|  |  |
| --- | --- |
| **Бюро стандартизации электросвязи** |  |
|  |  |

Женева, 7 января 2011 года

|  |  |  |
| --- | --- | --- |
| Осн.: | **Циркуляр 158 БСЭ**  COM 17/MEU | – Администрациям Государств – Членов Союза |
| Тел.:  Факс:  Эл. почта: | +41 22 730 5866 +41 22 730 5853  [tsbsg17@itu.int](mailto:tsbsg17@itu.int) | **Копии**:  – Членам Сектора МСЭ-Т  – Ассоциированным членам МСЭ-Т  – Председателю и заместителям председателя 17-й Исследовательской комиссии  – Директору Бюро развития электросвязи  – Директору Бюро радиосвязи |

|  |  |
| --- | --- |
| Предмет: | **Собрание 17-й Исследовательской комиссии, имеющее целью утверждение проектов новых Рекомендаций МСЭ-Т X.1261, X.1500, X.1520 и X.1521 в соответствии с положениями раздела 9 Резолюции 1 ВАСЭ (Йоханнесбург, 2008 г.), Женева**, **20 апреля 2011 года** |

Уважаемая госпожа,  
уважаемый господин,

1 По просьбе председателя 17-й Исследовательской комиссии *(Безопасность)* имею честь сообщить вам, что указанная исследовательская комиссия, собрание которой состоится с 11 по 20 апреля 2011 года, намеревается применить для утверждения вышеупомянутых проектов новых Рекомендацийпроцедуру, описанную в разделе 9 Резолюции 1 ВАСЭ (Йоханнесбург, 2008 г.).

2 Названия, краткое изложение предлагаемых к утверждению проектов новых Рекомендаций МСЭ‑Т и указание на место их размещения содержатся в **Приложении 1**.

3 Просьба ко всем Государствам – Членам МСЭ, Членам Сектора или Ассоциированным членам, располагающим информацией о принадлежащих им или другим сторонам патентах, которые могут полностью либо частично охватывать элементы проектов предлагаемых к утверждению Рекомендаций, сообщить об этом БСЭ в соответствии с общей патентной политикой для МСЭ‑Т/МСЭ‑R/ИСО/МЭК.

Имеющаяся патентная информация доступна в онлайновом режиме на веб-сайте МСЭ-Т ([www.itu.int/ITU-T/ipr/](http://www.itu.int/itu-t/ipr/)).

4 Учитывая положения раздела 9 Резолюции 1, заранее благодарю вас за информацию о том, дает ли ваша администрация 17-й Исследовательской комиссии полномочия рассмотреть на своем собраниипроекты указанных новых Рекомендаций на предмет их утверждения, направленную в мой адрес до 2400 UTC **30 марта 2011 года**.

Если какие-либо Государства-Члены сочтут, что рассматривать Рекомендации на предмет их утверждения не следует, им необходимо сообщить о причинах такого неодобрения и указать, какие возможные изменения могли бы способствовать дальнейшему рассмотрению и утверждению проектов указанных новых Рекомендаций.

5 В случае если 70% или более Государств-Членов в своих ответах выскажутся за рассмотрение на собрании исследовательской комиссии проектов указанных новых Рекомендаций на предмет их утверждения, одно пленарное заседание **20 апреля 2011 года** будет отведено для применения процедуры утверждения.

В связи с этим предлагаю вашей администрации направить на собрание своего представителя. **Администрациям Государств – Членов Союза** предлагается сообщить фамилии глав их делегаций. Если ваша администрация желает быть представленной на собрании признанной эксплуатационной организацией, научной или промышленной организацией либо иным объединением, занимающимся вопросами электросвязи, то в соответствии с п. 239 Статьи 19 Конвенции МСЭ необходимо должным образом сообщить об этом Директору БСЭ.

6 Повестка дня и вся соответствующая информация, касающаяся собрания 17‑й Исследовательской комиссии, будут предоставлены в Коллективном письме 5/17.

7 После собрания Директор БСЭ в Циркулярном письме уведомит о принятом по данным Рекомендациям решении. Эта информация будет также опубликована в Оперативном бюллетене МСЭ.

С уважением,

Малколм Джонсон  
Директор Бюро  
стандартизации электросвязи

**Приложение**: 1

ПРИЛОЖЕНИЕ 1  
(к Циркуляру 158 БСЭ)

Краткое изложение текстов и указание на место их размещения

Проект новой Рекомендации МСЭ-Т X.1500 (X.cybex), Методы обмена информацией по кибербезопасности   
COM 17 – R 25 *(скоро будет размещен на веб-сайте)*

Краткое изложение

В данной Рекомендации излагаются методы обмена информацией по кибербезопасности. Эти методы можно использовать по отдельности или в сочетании, по желанию или в зависимости от ситуации в целях повышения кибербезопасности благодаря обмену четкой, всесторонней, глобальной, своевременной и надежной информацией. Не предполагается каких-либо обязательств по обмену информацией либо средств получения или конечного использования рассматриваемой информации.

Проект новой Рекомендации МСЭ-Т X.1520 (X.cve), Общеизвестные уязвимости и незащищенность (CVE)   
COM 17 – R 26

Краткое изложение

В данной Рекомендации рассматриваются структурно оформленные средства для обмена сведениями об общеизвестных уязвимостях и незащищенности (CVE) в области информационной безопасности, предназначенные для того, чтобы дать одинаковые названия общеизвестным проблемам в коммерческом программном обеспечении или программном обеспечении с открытым исходным кодом, которые используются в сетях связи, устройствах конечных пользователей или же в любых других типах информационно-коммуникационных технологий (ИКТ), где может применяться программное обеспечение. Цель данной Рекомендации состоит в том, чтобы с помощью таких общих наименований облегчить совместное использование данных по отдельным возможностям, касающимся уязвимости (инструментов, депозитариев и услуг). Рекомендация предназначена для того, чтобы позволить увязать вместе базы данных по уязвимостям и другие возможности, а также облегчить сопоставление инструментов и услуг в области безопасности. По существу данная Рекомендация не содержит информации по таким вопросам, как риски, воздействие, установленная информация или подробная техническая информация. В ней содержатся только стандартный идентификационный номер с указанием статуса, краткое описание и ссылки на соответствующие отчеты и информационные материалы по уязвимостям.

Подразумевается, что данная Рекомендация будет иметь всесторонний характер, в том что касается всех общеизвестных уязвимостей и незащищенности. Хотя планируется, что Рекомендация будет содержать проработанную информацию, основное внимание уделяется определению уязвимостей и незащищенности, которые обнаруживаются с помощью средств обеспечения безопасности, и любым новым проблемам, которые становятся общими, а затем рассмотрению любых прежних проблем в области безопасности, которые требуют подтверждения.

Проект новой Рекомендации МСЭ-Т X.1521 (X.cvss), Система оценки общеизвестных уязвимостей (CVSS)  
COM 17 – R 27 *(скоро будет размещен на веб-сайте)*

Краткое изложение

В данной Рекомендации представлена открытая структура для сообщения характеристик и влияния уязвимостей информационно-коммуникационных технологий (ИКТ) в коммерческом программном обеспечении или программном обеспечении с открытым исходным кодом, которые используются в сетях связи, устройствах конечных пользователей или же в любых других типах ИКТ, где может применяться программное обеспечение. В Рекомендации рассматривается система оценки общеизвестных уязвимостей (CVSS), цель которой состоит в том, чтобы дать возможность руководителям в области ИКТ, тем, кто рассылает объявления об уязвимостях, поставщикам услуг в области безопасности, поставщикам различных приложений и исследователям изъясняться на общем языке оценки уязвимостей ИКТ.

Проект новой Рекомендации МСЭ-Т X.1261 (X.EVcert), Система сертификатов с расширенной валидацией (EVcert)  
COM 17 – R 30

Краткое изложение

В данной Рекомендации рассматривается система сертификатов с расширенной валидацией, и она представляет собой всестороннее сочетание технологий, протоколов, проверки подлинности идентичности, управления жизненным циклом и методов контроля, обеспечивающее описание минимальных требований, которые должны выполняться для выдачи и ведения сертификатов с расширенной валидацией ("сертификатов EV"), относящихся к той или иной организации. Затем информация о рассматриваемой организации из действительных "сертификатов EV" может особым образом воспроизводиться некоторыми приложениями программного обеспечения проверяющей стороны (например, программного обеспечения браузера), с тем чтобы предоставить пользователям заслуживающее доверия подтверждение идентичности организации, которая контролирует веб-сайт или другие услуги, за которыми обращаются пользователи. Хотя первоначально расширения этой системы предназначались для использования при создании кабельных каналов передачи данных на базе веб с помощью протоколов обеспечения безопасности транспортного уровня или уровня защищенных гнезд (TLS/SSL), такие расширения предусматриваются для защищенных многоцелевых расширений электронной почты интернета (S/MIME), отметок времени, передачи голоса по протоколу Интернет (VoIP), мгновенного обмена сообщениями (IM), веб-услуг и т. д.

Основные задачи данной Рекомендации состоят в следующем: 1) определение юридического лица, контролирующего веб- или сервис-сайт, и 2) обеспечение возможности зашифрованной связи с этим сайтом. Второстепенные задачи включают существенное увеличение кибербезопасности благодаря помощи в установлении законности организации, которая утверждает о том, что управляет веб‑сайтом, и предоставлению средства, которое может использоваться для содействия в решении проблем, связанных с распространением вредоносных программных средств, фишингом, кражей идентичности и различными формами онлайнового мошенничества.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_