на проблемы

182. В процессе технического обслуживания возникают три различных типа проблем, которые имеют свои особенности и решаются с помощью специальных процедур. Эти три типа проблем отражены на нижеследующем рисунке.

[33] См. раздел en.wikipedia.org/wiki/PDCA.

Рисунок XVIII
Типы проблем, связанных с обслуживанием

183. Более подробная информация по запросам содержится в разделе, посвященном службе поддержки eTIR. Оповещения более подробно описаны в разделе, посвященном системе управления мониторингом. Инциденты более подробно описаны в разделе, посвященном системе урегулирования инцидентов.

4. Служба поддержки eTIR

184. Служба поддержки eTIR является единым национальным координатором (ЕНК) для заинтересованных сторон eTIR в случае подачи любых запросов, связанных с системой eTIR. Это можно сделать, отправив соответствующее сообщение на его электронный адрес (etir@un.org) или с помощью формы «contact us» (связаться с нами) на веб-сайте eTIR[34]. Служба поддержки eTIR состоит из экспертов по ИТ и профильных экспертов Конвенции МДП ЕЭК.

185. Запросы, полученные службой поддержки eTIR, отправляются соответствующим сотрудником службы поддержки (уровень-1) соответствующему специалисту (уровень-2) в зависимости от характера запроса. Запросы в связи с инцидентом или технической проблемой рассматриваются в приоритетном порядке.

186. В контексте проектов по обеспечению взаимосвязи служба поддержки eTIR оказывает заинтересованным сторонам помощь в подключении их информационных систем к международной системе eTIR. Эти проекты находятся на более продвинутой стадии процессов разработки, притом что на начальном этапе проекта заинтересованные стороны eTIR сами определяют наиболее оптимальные способы общения со службой поддержки eTIR в целях получения соответствующей информации и подачи любого запроса. Учитывая ограниченные ресурсы службы поддержки eTIR, ее помощь ограничивается предоставлением экспертам заинтересованных сторон eTIR соответствующей информации и руководящих указаний в связи с их проектами по налаживанию взаимосвязи. Например, служба поддержки eTIR не может непосредственно вносить изменения в информационные системы участников eTIR с целью их подключения к международной системе eTIR.

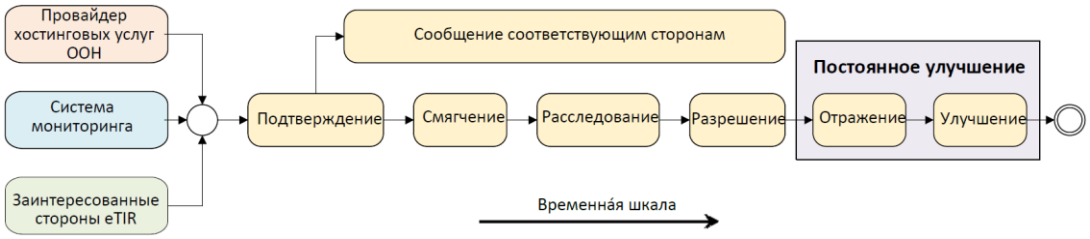
5. Реагирование на инциденты

187. Инциденты, как правило, представляют собой технические проблемы со значительными последствиями, которые должны решаться службой поддержки eTIR в приоритетном порядке. Инциденты характеризуются тем или иным уровнем тяжести, который определяет тип ответных мер, подлежащих принятию в каждом конкретном случае: критический, существенный и второстепенный. Весь процесс реагирования на инциденты строится на методологии управления услугами

[34] См. etir.org/contact-us.

Библиотеки инфраструктуры информационных технологий (ИТИЛ) и описан на нижеследующей диаграмме. Его этапы более подробно описаны ниже.

Рисунок XIX
Процесс реагирования на инциденты



a) **принять к сведению**: после оповещения эксперты по ИТ подтверждают инцидент в качестве (не ложнопозитивного) и текущего (еще не урегулированного). Они определяют его масштабы (затронутые компоненты), степень тяжести и перечень заинтересованных сторон. С этого момента все действия заносятся в журнал для дальнейшего анализа на этапе «отображение»;

b) **оповестить заинтересованные стороны**: прозрачное общение с заинтересованными сторонами по поводу инцидента имеет важное значение для информирования сторон о предполагаемом времени, необходимом для решения проблемы, поскольку это может побудить стороны принять какие-либо конкретные меры (например, воспользоваться резервными процедурами). Эксперты по ИТ принимают решение по поводу содержания и частоты сеансов связи до тех пор, пока инцидент не будет урегулирован (этап e));

c) **смягчить последствия**: по возможности, меры по смягчению последствий применяются либо в целях снижения остроты проблемы, либо в целях ее временного решения;

d) **расследовать**: эксперты по ИТ выделяют время, необходимое для всестороннего расследования инцидента и определения его первопричин(ы);

e) **урегулировать**: после проведения расследования первопричина(ы) устраняется(ются) и корректируется(ются), и инцидент должен считаться разрешенным, после чего можно переходить к следующему этапу;

f) **отобразить**: Эксперты по ИТ собирают все данные и информацию о действиях, предпринятых на данный момент в целях разрешения данного инцидента, и проводят совещание по анализу полученных результатов. Цель этой работы состоит в том, чтобы глубже взглянуть на инцидент и выяснить, что произошло, почему это произошло, как на это отреагировали эксперты по ИТ и что можно сделать, чтобы предотвратить повторение такого рода инцидентов, а также улучшить ответные действия в будущем в условиях взятия на себе коллективной ответственности за этот инцидент. В ходе этого совещания готовится соответствующий «отчет об инциденте» и с учетом этого определяются и планируются последующие действия;

g) **улучшить**: последующие действия, которые были определены на обоих предыдущих этапах, по очереди отбираются из категории «невыполненные работы eTIR» в соответствии с их приоритетом и выполняются в порядке совершенствования программного обеспечения, процессов, документации и других ресурсов таким образом, чтобы снизить вероятность повторного возникновения такого же инцидента.

188. На этапе «Отображение» эксперты по ИТ готовят отчет об инциденте, который затем хранится в системе управления базой знаний (СУБЗД) в порядке обеспечения организационной преемственности. Данный отчет содержит следующую информацию об инциденте (включая, в случае применимости, дату и время): тяжесть, описание, службы, которые были задействованы, как и кто уведомил о нем, ответные действия, предпринятые в целях смягчения и последующего устранения его последствий, отправленное и полученное сообщение, результаты расследования, перечень

первопричин, уроки, извлеченные по итогам безупречного анализа полученных результатов, а также перечень последующих действий.

189. С помощью этого процесса эксперты по ИТ желают добиться следующих преимуществ: предотвратить подобные инциденты (или, по крайней мере, снизить вероятность их возникновения), улучшить показатель среднего времени урегулирования инцидентов, дополнительно сократить время простоя международной системы eTIR и улучшить в общем и целом опыт заинтересованных сторон eTIR.

6. Инциденты, которыми занимается поставщик хостинговых услуг Организации Объединенных Наций

190. Как показано на рисунке VII, информация об инцидентах может поступать в службу поддержки eTIR от поставщика хостинговых услуг Организации Объединенных Наций, который размещает у себя международную систему eTIR. С этим поставщиком подписывается соответствующее соглашение об уровне обслуживания (СУО), обеспечивающее круглосуточную поддержку международной системы eTIR. Для сотрудников поставщика хостинговых услуг Организации Объединенных Наций экспертами по ИТ готовятся соответствующие СОПы, с тем чтобы они могли реагировать на конкретные виды инцидентов.

191. В случае возникновении какого-либо инцидента сотрудники поставщика хостинговых услуг Организации Объединенных Наций оповещаются с помощью предупреждений, направляемых системой мониторинга, и реагируют на него с помощью этих СОПов. Если полученный ответ позволяет разрешить этот инцидент, то они уведомляют службу поддержки eTIR о необходимости дополнительного расследования, указывая, что вопрос с данным инцидентом закрыт. Если полученный ответ не позволяет урегулировать данный инцидент, то они передают его в следующую инстанцию, обращаясь в этих целях в службу поддержки eTIR, как показано на рисунке VII, используя различные способы и процедуры связи в зависимости от тяжести инцидента.

7. Управление резервным копированием и восстановлением

192. Управление резервным копированием и восстановлением представляет собой соответствующую стратегию и связанные с ней процедуры, введенные в действие с целью обеспечить частое копирование данных, связанных с eTIR, и возможность быстрого восстановления в случае их потери. Фактически данные можно потерять в ходе некоторых видов событий, в частности: неисправность сервера, пожар в центре обработки данных или кибератака. За подготовку СОПов несут совместную ответственность провайдер хостинговых услуг Организации Объединенных Наций и ЕЭК, которые упоминаются в СУО.

193. Резервное копирование данных, хранящихся во всех местах хранения eTIR (база данных eTIR, журналы eTIR и документы eTIR), производится дважды в день. Эта резервная копия данных надежно хранится, как минимум, еще в одном месте, помимо основного, во избежание ее уничтожения в случае какого-либо стихийного бедствия на этом объекте. Она также недоступна из той же сети с целью избежать ее взлома вследствие какой-либо кибератаки с использованием так называемой программы-вымогателя. Хранению подлежат только самые последние и полные резервные копии, а старые резервные копии стирают.

194. В общем и целом сохранение последней резервной копии в случае потери данных должно занимать не более 6 часов. С целью обеспечить выполнение этого требования с провайдером хостинговых услуг Организации Объединенных Наций проводятся регулярные проверки.

8. Управление резервным копированием и восстановлением

195. Функция мониторинга информационной системы включает в себя сбор информации, генерируемой этой системой, и возможность генерирования оповещений в случае наступления определенных событий, в результате которых могут быть произведены в порядке реагирования на эти события соответствующие

(автоматизированные или ручные) действия. Мониторинг системы позволяет заблаговременно выявлять любую проблему, которая может привести к сбою в работе и в итоге повлиять на доступность этой системы. Способность быстро реагировать на эти заблаговременные предупреждения обычно позволяет снизить воздействие сбоев, а иногда и вовсе их предотвратить.

196. Система мониторинга обеспечивается поставщиком хостинговых услуг Организации Объединенных Наций и конфигурируется в сотрудничестве с ЕЭК в целях наблюдения за ресурсами и работой виртуальных серверов, а также за наличием и оказанием различных услуг по линии международной системы eTIR. В частности, перечень показателей, отслеживаемых системой мониторинга, включает следующие метрические параметры: потребление ресурсов центрального процессора, использование оперативной памяти, процент использования диска, процессы, доступность сервисов, время реагирования системы и использование ресурсов приложений.

197. Система оповещения настроена на срабатывание при превышении определенных пороговых значений. Оповещения характеризуются тем или иным уровнем серьезности, который определяет тип ответных мер, подлежащих принятию в каждом конкретном случае: критический, ошибка, предупреждение и информирование. В зависимости от конфигурации можно активировать несколько типов ответных мер: можно ввести в действие автоматический процесс или же одному или нескольким лицам можно отправить соответствующее сообщение (по электронной почте, СМС или по телефону) в целях их уведомления об оповещении, с тем чтобы дать им возможность как можно быстрее принять нужные меры. Первыми, кто получает такое уведомление, обычно являются сотрудники поставщика хостинговых услуг Организации Объединенных Наций, с тем чтобы они могли принять незамедлительные меры на основании СОПов, подготовленных для таких случаев. Оповещения могут также направляться в службу поддержки eTIR в зависимости от срочности и важности вопроса. Всеобъемлющий перечень показателей, пороговых значений, оповещений и соответствующих ответов оформляется документально на совместной основе провайдером хостинговых услуг Организации Объединенных Наций и ЕЭК и указываются в СУО.

198. В дополнение к собранным метрическим показателям виртуальных серверов и процессов, система мониторинга также использует данные, содержащиеся в журналах eTIR. Эта информация, также именуемая телеметрией, которая регистрируется международной системой eTIR, обеспечивает ценные данные, которые можно использовать для выявления любых потенциальных срочных проблем с системой. Она также выдает информацию об эффективности системы и соответствующие указания специалистам по ИТ о связанных с этим тенденциях. Эти данные необходимо отслеживать с целью убедиться в соблюдении целевых показателей, установленных в технических требованиях международной системы eTIR.

199. И наконец, важно учитывать один недостаток, который обычно ассоциируется с практикой мониторинга. При первоначальной настройке пороговые значения и оповещения могут приводить к ложнопозитивным результатам или, наоборот, «пропускать» проблемы, которые должны были быть обнаружены. По этой причине практика постоянного совершенствования приобретает особую актуальность, притом что конфигурацию системы мониторинга следует регулярно пересматривать в целях ее оптимизации.

9. Управление системой корректирующих вставок

200. Корректирующая вставка — это соответствующий набор изменений для внесения в программу, который предназначен для ее обновления, исправления или улучшения. Она включает устранение уязвимостей с точки зрения безопасности и других дефектов. В настоящем документе под управлением системой корректирующих вставок понимается стратегия и связанные с ней процедуры, установленные с целью обеспечить регулярное внесение исправлений в порядке устранения недавно обнаруженных проблем в соответствующие компоненты программного обеспечения, включая операционные системы базовых серверов.

201. Особенно важно устранять факторы уязвимости в защите, которые обнаруживаются в существующих версиях всего программного обеспечения специалистами в области кибербезопасности. Регулярное применение корректирующих вставок из уполномоченных и проверенных источников является одним из наиболее эффективных способов защиты международной системы eTIR от кибератак (см. раздел, посвященный безопасности системы eTIR).

202. Если есть соответствующая корректирующая вставка, то в этом случае готовят и применяют на регулярной основе необходимые СОПы (не реже одного раза в три месяца) для исправления следующих программных компонентов: базовых операционных систем, интегрированных систем и библиотек (например, виртуальная машина «Java») и систем управления базами данных. Нормальный технологический режим не препятствует применению — по мере необходимости и в большинстве случаев по соображениям безопасности — существенных корректирующих вставок. Программные компоненты исправляются провайдером хостинговых услуг Организации Объединенных Наций и ЕЭК в зависимости от обязанностей, подробно изложенных в СУО.

10. Управление обновлениями

203. Обновление, как правило, представляет собой замену аппаратного, программного или программно-технического обеспечения на более новую или более совершенную версию в целях обновления системы или улучшения ее функциональных возможностей. В настоящем документе управление обновлением означает стратегию и соответствующие процедуры, введенные в действие с целью обеспечить такое положение, при котором техническое отставание регулярно рассматривается и не растет с течением времени (см. требования к удобству эксплуатации международной системы eTIR). Управление системой обновления отличается от управления системой корректирующих вставок в том плане, что обновления представляют собой новые версии программного обеспечения, которые должны быть тщательно протестированы с целью выявить и устранить потенциальные проблемы, прежде чем их можно будет применить на практике.

204. Ответственность за замену аппаратного и соответствующего программно-технического обеспечения несет провайдер хостинговых услуг Организации Объединенных Наций. Что касается программного обеспечения, то обязанности распределяются между поставщиком хостинговых услуг Организации Объединенных Наций, который должен планировать и производить модернизацию всех компонентов программного обеспечения, входящих в сферу его компетенции (например, системы ферм виртуальных серверов и операционных систем виртуальных серверов), и ЕЭК, которая должна планировать и осуществлять модернизацию всех компонентов программного обеспечения международной системы eTIR.

205. Самые последние версии базового языка программирования, интегрированных систем и библиотек, используемых для компоновки международной системы eTIR, проверяют, как минимум, один раз в квартал. Далее специалисты по информационным технологиям регулярно анализируют и документально оформляют различные преимущества и недостатки перехода того или иного программного компонента на одну из его новых версий. При планировании такого перехода принимаются во внимание следующие критерии: дата прекращения поддержки используемой в настоящее время версии, зрелость новой версии на основании оценки экспертов по ИТ, потенциальные преимущества в плане безопасности и наличие дополнительных функций.

206. Когда принимается решение о переходе на новую версию данного программного компонента, начинается работа по реализации внутреннего проекта, притом что связанные с ним задачи включаются в категорию невыполненных работ eTIR, которые расставляются в порядке приоритетности и рассматриваются в ходе обычной разработки методом итерации. Цели проекта такого типа заключаются в следующем: всестороннее тестирование новой версии программного компонента в целях выявления любых проблем, которые могут возникнуть в контексте международной системы eTIR, устранение любой обнаруженной серьезной проблемы,

возможное использование новых функций, присущих новой версии, в целях модернизации международной системы eTIR и дальнейшее тестирование и проверка в среде UAT на этапе, предшествующем развертыванию новой версии международной системы eTIR в среде PRD.

IV. Безопасность системы eTIR

207. В настоящей части рассматриваются все аспекты системы eTIR, связанные с информационной безопасностью, в частности цели и требования, а также соответствующие меры и средства контроля, предусмотренные для их достижения. Информационная безопасность является одним из руководящих принципов, взятых на вооружение при разработке международной системы eTIR, в силу той важной роли, которая отводится ей в современных информационных системах, и ЕЭК намерена должным образом решить эту задачу. Преследуемой целью является определение всестороннего базового подхода, охватывающего все соответствующие аспекты информационной безопасности, который подлежит регулярному пересмотру и обновлению со стороны ТОО.

208. Информационная безопасность охватывает не только программное обеспечение, но и все области, способные повлиять на безопасность системы. Поэтому в настоящей части будут оговорены аспекты, относящиеся к следующим областям: безопасность и управление рисками, защита активов, архитектура и техника обеспечения безопасности, защита коммуникаций и безопасность сетей, управление идентификацией и доступом пользователей, оценка и тестирование защищенности, операции по обеспечению безопасности и безопасность разработки программного обеспечения.

209. Как подчеркивалось в предыдущей части, где рассматриваются технические аспекты международной системы eTIR, уровень детализации нижеследующих разделов зависит от описываемых аспектов, причем изложить все детали не представляется возможным по соображениям безопасности.

A. Задачи и принципы безопасности

1. Классификация информации и стратегия обеспечения ее безопасности

210. Отправной точкой любого обсуждения, связанного с информационной безопасностью, является определение степени чувствительности информации, управляемой по линии информационных систем. В структуре Организации Объединенных Наций эти аспекты регулируются положениями бюллетеня Генерального секретаря, озаглавленного «Конфиденциальность, классификация и использование информации»[35]. Данные, которыми обмениваются участники системы eTIR, а также данные, которыми обмениваются пользователи Международного банка данных МДП (МБДМДП), относятся к категории «конфиденциальных», как это определено в разделе 2 бюллетеня.

211. Этот уровень классификации затем используется и упоминается в других документах Организации Объединенных Наций для определения подлежащих применению правил, руководящих принципов и передовой практики. В частности, Управление информационно-коммуникационных технологий (УИКТ) издает стратегические установки, в том числе связанные с информационной безопасностью, которыми оговариваются различные средства контроля за безопасностью в зависимости от уровня классификации[36]. Технические спецификации eTIR соответствуют данным установкам, ибо предусматривают меры безопасности и средства контроля, которые являются не менее строгими, чем те, которые предписываются установками при управлении конфиденциальной информацией.

[35] См. Документ ST/SGB/2007/6.

[36] Перечень стратегических установок см. на сайте iseek.un.org/nyc/department/policies.

2. Задачи безопасности

212. Основу информационной безопасности составляют следующие три главные фундаментальные задачи[37]:

- **целостность** предполагает, что информация сохраняет свою достоверность и намеренно изменяется только авторизованными субъектами;
- **готовность к работе** предполагает, что авторизованным субъектам предоставляется своевременный и беспрепятственный доступ к информации;
- **конфиденциальность** предполагает, что информация не раскрывается посторонним субъектам.

213. Эти три основополагающие задачи, вкупе с вытекающими из них требованиями, предъявляемыми к разработке информационных систем, определяют основные аспекты информационной безопасности, как показано на следующем рисунке.

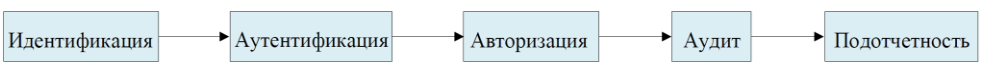
Рисунок XX
Основополагающие задачи информационной безопасности

214. В случае системы eTIR диктуемые тремя этими задачами требования являются весьма высокими. Действительно, раз уж данные классифицируются как конфиденциальные, их конфиденциальность должна обеспечиваться посредством адекватных средств контроля за безопасностью. Поскольку система eTIR предназначена для использования многими заинтересованными сторонами, то в интересах международных перевозок грузов по процедуре eTIR система должна быть всегда доступна для пользователей. Наконец, надлежит обеспечивать сохранность и целостность данных, передаваемых между заинтересованными сторонами eTIR, с тем чтобы все участники могли доверять им; это также необходимо для исключения возможности отказа.

3. Каким образом обеспечивается подотчетность и невозможность отказа

215. Помимо освещения таких аспектов, как целостность, готовность к работе и конфиденциальность, важно разобраться, каким образом субъект[38] аутентифицирует себя в системе и как его/ее действия способны повлечь за собой подотчетность и невозможность отказа. На практике это претворяется посредством пяти последовательных процедур, которые перечислены на следующем рисунке и описаны ниже.

Рисунок XXI
От идентификации к подотчетности



a) **Идентификация** — это процесс, посредством которого субъект заявляет о своей идентичности с последующим наступлением его подотчетности. Для целей аутентификации субъект должен подтвердить системе свою идентичность. К

[37] Исчерпывающие определения этих трех терминов приведены в техническом глоссарии.
[38] Под «субъектом» здесь следует понимать человека или информационную систему, который(ая) пытается получить доступ к другой системе.

возможным способам такого подтверждения относятся, например, введение имени пользователя либо проведение пальцем по сканирующему устройству. Основной принцип аутентификации состоит в том, что все субъекты должны иметь уникальные идентификаторы.

b) **Аутентификация** — это процесс проверки или тестирования, позволяющий удостовериться в том, что идентичность субъекта, который обратился с запросом, является подлинной. Аутентификация предполагает, что субъекты должны представить дополнительную информацию, подтверждающую подлинность заявленной им идентичности, например посредством введения пароля либо цифровым сертификатом. Этот процесс предусматривает проверку идентичности данного субъекта путем сравнения одного или нескольких факторов с базой данных действительных идентичностей, в частности с учетными записями пользователей.

c) **Авторизация** — это процесс предоставления доступа к ресурсу или объекту на основе идентичности, подлинность которой была удостоверена. В большинстве случаев система оценивает матрицу управления доступом, которая соотносит субъект, объект и предполагаемую деятельность. Субъект получает авторизацию только в том случае, если конкретное действие ему/ей разрешено.

d) Под **аудитом** понимается набор программных средств, с помощью которых отслеживаются и записываются действия субъекта с целью возложения на него — при аутентификации в системе — ответственности за выполняемые им действия. Это также процесс, с помощью которого система обнаруживает несанкционированные или аномальные действия.

e) **Подотчетность** — это процесс возложения на субъектов ответственности за выполняемые ими действия. Эффективность подотчетности зависит от способности подтверждения идентичности субъекта и отслеживания его действий. Подотчетность выявляется путем установления связи между человеком и конкретной деятельностью с привязкой к сетевому удостоверению посредством сервисов безопасности, а также механизмов аудита, аутентификации и идентификации.

216. Важной сопутствующей задачей, призванной гарантировать, что субъект, инициировавший какое-либо действие или событие, не сможет отрицать, что он/она его инициировали, является **невозможность отказа**. Это не позволяет тому или иному субъекту утверждать, что он не отправил сообщение, не выполнил какое-либо действие или не стал причиной какого-либо события. Задача исключения возможности отказа имеет весьма важное значение для системы eTIR, поскольку информация, хранящаяся в международной системе eTIR, может быть запрошена Договаривающимися сторонами в случае претензий[39]. При выполнении обеих задач, а именно обеспечении подотчетности субъектов и целостности данных, хранящихся в международной системе eTIR, достигается и цель невозможности отказа.

4. Принципы безопасности

217. Что касается руководящих принципов, взятых за основу при разработке международной системы eTIR, то ЕЭК также поддерживает и принимает следующие принципы, которые признаны и широко используются сообществом экспертов по информационной безопасности.

218. Первым является принцип **соблюдения осторожности**, который в контексте информационной безопасности означает принятие на постоянной основе надлежащих мер по защите активов организации. В этой связи требуются высокая инициативность и воспитание культуры безопасности. Реализация оговоренных в настоящей части концепций и процедур безопасности, наряду с проведением периодических аудитов и обзоров безопасности, позволяет продемонстрировать заинтересованным сторонам eTIR, что в плане соблюдения осторожности ЕЭК проявляет должную осмотрительность.

[39] В соответствии с пунктом 3 статьи 12 приложения 11 к Конвенции МДП.

219. Вторым является принцип **наименьшей привилегии**, согласно которому требуется, чтобы на определенном уровне абстракции от вычислительной среды каждый модуль (например, процесс, пользователь или программа, в зависимости от субъекта) мог получить доступ только к той информации и тем ресурсам, которые необходимы для выполнения его рабочей цели[40]. Этот принцип также применяется в отношении сотрудников ЕЭК, отвечающих за разработку и функционирование международной системы eTIR: разрешения и доступы для целей выполнения их работы предоставляются им избирательно, а в порядке периодического пересмотра списка разрешений и их удаления, если они больше не нужны, осуществляется административный контроль. И все это в дополнение к процедурам «отсева», призванным исключить всякий доступ со стороны лиц (сотрудников, консультантов, стажеров и т. д.), которые больше не будут работать в ЕЭК. Наконец, для обеспечения того, чтобы доступ к конкретной информации и системам имели исключительно авторизованные лица, выполняющие свои обязанности, также предусматриваются средства физического и технического контроля доступа.

220. Третьим является принцип **глубокоэшелонированной защиты**, под которым понимается концепция встроенных в информационную систему многоуровневых средств контроля за безопасностью (защита). Преследуемая цель состоит в том, чтобы продолжать обеспечивать адекватную безопасность системы в случае отказа средств контроля за безопасностью либо использования уязвимости, которая может охватывать аспекты кадровой, процедурной, технической безопасности и физической защищенности[41]. Этот принцип находит широкое применение и, например, используется в рамках международной системы eTIR путем внедрения нескольких уровней валидации для ввода данных (полученных в сообщениях eTIR) с целью проверки их качества и подтверждения соответствия спецификациям eTIR.

221. Четвертым является принцип **разделения обязанностей**, под которым понимается концепция, согласно которой для завершения выполнения той или иной задачи требуется более одного человека. В случае чувствительных операций раздельное выполнение одной конкретной задачи более чем одним человеком является средством внутреннего контроля, направленным на предотвращение мошенничества и ошибок[42]. Например, данный принцип используется и при разработке международной системы eTIR, когда другой ИТ-эксперт просматривает код первого ИТ-эксперта, который ввел и зафиксировал строки кода. Это позволяет выявить потенциальные упущения и ошибки, которые затем могут быть немедленно исправлены первоначальным поставщиком информации.

B. Требования по безопасности

1. Технические требования, уже упоминавшиеся ранее

222. Как пояснялось в разделе выше, информационная безопасность охватывает широкий спектр нефункциональных (технических) требований к информационной системе, и многие из них играют роль в достижении одной или нескольких из трех основных целей: обеспечение целостности, готовности к работе и конфиденциальности. В частности, следующие требования, уже рассмотренные в предыдущей части, посвященной международной системе eTIR[12], следует рассматривать как имеющие важное значение для компонента системы eTIR, связанного с информационной безопасностью:

- **готовность к работе** как одна из трех основных задач безопасности, несомненно, относится к числу самых важных, и ИТ-эксперты должны уделять особое внимание всему набору требований: AV.1, AV.2, AV.3 и AV.4;
- оба требования, касающиеся **резервного копирования** (BK.1 и BK.2), непосредственно относятся к задаче обеспечения готовности к работе,

[40] См. en.wikipedia.org/wiki/Principle_of_least_privilege.
[41] См. en.wikipedia.org/wiki/Defense_in_depth_(computing).
[42] См. en.wikipedia.org/wiki/Separation_of_duties.

поскольку имеют целью восстановление доступа к информации для авторизованных субъектов в случае потери данных;

- первое из требований, касающихся **пропускной способности** (CP.1), также непосредственно относится к задаче обеспечения готовности к работе, поскольку направлено на то, чтобы международная система eTIR могла в любое время обрабатывать сообщения, направляемые заинтересованными сторонами eTIR. Остальные требования (CP.2, CP.3 и CP.4) следуют той же логике, но в меньшей степени;

- все требования, касающиеся **управления настройками** (CM.1, CM.2, CM.3, CM.4 и CM.5), сказываются на решении всех трех задач (готовность к работе, целостность и конфиденциальность), поскольку характеризуют важные аспекты процессов разработки и обслуживания международной системы eTIR;

- требования, касающиеся **хранения данных** (RE.1 и RE.2), регламентируют конкретные аспекты задачи обеспечения готовности к работе, предписывая длительность хранения данных, которыми обмениваются в системе eTIR, и порядок получения к ним доступа;

- требования, касающиеся **послеаварийного восстановления** (DR.1 и DR.2), также, со всей очевидностью, связаны с задачей обеспечения готовности к работе, ибо они касаются конкретного случая восстановления международной системы eTIR в случае аварии;

- требования, касающиеся **устойчивости к сбоям** (FT.1, FT.2, FT.3 и FT.4), регламентируют различные технические аспекты режима нейтрализации неисправности международной системы eTIR и также сказываются на решении задачи обеспечения готовности к работе;

- первые два требования, касающиеся **удобства обслуживания** и относящиеся к «технической задолженности» (MT.1 и MT.2), непосредственно связаны с превентивными мерами, принимаемыми для предотвращения будущих проблем с информационной безопасностью, с которыми может столкнуться международная система eTIR;

- в связи с CP.1 следует указать, что два требования, касающиеся **производительности** (PE.2 и PE.3), также непосредственно относятся к задаче обеспечения готовности к работе, поскольку направлены на то, чтобы обмен сообщениями между международной системой eTIR и другой заинтересованной стороной eTIR неизменно производился в разумные сроки. Кроме того, последние два требования к производительности (PE.4 и PE.5) также непосредственно связаны с превентивными мерами по выявлению потенциальных проблем в рамках международной системы eTIR, способных повлиять на ее готовность к работе;

- большинство требований, касающихся **надежности** (RL.1, RL.2, RL.3, RL.5 и RL.7), также относится к числу механизмов, призванных, насколько это возможно, предотвратить возникновение в рамках международной системы eTIR проблем, способных повлиять на ее готовность к работе.

223. Совершенно очевидно, что информационная безопасность — это сквозная, всеобъемлющая тема, которая не может рассматриваться обособленно и требует применения последовательного подхода для ее охвата на всех стадиях жизненного цикла разработки программного обеспечения. Представленные ниже нефункциональные (причем не обязательно технические) требования являются специфическими для информационной безопасности и в целом применимы ко всем компонентам системы eTIR: к международной системе eTIR, к информационным системам всех других заинтересованных сторон eTIR (в том числе предоставляемым в распоряжение держателей для передачи предварительных данных) и к сетевым соединениям между всеми этими системами. Важно, однако, отметить, что некоторые из указанных ниже требований могут относиться лишь к части этих компонентов.

224. В последующих разделах под «учетной записью пользователя» следует понимать учетную запись, однозначно идентифицирующую либо отдельно взятое лицо, либо информационную систему в другой информационной системе (которая использует эти учетные записи и управляет ими).

2. Аудит

225. В нижеследующей таблице приведено требование, касающееся процесса аудита, ссылка на который дается на рис. XXI. Хотя данное требование относится в основном к международной системе eTIR, рекомендуется, чтобы ему соответствовали и другие информационные системы, задействованные в системе eTIR.

Таблица 20
Качественные требования, касающиеся готовности к работе

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
AU.1	Вся информация, отправляемая в международную систему eTIR и получаемая этой системой, привязана к учетной записи пользователя и может быть проверена.	Все сообщения, отправляемые в систему eTIR и получаемые этой системой, целиком заносятся в журнал вместе с цифровой подписью. Эти журналы затем надежно хранятся и обслуживаются в хранилище журналов eTIR, откуда они могут быть запрошены таможенными органами в случае претензий.

3. Аутентификация

226. В нижеследующей таблице перечислены требования, касающиеся процесса аутентификации, ссылка на который дается на рис. XXI. Собственно к аутентификации заинтересованных сторон eTIR из числа участников международной системы eTIR относится только первое требование (AE.1), тогда как остальные требования применяются к другим информационным системам, задействованным в системе eTIR.

Таблица 21
Требования, касающиеся аутентификации

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
AE.1	Выбор для международной системы eTIR надежного механизма аутентификации с целью предотвращения несанкционированного доступа.	Заинтересованные стороны eTIR, желающие получить доступ к веб-услугам международной системы eTIR, должны аутентифицировать себя с помощью цифрового сертификата. Закрытый ключ этого сертификата должен надежно храниться у каждого участника eTIR.
AE.2	Задействование после периода бездействия функции блокировки сеанса для защиты доступа к учетным записям пользователей.	Только для учетных записей, назначенных пользователям из числа физических лиц: при предоставлении пользовательского интерфейса для доступа к информационной системе (на веб-сайте или в мобильном приложении) следует установить временно́е ограничение в 15 минут для закрытия сессии, если она становится неактивной.
AE.3	Надежное управление паролями для предотвращения несанкционированного доступа.	Пароль должен надежно храниться в базах данных с использованием современных криптографических хэш-функций. Пароли должны отвечать самым передовым требованиям, в том числе в отношении минимальной длины и сложности.
AE.4	Рекомендуемое использование для доступа в систему многофакторной	Когда это применимо, учетные записи, назначенные пользователям из числа физических лиц, должны использовать

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
	аутентификации с целью защиты учетных записей пользователей.	многофакторную аутентификацию, например двухфакторный подход с использованием «того, что пользователь знает» (пароль) и «того, что пользователь имеет» (удостоверение или мобильный телефон).

4. Авторизация

227. В нижеследующей таблице перечислены — применительно к информационным системам, задействованным в системе eTIR, — требования, касающиеся процесса авторизации, ссылка на который дается на рис. XXI выше.

Таблица 22
Требования, касающиеся авторизации

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
АО.1	Предоставление минимального, но достаточного уровня доступа или привилегий для предотвращения несанкционированного доступа.	Любой учетной записи пользователя должны быть назначены минимальный уровень доступа и разрешения, необходимые для извлечения информации, которую пользователю разрешено получать, и для осуществления операций, которые ему разрешено выполнять.
АО.2	Использование ролевой модели управления доступом (RBAC) для улучшения сопровождения учетных записей пользователей.	Когда это применимо, пользователям с учетной записью следует предоставлять доступ и разрешения по критерию исполняемых ролей или на основе групп. Это устойчивый способ управления списками контроля доступа, поскольку глобально просматривать и обновлять права доступа и разрешения для всех членов группы проще и менее чревато ошибками, чем делать это для каждой учетной записи пользователя.
АО.3	Отмена полномочий по доступу при кадровых перестановках для предотвращения несанкционированного доступа.	Должны быть предусмотрены процедуры «лишения полномочий» для отзыва доступа и разрешений, назначенных учетным записям тех пользователей, чьи контракты прекращаются. Затем эти учетные записи пользователей должны быть отключены.
АО.4	Проверка учетных записей пользователей не реже одного раза в год во избежание ущемления привилегий.	Должна быть предусмотрена процедура по крайней мере ежегодной проверки всех учетных записей пользователей для контроля и подтверждения правильности назначенных им уровня доступа и разрешений.

5. Повышение осведомленности и подготовка

228. Не раз уже подтверждалось, что человек является самым слабым звеном в цепи информационной безопасности. Поэтому крайне важно повышать уровень осведомленности и налаживать подготовку персонала, который будет использовать информационные системы, задействованные в системе eTIR, в области информационной безопасности, а также по вопросам передовой практики и распространенных видов угрозы. Поскольку люди являются мишенью таких специфических атак, как фишинг-мошенничество, адресный фишинг и социальная инженерия, на этих аспектах важно акцентировать особое внимание. Поэтому всем заинтересованным сторонам eTIR рекомендуется внедрять аналогичные практические подходы и процессы.

229. В нижеследующей таблице перечислены требования, касающиеся налаживания процессов повышения уровня осведомленности и подготовки всего соответствующего персонала.

Таблица 23
Требования, касающиеся повышения осведомленности и подготовки

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
AW.1	Обеспечить прохождение всеми соответствующими сотрудниками базовых курсов подготовки по информационной безопасности для повышения уровня их осведомленности.	Для персонала, использующего информационные системы, задействованные в системе eTIR, должны быть доступны базовые учебные курсы по информационной безопасности (включая передовую практику и распространенные виды угрозы). Необходимо наладить процедуры, обеспечивающие прохождение таких учебных курсов всем персоналом, использующим информационные системы, связанные с системой eTIR.
AW.2	Ведение учета участия в обязательных учебных курсах.	Необходимо вести надлежащий учет в порядке обеспечения того, чтобы весь персонал, использующий информационные системы, связанные с системой eTIR, прошел базовые курсы подготовки в области информационной безопасности. В идеале такие учебные курсы надлежит организовывать на регулярной основе (например, раз в три года).

6. Конфиденциальность

230. Информация, обмен которой осуществляется по линии системы eTIR и которая хранится в ней, относится к конфиденциальной. Следовательно, должны быть предусмотрены средства контроля, обеспечивающие защиту данных от несанкционированного доступа в процессе их обмена по линии международной системы eTIR (данные в движении) и во время их хранения в ней (хранимые данные). В нижеследующей таблице перечислены требования к системе eTIR, касающиеся конфиденциальности.

Таблица 24
Требования, касающиеся конфиденциальности

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
CO.1	Информация, передаваемая между информационными системами, задействованными в системе eTIR, остается конфиденциальной.	Все сообщения, которыми обмениваются все информационные системы, задействованные в системе eTIR, шифруются с использованием таких протоколов и механизмов шифрования, которые международное InfoSec-сообщество[43] считает защищенными. Они должны быть указаны в технических спецификациях eTIR, и этот список подлежит регулярному пересмотру для изъятия механизмов, которые больше не считаются защищенными, с их заменой на более защищенные.
CO.2	Доступ к информации, хранящейся в международной	Информация, записанная в трех местах хранения международной системы eTIR (база данных eTIR, документы eTIR и журналы eTIR), ограничена только учетными записями авторизованных

[43] Термин «InfoSec» — это сокращение от «Information Security» (информационная безопасность). Международное InfoSec-сообщество объединяет национальные агентства, специализирующиеся на информационной безопасности и выпускающие регулярные публикации на эту тему, а также ИТ-экспертов и исследователей, специализирующихся в данной области.

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
	системе eTIR, является ограниченным.	пользователей. Эти места хранения расположены в защищенной среде, защищенной физическими и программными средствами контроля безопасности.

7. Идентификация

231. В нижеследующей таблице приведено — применительно к информационным системам, задействованным в системе eTIR, — требование, касающееся процесса идентификации, ссылка на который дается на рис. XXI.

Таблица 25
Требование, касающееся идентификации

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
ID.1	Однозначная идентификация человека или информационной системы с помощью учетной записи пользователя в целях обеспечения подотчетности за совершаемые действия.	Любая учетная запись пользователя должна быть назначена и привязана к отдельному лицу, а не к группе пользователей (в случае людей) или к конкретной информационной системе (в случае систем). Одна и та же информационная система должна иметь разные идентификаторы в зависимости от прикладной среды (разработка, пользовательское приемочное тестирование и производство продукта).

8. Целостность

232. Необходимо гарантировать сохранность и целостность информации, обмен которой осуществляется по линии международной системы eTIR и которая хранится в ней. Следовательно, должны быть предусмотрены средства контроля, обеспечивающие защиту данных от любых изменений, независимо от их характера: ошибки при передаче данных, человеческого фактора, неправильной конфигурации или кибератаки. В нижеследующей таблице перечислены требования к международной системе eTIR, касающиеся целостности.

Таблица 26
Требования, касающиеся целостности

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
IN.1	Целостность информации, передаваемой между информационными системами, задействованными в международной системе eTIR, остается ненарушенной.	Все сообщения, отправляемые в международную систему eTIR или получаемые этой системой, имеют цифровую подпись отправителя. По получении сообщения получатель удостоверяет подлинность электронной подписи либо отвергает подпись, если она недействительна.
IN.2	Целостность информации, хранящейся в системе eTIR, остается ненарушенной.	Все сообщения, отправляемые в международную систему eTIR или получаемые этой системой, целиком заносятся в журнал вместе с цифровой подписью. Эти журналы затем надежно хранятся и обслуживаются в хранилище журналов eTIR, доступ к которому ограничен.

9. Безопасность узлов

233. Как определено в части, касающейся архитектуры, узел представляет собой любое устройство, физическое или виртуальное, служащее для размещения программ или информации, составляющих международную систему eTIR, или взаимодействия с ними. Узлами могут быть виртуальные серверы, на которых размещаются различные

программные компоненты международной системы eTIR, либо устройства, являющиеся частью сетевой инфраструктуры, такие как брандмауэры, маршрутизаторы, прокси-серверы, обратные прокси-серверы или специализированные устройства информационной безопасности (СОВ, СОИ и т. д.). В нижеследующей таблице перечислены требования к международной системе eTIR, касающиеся безопасности узлов.

Таблица 27
Требования, касающиеся безопасности узлов

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
NS.1	Безопасная настройка конфигурации виртуальных серверов, контейнеров или модулей для предотвращения несанкционированного доступа.	Обеспечивать соблюдение всех рекомендаций поставщиков операционной системы по информационной безопасности. Реквизиты учетных записей служб на этих серверах должны надежно храниться в системе управления паролями и быть доступны только авторизованному персоналу. Когда это применимо, активировать программный брандмауэр и ввести политику запрета по умолчанию и наименьших привилегий.
NS.2	Безопасная настройка конфигурации устройств сетевой инфраструктуры для предотвращения несанкционированного доступа.	Вводить на сетевых устройствах, таких как брандмауэры, политику запрета по умолчанию и наименьших привилегий. Обеспечивать соблюдение всех рекомендаций поставщиков. Вести точную документацию по сетевым соединениям и конфигурации устройств. Эти действия выполняются хостинговой структурой.
NS.3	Изолирование достоверных сетей, содержащих конфиденциальные данные, от недостоверных для предотвращения несанкционированного доступа.	Применение передовых методов проектирования сетевой инфраструктуры с разделением серверов на различные зоны безопасности в зависимости от их роли и чувствительности хранящейся на них информации. Ведение списков разрешенных IP-приложений для запрещения доступа к международной системе eTIR по умолчанию; исключение делается для заданного списка внешних серверов (заинтересованных сторон eTIR). Эти действия выполняются хостинговой структурой.
NS.4	Мониторинг событий на узлах для обнаружения потенциальных проблем безопасности.	Ведение журнала для узлов, которые поддерживают эту функцию, с направлением показателей в систему мониторинга. Ограничение доступа к журналу только для авторизованных сотрудников. Защита данных журнала от несанкционированных изменений и эксплуатационных неисправностей. Настройка автоматических предупреждений на основе правил, в том числе касающихся сбоев при регистрации.

10. Невозможность отказа

234. В нижеследующей таблице перечислены требования к международной системе eTIR, касающиеся невозможности отказа.

Таблица 28
Требования, касающиеся невозможности отказа

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
NR.1	Заинтересованные стороны eTIR несут ответственность за сообщения, которые они направляют в международную систему eTIR.	При отправке сообщений в международную систему eTIR заинтересованные стороны eTIR должны однозначно идентифицироваться и аутентифицироваться путем подписания сообщений своей электронной подписью. Кроме того, должно быть выполнено требование AU.1.
NR.2	Обеспечивается целостность сообщения, отправленного заинтересованными сторонами eTIR в международную систему eTIR.	Должны быть выполнены требования IN.1 и IN.2.
NR.3	Международная система eTIR может продолжать проверку сообщений, хранящихся в журналах eTIR, до истечения срока, указанного в периоде хранения данных.	Поскольку цифровые сертификаты подлежат периодическому обновлению, надлежит внедрить систему управления ключами, обеспечивающую хранение старых цифровых сертификатов всех участников eTIR, с тем чтобы иметь возможность продолжать аутентификацию и проверку целостности сообщений, обмен которыми происходил в прошлом и которые хранятся в журналах eTIR.

11. Физическая защищенность

235. В настоящем разделе сводятся воедино основные требования и соответствующие меры, призванные обеспечить физическую защищенность помещений, зданий и инфраструктур Организации Объединенных Наций, в которых размещена международная система eTIR. В нижеследующей таблице перечислены требования, касающиеся физической защищенности зданий и инфраструктур, в которых размещена международная система eTIR.

Таблица 29
Требования, касающиеся физической защищенности

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
PS.1	Центр обработки данных, в котором размещена международная система eTIR, должен — в порядке защиты хранящейся в нем информации — пользоваться иммунитетом от обыска, реквизиции или конфискации.	Международная система eTIR размещена в центре обработки данных, расположенном в одном из помещений Организации Объединенных Наций, и обслуживается только сотрудниками Организации Объединенных Наций. Поэтому она защищается положениями Конвенции о привилегиях и иммунитетах Объединенных Наций.
PS.2	Центр обработки данных, в котором размещена международная система eTIR, должен быть в достаточной мере защищен для предотвращения вторжений и аварий.	Помещения Организации Объединенных Наций находятся внутри замкнутого защитного периметра, круглосуточно охраняются сотрудниками службы безопасности и охвачены системой видеонаблюдения. Доступ в эти помещения ограничен зарегистрированными лицами, носящими электронные пропуска. Доступ в центр обработки данных ограничен только несколькими авторизованными сотрудниками ИТ-отдела. В центре обработки данных

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
		установлены соответствующие системы обнаружения и тушения пожара.

12. Защитное кодирование и безопасность приложений

236. Защитное кодирование — это такая практика разработки программного обеспечения, при которой обеспечивается защита от случайного внесения в систему безопасности факторов уязвимости. Дефекты и логические недостатки неизменно являются основной причиной наиболее распространенных уязвимостей программного обеспечения. В нижеследующей таблице перечислены требования к международной системе eTIR, касающиеся защитного кодирования и безопасности приложений.

Таблица 30
Требования, касающиеся защитного кодирования и безопасности приложений

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
SC.1	Определение предъявляемых к безопасности требований на ранних стадиях жизненного цикла разработки программного обеспечения (ЦРПО)[44] в целях снижения затрат и уменьшения количества проблем безопасности.	Учет всех связанных с безопасностью аспектов применительно к каждой функции при ее разработке и добавлении в категорию невыполненных работ по eTIR. Неизменная проверка входных данных перед их обработкой. Разработка и интеграция проверочных тестов с акцентом на безопасность («злокозненные истории»). Проведение надлежащей обработки ошибок с целью неизменного поддержания системы в стабильном состоянии. Обязательная и надлежащая регистрация всех связанных с безопасностью событий в журнале с присвоением им правильной степени серьезности. Регулярный просмотр исходного кода для удаления ненужных классов и функций; а также выполнение перепроектирования фрагментов кода.
SC.2	Разделение стадий ЦРПО во избежание смешивания различных версий.	Использование различных сред с соответствующими средствами контроля за безопасностью и процедурами для этапов разработки (DEV), системной интеграции и тестирования (SIT), пользовательского приемочного тестирования (UAT) и производства продукта (PRD).

13. Управление уязвимостями

237. Управление уязвимостями охватывает практику выявления, классификации, определения приоритетности, устранения и смягчения уязвимостей программного обеспечения. Управление уязвимостями является неотъемлемой частью компьютерной и сетевой безопасности и включает в себя оценку уязвимостей. В нижеследующей таблице перечислены требования к международной системе eTIR, касающиеся управления уязвимостями.

[44] См. en.wikipedia.org/wiki/Systems_development_life_cycle.

Таблица 31
Требования, касающиеся управления уязвимостями

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
VU.1	Обеспечить устранение известных уязвимостей для предотвращения потенциальных проблем безопасности.	Регулярное обновление и исправление узлов, включая операционные системы и промежуточное ПО. Регулярное обновление до последних стабильных версий сторонних зависимостей компонентов программного обеспечения. Регулярный переход на последние версии компонентов внешних систем (МБДМДП, почтовая система и система исключения возможности отказа).
VU.2	Проводить оценку и тестирование уязвимостей для предотвращения потенциальных проблем безопасности.	Регулярное сканирование узлов, систем и их компонентов на наличие известных уязвимостей. Проведение проверок безопасности кода (например, тестирование на возможность проникновения) для валидации новых версий международной системы eTIR.
VU.3	Обеспечить надлежащее управление инцидентами для предотвращения потенциальных проблем безопасности.	Предупреждения, полученные от системы мониторинга, подлежат расследованию в зависимости от степени их серьезности с соблюдением соответствующих процедур. Процесс управления инцидентами соблюдается в отношении каждого инцидента, что позволяет извлечь уроки, внести усовершенствования и принять последующие меры, способствующие предотвращению в дальнейшем подобных проблем.

C. Безопасность международной системы eTIR

1. Введение

238. В дополнение к предыдущим частям, касающимся технических спецификаций eTIR, в настоящем разделе дополнительно освещаются различные аспекты безопасности международной системы eTIR, с тем чтобы Договаривающиеся стороны Конвенции МДП и другие заинтересованные стороны eTIR имели четкое представление об этих особенностях. В настоящем разделе подробно оговорено, каким образом ЕЭК будет добиваться выполнения ряда перечисленных в предыдущем разделе требований безопасности, относящихся к международной системе eTIR. Прозрачность этих аспектов позволяет также всем заинтересованным сторонам eTIR вносить предложения по их совершенствованию, имеющие конечной целью создание в долгосрочной перспективе более защищенной системы eTIR.

2. Повышение осведомленности в области информационной безопасности

239. Важно отдавать себе отчет, что информационная безопасность подобна цепи, которая не крепче своего самого слабого звена. Поскольку же люди являются звеном этой цепи, то — вне зависимости от того, сколько на ней еще нанизано звеньев из устройств безопасности или программных барьеров, — если люди не имеют знаний и опыта, необходимых для понимания распространенных факторов угрозы и способов реагирования, общая безопасность системы оказывается под угрозой.

240. Осведомленность в области информационной безопасности направлена прежде всего на повышение степени осознания потенциальных рисков быстро развивающихся форм кибератак, нацеленных на поведение человека. В условиях вызревания все новых факторов угрозы и повышения ценности информации злоумышленники также нарастили свои возможности, вынашивают более амбициозные намерения, разработали новые способы и методологии атак и действуют более разносторонне. Все чаще и чаще (причем успешно) они используют поведение отдельных людей для

взлома корпоративных сетей и систем критически важной инфраструктуры. Являющиеся мишенью злоумышленников лица, не осведомленные о чувствительности информации и факторах угроз, могут неосознанно обойти традиционные средства контроля и протоколы безопасности и создать условия для проникновения в сеть организации.

241. Для обеспечения эффективности усилий, предпринимаемых в этой области, весьма важно, чтобы представление об информационной безопасности имели не только ИТ-эксперты, непосредственно участвующие в работе международной системы eTIR, но и все сотрудники ЕЭК. Так, например, любой сотрудник, открывающий документ, зараженный вредоносной программой (который был бы прикреплен к электронному сообщению), потенциально может открыть злоумышленнику «черный ход» для нарушения информационной безопасности организации. Именно поэтому в 2015 году УИКТ разработало набор из трех учебных курсов по повышению осведомленности в области информационной безопасности (базовый, продвинутый и специальный). Все сотрудники Организации Объединенных Наций в обязательном порядке должны пройти базовый курс подготовки, с тем чтобы весь персонал обладал необходимыми знаниями и имел представление о передовых методах, которые следует применять в случае потенциальной угрозы.

3. Повышение осведомленности в области информационной безопасности

242. Конвенция о привилегиях и иммунитетах Объединенных Наций[45], принятая Генеральной Ассамблеей ООН 13 февраля 1946 года в Нью-Йорке, определяет и конкретизирует многочисленные положения, касающиеся статуса Организации Объединенных Наций, ее имущества и должностных лиц с точки зрения привилегий и иммунитетов, которые должны быть предоставлены им государствами-членами. В частности, как указано в статье 2, помещения Организации Объединенных Наций неприкосновенны: ее имущество и активы, где бы и в чьем бы распоряжении они ни находились, не подлежат обыску, реквизиции, конфискации, экспроприации и какой-либо другой форме вмешательства.

243. На практике это означает, что за охрану и безопасность имущества и активов, находящихся в помещениях Организации Объединенных Наций, отвечают только сотрудники Департамента по вопросам охраны и безопасности Организации Объединенных Наций (ДОБООН). Полиция и любые другие силы безопасности принимающей страны не могут проникать в помещения Организации Объединенных Наций без разрешения сотрудников ДОБООН. Поэтому до тех пор, пока международная система eTIR размещается в центре обработки данных, расположенном в помещениях Организации Объединенных Наций, на нее распространяются привилегии и иммунитеты, описанные выше.

4. Физическая защищенность

244. Под физической защищенностью понимаются меры безопасности, направленные на пресечение несанкционированного доступа к объектам, оборудованию и ресурсам, а также на защиту персонала и имущества от ущерба или вреда (например, шпионажа, кражи или террористических актов). Физическая защищенность предполагает использование многоуровневых взаимосвязанных систем, которые могут включать видеонаблюдение, вооруженную охрану, защитные ограждения, замки, контроль доступа, системы обнаружения вторжения по периметру, системы сдерживания, противопожарную защиту и прочие системы, предназначенные для защиты людей и имущества. В структуре Организации Объединенных Наций этим аспектом безопасности занимается ДОБООН, предоставляющий профессиональные услуги по охране и безопасности, с тем чтобы Организация могла беспрепятственно осуществлять свои программы на глобальном уровне. По очевидным соображениям безопасности в настоящем разделе освещаются только основные аспекты физической защищенности.

[45] См. treaties.un.org/doc/treaties/1946/12/19461214%2010-17%20pm/ch_iii_1p.pdf.

245. Помещения Организации Объединенных Наций находятся внутри замкнутого защитного периметра (стены, заборы, оградительные тумбы и т. д.), проникнуть внутрь которого без специального разрешения ни одному человеку или транспортному средству нельзя. Помещения круглый год круглосуточно охраняются сотрудниками службы безопасности. Помещения охвачены системой видеонаблюдения, находящейся под постоянным контролем диспетчеров службы охраны, а записи хранятся для целей возможных будущих расследований. Доступ в помещения ограничен зарегистрированными лицами, имеющими электронные пропуска, выданные ДОБООН. Доступ в центр обработки данных ограничен только несколькими авторизованными сотрудниками ИТ-отдела, а местонахождение этого центра внутри помещений не разглашается.

246. Кроме того, что касается безопасности, то в большей части помещений и, в частности, в центре обработки данных установлены системы обнаружения и тушения пожара, а несколько раз в год проводятся учения по безопасности.

5. Хостинговая структура Организации Объединенных Наций

247. Если говорить о хостинговой структуре Организации Объединенных Наций (далее — «хостинговая структура»), то в предыдущих частях, касающихся технических спецификаций eTIR, уже оговаривались несколько аспектов, связанных с безопасностью:

- в разделе «Системная архитектура» части, посвященной детальной архитектуре международной системы eTIR, дается описание того, каким образом использование инфраструктуры пула виртуальных серверов, а также балансировщика нагрузки может сыграть роль в проектировании системы, исключающей возникновение любых единичных отказов (SPOF);
- в части, посвященной техническим требованиям, подробно освещена важная роль хостинговой структуры в связи с требованиями, касающимися обеспечения готовности к работе, резервного копирования и — особенно — устойчивости к сбоям; именно эти характеристики присущи ее центру обработки данных;
- в части, посвященной процессам обслуживания, хостинговой структуре также отведена важная роль в таких областях, как управление инцидентами, резервное копирование и восстановление, мониторинг, управление системой корректирующих вставок и обновлениями.

248. Хостинговая структура также несет ответственность за общую безопасность своего центра обработки данных, соответствующих сетей и инфраструктуры (как указано выше в контексте требований, касающихся безопасности узлов). Кроме того, в подтверждение своей приверженности информационной безопасности и «компетентности» в данной сфере хостинговая структура в идеале должна обладать таким признанным сертификатом, как ISO/IEC 27001:2013.

249. Наконец, поскольку хостинговой структуре предстоит регулярно вносить изменения в свои сети, инфраструктуру и узлы (сетевые, защитные или серверные устройства), необходимо наладить четко выверенный процесс управления изменениями для обеспечения тестирования, определения приоритетности, авторизации и внедрения изменений контролируемым и эффективным образом. Извещение клиентов хостинговой структуры об этих изменениях должно быть надлежащим и своевременным, а возможные неизбежные периоды простоя должны обсуждаться заранее с целью изыскания альтернативных решений или, по крайней мере, информирования заинтересованных сторон eTIR. В идеале ЕЭК должна иметь право голоса при авторизации и планировании изменений, сказывающихся на международной системе eTIR или на МБДМДП, возможно, путем предоставления ей места в Консультативном совете по изменениям (КСИ) при хостинговой структуре.

6. Защита программного обеспечения

250. Одна из целей подхода DevOps (также известен под названием DevSecOps) — «добиваться в вопросах безопасности левого уклона», т. е. думать об информационной безопасности на самой ранней стадии процесса разработки, а не решать эту проблему в конце, когда изменения, внесенные в какое-либо программное обеспечение, обходятся гораздо дороже. Для достижения этой цели ЕЭК были утверждены следующие практические подходы и приняты следующие проектные решения:

- **требования к безопасности как функции**: безопасность и соответствие требованиям — это не обособленные процессы, которые происходят в конце разработки программного обеспечения, а «сдвигаются влево» в процессе разработки и включаются в ту же категорию невыполненных работ по eTIR, что и любые другие функции;
- **механизмы проверки**: все входные данные, содержащиеся в сообщениях eTIR, проверяются на нескольких уровнях для обеспечения их правильности, соответствия спецификациям и релевантности. Такие механизмы включают, в частности: специальный уровень проверки для каждого запросного сообщения, уровень проверки с использованием соответствующего XSD-файла и ограничения соблюдения целостности базы данных eTIR. Кроме того, предусматривается проведение автоматизированных валидационных тестов для проверки неправильных входных данных, нулевых или пустых значений, слишком длинных значений и прогона специфических «злокозненных историй»[46];
- **обработка ошибок**: в порядке обеспечения неизменно корректного состояния системы все ошибки, возникающие при выполнении процесса по линии международной системы eTIR, подлежат надлежащей обработке. Такие ошибки следует регистрировать для дальнейшего изучения и, по возможности, подвергать тестированию с помощью автоматизированных тестов с целью убедиться, что механизм обработки ошибок ведет себя предсказуемым образом;
- **проверка уязвимостей**: для регулярной проверки исходного кода на наличие недобросовестных практик, способных повлечь за собой внесение в систему безопасности потенциальных факторов уязвимости, используют инструмент статического анализа кода. Кроме того, поскольку в настоящее время в любом программном обеспечении используется множество программных библиотек, то для проверки версий библиотек по базе данных известных уязвимостей — с тем чтобы отметить важные обновления, которые необходимо загрузить для устранения этих уязвимостей, — задействуют инструмент проверки зависимостей;
- **защита инструментария разработки**: важно обеспечить безопасность всех инструментов и внутренних баз знаний, используемых и создаваемых ИТ-экспертами. Прежде всего, это система контроля версий (СКВ), хранящая исходный код международной системы eTIR и всех связанных с ней утилит. Во-вторых, внутренняя документация, хранящаяся в системе управления базой знаний (СУБЗ) и в системе отслеживания проблем. Наконец, конвейер непрерывной интеграции (НИ) и все сопутствующие инструменты, необходимые для различных процессов разработки, включая документацию для заинтересованных сторон eTIR (например, технические руководства);
- **телеметрия**: это процесс регистрации поведения международной системы eTIR, подлежащий разработке и внедрению ИТ-экспертами для выведения и записи показателей, которые затем можно проанализировать, в частности, с целью предотвращения потенциальных инцидентов (в системе безопасности). К числу таких показателей могут относиться следующие: успешность/

[46] «Злокозненные истории», в случае которых за основу берется подход, аналогичный используемому применительно к «пользовательским историям», описывают сценарии, которым мог бы следовать злоумышленник, чтобы нарушить безопасность международной системы eTIR.

неуспешность проверки сообщений eTIR, использование недействительных цифровых подписей, исключения, сгенерированные системой, производительность обработки сообщений и т. д. Все эти выведенные и записанные в журналы eTIR показатели используются впоследствии и могут быть отображены в виде графиков для изучения вариаций и потенциального инициирования — на основе определенных моделей — предупреждений, которые могут сигнализировать о потенциальной кибератаке;

- **постоянное отслеживание новых технологий**: чтобы быть в курсе развивающихся технологий и методов защиты программного обеспечения ИТ-эксперты должны регулярно участвовать в учебных мероприятиях, включая изучение новейших продуктов таких организаций, как OWASP[47].

7. Оценки безопасности

251. Оценка ИТ-безопасности — это конкретное исследование, направленное на выявление связанных с информационной безопасностью уязвимостей и факторов риска. Она может проводиться по внутренней линии ЕЭК, силами экспертов Организации Объединенных Наций по информационной безопасности либо внешними специализированными компаниями по поручению ЕЭК. Оценка безопасности имеет целью обеспечить интегрирование необходимых средств контроля за безопасностью уже на этапах разработки и внедрения международной системы eTIR. Правильно проведенная оценка безопасности должна вылиться в подготовку документов с указанием любых пробелов в системе безопасности и предложениями по их устранению. Результаты оценки безопасности носят конфиденциальный характер.

252. ИТ-специалисты должны стремиться к регулярному проведению оценок безопасности, а в идеале — перейти на автоматизацию некоторых из них, подлежащих выполнению с высокой периодичностью. Например, тип оценки безопасности, именуемый «оценка уязвимостей» и имеющий целью сканирование исходного кода и программных компонентов, используемых для создания и функционирования международной системы eTIR, должен быть автоматизирован с помощью специальных инструментальных средств и выполняться регулярно. Это позволит немедленно выявлять (и устранять) потенциальные уязвимости при внесении исправлений и обновлении компонентов программного обеспечения.

253. При разработке любой новой основной версии международной системы eTIR следует проводить более тщательную оценку безопасности силами либо экспертов Организации Объединенных Наций по информационной безопасности, либо внешней специализированной компании по поручению ЕЭК. Такая оценка безопасности, скорее всего, будет иметь форму «тестирования на возможность проникновения», где тест-инженеры берут на себя роль злоумышленников и пытаются обнаружить и использовать уязвимости безопасности в международной системе eTIR. В зависимости от различных факторов такое тестирование может осуществляться по принципу «черного», «серого» или «белого ящика». Цвет указывает на объем информации, имеющейся в распоряжении тест-инженера. При оценке по принципу «черного ящика» тестировщик изначально ничего не знает о системе, которая будет объектом тестирования. При оценке по принципу «серого ящика» уровень доступа и объем располагаемой информации являются не полными; доступ носит ограниченный характер, а информация предоставлена лишь частично. Наконец, оценка по принципу «белого ящика» означает тест, при котором тестировщик имеет полный доступ к исходному коду, сетевым схемам и другой соответствующей информации.

[47] Open Web Application Security Project® (OWASP) (Проект по обеспечению безопасности открытых веб-приложений) — это некоммерческий фонд, который работает над повышением безопасности программного обеспечения. См. owasp.org.

D. Security of exchanges with the eTIR international system[48]

1. Introduction

254. This section describes the security model and controls that should be followed by the different eTIR stakeholders while exchanging messages with the eTIR international system. The security model is designed to meet the requirements in terms of confidentiality, integrity and non-repudiation listed above. The technical details and versions of the algorithms and protocols mentioned should be regularly reviewed by TIB to ensure that the objectives and exigencies, in terms of security, are continuously covered.

2. Confidentiality

255. As the eTIR messages are exchanged between the eTIR stakeholders over the internet, these exchanges need to be encrypted to prevent any third party from being able to read the messages exchanged and, thus, get access to this confidential information. The HyperText Transfer Protocol Secure (HTTPS), used to access the eTIR international system endpoints, is an extension of the HyperText Transfer Protocol (HTTP) where communication is encrypted using Transport Layer Security (TLS), a cryptographic protocol designed to provide communications security over public networks like the internet. The bidirectional encryption of the exchanges using HTTPS/TLS between a client and server protects against eavesdropping and tampering of the communication. The version of TLS to be used should be either version 1.2 or 1.3[49].

256. As the encryption of the exchanges between the eTIR stakeholders uses the HTTPS/TLS protocols to ensure the confidentiality of the communication, there is no need to either set up Virtual Private Networks (VPN) or to perform a double encryption at the eTIR messages level using the techniques available using SOAP.

3. Integrity and non-repudiation

257. Messages exchanged with the eTIR international system must be authenticated and their integrity must be ensured to achieve non-repudiation. This is accomplished using the concept of electronic signatures. Definitions of electronic signatures vary depending on the applicable jurisdiction and a common denominator is therefore set in the context of the eTIR specifications. This common denominator states that electronic signatures should achieve the following requirements:

- The signatory can be uniquely identified and linked to the electronic signature;
- The signatory must have sole control of the private key that was used to create the electronic signature;
- The electronic signature must be capable of identifying if its accompanying data has been tampered with after the message was signed.

258. From a technical point of view, this is achieved using a digital certificate (also known as public key certificate) following the X.509 standard[50], version 3. Each eTIR stakeholder wishing to interconnect his or her information systems with the eTIR international system should be issued a X.509 certificate from a trusted Certificate Authority (CA)[51]. The X.509 certificate, which uniquely identifies the eTIR stakeholder is used to sign the eTIR messages. This way of implementing electronic signature not only ensures the identity of the sender but also guarantees that the message content has not been tampered during the transmission, thus ensuring integrity.

[48] Этот и следующий разделы написаны на английском языке, чтобы можно было заполнить часть о безопасности. Эти разделы будут переведены на русский язык в неофициальном документе 12.

[49] Versions 1.0 and 1.1 of the TLS have been deprecated in 2020 as they are no longer considered as secure.

[50] See itu.int/ITU-T/recommendations/rec.aspx?rec=X.509.

[51] Also known as Trusted Third Parties.

259. In order for the X.509 certificates to ensure a high level of security, they should be created using the following parameters:

- The validity period should be, maximally, one year;
- The public key algorithm should be RSA with a key length of 4096 bits;
- The signature algorithm should be one of the following: SHA-256 with RSA, SHA-384 with RSA or SHA-512 with RSA (recommended).
- The "Country (C)", "State Name (ST)" and "Locality Name (L)" parameters should reflect where the eTIR stakeholder is located. Only the "State Name (ST)" parameter is optional;
- The "Email (E)" parameter should provide the email address of the IT service desk of the eTIR stakeholder;
- The "Common Name (CN)" and the "Organization Name (O)" parameters should hold the same value which is the full name of the eTIR stakeholder as an entity/organization.

260. As the X.509 certificates have a limited validity period, they will be regularly replaced with new ones and the exchange of new certificates should be properly planned between ECE and the other eTIR stakeholders to prevent any interruption of service. Also, since data exchanged and stored with the eTIR international system should be kept for ten years[52], ECE will keep all previous X.509 certificates of the eTIR stakeholders in a secure location to be able to verify the electronic signature of old eTIR messages, in case ECE is requested by the competent authorities of contracting parties to provide all data related to a TIR transport.

4. Whitelisting

261. As the eTIR stakeholders who wish to communicate with the eTIR international system need to complete an interconnection project, ECE keeps an accurate and up-to-date list of these companies/entities/organizations. This approach allows to put an extremely effective security measure in place: whitelisting. The eTIR international system is configured not to be accessible by anyone from the internet, except by a restricted list of IP addresses which correspond to the main servers of the eTIR stakeholders which have completed their interconnection projects. This approach drastically reduces the potentiality of cyberattacks to the eTIR international system, including "denial of service" and trying to "spoof"[53] an eTIR stakeholder.

262. During the course of the interconnection project, ECE requests the IP addresses of the servers of the eTIR stakeholder which will connect with the eTIR international system, both on the UAT and PRD environments, and liaises with the United Nations hosting entity to configure the network appliances accordingly.

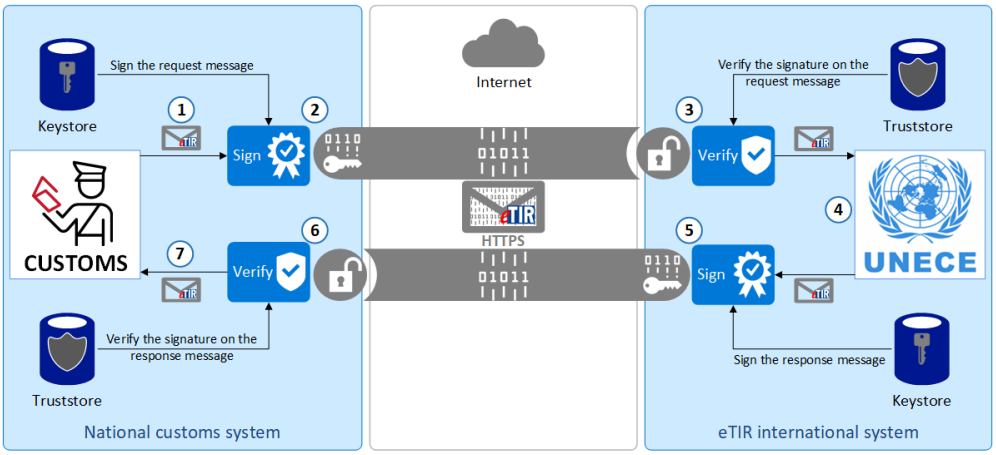
5. eTIR security model

263. The eTIR security model combines all security aspects mentioned above to provide a highly secured approach. The following figure illustrates how this security model works with an eTIR message being sent from a national customs systems to the eTIR international system using web services. The same approach applies when communicating in the same way with guarantee chains and holders.

[52] As per Article 12 of Annex 11 of the TIR Convention.

[53] A spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.

Рисунок XXII
eTIR security model



264. In the example above, as a preliminary step, the X.509 certificate of the national customs system is installed in the eTIR international system truststore and the eTIR international system X.509 certificate is installed in the national customs system truststore. This mandatory initial step allows the validation of the digital signatures that are transferred as security tokens in all eTIR messages exchanged in the context of the eTIR procedure. The procedure below describes the steps numbered in the figure above and explains how a request message is sent by the national customs system to the eTIR international system, and how the related response is sent back:

(1) The national customs system generates a request message to be sent to the eTIR international system web service;

(2) The request message is signed with the private key of the national customs system X.509 certificate. It is then encrypted using HTTPS/TLS and sent over the internet. The connection can be successfully established, as the national customs system is whitelisted by the network appliances of the eTIR international system;

(3) The eTIR international system receives the request message, decrypts it, verifies the signature of the message using the public key of the national customs system X.509 certificate to authenticate it and to confirm its integrity. The full message including its digital signature is then securely stored in the eTIR logs;

(4) The eTIR international system processes the request message and generates a response message in return;

(5) The response message is signed with the private key of the eTIR international system X.509 certificate and securely stored in the eTIR logs. It is then encrypted using HTTPS/TLS and sent over the internet;

(6) The national customs system receives the response message, decrypts it, and verifies the signature of the message using the public key of the eTIR international system X.509 certificate to authenticate it and to confirm its integrity;

(7) The national customs system finally processes the response message.

265. The completion of this whole process illustrates the implementation of the various security measures described in the sections above to achieve the requirements of confidentiality, integrity and non-repudiation.

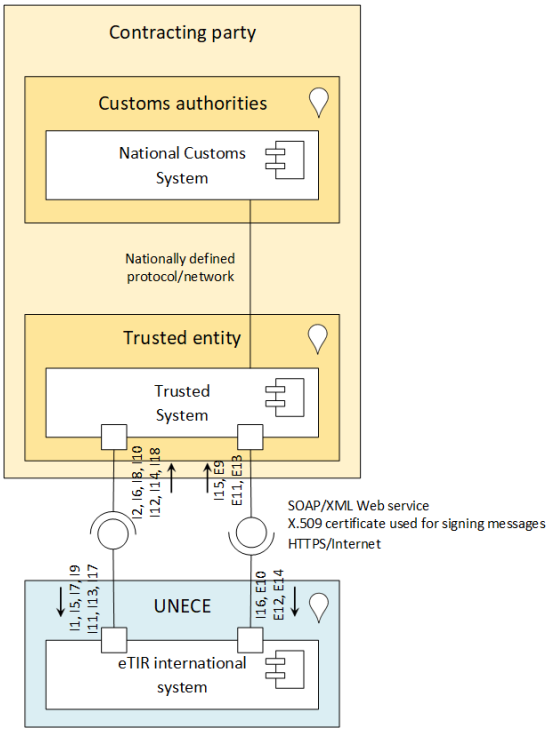
6. Alternative security models

266. National legislations and regulations in contracting parties may prevent their customs authorities from interconnecting their national customs systems to the eTIR international system by following the specifications described above. In that case, an alternative security model should be designed and agreed between the IT experts of ECE and of the customs authorities. It should also be reviewed and approved by TIB. This alternative security model

should meet the same security requirements in terms of confidentiality, integrity and non-repudiation, to be accepted.

267. A possible alternative security model is described below in case the customs authorities of a contracting party are required to use specific encryption algorithms or other technical aspects that would prevent them to initiate a direct connection with the eTIR international system. This security model is similar to the one described above, except that another entity under the contracting party government jurisdiction would play the role of a proxy between the eTIR international system and the national customs system. This entity should be trusted by the customs authorities and the technical details of the connection between this entity and the national customs system would be the sole decision of the contracting party and should be described in the eTIR technical specifications. The following figure shows the architecture of this alternative security model.

Рисунок XXIII
An alternative security model



268. This alternative security model still requires that the communication between the eTIR international system and the trusted system be done using HTTPS/TLS and signing the eTIR messages using X.509 certificates that would comply with the technical specifications described above. On the contracting party's end, the X.509 certificate signing messages sent by the customs authorities could belong to the customs authorities or to the trusted entity, at the decision of the customs authorities.

7. Common threats and mitigation measures

269. A table is provided in annex VI.D of the present document to summarize all security measures and controls that should be put in place for the eTIR international system, and to give an overview for the contracting parties to the TIR Convention on how these measures will mitigate the risks posed by common security threats.

E. Security of exchanges between other eTIR stakeholders

1. Introduction

270. The previous section describes the technical specifications of the exchanges between any eTIR stakeholders and the eTIR international system using web services. These eTIR stakeholders include customs authorities, guarantee chains and holders and all of them should

have undergone an interconnection project. In addition to these types of exchanges, holders can also exchange information (advance TIR data and advance amendment data) directly with the customs authorities[54]. This section describes the technical specifications of this latter type of communication only.

2. Authentication of the holder

271. Each contracting party shall publish a list of all electronic means by which advance TIR data and advance amendment data can be submitted by the holder to the customs authorities[55]. The authentication mechanisms used by these electronic means should uniquely identify the holder and should feature security measures and controls which provide sufficient assurance that the authentication mechanism is secure, in accordance with national laws[56]. In order to be specific and transparent about this important point, each contracting party shall publish the list of authentication mechanisms used by these electronic means[57]. Finally, it is also important to mention that the authentication of the holder performed in this context shall be recognized by the other contracting parties along the itinerary of the TIR transport following the eTIR procedure[58].

272. The authentication of the holder exchanging data directly with the customs authorities is, therefore, a matter of national concern and is not governed by the eTIR specifications. In order to assist and facilitate the decision of contracting parties about this important topic, the next sections provide guidelines and best practices of authentication mechanisms that do not rely on electronic signatures.

3. Multi-Factor Authentication (MFA)

273. MFA is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two (or more) pieces of evidence (or factors) to an authentication mechanism. These two (or more) pieces should belong to at least two different classes among the three that exist:

- **Knowledge**: something only the user knows, like a password or a personal identification number (PIN) code;
- **Possession**: something only the user has, like a smartphone with a configured software-based authenticator, a smartcard or a security card (as used in ITDB);
- **Inherence**: something only the user is, like fingerprints, voice prints, retina patterns, iris patterns or face shapes.

274. It is recommended to use MFA in the authentication mechanism as it provides a high level of assurance that the user is indeed who he or she claims to be.

4. Password strength

275. Most of the web sites and web applications rely on passwords (either solely or as part of an MFA) to authenticate their users. It is important to understand and comply with the minimum requirements in terms of password length and complexity as effective attacks can crack passwords that would not be compliant in seconds. All passwords should conform to the following specifications:

- At least 12 characters long; more than 14 characters is better;
- Different from the default (initial) password;
- Not be the same as the username;
- Composed of, at least, three of the following character classes:

[54] As per paragraph 2 of Article 6 of Annex 11 of the TIR Convention.
[55] As per paragraph 4 of Article 6 of Annex 11 of the TIR Convention.
[56] As per paragraph 1 of Article 7 of Annex 11 of the TIR Convention.
[57] As per paragraph 3 of Article 7 of Annex 11 of the TIR Convention.
[58] As per Article 8 of Annex 11 of the TIR Convention.

- upper case letters: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- lower case letters: abcdefghijklmnopqrstuvwxyz
- numbers: 0123456789
- punctuation marks: !@#$%^&*()+=\`{}[]:";'< >?,./)

- Not be based on words found in dictionaries of any language or based on simple patterns such as “aaabbb”, “qwerty”, “zyxwvuts”, “123321”, etc.

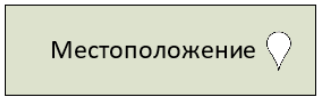
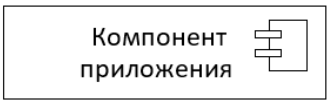
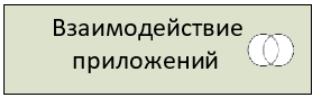
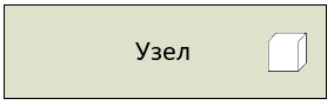
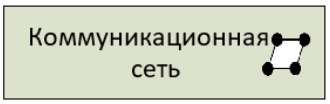
276. In addition, users should be encouraged not to base their password on any personal information that is easily available to potential adversaries, such as names of family members, pets, friends, co-workers, birthdays, addresses, phone numbers, etc. And, finally, passwords should be regularly changed, at least once per year.

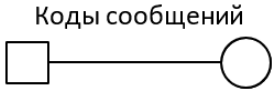
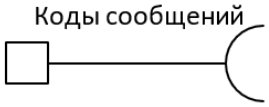
V. Приложение

A. Обозначения на диаграммах

277. Спецификация ArchiMate® 3.0.1 См.: pubs.opengroup.org/architecture/archimate3-doc/ обозначения используются для представления различных архитектурных точек просмотра на диаграммах, содержащихся в этом документе. В таблице ниже описаны только концепции языка моделирования «ArchiMate», используемые на диаграммах. Просьба обратить внимание на тот факт, что цвета, используемые на заднем плане рисунков, отображают различные субъекты или системы, а не какую-либо конкретную концепцию «ArchiMate».

Таблица 32
Обозначения на диаграммах «ArchiMate»

Концепция	*Описание*	*Символ*
Местоположение	Местоположение используется для моделирования мест, в которых отображены иные концепции.	
Компонент приложения	Модульная, развертываемая и заменяемая часть системы программного обеспечения, которая формирует ее поведение и данные и пропускает их через соответствующий набор интерфейсов.	
Взаимодействие приложений	Взаимодействие приложений представляет собой совокупность двух или более компонентов приложения, которые действуют на взаимной основе в порядке формирования совместного поведения приложений.	
Узел	Узел представляет собой соответствующий вычислительный или физический ресурс, который содержит, манипулирует или взаимодействует с другими вычислительными или физическими ресурсами.	
Коммуникационная сеть	Коммуникационная сеть представляет собой совокупность структур, соединяющих компьютерные системы или другие электронные устройства в целях передачи, маршрутизации и приема данных.	

Концепция	*Описание*	*Символ*
Интерфейс имеется	Точка доступа, в которой сервисные средства поддержки данного приложения доступны для другого компонента приложения. Коды сообщений, передаваемые этим интерфейсом, могут быть перечислены в верхней части символа.	
Интерфейс требуется	Указывает на необходимость подключения к сервисам данного приложения, которым обеспечивается доступ со стороны другого компонента данного приложения. Коды сообщений, передаваемые обратно этим интерфейсом, могут быть перечислены в верхней части символа.	

B. Технический глоссарий

278. В данном разделе содержится нижеследующая таблица, в которой приводится определение всех технических терминов, используемых в технических спецификациях eTIR.

Таблица 33
Технический глоссарий

Термин	*Определение*
Интерфейс программирования приложений	Интерфейс программирования приложений (API) — программный интерфейс, который используется для обеспечения доступа к соответствующему приложениюили услуге из какой-либо программы.
Асимметричноешифрование	Криптографическая система, использующая два ключа: открытый ключ, известный всем, и частный (или секретный) ключ, известный только владельцуспаренных ключей. Например, когда Алиса желает отправить защищенное сообщение Бобу, она использует для шифрования этого сообщения открытый ключ Боба. Затем для расшифровки этого сообщения Боб использует свой персональный ключ. RSA — пример асимметричного алгоритма.
Удостоверениеподлинности	Аутентификация представляет собой процесс проверки или тестирования, позволяющий удостовериться в том, что идентичность субъекта, который обратился с запросом, является подлинной. Аутентификация предполагает, что субъекты должны представить дополнительную информацию, подтверждающую подлинность заявленной им идентичности. Наиболее распространенной формой аутентификации является использование соответствующего пароля (она включаетвариации паролей персональных идентификационных номеров (PIN) и парольных фраз). Аутентификация предполагает проверку идентичности данного субъекта, путем сравнения одного или несколько факторов с базой данных действительных идентичностей (т. е. учетных записей пользователей).
Сертификационный орган	Сертификационный орган CO признается в виде субъекта, пользующегося доверительным статусом, поскольку выдаваемый им сертификат увязывает идентичность того или иного лица или предприятия с парой открытых или закрытых ключей (асимметричная криптография), которые используются для обеспечения безопасности большинства транзакций, осуществляемых по Интернету. Например, в тех случаях, когда какое-либо предприятие или лицо желает использовать эти технологии, оно обращается в CO с просьбой выдать ему соответствующий сертификат. Прежде чем выдать сертификат этому лицу или предприятию, которое должен сертифицировать CO, он собирает о нем необходимую информацию.
Конфиденциальность	Конфиденциальность — это концепция мер, используемых для обеспечения защиты секретности данных, объектов или ресурсов. Целью защиты конфиденциальности является

Термин	*Определение*
	предотвращение или минимизация несанкционированного доступа к данным. Конфиденциальность сосредоточена намерах безопасности, позволяющих обеспечить такое положение, при котором никто, кроме предполагаемого получателя сообщения, не сможет его получить или прочитать. Защита конфиденциальности дает возможность уполномоченным пользователям получать доступ к ресурсам и воздействовать на них, но активно предотвращает это воздействие со стороны не уполномоченных пользователей.
Дефект	В ИТ-литературе обычно проводится различие между терминами «ошибка» и «дефект». Действительно, «ошибка» — это результат ошибки кодирования, а «дефект» — это отклонение от требований. В контексте настоящего документа используется только термин «дефект», охватывающий оба значения.
Цифровой сертификат	В криптографии цифровым сертификатом (или, проще говоря, сертификатом в этом документе) является электронный документ, используемый для доказательства права собственности на открытый ключ. Сертификат включает в себя информацию о ключе, сведения о личности его владельца (называемого субъектом), а также цифровую подпись субъекта (называемого эмитентом), который проверил содержание сертификата. Если подпись действительна, а программное обеспечение, проверяющее сертификат, доверяет эмитенту, то оно может использовать этот ключ для безопасной связи с субъектом сертификата.
Цифровая подпись	Цифровой код (набор знаков), который может прилагаться к электронному сообщению и преследует две различные цели: 1) сообщения с цифровой подписью гарантируют получателю тот факт, что данное сообщение действительно пришло от заявленного отправителя. Они исключают невозможность отказа (т. е. не позволяют отправителю впоследствии утверждать, что данное сообщение — это подделка) и 2) сообщения с цифровой подписью гарантируют получателю тот факт, что данное сообщение не было изменено на этапе его передачи от отправителя получателю по каналу связи (его целостность была сохранена). Это предохраняет сообщение как от злонамеренного изменения (когда какая-либо третья сторона изменяет смысл сообщения), так и от непреднамеренного изменения (по причине сбоев в процессе передачи данных, например в случае электрических помех).
Среды	В течение своего жизненного цикла часть программного обеспечения разрабатывается и поддерживается в нескольких средах, которые служат различным целям. Некоторые из них используются для разработки, некоторые — для тестирования, и, наконец, другая, производственная среда, используется для работы системы, когда она «жива» и доступна в качестве своего рода услуги для ее конечных пользователей.
Ошибка	Ошибка — это серьезный сбой в подтверждении данных, который приведет к тому, что сообщение будет отклонено.
Интерфейсные веб-серверы	Веб-сервер, принимающий запросные сообщения из конечных точек веб-службы международной системы eTIR (или отправляющий запросные сообщения на конечные точки веб-службы других заинтересованных сторон eTIR).
Гит	Гит — система контроля версий для отслеживания изменений в любом наборе файлов, обычно используемая для координации работы программистов, разрабатывающих на совместной основе исходный код в процессе разработки программного обеспечения. Цель этой системы включает оптимизацию производительности, целостности данных и поддержку распределенных нелинейных рабочих процессов.
Хэш	Хэш-значение (или просто хэш), также называемое профилем сообщения, представляет собой определенное значение, генерируемое из соответствующего текста. Хэш значительно меньше самого текста и генерируется по соответствующей формуле таким образом, что вероятность выдачи такого же значения хэша любым другим текстом чрезвычайно мала.
Целостность	Целостность представляет собой концепцию защиты надежности и правильности данных. Защита целостности позволяет предотвратить несанкционированное изменение данных. Она гарантирует, что данные останутся правильными, неизменными и сохраненными. Надлежащим образом организованная защита целостности предусматривает соответствующие средства, допускающие внесение санкционированных изменений в условиях одновременной защиты от преднамеренных и злонамеренных несанкционированных действий (таких как вирусы и взломы), а также от ошибок, допущенных уполномоченными пользователями (таких как обычные ошибки или просмотры).
Java	Java — это объектно-ориентированный язык программирования, который строится на основе классов и разработан таким образом, чтобы свести зависимость от средств реализации к минимуму. Это один из языков программирования общего назначения, позволяющий разработчикам приложений написать программу один раз и запустить ее где угодно. Это

Термин	*Определение*
	означает, что скомпилированный Java-код может быть использован на всех платформах, поддерживающих язык Java, не прибегая к перекомпиляции.
Хранилище ключей	Хранилище ключей — это соответствующая база данных, используемая для хранения сертификатов информационных систем владельца хранилища ключей, и может включать в себя сертификаты доверенных лиц (трастовых хранилищ), предназначенные для использования программой. С помощью хранилища ключей тот или иной уполномоченный субъект может подтвердить свою аутентичность перед другими сторонами, а также проверить аутентичность других сторон.
Балансировщик нагрузки	Балансировщик нагрузки — это программный компонент, который распределяет набор задач по выборке ресурсов (серверных узлов) в целях повышения эффективности их общей обработки.
Исключение возможности отказа	Исключение возможности отказа гарантирует, что субъект какого-либо действия или лицо, по вине которого произошло какое-либо событие, не может отрицать, что данное событие произошло. Исключение возможности отказа не позволяет тому или иному субъекту утверждать, что он не отправил сообщение, не выполнил какое-либо действие или не стал причиной какого-либо события. Такая возможность существует благодаря идентификации, аутентификации, санкционированию, подотчетности и аудиту. Исключение возможности отказа может быть установлено с помощью цифровых сертификатов, идентификаторов сессий, журналов транзакций и многих других механизмов контроля за транзакциями и доступом.
OPCCИ	Организация по развитию стандартов структурированной информации (OPCCИ) является некоммерческим международным консорциумом, цель которого состоит в содействии принятию стандартов, не зависящих от конкретной продукции.
Инфраструктура публичных ключей	Инфраструктура открытых ключей (PKI) представляет собой набор ролей, директивных принципов, аппаратного и программного обеспечения и процедур, необходимых для создания, организации, распространения, использования, хранения и отзыва цифровых сертификатов и организации асимметричного шифрования.
Получатель	В контексте данного документа «получателем» является информационная система соответствующей заинтересованной стороны eTIR, которая получает сообщение, отправленное другой заинтересованной стороной eTIR, и обрабатывает его.
RSA	Алгоритм RSA был изобретен в 1977 году Рональдом Л. Ривестом, Ади Шамиром и Леонардом Адлеманом. Это асимметричный алгоритм шифрования, в случае которого используются два разных ключа с математической зависимостью друг от друга. Открытый и закрытый ключи тщательно генерируются с использованием алгоритма RSA; их можно использовать для шифрования информации или ее подписания.
Отправитель	В контексте данного документа «отправителем» является информационная система соответствующей заинтересованной стороны eTIR, которая генерирует и отправляет сообщение eTIR другой заинтересованной стороне eTIR.
Единая точка сбоя	Единая точка сбоя (SPOF) — это та часть системы, которая в случае сбоя вызовет остановку работы всей системы. Точки SPOF нежелательны в любой системе, которая ориентирована на обеспечение высокой доступности или надежности, будь то бизнес-практика, программное приложение или другая промышленная система.
SOAP	Простой протокол доступа к объектам (SOAP) — это спецификация соответствующего протокола сообщений в целях обмена информацией в процессе оказания соответствующих веб-услуг. Он представляет собой протокол на основе стандарта XML, состоящий из трех частей: • оболочка, определяющая структуру сообщения (хедер и текстовая часть) и способ его обработки; • соответствующий набор правил шифрования для описания таких типов данных, которые определяются соответствующими приложениями; • условные обозначения для отображения процедурных вызовов и ответов.
Программная энтропия	Второй закон термодинамики, в принципе, гласит, что неупорядоченность в замкнутой системе не может уменьшаться, она может только оставаться неизменной или расти. Мерой этой неупорядоченности является энтропия. Согласно исследованиям, этот закон, судя по всему, вполне логичен и в случае программных систем: по мере изменения системы, ее неупорядоченность или энтропия стремится возрастать. Это явление известно как программная энтропия. Процесс перестройки кода может привести к поэтапному снижению энтропии программного обеспечения.

Термин	*Определение*
Маркер	Маркер (иногда называемый маркером безопасности) — это объект, который контролирует доступ к цифровому активу. Традиционно этот термин используется для описания соответствующего аппаратного аутентификатора (небольшого устройства) для создания одноразового пароля, который вводится владельцем с клавиатуры в окно входа в систему вместе с идентификатором и PIN-кодом. Однако в случае веб-служб и в связи с растущей потребностью в устройствах и процессах взаимной аутентификации по открытым сетям термин «маркер» был расширен и сейчас включает в себя также соответствующие механизмы программного обеспечения. Маркер может быть сертификатом X.509, который, например, увязывает идентичность с открытым ключом.
Совокупная стоимость владения	Совокупная стоимость владения (TCO) представляет собой общую сумму денег, которую владелец информационной системы должен был потратить на протяжении жизненного цикла этой системы. В расчет принимаются все расходы (прямые и косвенные).
Хранилище доверенных сертификатов	Хранилище доверенных сертификатов представляет собой соответствующий файл хранилища ключей, в котором хранятся сертификаты других сторон, с которыми вы намерены связаться, или сертификационного органа, которому вы доверяете в плане идентификации других сторон.
Виртуальная ферма серверов	Виртуальная ферма серверов представляет собой сетевую среду, которая использует несколько серверов приложений и инфраструктуры, работающих на двух или более физических серверах с использованием соответствующей программы виртуализации сервера. Эта архитектура обеспечивает ряд преимуществ, включая консолидацию серверов, избыточность, преодоление отказов, высокую доступность и оптимизированное использование ресурсов.
Веб-служба	Виртуальная служба/функция, действующая в пределах соответствующей сети (частной или через Интернет), которая позволяет системе поддерживать связь с помощью сообщений в строгом формате. Межмашинная коммуникация — это еще один термин для определения этого вида связи.
Безопасность веб-служб	Спецификация «безопасность веб-служб» (BC-безопасность) описывает усовершенствованные версии SOAP 1.1, повышающие защиту (целостность) и конфиденциальность сообщений. Эти усовершенствования включают в себя функциональные параметры обеспечения безопасности сообщений SOAP с помощью цифровой подписи XML, конфиденциальности с помощью шифрования XML и расширения учетных данных с помощью маркеров безопасности (например, маркера X.509).
Язык описания веб-службы	Язык описания веб-служб (WSDL) — это язык описания интерфейса на базе XML, который используется для описания функциональных параметров, предлагаемых веб-службами.
X.509 сертификат	X.509 — это распространенный формат цифровых сертификатов, который широко используется в интернете вместе с протоколом TLS. Сертификат X.509 определяет связь между открытым ключом и соответствующим набором атрибутов, который включает (как минимум) название субъекта, название эмитента, серийный номер и срок действия. Этот момент определяется в запросе на комментарии (RFC) по документу 5280[59].
Маркер X.509	Маркер X.509 представляет собой цифровую подпись, которая генерируется с помощью сертификата X.509 отправителя и которая будет использоваться для аутентификации отправителя сообщения. По этой причине он является частью самого сообщения, в заголовке соответствующего раздела оболочки SOAP.
XML	XML означает «eXtensible Markup Language» (расширяемый язык разметки) — язык, определяющий набор правил для кодирования документов в формате, который одновременно является человеко- и машиночитаемым. Он используется SOAP для кодирования сообщений, отправляемых веб-службами.
XML-подпись	Спецификация подписи XML является совместным проектом W3C и IETF. Подписи XML обеспечивают целостность, подтверждение подлинности сообщений и/или проверку подлинности подписи для данных любого типа независимо от того, выполнены ли они в формате XML, который включает подпись, или в другом формате.
Определение схемы XML	Определение схемы XML (XSD) — это рекомендация W3C, описывающая структуру и форматирование элементов XML-документа.

[59] См. tools.ietf.org/html/rfc5280.

C. Анализ в целях определения потребностей в части пропускной способности и масштабируемости международной системы eTIR

1. Введение

279. В данном разделе анализируются — на основе существующих данных (по состоянию на февраль 2021 года) и опыта, накопленного в ходе разработки международной системы eTIR, — требования к способности системы пропускать сообщения и к объему данных, подлежащих обработке международной системой eTIR.

280. Поскольку международная система eTIR пока еще не действует, в данном анализе нет возможности использовать реальные данные, вследствие чего к нему нужно подходить с осторожностью, принимая всегда во внимание наихудшие сценарии и рассчитывая оценки на основе не средних, а максимальных показателей. Когда международная система eTIR начнет использоваться в реальных условиях эксплуатации, ЕЭК еще раз вернется к этому анализу с целью составить более точные прогнозы в части потребностей в пропускной способности на ближайшие годы в увязке с количеством проданных электронных гарантий.

2. Анализ на основе количества сообщений

281. На основе последних статистических данных, касающихся продажи книжек МДП (и количества электронных гарантий, выданных в ходе пилотных проектов eTIR), в следующей таблице представлен обобщенный обзор статистических данных за прошлые годы в сочетании с оценками объема продажи книжек МДП и электронных гарантий на следующие пять лет.

Таблица 34
Статистика и прогнозирование продаж книжек МДП и электронных гарантий

Год	*Количество проданных книжек МДП*	*Количество проданных электронных гарантий*	*Увеличение количества проданных электронных гарантий в расчете на год*
2001	2 707 950	*Н/П*	*Н/П*
2002	3 095 200	*Н/П*	*Н/П*
2003	3 298 000	*Н/П*	*Н/П*
2004	3 211 050	*Н/П*	*Н/П*
2005	3 240 650	*Н/П*	*Н/П*
2006	3 599 850	*Н/П*	*Н/П*
2007	3 076 250	*Н/П*	*Н/П*
2008	3 253 800	*Н/П*	*Н/П*
2009	2 230 400	*Н/П*	*Н/П*
2010	2 822 200	*Н/П*	*Н/П*
2011	3 074 500	*Н/П*	*Н/П*
2012	3 158 300	*Н/П*	*Н/П*
2013	2 920 150	*Н/П*	*Н/П*
2014	1 945 050	*Н/П*	*Н/П*
2015	1 500 450	(пилотный проект eTIR) 5	*Н/П*
2016	1 223 400	(пилотный проект eTIR) 59	*Н/П*
2017	1 154 650	(пилотный проект eTIR) 82	*Н/П*
2018	1 020 650	(пилотный проект eTIR) 81	*Н/П*
2019	858 100	(пилотный проект eTIR) 78	*Н/П*
2020	679 300	(пилотный проект eTIR) 2	*Н/П*
2021	(оценка) 600 000	(пилотный проект eTIR) 63, (оценка) 5 000	*Н/П*
2022	(оценка) 550 000	(оценка) 15 000	200 %

Год	*Количество проданных книжек МДП*	*Количество проданных электронных гарантий*	*Увеличение количества проданных электронных гарантий в расчете на год*
2023	(оценка) 500 000	(оценка) 60 000	300 %
2024	(оценка) 450 000	(оценка) 200 000	233 %
2025	(оценка) 400 000	(оценка) 400 000	100 %
2026	(оценка) 300 000	(оценка) 700 000	75 %

282. В целях расчета оценок проданных электронных гарантий были приняты во внимание следующие факторы:

a) число стран, приступивших к реализации в течение 2020 года соответствующих проектов по обеспечению взаимосвязи между своей национальной таможенной системой и международной системой eTIR;

b) число стран, которые уже выразили заинтересованность в налаживании этой взаимосвязи и которые должны приступить к реализации таких проектов, скорее всего, в 2021 году;

c) количество книжек МДП, выданных в последние годы на перевозки по транспортным коридорам, которыми пользуются те договаривающиеся стороны, которые приступили или в скором времени приступят к реализации проектов по налаживанию взаимосвязи;

d) предпринятые усилия или заинтересованность региональных экономических организаций в целях подготовки доказательств, подтверждающих целесообразность концепции взаимосвязи своей системы таможенного союза с международной системой eTIR, а также возможные даты этих взаимосвязей;

e) результаты «исследования причин сокращения количества используемых книжек МДП» (здесь и далее «исследование»), подготовленного Исполнительным советом МДП (ИСМДП) в 2020 году и, в частности, тенденции, связанные с продажей книжек МДП;

f) усилия, которые будут прилагать в ближайшие годы ЕЭК и международная организация в целях привлечения большего числа стран и рынков (интермодальных, почтовых) и распространения действия Конвенции МДП на новые регионы, как это указано в упомянутом выше исследовании;

g) вместе с тем на данный момент для подготовки таких оценок никто не использовал ни анализ чувствительности, ни другие научные методы прогнозирования.

283. Оценки расширения сбыта электронных гарантий на ежегодной основе показывают, что после первых лет их использования долгосрочное увеличение в процентах, как правило, становится линейным и может оставаться таковым, если число договаривающихся сторон Конвенции МДП, подключенных к международной системе eTIR, будет продолжать увеличиваться. Поэтому нам следует разрабатывать международную систему eTIR таким образом, чтобы ее можно было легко масштабировать в расчете на устойчивое ежегодное увеличение объема перевозок МДП в соответствии с процедурой eTIR на все 100 %.

284. Количество отправленных и полученных сообщений в расчете на одну перевозку МДП зависит от целого ряда таких критериев, как: количество операций МДП, количество сообщений в порядке предварительного декларирования (сообщения, касающиеся предварительных данных МДП, а равно предварительных данных о внесении изменений и аннулировании предварительных данных), отправленных держателем, количество случаев использования механизма запроса, количество случаев замены пломб, происходит ли какое-либо происшествие или авария во время перевозки МДП и т. п. В следующей таблице приведены некоторые сценарии перевозки МДП и соответствующие детали по каждому из них, максимальное количество сообщений, полученных и отправленных международной

системой eTIR (в случае, если держатель отправляет сообщения в порядке предварительного декларирования через международную систему eTIR), а также количество только запросных сообщений.

Таблица 35
Сообщения, полученные и отправленные международной системой eTIR, в разбивке по сценариям

Количество операций МДП	*Полученные и отправленные сообщения по операциям МДП*	*Полученные и отправленные сообщения по предварительной декларации*	*Общее количество сообщений в разбивке по сценарию*	*Количество сообщений только с запросами в разбивке по сценариям*
2	E1/E2, I1/I2, I7/I8, (I15/I16) x 2, (I9/I10, I11/I12, I13/I14) x 2, (E7/E8) x 9, (E5/E6) x 9, (I5/I6) x 2	E9/E10	64	21
3	E1/E2, I1/I2, I7/I8, (I15/I16) x 2, (I9/I10, I11/I12, I13/I14) x 3, (E7/E8) x 12, (E5/E6) x 12, (I5/I6) x 3	E9/E10	88	28
4	E1/E2, I1/I2, (I7/I8) x 2, (I15/I16) x 5, (I9/I10, I11/I12, I13/I14) x 4, (E7/E8) x 14, (E5/E6) x 14, (I5/I6) x 4	E9/E10, E11/E12	110	36
4	E1/E2, I1/I2, (I7/I8) x 2, (I15/I16) x 5, (I9/I10, I11/I12, I13/I14) x 4, (E7/E8) x 14, (E5/E6) x 14, (I5/I6) x 4	E9/E10, E13/E14, E9/E10, E11/E12, E13/E14, E11/E12	118	40
5	E1/E2, I1/I2, (I7/I8) x 2, (I15/I16) x 7, (I9/I10, I11/I12, I13/I14) x 5, (E7/E8) x 17, (E5/E6) x 17, (I5/I6) x 5	E9/E10, E11/E12, E11/E12	136	44
6	E1/E2, I1/I2, (I7/I8) x 2, (I15/I16) x 9, (I9/I10, I11/I12, I13/I14) x 6, (E7/E8) x 20, (E5/E6) x 20, (I5/I6) x 6	E9/E10, E11/E12, E11/E12	160	51
7	E1/E2, I1/I2, (I7/I8) x 3, (I15/I16) x 15, (I9/I10, I11/I12, I13/I14) x 7, (E7/E8) x 24, (E5/E6) x 24, (I5/I6) x 7	E9/E10, E11/E12, E11/E12, E11/E12	198	61
8	E1/E2, I1/I2, (I7/I8) x 3, (I15/I16) x 18, (I9/I10, I11/I12, I13/I14) x 8, (E7/E8) x 27, (E5/E6) x 27, (I5/I6) x 8	E9/E10, E11/E12, E11/E12, E11/E12	224	68
9	E1/E2, I1/I2, (I7/I8) x 3, (I15/I16) x 21, (I9/I10, I11/I12, I13/I14) x 9, (E7/E8) x 30, (E5/E6) x 30, (I5/I6) x 9	E9/E10, E11/E12, E11/E12, E11/E12	250	75
10	E1/E2, I1/I2, (I7/I8) x 4, (I15/I16) x 30, (I9/I10, I11/I12, I13/I14) x 10, (E7/E8) x 34, (E5/E6) x 34, (I5/I6) x 10	E9/E10, E11/E12, E11/E12, E11/E12, E11/E12	292	85

285. 2020 году МСАТ сообщил о следующих показателях продажи[60]: 4300 книжек МДП с 4 отрывными листками (0,6 %), 544 200 книжек МДП с 6 отрывными листками (80 %), 131 050 книжек МДП с 14 отрывными листками (19,3 %) и 0 книжек МДП с 20 отрывными листками. Таким образом, большинство перевозок МДП, произведенных в указанном выше году, включали 3 операции МДП (6 отрывных листков). С учетом предыдущей таблицы и осторожного подхода к пропускной способности международной системы eTIR, можно считать, что в среднем общее количество взаимных сообщений в расчете на одну перевозку МДП составляет 120, а среднее количество запросных сообщений — 40.

286. Мы также будем предполагать, что среднее количество взаимных сообщений в расчете на одну перевозку МДП также будет увеличиваться на 5 % в год. Это

[60] См. неофициальный документ WP.30/AC.2 (2021) № 5.

предположение подкрепляется тем фактом, что со временем к международной системе eTIR подключится большее число договаривающихся сторон, что позволит расширить возможности для более продолжительных перевозок МДП в режиме eTIR. Наконец, этому может также способствовать появление новых версий спецификаций eTIR.

287. В нижеследующей таблице приводятся оценочные данные о количестве сообщений, которые могла бы отправлять и получать международная система eTIR и, как следствие, поддерживать его в течение следующих лет.

Таблица 36
Оценочное число сообщений, которое будет поддерживаться международной системой eTIR

Год	*A. Оценочное количество проданных электронных гарантий*	*B. Оценочное среднее количество всех сообщений в расчете на одну перевозку МДП*	*C. Оценочное среднее количество всех сообщений в год в миллионах (A x B)*	*D. Оценочное среднее количество всех запросных сообщений в расчете на одну перевозку МДП*	*E. Оценочное среднее количество запросных сообщений в расчете на один год в миллионах (A x D)*
2021	5 000	130	0,65	40	0,20
2022	15 000	137	2,06	42	0,63
2023	60 000	143	8,58	44	2,64
2024	200 000	150	30,00	46	9,20
2025	400 000	158	63,20	49	19,60
2026	700 000	166	116,20	51	35,70

288. В этом случае мы могли бы предположить, в качестве гипотетического варианта, что максимальное количество сообщений будет в пять–десять раз больше среднего количества сообщений. Затем мы можем составить следующие две таблицы: одну для максимального количества полученных и отправленных сообщений международной системой eTIR, а другую — для максимального количества полученных запросных сообщений, причем речь идет о количестве обоих сообщений в минуту.

Таблица 37
Расчетное максимальное количество полученных и отправленных сообщений

Год	*A. Оценочное среднее количество всех сообщений в год в миллионах*	*B. Расчетное среднее количество всех сообщений в минуту (A / (365 x 24 x 60))*	*Расчетная нижняя граница максимального количества всех сообщений в минуту (B x 5)*	*Расчетная верхняя граница максимального количества всех сообщений в минуту (B x 10)*
2021	0,65	1,24	6,2	12,4
2022	2,06	3,92	20,0	39,2
2023	8,58	16,32	81,6	163,2
2024	30,00	57,23	286,2	572,3
2025	63,20	120,57	602,9	1 205,7
2026	116,20	221,69	1 108,5	2 216,9

Таблица 38
Расчетное максимальное количество полученных запросных сообщений

Год	*A. Оценочное среднее количество запросных сообщений в год в миллионах*	*B. Расчетное среднее количество запросных сообщений в минуту (A / (365 x 24 x 60))*	*Расчетная нижняя граница максимального количества всех запросных сообщений в минуту (B x 5)*	*Расчетная верхняя граница максимального количества всех запросных сообщений в минуту (B x 10)*
2021	0,20	0,38	1,9	3,8
2022	0,63	1,20	6,0	12,0
2023	2,64	5,02	25,1	50,2
2024	9,20	17,50	87,5	175,0
2025	19,60	37,29	186,5	372,9
2026	35,70	67,92	339,6	679,2

3. Анализ на основе количества сообщений

289. Способность системы пропускать сообщения, которая должна поддерживаться международной системой eTIR, определяется как количество запросных сообщений, которые должны быть получены и обработаны за определенную единицу времени. Средняя и верхняя граница максимального количества запросных сообщений в минуту выбирается на основе предыдущего анализа.

Таблица 39
Оценочные средние и максимальные требования к способности системы пропускать сообщения

Год	*Оценочное среднее количество запросных сообщений в минуту*	*Оценочное максимальное количество запросных сообщений в минуту*
2021	0,38	3,8
2022	1,20	12,0
2023	5,02	50,2
2024	17,50	175,0
2025	37,29	372,9
2026	67,92	679,2

4. Анализ объема данных

290. В дополнение к оценке способности системы пропускать сообщения, которая должна поддерживаться международной системой eTIR, важно также принимать во внимание фактор размера этих сообщений и общий объем данных, которые подлежат обмену, обработке и регистрации международной системой eTIR.

291. Опыт, накопленный в ходе разработки международной системы eTIR, свидетельствует о том, что 70 % сообщений имеют объем менее 10 Кб, 25 % сообщений — от 11 Кб до 50 Кб, а объем остальных 5 % сообщений — от 51 Кб до 20 Мб (максимально допустимый объем). Мы предполагаем, что в случае 5 % сообщений будут вложены дополнительные документы (что значительно увеличит объем сообщения).

292. Поэтому можно предположить, что средний объем сообщения может составить (90 % x 5 Кб) + (9 % x 25 Кб) + (1 % x 5 Мб) = 57 Кб. Основываясь на предыдущих результатах, мы можем вывести оценку максимального общего объема данных, который должен обрабатываться международной системой eTIR и, в частности, храниться в журналах eTIR.

Таблица 40
Расчетный максимальный объем данных, подлежащих хранению в журналах eTIR

Год	*A. Расчетная верхняя граница максимального количества всех сообщений в минуту*	*B. Расчетный максимальный объем данных в минуту в Мб (A x 0,057)*	*C. Расчетный максимальный объем данных в минуту в Тб (B x 60 x 24 x 365)*
2021	12,4	0,7	0,371
2022	39,2	2,2	1,174
2023	163,2	9,3	4,889
2024	572,3	32,6	17,146
2025	1 205,7	68,7	36,121
2026	2 216,9	126,4	66,417

293. Только небольшая часть этого объема хранится в базе данных eTIR. Сначала в этом хранилище обрабатываются и записываются только запросные сообщения. После этого дополнительные документы в базе данных не хранятся, поэтому мы можем удалить 1 % самых больших сообщений, что дает следующий новый средний объем сообщения: (91 % x 5 Кб) + (9 % x 25 Кб) = 6,8 Кб. Кроме того, следует иметь в виду, что заголовок каждого сообщения в базе данных не хранится и что сохраняются только значения тела сообщения, которые составляют от 3 % до 10 % от объема сообщения, следовательно, максимум 0,68 Кб.

Таблица 41
Расчетный максимальный объем данных, подлежащих хранению в журналах eTIR

Год	*A. Расчетная верхняя граница максимального количества запросных сообщений в минуту*	*B. Расчетный максимальный объем данных в минуту в Кб (A x 0,68)*	*C. Расчетный максимальный объем данных в год в Гб (B x 60 x 24 x 365)*
2021	3,8	2,6	1,36
2022	12,0	8,2	4,29
2023	50,2	34,1	17,94
2024	175,0	119,0	62,55
2025	372,9	253,6	133,28
2026	679,2	461,9	242,75

294. Включенные в сообщения документы хранятся отдельно в системе электронных документов eTIR. Что касается базы данных eTIR, то в расчет принимаются только запросы. Исходя из предыдущих предположений, мы можем, таким образом, хранить только 1 % самых больших сообщений, содержащих встроенные документы, что дает следующий новый средний объем сообщения: 1 % x 5 Мб = 50 Кб. Аналогичным образом, мы можем рассчитать максимальный общий объем данных, который необходимо будет хранить в документах eTIR.

Таблица 42
Расчетный максимальный объем данных, подлежащих хранению в документах eTIR

Год	*A. Расчетная верхняя граница максимального количества запросных сообщений в минуту*	*B. Расчетный максимальный объем данных в минуту в Мб (A x 0,05)*	*C. Расчетный максимальный объем данных в год в Тб (B x 60 x 24 x 365)*
2021	3,8	0,2	0,100
2022	12,0	0,6	0,315

Год	*A. Расчетная верхняя граница максимального количества запросных сообщений в минуту*	*B. Расчетный максимальный объем данных в минуту в Мб (A x 0,05)*	*C. Расчетный максимальный объем данных в год в Тб (B x 60 x 24 x 365)*
2023	50,2	2,5	1,319
2024	175,0	8,8	4,599
2025	372,9	18,6	9,800
2026	679,2	34,0	17,849

5. Выводы

295. Оценки и прогнозы с точки зрения способности системы пропускать сообщения и объема данных правильны лишь настолько, насколько правильны различные допущения. Поскольку международная система eTIR еще не работает, в данном анализе фактические данные отсутствуют. По этой причине международную систему eTIR следует проектировать с учетом требований к пропускной способности и масштабируемости только на первые два года, поскольку существует высокая вероятность того, что реальные данные приведут к необходимости корректировки некоторых допущений, что полностью изменит расчеты и прогнозы на последующие годы.

296. По этой причине настоятельно рекомендуется провести данный анализ еще раз, через шесть месяцев после введения международной системы eTIR в эксплуатацию с целью пересмотреть допущения, повторить расчеты и сделать соответствующие выводы на основе более надежных оценок и прогнозов, касающихся будущих потребностей в части возможностей и масштабируемости международной системы eTIR. После этого необходимо будет также выйти с рекомендацией на предмет ежегодного пересмотра этого анализа в целях его постоянного уточнения.

D. Коды ошибок

297. В данном разделе представлена дополнительная информация о кодах ошибок, используемых в контексте системы eTIR.

298. В перечне кодов 99 определяются все коды ошибок, которые можно использовать в ответных сообщениях в порядке указания тех проблем, которые возникли в процессе обработки соответствующего запросного сообщения. Данный перечень кодов относится только к системе eTIR, поэтому ЕЭК постоянно обновляет этот список, который представлен в следующей таблице.

Таблица 43
Перечень кодов ошибок (CL99)

Код	*Название*	*Описание*
100	Неверное сообщение	Сообщение является неверным, без каких-либо дополнительных уточнений относительно ошибки
101	Отсутствует параметр	В сообщении отсутствует необходимый параметр
102	Неверный параметр значения домена	Значение параметра выходит за пределы установленного перечня допустимых значений
103	Неправильный формат даты	Параметр, содержащий дату, невозможно правильно преобразовать
104	Не целое число	Числовое поле содержит данные, которые не являются числовыми
105	Длина параметра превышена	Строковое поле содержит слишком много знаков
106	Неверный шаблон	Строковое поле не соответствует шаблону, определенному в схеме XML «Определение сообщения»
151	Несоблюдение условия C001	Условие C001 не выполняется
152	Несоблюдение условия C002	Условие C002 не выполняется
153	Несоблюдение условия C003	Условие C003 не выполняется

Код	*Название*	*Описание*
154	Несоблюдение условия C004	Условие C004 не выполняется
155	Несоблюдение условия C005	Условие C005 не выполняется
158	Несоблюдение условия C008	Условие C008 не выполняется
168	Несоблюдение правила R008	Правило R008 не выполняется
200	Неверное состояние	Состояние внутреннего объекта является неверным, без каких-либо дополнительных уточнений относительно ошибки
201	Неприемлемая гарантия	Статус гарантии не позволяет принять ее
203	Неотменяемая гарантия	Статус гарантии не позволяет отменить ее
204	Гарантия уже зарегистрирована	Гарантия уже была зарегистрирована
205	Гарантия уже отменена	Гарантия уже была отменена или запрос на ее отмену уже был отправлен
210	Операция уже началась	Данная операция уже начата
211	Операция уже прекращена	Данная операция уже прекращена
212	Операция уже завершена	Данная операция уже завершена
213	Операция еще не началась	Данная операция еще не началась
214	Идентификатор операции уже зарегистрирован	«Отказ начать операцию» — это самостоятельная операция, которая должна иметь соответствующий уникальный идентификатор
215	Последовательность операции уже зарегистрирована	«Отказ начать операцию» — это самостоятельная операция, которая должна иметь уникальную последовательность действий
216	Отказ начать операцию не разрешен	«Отказ начать операцию» не может быть выполнен по причине текущего статуса гарантии или из-за того, что это первая операция для данной перевозки
220	Декларация еще не получена	Операцию нельзя начинать, так как декларация не была получена
299	Повторное сообщение	Такое же сообщение уже было получено из того же источника
300	Неверная операция	Была произведена неверная операция, без каких-либо дополнительных уточнений относительно ошибки
301	Гарантия не найдена	Информация о гарантии в базе данных не найдена
302	Гарантийная цепь не найдена	Информация о гарантийной цепи в базе данных не найдена
303	Тип гарантии не найден	Информация о типе гарантии в базе данных не найдена
304	Таможня не найдена	Данный код ошибки в спецификациях eTIR v4.3 не используется
305	Страна не найдена	Информация о стране в базе данных не найдена
306	Вид контроля не найден	Информация о виде контроля в базе данных не найдена
320	Несоответствие информациио держателе/гарантии	Параметр «Идентификатор держателя» и параметр «Контрольный номер гарантии» не соответствуют тому, что зарегистрировано в базе данных
321	Держатель не уполномочен	Держатель не уполномочен в Международном банке данных МДП (МБДМДП)
322	Держатель не найден	Информация о держателе в МБДМДП на найдена
330	Гарантийная цепь не уполномочена	Гарантийная цепь не уполномочена в базе данных
331	Несоответствие информациио гарантийной цепи/гарантии	Параметр «Код гарантийной цепи» и параметр «Идентификационный номер гарантии» не соответствуют тому, что зарегистрировано в базе данных
332	Несоответствие информации о типе гарантии/гарантии	Параметр «Тип гарантии» и параметр «Идентификационный номер гарантии» не соответствуют тому, что зарегистрировано в базе данных
400	Проблема eTIR	Произошел внутренний сбой в работе международной системы eTIR,без каких-либо дополнительных уточнений относительно ошибки

299. В ответных сообщениях могут быть указаны не все коды ошибок; в следующей таблице показано, на какие коды ошибок можно ссылаться в ответных сообщениях. Эта информация полезна для ИТ-специалистов заинтересованных сторон eTIR в плане правильной реализации последующих действий при получении конкретных кодов ошибок. Этот список представлен в том виде, в котором он был составлен на момент

подготовки настоящего документа. Просьба ознакомиться с самой последней версией eTIR на веб-сайте[61].

Таблица 44
Список возможных кодов ошибок в разбивке по ответным сообщениям

Код ошибки	*I2*	*I4*	*I6*	*I8*	*I10*	*I12*	*I14*	*I16*	*I18*	*I20*	*E2*	*E4*	*E6*	*E8*	*E10*	*E12*	*E14*
100	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
101	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
102	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
103	X			X	X	X	X				X				X		
104				X											X	X	X
105	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
106	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
151				X											X		
152				X											X		
153				X											X		
154				X											X		
155				X											X		
158				X											X	X	
168				X													
200	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
201	X																
203												X					
204											X						
205												X					
210					X												
211						X											
212							X										
213						X	X										
214					X	X	X		X								
215					X	X	X		X								
216									X								
220					X												
299					X	X	X										
300	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

[61] См. etir.org/error-codes-list.

Код ошибки	*I2*	*I4*	*I6*	*I8*	*I10*	*I12*	*I14*	*I16*	*I18*	*I20*	*E2*	*E4*	*E6*	*E8*	*E10*	*E12*	*E14*
301	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
302	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
303	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
304																	
305				X	X	X	X								X		
306					X	X	X										
320	X			X								X			X	X	X
321	X				X	X	X				X						
322	X	X	X		X	X	X				X		X				
330	X										X		X				
331	X											X					
332	X											X					
400	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

300. В заключение, в нижеследующей таблице указан комплекс рекомендуемых действий для рассмотрения ИТ-специалистами данной информационной системы при получении ответного сообщения с одним или несколькими кодами ошибок.

Таблица 45
Рекомендуемые действия при получении соответствующих кодов ошибок

Код	*Название*	*Рекомендуемые действия*
100	Неверное сообщение	Просьба проверить само сообщение и его формат, так как международной системой оно не распознается. **Просьба связаться со службой поддержки eTIR, направив ей содержание переданного сообщения, временны́е метки и предпринятые шаги с целью воспроизвести эту проблему и решить ее.**
101	Отсутствует параметр	Просьба проверить параметры сообщения, в частности параметры, помеченные в разделе описания сообщения данного документа как обязательные, и убедиться в том, что все обязательные параметры являются частью сообщения.
102	Неверный параметр значения домена	Просьба проверить закодированный параметр, его значения и соответствующие перечни кодов. Убедитесь в том, что каждый закодированный параметр использует одно из значений соответствующего перечня кодов.
103	Неправильный формат даты	Просьба проверить параметры даты и их формат. Убедитесь в том, что каждый формат даты соответствует указанному формату, что значение следует за форматом/шаблоном и что атрибут «formatCode» установлен на правильное значение.
104	Нецелое число	Просьба проверить целочисленность параметров. Убедитесь в том, что каждый целочисленный параметр имеет значение, которое можно без труда представить в виде целого числа.
105	Длина параметра превышена	Просьба проверить длину значений параметров. Убедитесь в том, что длина каждого параметра не превышает максимальную длину, указанную в документации в столбце «Формат».
106	Неверный шаблон	Просьба проверить шаблон значения параметра, так как он не соответствует требованиям, установленным для этого атрибута в сообщении «Определение схемы XML».

Код	*Название*	*Рекомендуемые действия*
151	Несоблюдение условия C001	Просьба проверить параметры, ограниченные условием C001, и убедиться в том, что их значения соответствуют псевдокоду данного условия.
152	Несоблюдение условия C002	Просьба проверить параметры, ограниченные условием C002, и убедиться в том, что их значения соответствуют псевдокоду данного условия.
153	Несоблюдение условия C003	Просьба проверить параметры, ограниченные условием C003, и убедиться в том, что их значения соответствуют псевдокоду данного условия.
154	Несоблюдение условия C004	Просьба проверить параметры, ограниченные условием C004, и убедиться в том, что их значения соответствуют псевдокоду данного условия.
155	Несоблюдение условия C005	Просьба проверить параметры, ограниченные условием C005, и убедиться в том, что их значения соответствуют псевдокоду данного условия.
158	Несоблюдение условия C008	Просьба проверить параметры, ограниченные условием C008, и убедиться в том, что их значения соответствуют псевдокоду данного условия.
168	Несоблюдение правила R008	Просьба проверить параметры, ограниченные правилом R008, и убедиться в том, что их значения соответствуют условиям, установленным данным правилом.
200	Неверное состояние	Просьба проверить состояние указанного объекта (перевозка, гарантия, ...) и убедиться в том, что он соответствует запрашиваемой веб-службе международной системы eTIR.
201	Неприемлемая гарантия	Просьба проверить состояние гарантии, которую вы пытались принять, и убедиться в том, что оно правильное и соответствует рабочему процессу,описанному на диаграмме состояния гарантии.
203	Неотменяемая гарантия	Просьба проверить состояние гарантии, которую вы пытались принять, и убедиться в том, что оно правильное и соответствует рабочему процессу,описанному на диаграмме состояния гарантии.
204	Гарантия уже зарегистрирована	Просьба проверить состояние гарантии, которую вы пытались зарегистрировать, так как она, судя по всему, уже зарегистрирована. Вы можете использовать веб-службу «Запрос гарантии» с целью проверитьее наличие в международной системе eTIR.
205	Гарантия уже отменена	Просьба проверить состояние гарантии, которую вы пытались зарегистрировать, так как она, судя по всему, уже отменена. Вы можете использовать веб-службу «Запрос гарантии» с целью проверить ее наличие в международной системе eTIR.
210	Операция уже началась	Это сообщение пытается начать операцию МДП, которая уже начата. Просьба убедиться в том, что данное сообщение не является повтором ранее отправленного сообщения, и проверить значения, отраженные в его параметрах.
211	Операция ужепрекращена	Это сообщение пытается прекратить операцию МДП, которая уже прекращена. Просьба убедиться в том, что данное сообщение не является повтором ранее отправленного сообщения, и проверить значения, отраженные в его параметрах.
212	Операция уже завершена	Это сообщение пытается завершить операцию МДП, которая уже завершена. Просьба убедиться в том, что данное сообщение не является повтором ранее отправленного сообщения, и проверить значения, отраженные в его параметрах.
213	Операция еще не началась	Это сообщение пытается выполнить операцию МДП, которую необходимо было начать, но которая еще не начата. Просьба убедиться в том, что данное сообщение отправлено в правильном порядке, и проверить значения, отраженные в его параметрах.
214	Идентификатор операции уже зарегистрирован	Просьба проверить идентификатор сообщения и убедиться в том, что он не противоречит другому идентификатору операции.
215	Последовательность операции уже зарегистрирована	Просьба проверить порядковый номер последней операции для данной перевозки и увеличить его.
216	Отказ начать операциюне разрешен.	Отказ начать операцию не может быть принят, если это первая зарегистрированная операция или если гарантия не была принята. Просьба проверить также правильность ваших ссылок на гарантию.

Код	*Название*	*Рекомендуемые действия*
220	Декларация еще не получена	Это сообщение пытается выполнить операцию в тот момент, когда декларация еще не получена. Просьба убедиться в том, что данное сообщение отправлено в правильном порядке, и проверить значения,отраженные в его параметрах.
299	Повторное сообщение	Просьба проверить, отправлено ли уже данное сообщение в эту конечную точку, так как оно уже получено международной системой eTIR.
300	Неверная операция	Просьба проверить содержание сообщения, поскольку оно явилось причиной технической ошибки в международной системе eTIR, которая, однако, не смогла определить источник проблемы.
301	Гарантия не найдена	Просьба проверить значение идентификатора ссылки на гарантию в сообщении и убедиться в том, что оно совпадает со значением, полученным в предыдущих сообщениях.
302	Гарантийная цепьне найдена	Просьба проверить значение идентификатора ссылки на гарантийную цепь в сообщении и убедиться в том, что оно совпадает со значением, полученным в предыдущих сообщениях.
303	Тип гарантии не найден	Просьба проверить значение типа гарантии в сообщении и убедиться в том, что оно относится к кодовому перечню «код типа гарантии (eTIR)» (CL12) и что оно совпадает со значением, полученным в предыдущих сообщениях.
304	Таможня не найдена	Данный код ошибки в спецификациях eTIR v4.3 не используется.
305	Страна не найдена	Просьба проверить значение кода страны в сообщении и убедиться в том, что оно совпадает со значением, полученным в предыдущих сообщениях, и проверить, отражено ли оно в перечне кодов «Код названия стран(ISO 3166-1-alpha-2)» (CL04).
306	Вид контроля не найден	Просьба проверить значение вида контроля в сообщении и убедиться в том, что оно совпадает со значением, полученным в предыдущих сообщениях, и проверить, отражено ли оно в перечне «Код видов контроля (eTIR)»(CL25).
320	Несоответствие информации о держателе/гарантии	Просьба проверить формат и значение держателя книжки МДП в сообщении и убедиться в том, что оно совпадает со значением, полученным в предыдущих сообщениях. Если это так, то необходимо проверить, есть ли такой держатель и его статус, используя либо сообщение «I3 — Получение информации о держателе», специальные веб-службы МБДМДП или веб-приложение МБДМДП.
321	Держатель не уполномочен	Просьба проверить значение держателя книжки МДП в сообщении и убедиться в том, что оно совпадает со значением, полученным в предыдущихсообщениях. Если это так, то необходимо проверить статус держателя, используя либо сообщение «eTIR I3», специальные веб-службы МБДМДП, или веб-приложение МБДМДП.
322	Держатель не найден	Просьба проверить значение держателя книжки МДП в сообщении и убедиться в том, что оно совпадает со значением, полученным в предыдущихсообщениях. Если это так, то необходимо еще раз проверить статус держателя, используя либо сообщение «eTIR I3», специальные веб-службы МБДМДП или веб-приложение МБДМДП.
330	Гарантийная цепьне уполномочена	Просьба проверить значение идентификатора гарантийной цепи в сообщении и убедиться в том, что оно совпадает со значением, полученным в предыдущих сообщениях.
331	Несоответствие информации о гарантийной цепи/гарантии	Просьба проверить значение идентификатора гарантийной цепи в сообщении и убедиться в том, что оно совпадает со значением, полученным в предыдущих сообщениях.
332	Несоответствие информации о типегарантии/гарантии	Просьба проверить значение идентификатора типа гарантии в сообщении и убедиться в том, что оно совпадает со значением, полученным в предыдущих сообщениях.
400	Проблема eTIR	**Просьба связаться со службой поддержки eTIR, направив ей содержание переданного сообщения, временны́е метки и предпринятые шаги с целью воспроизвести эту проблему и решить ее.**

Список таблиц

Список рисунков