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

Женева, 27 сентября 2012 года

|  |  |  |
| --- | --- | --- |
| Осн.: | **Циркуляр 311 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 c целью утверждения проектов новых Рекомендаций МСЭ-Т X.1126, X.1154, X.1526 и X.1544 в соответствии с положениями раздела 9 Резолюции 1 (Йоханнесбург, 2008 г.) ВАСЭ, Женева, 26 апреля 2013 года** |

Уважаемая госпожа,  
уважаемый господин,

1 По просьбе председателя 17‑й Исследовательской комиссии, *Безопасность*, имею честь сообщить вам о том, что указанная исследовательская комиссия, собрание которой состоится с 17 по 26 апреля 2013 года, собирается применить для утверждения вышеупомянутых проектов новых Рекомендаций процедуру, описанную в разделе 9 Резолюции 1 (Йоханнесбург, 2008 г.) ВАСЭ.

2 Названия, краткое изложение проектов новых Рекомендаций МСЭ‑Т, предлагаемых к утверждению, и указание документа, в котором они размещены, содержатся в **Приложении 1**.

3 Просьба ко всем Государствам – Членам МСЭ, Членам Сектора, Ассоциированным членам или академическим учреждениям, располагающим информацией о принадлежащим им или другим сторонам патентах, которые могут полностью либо частично охватывать элементы проектов Рекомендаций, предлагаемых к утверждению, сообщить об этом БСЭ в соответствии с общей патентной политикой, принятой 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, был бы вам признателен, если бы вы проинформировали меня до 2400 UTC **5 апреля 2013 года** о том, дает ли ваша администрация 17‑й Исследовательской комиссии полномочия рассмотреть на ее собрании проекты этих новых Рекомендаций на предмет их утверждения.

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

5 Если в своих ответах 70% или более Государств-Членов выскажутся за рассмотрение на собрании исследовательской комиссии проектов указанных новых Рекомендаций на предмет их утверждения, то для применения процедуры утверждения будет отведено одно пленарное заседание **26 апреля 2013 года**.

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 она должна надлежащим образом проинформировать об этом Директора БСЭ.

6 Повестка дня и вся соответствующая информация, касающиеся собрания 17‑й Исследовательской комиссии, будут изложены в Коллективном письме, которое будет направлено вам позднее.

7 После собрания Директор БСЭ в Циркулярном письме уведомит вас о решении, принятом в отношении данных Рекомендаций. Эта информация будет также опубликована в Оперативном бюллетене МСЭ.

С уважением,

Малколм Джонсон  
Директор Бюро  
стандартизации электросвязи

**Приложение**: 1

ПРИЛОЖЕНИЕ 1  
(к Циркуляру 311 БСЭ)

Резюме и место размещения текстов

Проект новой Рекомендации МСЭ-T X.1126 (X.msec-6), Аспекты безопасности смартфонов  
COM 17 – R 67

Резюме

По мере постоянного развития функциональных возможностей и расширения приложений смартфоны все чаще подвергаются многочисленным угрозам безопасности, способным создать серьезные социально-экономические проблемы. Рекомендация МСЭ-T X.1126 ставит перед собой цели защитить неприкосновенность частной жизни пользователей и повысить информационную безопасность смартфонов.

В настоящей Рекомендации определяются угрозы в разбивке на уязвимости и атаки. Чтобы удовлетворить этим целям безопасности, в Рекомендации определяется иерархическая структура безопасности и соответствующие требования безопасности, предъявляемые к смартфонам. В отношении структуры безопасности в Рекомендации предлагаются необходимые решения по обеспечению безопасности путем улучшения систем и с помощью средств защиты.

Проект новой Рекомендации МСЭ-T X.1154 (X.sap-4), Общая структура комбинированной аутентификации в средах со многими поставщиками услуг определения идентичности   
COM 17 – R 68

Резюме

В последнее время многие прикладные услуги, особенно финансовые услуги, требуют использования более надежных или комбинированных методов аутентификации, таких как многофакторная аутентификация, в связи с участившимися случаями хищения данных идентичности (ID). Например, вместо традиционной аутентификации на основе пароля используется аутентификация на основе одноразового пароля и другие новые методы аутентификации.

Комбинирование методов аутентификации позволяют многим поставщикам услуг определения идентичности (IdSP) повысить гарантии надежности аутентификации. В Рекомендации МСЭ-T X.1154 представлена общая структура комбинированной аутентификации в средах со многими IdSP для поставщика услуг. В этой Рекомендации рассматриваются три типа комбинированных методов аутентификации: многофакторная аутентификация, многометодная аутентификация и многократные аутентификации.

В Рекомендации содержится также описание моделей, основных операций и требований безопасности для каждой составляющей модели и каждого сообщения между составляющими модели для поддержания общего уровня гарантии аутентификации в условиях комбинации многих IdSP.

Кроме того, в ней описываются модели, основные операции и требования безопасности для обеспечения услуги аутентификации, управляющей комбинацией многих IdSPs.

Проект новой Рекомендации МСЭ-T X.1526 (X.oval), Открытый язык описания уязвимостей и оценки  
COM 17 – R 64

Резюме

Настоящая Рекомендация об использовании открытого языка описания уязвимостей и оценки (OVAL) является общим международным стандартом информационной безопасности, направленным на создание открытых и общедоступных данных безопасности и на стандартизацию передачи этой информации между всеми существующими средствами и услугами безопасности. OVAL включает язык, используемый для кодирования подробных данных о системе, а также ряд репозиториев контента, которые ведутся во всем сообществе. Этот язык стандартизирует три основных этапа процесса оценки: представление информации о конфигурации системы для проверки; анализ системы на наличие определенного машинного состояния (уязвимости, конфигурации, состояния корректировки и т. д.); и представление отчета о результатах данной оценки. Репозитории являются сборниками общедоступного и открытого контента, в котором используется этот язык.

Сообщество OVAL разработало три схемы, написанные в расширяемом языке разметки (XML), которые служат в качестве структуры и словаря языка OVAL. Эти схемы соответствуют трем этапам процесса оценки: схема "характеристики системы OVAL", предназначенная для представления информации о системе, схема "определение OVAL", предназначенная для описания того или иного конкретного машинного состояния, а также схема "результаты OVAL" – для представления сообщений о результатах оценки.

Контент, написанный на языке OVAL, размещается в одном из многочисленных репозиториев сообщества. Один такой репозиторий известен как репозиторий OVAL. Это центральное место для встреч представителей сообщества OVAL, обсуждения, анализа, хранения и распространения определений OVAL. Каждое определение в репозитории OVAL определяет наличие в системе конкретной уязвимости программных средств, задачи конфигурации, программы или корректировки.

Сообщество информационной безопасности содействует разработке OVAL, участвуя в создании языка OVAL на Форуме разработчиков OVAL и в написании определений для репозитория OVAL через Форум сообщества OVAL. Совет OVAL, состоящий из представителей различных предприятий отрасли, академических организаций и правительственных учреждений всего мира, осуществляет контроль за языком OVAL и утверждает его, а также следит за размещением определений на веб‑сайте OVAL. Это значит, что OVAL отражает идеи и совокупные специальные знания самого широкого круга специалистов в области системного администрирования и безопасности в мире.

Проект новой Рекомендации МСЭ-T X.1544 (X.capec), Перечень и классификация общеизвестных схем атак  
COM 17 – R 65

Резюме

Рекомендация, Перечень и классификация общеизвестных схем атак (CAPEC), представляет собой основанную на XML/XSD спецификацию для определения, описания и составления перечня схем атак. Схемы атак являются высокоэффективным средством, позволяющим получать и представлять информацию о подходах, используемых злоумышленником. Эти схемы являются описаниями общеизвестных методов использования программного обеспечения. Они выводятся из схем проектных решений, применяемых деструктивным, а не конструктивным образом, и вырабатываются на основе углубленного анализа конкретных примеров реального вторжения. Цель CAPEC состоит в том, чтобы обеспечить общедоступный каталог схем атак, наряду с комплексной схемой и классификационной таксономией.

CAPEC позволяет:

• стандартизировать получение и описание схем атак;

• собирать известные схемы атак в единый перечень, который может систематически и эффективно использоваться сообществом;

• классифицировать схемы атак таким образом, чтобы пользователи могли легко выявить во всем перечне то подмножество, которое подходит к их условиям;

• с помощью прямых ссылок установить связь между схемами атак и слабыми местами (CWE – перечень общеизвестных слабых мест), в которых такие атаки могут быть эффективными.

Поскольку используется максимально возможное количество источников и примеров от сообщества CAPEC и других заинтересованных сторон, то следует разработать конкретные и краткие определения элементов словаря CAPEC и выработать различные мнения и классификационные древовидные структуры.

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