Экономический и Социальный Совет

Distr.: General
18 May 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

Безопасность системы eTIR*

Записка секретариата

I. Мандат

1. Комитет по внутреннему транспорту (КВТ) 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 (КВ)[2] (ECE/TRANS/WP.30/2019/9 и ECE/TRANS/WP.30/2019/9/Corr.1) в ожидании утверждения Исполнительным комитетом (Исполкомом) Европейской экономической комиссии (ЕЭК) Организации Объединенных Наций. Исполком на своем дистанционном неофициальном совещании 20 мая 2020 года одобрил учреждение WP.30/GE.1 до 2022 года на основе КВ, содержащегося в документах 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].

* Настоящий документ был представлен для обработки с опозданием, поскольку для получения санкции на его окончательную доработку потребовалось больше времени, чем предполагалось.

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

[2] Круг ведения вновь созданной Группы, утвержденный Комитетом по внутреннему транспорту и Исполнительным комитетом (Исполкомом) ЕЭК ООН, https://unece.org/fileadmin/DAM/trans/bcf/wp30/documents/2019/ECE-TRANS-WP30-2019-09r.pdf и исправление https://unece.org/fileadmin/DAM/trans/bcf/wp30/documents/2019/ECE-TRANS-WP30-2019-09c1r.pdf.

[3] Решение Исполнительного комитета, ECE/EX/2020/L.2, пункт 5 b), http://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.

2. Кругом ведения Группы предусматривается, что Группе следует сосредоточить свои усилия на подготовке новой версии спецификаций eTIR в ожидании официального учреждения Технического органа по осуществлению (ТОО). В частности, по просьбе Рабочей группы по таможенным вопросам, связанным с транспортом (WP.30), Группе следует a) подготовить новый вариант технических спецификаций процедуры eTIR и поправки к ним для обеспечения их соответствия функциональным спецификациям процедуры eTIR; b) подготовить новый вариант функциональных спецификаций процедуры eTIR и поправки к ним для обеспечения их соответствия концептуальным спецификациям процедуры eTIR; c) подготовить поправки к концептуальным спецификациям процедуры eTIR.

3. Настоящим документом охватываются все аспекты обеспечения безопасности системы eTIR, которые найдут отражение в документе с техническими спецификациями eTIR.

II. Безопасность системы eTIR

4. 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.

5. 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.

6. 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

7. 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»[4]. 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.

[4] ST/SGB/2007/6.

8. 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[5]. 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.

2. Задачи безопасности

9. Основу информационной безопасности составляют следующие три главные фундаментальные задачи[6]:

- **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.

10. 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.

Рис. I
Основополагающие задачи информационной безопасности

11. 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.

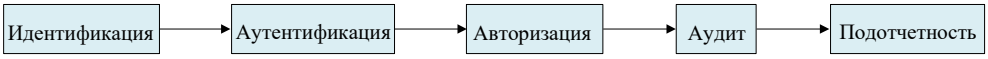
3. Каким образом обеспечивается подотчетность и невозможность отказа

12. Помимо освещения таких аспектов, как целостность, готовность к работе и конфиденциальность, важно разобраться, каким образом субъект[7] аутентифицирует себя в системе и как его/ее действия способны повлечь за собой подотчетность и

[5] Перечень стратегических установок см. на сайте iseek.un.org/nyc/department/policies.
[6] Исчерпывающие определения этих трех терминов приведены в техническом глоссарии.
[7] Под «субъектом» здесь следует понимать человека или информационную систему, который(ая) пытается получить доступ к другой системе.

невозможность отказа. На практике это претворяется посредством пяти последовательных процедур, которые перечислены на следующем рисунке и описаны ниже.

Рис. II
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 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.

13. 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[8]. При выполнении обеих задач, а именно обеспечении подотчетности субъектов и целостности данных, хранящихся в международной системе eTIR, достигается и цель невозможности отказа.

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

4. Принципы безопасности

14. 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.

15. 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.

16. 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[9]. 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.

17. 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[10]. 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.

18. 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[11]. 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.

[9] См. en.wikipedia.org/wiki/Principle_of_least_privilege.
[10] См. en.wikipedia.org/wiki/Defense_in_depth_(computing).
[11] См. en.wikipedia.org/wiki/Separation_of_duties.

B. Требования по безопасности

1. Технические требования, уже упоминавшиеся ранее

19. 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, 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

[12] ECE/TRANS/WP.30/GE.1/2021/31.

потенциальных проблем в рамках международной системы eTIR, способных повлиять на ее готовность к работе;

- большинство требований, касающихся **надежности** (RL.1, RL.2, RL.3, RL5 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.

20. 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.

21. 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

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

Таблица 1
Требование, касающееся аудита

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

23. В нижеследующей таблице перечислены требования, касающиеся процесса аутентификации, ссылка на который дается на рис. II. 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 2
Требования, касающиеся аутентификации

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
AE.1	Выбор для международной системы eTIR надежного механизма аутентификации с	Заинтересованные стороны eTIR, желающие получить доступ к веб-услугам международной системы eTIR, должны

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
	целью предотвращения несанкционированного доступа.	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 аутентификации с целью защиты учетных записей пользователей.	Когда это применимо, учетные записи, назначенные пользователям из числа физических лиц, должны использовать многофакторную аутентификацию, например двухфакторный подход с использованием «того, что пользователь знает» (пароль) и «того, что пользователь имеет» (удостоверение или мобильный телефон).

4. Авторизация

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

Таблица 3
Требования, касающиеся авторизации

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
AO.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.
AO.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.

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
AO.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.
AO.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

25. 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.

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

Таблица 4
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

27. 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 5
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[13] 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 системе eTIR, является ограниченным.	Информация, записанная в трех местах хранения международной системы eTIR (база данных eTIR, документы eTIR и журналы eTIR), ограничена только учетными записями авторизованных пользователей. Эти места хранения расположены в защищенной среде, защищенной физическими и программными средствами контроля безопасности.

7. Идентификация

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

Таблица 6
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).

[13] 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.

8. Целостность

29. 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 7
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

30. 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 8
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.

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
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

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

Таблица 9
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.

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
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

32. 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 10
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 установлены соответствующие системы обнаружения и тушения пожара.

12. Защитное кодирование и безопасность приложений

33. 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 11
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)[14] 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

34. 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.

Таблица 12
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).

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

Идентификатор	*Описание и цель*	*Каким образом выполнить требование*
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

35. 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

36. 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.

37. 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.

38. 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. Правовые аспекты

39. Конвенция о привилегиях и иммунитетах Объединенных Наций[15], 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.

40. 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

41. 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.

42. 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,

[15] См. un.org/en/ethics/assets/pdfs/Convention%20of%20Privileges-Immunities%20of%20the%20UN.pdf.

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.

43. 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

44. 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[16], 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[17], 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[18], хостинговой структуре также отведена важная роль в таких областях, как управление инцидентами, резервное копирование и восстановление, мониторинг, управление системой корректирующих вставок и обновлениями.

45. 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.

46. 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

47. Одна из целей подхода DevOps (также известен под названием DevSecOps) — «добиваться в вопросах безопасности левого уклона», т. е. думать об информационной

[16] ECE/TRANS/WP.30/GE.1/2021/30.
[17] ECE/TRANS/WP.30/GE.1/2021/31.
[18] ECE/TRANS/WP.30/GE.1/2021/33.

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»[19];

- **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/неуспешность проверки сообщений eTIR, использование недействительных цифровых подписей, исключения, сгенерированные системой, производительность обработки сообщений и т. д. Все эти выведенные и

[19] «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.

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[20].

7. Оценки безопасности

48. 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.

49. 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.

50. 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.

[20] 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.