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

Женева, 9 сентября 2011 года

|  |  |  |
| --- | --- | --- |
| Осн.: | **Циркуляр 228 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  – Академическим организациям − 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.1037, X.1500.1, X.1524 и X.1541 в соответствии с положениями раздела 9 Резолюции 1 (Йоханнесбург, 2008 г.) ВАСЭ  Женева, 2 марта 2012 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 20 февраля по 2 марта 2012 года, намеревается применить для утверждения вышеупомянутых проектов новых Рекомендаций процедуру, описанную в разделе 9 Резолюции 1 (Йоханнесбург, 2008 г.) ВАСЭ.

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, Ассоциированным членам или академическим учреждениям, 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 собрании проекты указанных новых Рекомендаций на предмет их утверждения, направленную в мой адрес до **8 февраля 2012 года** 2400 UTC.

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 **2 марта 2012 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 7/17.

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

С уважением,

Малколм Джонсон  
Директор Бюро  
стандартизации электросвязи

**Приложение**: 1

ПРИЛОЖЕНИЕ 1  
(к Циркуляру 228 БСЭ)

Краткое изложение текстов и указание на место их размещения

**Проект новой Рекомендации МСЭ-Т X.1037 (X.rev) − Архитектурные системы мер обеспечения безопасности, предназначенные для предотвращения мошеннических действий в сетях операторов общего пользования  
COM 17 – R 41**

**Краткое изложение**

В Рекомендации МСЭ-T X.1037 описывается методика оценки систем мер обеспечения безопасности, предназначенных для предотвращения мошеннических действий, и критерии отбора этих систем, с учетом современного уровня развития архитектурных характеристик сетей поставщиков услуг связи (ПУС). В Рекомендации содержатся технические методы рассмотрения мер обеспечения безопасности и оценки потерь, вызванных мошенническими действиями, а также приводятся руководящие указания по обмену информацией о мошеннических действиях.

**Проект Рекомендации МСЭ-T X.1500.1 (X.cybex.1) − Процедуры регистрации дуг в рамках дуги идентификатора объекта (OID), используемые для обмена информацией о кибербезопасности  
COM 17 – R 42**

**Краткое изложение**

В настоящей Рекомендации описывается регистрация дуг OID, которые обеспечивают возможность согласованной, однозначной и глобальной идентификации информации о кибербезопасности, а также идентификации организаций, осуществляющих обмен данной информацией и соответствующей политикой. В настоящей Рекомендации определяются информация и подтверждение, которое должно предоставляться при осуществлении запроса OID для целей обмена информацией о кибербезопасности, а также процедуры функционирования регистрационного органа.

**Проект Рекомендации МСЭ-T X.1524 (X.cwe) − Перечень общеизвестных слабых мест (CWE)  
COM 17 – R 43**

**Краткое изложение**

В настоящей Рекомендации по вопросам использования перечня общеизвестных слабых мест (CWE) представлены структурированные средства обмена сведениями о слабых местах в области информационной безопасности, обеспечивающие одинаковые названия для общеизвестных проблем в коммерческом программном обеспечении или программном обеспечении с открытым исходным кодом, которое используется в сетях связи, устройствах конечных пользователей или же в любых других типах информационно-коммуникационных технологий (ИКТ), где может применяться программное обеспечение. Цель CWE состоит в том, чтобы обеспечить более эффективное обсуждение, описание, отбор и использование средств и услуг по защите программного обеспечения, которые могут обнаруживать эти слабые места в кодах источников и операционных системах, а также улучшить понимание слабых мест программного обеспечения, связанных с архитектурой и разработкой, и управление этими слабыми местами. В настоящей Рекомендации определяется применение CWE для предоставления механизма совместного использования средств, услуг, баз данных и других возможностей защиты программного обеспечения, а также для сравнения средств и услуг по его защите. CWE также предоставляет полезную контекстную информацию о возможных рисках, воздействии, исправлении, а также подробную техническую информацию о том, что может значить данное слабое место в программном обеспечении для той или иной системы программного обеспечения. Хранилище идентификаторов CWE и относящейся к ним контекстной информации представлено по адресу: [cwe.mitre.org/data] в виде файла XML или pdf. Версия того же самого контента с веб-интерфейсом представлена по адресу: [http://cwe.mitre.org/data/slices/2000.html]

Перечень CWE, применение которого определено в настоящей Рекомендации, призван обеспечить комплексный охват применительно к архитектуре, разработке, кодированию и ошибкам внедрения программного обеспечения, которые являются основными причинами уязвимости и незащищенности. Хотя планируется, что CWE будет содержать проработанную информацию, основное внимание уделяется определению и описанию этих основных причин уязвимости и незащищенности, а также просветительской работе в их отношении, с тем чтобы разработчики могли их избегать, группы разработчиков могли с ними справляться, а также чтобы о них можно было сообщать в согласованной форме, используя средства и услуги по защите.

**Проект Рекомендации МСЭ-T X.1541 (X.iodef) − Формат обмена описаниями инцидентов как объектов  
COM 17 – R 44**

Краткое изложение

Формат обмена описаниями инцидентов как объектов (IODEF) определяет представление данных, обеспечивающее основу для обмена информацией об инцидентах в сфере компьютерной безопасности, которой обычно обмениваются группы реагирования на инциденты в сфере компьютерной безопасности (CSIRT). В настоящей Рекомендации описывается информационная модель IODEF и приводится соответствующая модель данных, определенная в виде схемы XML.

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