Международный союз электросвязи

МСЭ-Т X.1520

(04/2011)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

Обмен информацией, касающейся кибербезопасности – Обмен информацией об уязвимости/состоянии

Общеизвестные уязвимости и незащищенность

Рекомендация МСЭ-Т X.1520

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.379
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	**X.1520–X.1539**
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1520

Общеизвестные уязвимости и незащищенность

Резюме

В Рекомендации МСЭ-Т X.1520 об использовании общеизвестных уязвимостях и незащищенности (CVE) предлагается структурированное средство обмена информацией об уязвимостях и незащищенности в области безопасности, обеспечивающее общие названия широко известных проблем в коммерческом программном обеспечении и программном обеспечении с открытым исходным кодом, используемых в сетях связи, устройствах конечного пользователя или иных устройствах на базе любого другого вида информационно-коммуникационных технологий (ИКТ), способных использовать программное обеспечение. Цель настоящей Рекомендации заключается в определении использования CVE, с тем чтобы упростить обмен данными между отдельными средствами идентификации уязвимости (инструментальные средства, репозитарии и услуги), которые имеют такое общее наименование. В настоящей Рекомендации определяется применение CVE для обеспечения механизма, который позволит использовать совместно базы данных, касающиеся уязвимости, и другие средства и упростить сравнение инструментальных средств и услуг обеспечения безопасности. В CVE не содержится информация, касающаяся, например, рисков, влияния, постоянная или подробная техническая информация. В CVE содержится только стандартный номер идентификатора с индикатором состояния, краткое описание и ссылки на соответствующие сообщения об уязвимостях и инструкции. Репозитарий идентификаторов CVE доступен по адресу: [cve.mitre.org/cve/cve.html].

Назначение CVE, использование которых определяется в настоящей Рекомендации, заключается в том, чтобы охватить все широко известные виды уязвимости и незащищенности. Хотя CVE предназначены для включения в них тщательно проработанной информации, основное внимание отводится определению уязвимостей и незащищенности, выявленных средствами обеспечения безопасности, любых новых проблем, ставших известными, а также рассмотрению более ранних проблем безопасности, требующих валидации.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1520	20.04.2011 г.	17-я

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы.

Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

© ITU 2012

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

Содержание

Введение

В настоящей Рекомендации об использовании общеизвестных уязвимостях и незащищенности (CVE) предлагается структурированное средство обмена информацией об уязвимостях и незащищенности в области безопасности, обеспечивающее общие названия широко известных проблем в коммерческом программном обеспечении и программном обеспечении с открытым исходным кодом, используемых в сетях связи, устройствах конечного пользователя или иных устройствах на базе любого другого вида информационно-коммуникационных технологий (ИКТ), способных использовать программное обеспечение. Цель настоящей Рекомендации заключается в определении использования CVE, с тем чтобы упростить обмен данными между отдельными средствами идентификации уязвимости (инструментальные средства, репозитарии и услуги), которые имеют такое общее наименование. В настоящей Рекомендации определяется применение CVE для обеспечения механизма, который позволит использовать совместно базы данных, касающиеся уязвимости, и другие средства и упростить сравнение инструментальных средств и услуг обеспечения безопасности. В CVE не содержится информация, касающаяся, например, рисков, влияния, постоянная или подробная техническая информация. В CVE содержится только стандартный номер идентификатора с индикатором состояния, краткое описание и ссылки на соответствующие сообщения об уязвимостях и инструкции. Репозитарий идентификаторов CVE доступен по адресу: [cve.mitre.org/cve/cve.html].

Назначение CVE, использование которых определяется в настоящей Рекомендации, заключается в том, чтобы охватить все широко известные виды уязвимости и незащищенности. Хотя CVE предназначены для включения в нее тщательно проработанной информации, основное внимание отводится определению уязвимостей и незащищенности, выявленных средствами обеспечения безопасности, любых новых проблем, ставших известными, а также рассмотрению более ранних проблем безопасности, требующих валидации.

Настоящая Рекомендация является одной из класса Рекомендаций МСЭ-Т, вышедшей из широкого, существующего, глобального сообщества развития и пользователей, которое осуществило подготовку и развитие открытой спецификации, представляемой МСЭ-Т для принятия, при том понимании, что любые изменения или обновления этой спецификации будут осуществляться таким образом, чтобы сохранить полную техническую эквивалентность и совместимость, что дискуссии по поводу изменений и улучшений будут осуществляться в рамках процессов с участием того же сообщества пользователей, и включает прямые ссылки на соответствующую конкретную версию, сохраняемую сообществом пользователей.

Рекомендация МСЭ-Т X.1520

Общеизвестные уязвимости и незащищенность

1 Сфера применения

В настоящей Рекомендации об использовании общеизвестных уязвимостях и незащищенности предлагается "структурированное средство" для глобального обмена информацией о широко известных, сложившихся уязвимостях и незащищенности, выявленных средствами защиты, или иным образом ставших известными. Это "структурированное средство" часто называют "средством CVE". Уязвимость информационной безопасности является следствием ошибки в программном обеспечении, которая может быть напрямую использована хакером для получения доступа в систему или сеть. Незащищенность информационной безопасности является следствием ошибки в программном обеспечении, позволяющей получить доступ к информации или возможностям, которые могут быть использованы хакером в качестве средства для проникновения в систему или сеть. Присвоение идентификаторов CVE не входит в сферу применения настоящей Рекомендации.

Настоящая Рекомендация в техническом аспекте эквивалентна и совместима с версией 1.2 "Требований и Рекомендаций в отношении совместимости CVE" от 1 октября 2009 года, размещенных на веб-сайте по адресу: [cve.mitre.org/compatible/requirements.html].

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

Отсутствуют.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 точность в процентах (accuracy percentage): Процент элементов безопасности в анализируемой выборке, указывающих корректные идентификаторы CVE.

3.2.2 средство (capability): Средство защиты, база данных, веб-сайт, инструкция или услуга, выполняющая функцию идентификации уязвимости или незащищенности.

3.2.3 незащищенность (exposure): Незащищенность информационной безопасности – это следствие ошибки в программном обеспечении, позволяющей получить доступ к информации или возможностям, которые могут быть использованы хакером для проникновения в систему или сеть.

3.2.4 отображать/отображение (map/mapping): Описание связей между элементами безопасности в репозитарии и названиями CVE, относящимися к этим элементам.

3.2.5 владелец (owner): Хранитель (реальное физическое лицо или компания), несущий ответственность за данное средство.

3.2.6 репозитарий (repository): Явная или неявная совокупность элементов безопасности, поддерживающая средство, т. е. база данных уязвимостей, архив инструкций, набор сигнатур в системе обнаружения проникновений (IDS) или веб-сайт.

3.2.7 анализ (review): Процесс определения того, является ли какое-либо средство совместимым с CVE.

3.2.8 организация по анализу (review authority): Любая организация, осуществляющая анализ.

ПРИМЕЧАНИЕ. – В настоящее время единственной организацией по анализу является MITRE.

3.2.9 дата анализа (review date): Дата контента о CVE, используемого для определения совместимости с CVE какого-либо средства.

3.2.10 выборка для анализа (review sample): Набор элементов безопасности в репозитарии соответствующего средства, который используется организацией по анализу для определения степени точности.

3.2.11 метод формирования выборки (sampling method): Метод, с помощью которого организация по анализу определяет набор элементов безопасности в выборке для анализа.

3.2.12 размер выборки (sample size): Процент и/или количество элементов безопасности, которые должны быть изучены организацией по анализу.

3.2.13 элемент безопасности (security element): Запись в базе данных, электронное сообщение, инструкция по безопасности, проба оценки, сигнатура и т. д., относящиеся к конкретной уязвимости или незащищенности.

3.2.14 задача (task): Проба инструментального средства, проверка, сигнатура и т. д., выполняющие некоторые действия, в результате которых создается информация о безопасности (т. е. элемент безопасности).

3.2.15 инструментальное средство (tool): Программное приложение или устройство, которое либо изучает хост-компьютер или сеть и вырабатывает информацию, относящуюся к уязвимостям или незащищенности, либо сводит воедино информацию подобного типа, например сканер уязвимости, система обнаружения проникновений, система управления рисками, система управления информацией о безопасности, а также средство или услуга информирования о соответствии.

3.2.16 пользователь (user): Пользователь или потенциальный клиент соответствующего средства.

3.2.17 уязвимость (vulnerability): Любой дефект программного обеспечения, который может быть использован для нарушения целостности системы или содержащейся в этой системы информации (на основе МСЭ-Т X.1500).

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ASCII	American Standard Code for Information Interchange		Американский стандартный код для обмена информацией
CVE	Common Vulnerabilities and Exposures		Общеизвестные уязвимости и незащищенность
GUI	Graphical User Interface		Графический интерфейс пользователя
HTML	HyperText Markup Language		Язык разметки гипертекста
HTTP	HyperText Transfer Protocol		Протокол передачи гипертекста
ICT	Information and Communications Technology	ИКТ	Информационно-коммуникационные технологии
IDS	Intrusion Detection System		Система обнаружения проникновений
PDF	Portable Document Format		Переносимый формат документа
POC	Point Of Contact		Контактное лицо
URL	Uniform Resource Locator		Универсальный указатель ресурса
XML	Extensible Markup Language		Расширяемый язык разметки

5 Условные обозначения

В настоящей Рекомендации сокращение CVE используется как имя существительное.

6 Требования высокого уровня

В следующих далее пунктах определяются понятия, функции и ответственность, связанные с надлежащим использованием идентификаторов CVE для обмена данными между отдельными средствами идентификации уязвимости (инструментальные средства, репозитарии и услуги), с тем чтобы обеспечить возможность совместного использования баз данных, касающихся уязвимости, и других средств, а также упростить сравнение инструментальных средств и услуг обеспечения безопасности.

Необходимые условия

6.1 Владелец средства должен являться действительным юридическим лицом, т. е. организацией или конкретным физическим лицом, имеющим действительный номер телефона, адрес электронной почты и уличный почтовый адрес.

6.2 Средство должно обеспечивать дополнительную ценность или информацию, помимо той, которая обеспечивается самими данными CVE (т. е. название, описание, ссылки и соответствующие даты).

6.3 Владелец средства должен предоставить организации по анализу техническое контактное лицо, которое обладает достаточной квалификацией, для того чтобы отвечать на вопросы, касающиеся отображения и какой-либо относящейся к CVE функциональной возможности средства.

6.4 Средство – в производственной версии – должно быть общедоступным или доступным кругу потребителей.

6.5 Владелец средства должен предоставить организации по анализу заполненную "Форму оценки требований совместимости, относящихся к CVE".

6.6 В отношении средства с репозитарием, владелец средства должен предоставить организации по анализу свободный доступ к репозитарию, для того чтобы эта организация могла убедиться в том, что этот репозитарий удовлетворяет всем установленным требованиям.

6.7 В отношении средства с репозитарием, владелец средства должен предоставить организации по анализу возможность использовать репозитарий, для того чтобы определить любые уязвимости, которые должны быть добавлены к CVE.

6.8 Владелец средства должен согласиться соблюдать все обязательные требования совместимости, относящиеся к CVE, которые включают обязательные требования для данного конкретного типа средства.

Функциональные возможности

6.9 Средство должно предоставлять пользователям возможность определять местоположение элементов безопасности, используя названия CVE ("поиск по названиям CVE").

6.10 Если средство представляет пользователю элементы безопасности, то оно должно позволять ему получить соответствующие названия CVE ("вывод названий CVE").

6.11 В отношении средства с репозитарием, отображение средства должно точно связывать элементы безопасности с соответствующими названиями CVE ("точность отображения").

6.12 Документация, касающаяся средства, должна надлежащим образом описывать CVE, совместимость в отношении CVE, а также порядок использования относящихся к CVE функциональных возможностей в данном средстве ("документация по CVE ").

6.13 Средство должно указывать срок его действия в отношении CVE ("срок использования").

6.14 Средство должно удовлетворять любым дополнительным требованиям, установленным для данного конкретного типа средства, как это предусмотрено в Приложении A.

6.15 Средство должно удовлетворять всем требованиям в отношении среды его распространения, как это предусмотрено в Приложении B.

6.16 От средства не требуется выполнения следующего:

- использования тех же описаний или ссылок, как CVE;
- включения каждого названия CVE в свой репозитарий.

Прочее

6.17 Если средство удовлетворяет не всем применимым требованиям, изложенным выше (6.1−6.16), то владелец средства не должен публично объявлять о том, что оно совместимо с CVE.

7 Точность

Совместимость с CVE облегчает обмен данными только в том случае, если отображение средства является точным. Поэтому средства, совместимые с CVE, должны удовлетворять минимальным требованиям точности, изложенным ниже.

7.1 В отношении средства с репозитарием, репозитарий должен характеризоваться процентом точности на уровне 90 процентов или выше.

7.2 В период анализа владелец средства должен исправить любые ошибки отображения, выявленные организацией по анализу.

7.3 По истечении периода анализа владельцу средства следует исправить ошибки отображения в течение разумного периода времени, начиная с того момента, когда о соответствующей ошибке было сообщено впервые, т. е. в пределах двух (2) версий репозитария или шести (6) месяцев в случае инструментальных средств и трех (3) месяцев в случае онлайновых средств и услуг.

7.4 В отношении средства с репозитарием, владельцу средства следует подготовить и подписать заявление о том, что, по имеющимся у владельца средств сведениям, ошибок в отображении не имеется.

7.5 Если данное средство основывается на другом совместимом с CVE средстве или использует это средство ("исходное" средство) и владельцу средства становится известно о наличии ошибок отображения в исходной средстве, то владелец средства должен сообщить об этих ошибках владельцу исходного средства.

7.6 Точность отображения для архивов инструкций должна достигаться с учетом всех элементов безопасности архивного репозитария после и включая первое использование архивом названия CVE в элементе безопасности.

8 Документация

К документации, предоставляемой вместе со средством, применяются следующие требования.

8.1 Документация должна включать краткое описание CVE и совместимости с CVE, которое может быть основано на дословных частях документов с веб-сайта CVE.

8.2 В документации должно содержаться описание того, как пользователь может найти отдельные элементы безопасности в репозитарии средства, используя названия CVE.

8.3 В документации должно содержаться описание того, как пользователь может получить названия CVE из отдельных элементов в репозитарии средства.

8.4 Если документация включает индекс, то он должен включать ссылки на относящуюся к CVE документацию согласно термину "CVE".

9 Использование данных CVE

Пользователи должны иметь возможность определить, насколько "обновленным" является репозитарий средства в отношении его отображения в CVE. Владельцам средства необходимо указать срок действия отображения, указав при этом дату последнего обновления информации о CVE, а также то, какую часть контента о CVE они используют и откуда они получили этот контент о CVE.

9.1 Каждая новая версия средства должна содержать самую последнюю дату контента о CVE, который был использован при создании или обновлении отображения, с помощью, по крайней мере, одного из следующих механизмов: журналы регистрации изменений, перечни новых свойств, справочные файлы или иные механизмы. Средство является "обновленным" относительно этой даты.

9.2 Каждая новая версия средства должна быть обновленной относительно заявленной даты CVE, т. е. не более трех (3) месяцев до того, как данное средство стало доступно его пользователям. Если средство не удовлетворяет этому требованию, то оно по определению считается "устаревшим".

9.3 Владелец средства должен открыто сообщить, как быстро он собирается обновить репозитарий средства, для того чтобы включить в него новую информацию о CVE.

9.4 Владелец средства должен описать критерии и механизм отбора информации о CVE, которую он включает в свое средство.

9.5 Владелец средства должен описать, откуда он получают новый контент о CVE.

10 Поддержка старого стиля названия CVE

Средство должно функционировать с названиями CVE, независимо от формата представления в нем названий CVE.

10.1 Если пользователь осуществляет поиск, используя символы YYYY-NNNN, то средство должно вернуть элементы безопасности, соответствующие символам CVE-YYYY-NNNN, независимо от того, какое обозначение имеет название CVE как часть своего названия в репозитарии средства – CVE или CAN.

10.2 Если средство содержит название CVE, соответствующие символам CVE-YYYY-NNNN, а пользователь осуществляет поиск, используя старый формат для названия CVE, т. е. CAN-YYYY-NNNN (использовался до изменения схемы наименований CVE, введенной 19 октября 2005 года), то средство должно вернуть ему CVE-YYYY-NNNN.

11 Отзыв совместимости с CVE

11.1 Если организация по анализу проверила и выявила, что средство совместимо с CVE, однако впоследствии обнаружила, что установленные требования не соблюдаются, то она может отозвать свое утверждение.

11.1.1 Организация по анализу должна выявить конкретные требования, которые не соблюдаются.

11.2 Организация по анализу должна определить, являются ли действия или требования владельца средства "намеренно недостоверными".

11.2.1 Организация по анализу может интерпретировать выражение "намеренно недостоверные" по своему усмотрению.

11.3 Если это не рекомендовано двумя членами редакционного совета по CVE, не имеющими конфликта интересов, то организации по анализу не следует рассматривать вопрос об отзыве совместимости с CVE в отношении данного конкретного средства чаще одного раза в шесть (6) месяцев.

Предупреждение и оценка

11.4 Организация по анализу должна предоставить владельцу средства и техническому контактному лицу (POC) предупреждение об отзыве не позднее чем за два (2) месяца до даты планируемого отзыва.

11.4.1 Если организация по анализу сочтет, что действия или требования владельца средства являются намеренно недостоверными, то она может игнорировать период предупреждения.

11.5 Если владелец средства считает, что установленные требования соблюдаются, то он может ответить на предупреждение об отзыве, предоставив конкретные данные, объясняющие, каким образом соответствующее средство удовлетворяет данным требованиям.

11.6 Если в течение периода предупреждения владелец средства вносит изменения в соответствующее средство, для того чтобы оно соответствовало данным требованиям, то организации по анализу следует прекратить действия по отзыву в отношении данного средства.

Отзыв

11.7 Организация по анализу может отложить дату отзыва.

11.8 Организация по анализу должна открыто сообщить о том, что совместимость с CVE в отношении данного средства отозвана.

11.9 Если организация по анализу считает, что действия владельца средства в отношении требований совместимости с CVE являются намеренно недостоверными, то период действия отзыв должен составлять не менее одного года.

11.10 Организация по анализу может открыто сообщить о причинах отзыва.

11.11 Если утверждение отозвано, то владелец средства не должен обращаться с просьбой о проведении нового анализа в течение периода отзыва.

12 Организация по анализу

В отношении любого анализа, проводимого организацией по анализу:

12.1 Организация по анализу должна проанализировать средство в аспекте совместимости с CVE относительно конкретной даты контента о CVE, т. е. даты анализа.

12.2 Организация по анализу должна четко определить дату анализа, которая была использована для определения совместимости для данного средства.

12.3 Организация по анализу должна четко определить версию документа, содержащего требования совместимости с CVE, который был использован для определения совместимости для данного средства.

12.4 Организация по анализу должна определить и опубликовать размер выборки.

12.4.1 Организация по анализу должна использовать выборку размером в 50 элементов плюс 5 процентов репозитария средства, при максимальном размере выборки в 400 элементов.

12.4.2 Организация по анализу может проанализировать каждый элемент в репозитарии средства.

12.5 Организация по анализу должна огласить метод формирования выборки.

12.6 Организация по анализу может использовать выборку для анализа, сформированную на основе не произвольного выбора.

12.7 Организация по анализу должна использовать тот же метод формирования выборки и размер выборки для всех средств, которые оцениваются в рамках того же периода времени.

Приложение A

Специфические для типа требования

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

В силу широкого разнообразия средств, использующих CVE, некоторые типы средств могут характеризоваться уникальными свойствами, требующими особого внимания в отношении совместимости с CVE.

A.1 Средство должно удовлетворять всем дополнительным требованиям, относящимся к данному конкретному типу средства.

A.1.1 Если таким средством является сканер оценки уязвимости, система обнаружения проникновений (IDS) или какой-либо продукт, сводящий воедино результаты оценки одного или нескольких сканеров и IDS, то он должен удовлетворять требованиям, предъявляемым к инструментальным средствам, A.2.1–A.2.8.

A.1.2 Если таким средством является услуга (например, управляемая услуга обнаружения проникновения и реагирования или услуга дистанционного сканирования), то она должна удовлетворять требованиям, предъявляемым к услугам обеспечения безопасности, A.3.1–A.3.5.

A.1.3 Если таким средством является онлайновая база данных уязвимостей или сигнатур, архив на базе веб-сети или сайт обслуживания/исправлений, то он должно удовлетворять требованиям, предъявляемым к онлайновым средствам, A.4.1–A.4.3.

A.1.4 Если таким средством является инструмент агрегирования, подобный программе управления информацией о безопасности, инструментальное средство генерации отчетов о соответствии или услуга, обеспечивающая эти типы агрегирования информации о типах уязвимостях, то она должна удовлетворять требованиям, предъявляемым к средствам агрегирования, A.5.1–A.5.6.

Требования, предъявляемые к инструментальным средствам

A.2.1 Инструментальное средство должно предоставлять пользователю возможность использовать названия CVE для установления местоположения соответствующих задач в данном инструментальном средстве ("поиск по названиям CVE") путем обеспечения, по крайней мере, одной из следующих функций: функция "нахождение" или "поиск", отображение между названиями задачи этого средства и названиями CVE, или же используя какой-либо иной механизм.

A.2.2 В отношении любого отчета, определяющего отдельные элементы безопасности, инструментальное средство должно предоставлять пользователю возможность определить соответствующие названия CVE для этих элементов ("вывод названий CVE") путем выполнения, по крайней мере, одного из следующих действий: включение названий CVE непосредственно в отчет, обеспечение отображения между названиями задачи данного инструментального средства и названиями CVE, или же используя какой-либо иной механизм.

A.2.3 Любые требуемые отчеты или отображения должны удовлетворять требованиям к среде передачи, предусмотренным в Приложении B.

A.2.4 Инструментальному средству или владельцу средства следует предоставить пользователю перечень всех названий CVE, связанных с задачами данного инструментального средства.

A.2.5 Инструментальное средство должно обеспечивать пользователю возможность выбирать набор задач, предоставив ему файл, содержащий перечень названий CVE.

A.2.6 Интерфейс инструментального средства должен предоставлять пользователю возможность просматривать, выбирать и отменять выбор набора задач, используя названия отдельных CVE.

A.2.7 Если инструментальное средство не имеет задачи, связанной с каким-либо названием CVE, указанным пользователем в требованиях к инструментальному средству A.2.5 или A.2.6, то инструментальное средство должно уведомить пользователя о том, что оно не может выполнить соответствующую задачу.

A.2.8 Владелец средства должен обеспечить, чтобы 1) уровень ложных положительных результатов составлял менее 100 процентов, т. е. если инструментальное средство сообщает в своем отчете о каком-либо конкретном элементе безопасности, то этот элемент, по крайней мере, иногда является правильным; и чтобы 2) уровень ложных отрицательных результатов составлял менее 100 процентов, т. е. если происходит какое-либо событие, связанное с каким-либо конкретным элементом безопасности, то инструментальное средство иногда сообщает об этом событии.

Требования, предъявляемые к услугам обеспечения безопасности

Услуги обеспечения безопасности могут использовать в своей работе инструменты, совместимые с CVE, однако они не могут предоставить своим клиентам прямой доступ к этим инструментам. Поэтому для клиентов может быть сложным определение и сравнение возможностей различных услуг. Требования, предъявляемые к услугам обеспечения безопасности, позволяют устранить это потенциальное ограничение.

A.3.1 Услуга обеспечения безопасности должна иметь возможность использовать названия CVE, для того чтобы сообщить пользователю, какие элементы безопасности протестированы или обнаружены данной услугой ("поиск по названиям CVE") путем выполнения одного или нескольких из следующих действий: предоставление пользователю перечня названий CVE, определяющих элементы, протестированные или обнаруженные этой услугой, предоставление пользователю отображения между элементами данной услуги и названиями CVE, реагирование на введенный пользователем перечень названий CVE, определяя какие из названий CVE протестированы или обнаружены этой услугой, или же используя какой-либо иной механизм.

A.3.2 В отношении любого отчета, определяющего отдельные элементы безопасности, данная услуга должна предоставлять пользователю возможность определить соответствующие названия CVE для этих элементов ("вывод названий CVE") путем совершения одного или нескольких из следующих действий: предоставление пользователю возможности включения названий CVE непосредственно в отчет, предоставление пользователю отображения между элементами безопасности и названиями CVE, или же используя какой-либо иной механизм.

A.3.3 Любые требуемые отчеты или отображения, предоставленные услугой, должны удовлетворять требованиям к среде передачи, предусмотренным в Приложении B.

A.3.4 Если данная услуга предоставляет пользователю прямой доступ к продукту, определяющему элементы безопасности, то данный продукт должен быть совместим с CVE.

A.3.5 Владелец средства должен обеспечить, чтобы 1) уровень ложных положительных результатов составлял менее 100 процентов, т. е. если инструментальное средство сообщает в своем отчете о каком-либо конкретном элементе безопасности, то этот элемент, по крайней мере, иногда является правильным; и чтобы 2) уровень ложных отрицательных результатов составлял менее 100 процентов, т. е. если происходит какое-либо событие, связанное с каким-либо конкретным элементом безопасности, то эта услуга иногда сообщает об этом событии.

Требования, предъявляемые к онлайновым средствам

A.4.1 Онлайновое средство должно предоставлять пользователю возможность находить соответствующие элементы безопасности в репозитарии онлайнового средства ("поиск по названиям CVE") путем обеспечения одной из следующих функций: поиск с возвратом названий CVE для соответствующих элементов, отображение, связывающее каждый элемент безопасности с соответствующим(и) названием(ями) CVE, или же используя какой-либо иной механизм.

A.4.1.1 Онлайновое средство должно предоставлять "шаблон" URL, позволяющий компьютерной программе легко создавать ссылку, обеспечивающую доступ к функции поиска, как это указано в п. A.4.1 требований, предъявляемых к онлайновым средствам.

Примеры: `http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY-NNNN`

`http://www.example.com/cve/CVE-YYYY-NNNN.html`.

A.4.1.2 Если шаблон URL предназначен для CGI-программы, то эта программа должна принимать метод HTTP "GET".

A.4.2 В отношении любого отчета, определяющего отдельные элементы безопасности, онлайновое средство должно предоставлять пользователю возможность определить соответствующие названия CVE для этих элементов ("вывод названий CVE") путем выполнения, по крайней мере, одного из следующих действий: предоставление пользователю возможности включения названий CVE непосредственно в отчет, предоставление пользователю отображения между элементами безопасности и названиями CVE, или же используя какой-либо иной механизм.

A.4.3 Если онлайновое средство не предоставляет подробной информации в отношении отдельных элементов безопасности, то это онлайновое средство должно обеспечить отображение, связывающее каждый элемент с соответствующим(и) названием(ями) CVE.

Требования, предъявляемые к средствам агрегирования

A.5.1 Средство агрегирования должно предоставлять пользователю возможность использовать названия CVE для установления местоположения соответствующих элементов в данном средстве ("поиск по названиям CVE") путем обеспечения, по крайней мере, одной из следующих функций: функция "нахождения" или "поиска", отображение между названиями этого средства и названиями CVE или другого механизма по согласованию с организацией по анализу.

A.5.2 В отношении любого отчета, определяющего отдельные элементы безопасности, средство агрегирования должно предоставлять пользователю возможность определить соответствующие названия CVE для этих элементов ("вывод названий CVE") путем выполнения, по крайней мере, одного из следующих действий: включение названий CVE непосредственно в отчет, обеспечение отображения между названиями этого средства и названиями CVE, или же используя какой-либо иной механизм.

A.5.3 Любые требуемые отчеты или отображения должны удовлетворять требованиям к среде передачи, предусмотренным в Приложении B.

A.5.4 Инструментальному средству или владельцу средства следует предоставлять пользователю перечень всех названий CVE, связанных с задачами данного инструментального средства.

A.5.5 Инструментальное средство должно обеспечивать пользователю возможность выбирать набор задач, предоставив ему файл, содержащий перечень названий CVE.

A.5.6 Интерфейс инструментального средства должен предоставлять пользователю возможность просматривать, выбирать и отменять выбор набора задач, используя названия отдельных CVE.

Приложение B

Требования, предъявляемые к среде передачи

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

B.1 В среде распространения, используемой средством, совместимым с CVE, должен использоваться медиаформат, представленный в настоящем Приложении.

B.2 Медиаформат должен удовлетворять конкретным требованиям, предъявляемым к данному формату.

Электронные документы (HTML, текстовый редактор, PDF, ASCII-текст и т. д.)

B.3.1 Документ должен быть составлен в общедоступном формате, для которого имеются считывающие устройства, поддерживающие функцию "нахождения" или "поиска" ("поиск по названию CVE"), например необработанный ASCII-текст, HTML или PDF.

B.3.2 Если в документе содержатся только короткие названия или наименования для отдельных элементов, то он должен содержать перечень названий CVE, связанных с этими элементами ("вывод названий CVE").

B.3.3 Документ должен включать отображение элементов в названия CVE, содержащее перечень соответствующих страниц для каждого элемента.

Графический интерфейс пользователя (GUI)

B.4.1 GUI должен предоставлять пользователю функцию поиска, позволяющую ему вводить названия CVE и получать соответствующие элементы ("поиск по названиям CVE").

B.4.2 Если GUI предоставляет подробную информацию по какому-либо отдельному элементу, то он должен предоставлять название (или названия) CVE, отображаемые в данный элемент ("вывод названий CVE"). Иначе, GUI должен предоставлять пользователю отображение в формате, удовлетворяющем требованию B.3.1, предъявляемому к электронным документам.

B.4.3 GUI должен предоставлять пользователю возможность экспортировать данные, относящиеся к CVE, или получать доступ к этим данным в альтернативном формате, удовлетворяющем требованию B.3.1, предъявляемому к электронным документам.

Приложение C

Требования, предъявляемые к среде передачи

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Схема CVE XML, включенная в настоящее Приложение, доступна по адресу: http://cve.mitre.org/schema/cve/cve_1.0.xsd и воспроизводится ниже.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns="http://cve.mitre.org/cve/downloads/1.0"
    targetNamespace="http://cve.mitre.org/cve/downloads/1.0"
    elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0">

  <!--  ********************************************************************** -->
  <!--  Changelog: 1.0 - Initial version -->
  <!--  ********************************************************************** -->
  <xsd:annotation>
    <xsd:documentation xml:lang="en">
      Simple schema that defines the format of the CVE List provided by MITRE
    </xsd:documentation>
  </xsd:annotation>

  <!--  ********************************************************************** -->
  <!--  Start Item Element Definition -->
  <!--  ********************************************************************** -->
  <xsd:element name="cve">
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        cve is the top level element of the CVE List provided by MITRE.
        It represents holds all CVE Items.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="item" type="ItemType" minOccurs="1" maxOccurs="unbounded"/>
      </xsd:sequence>
      <xsd:attribute name="schemaVersion" type="xsd:token" use="optional"/>
    </xsd:complexType>
  </xsd:element>

  <!--  ********************************************************************** -->
  <!--  Simple Types -->
  <!--  ********************************************************************** -->
  <!-- CUSTOM TYPE DEFINITIONS-->
  <xsd:simpleType name="typeEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="CAN"/>
      <xsd:enumeration value="CVE"/>
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="statusEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="Entry"/>
      <xsd:enumeration value="Candidate"/>
    </xsd:restriction>
  </xsd:simpleType>

  <!-- need to verify enumeration -->
  <xsd:simpleType name="simplePhaseEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="Proposed"/>
      <xsd:enumeration value="Interim"/>
      <xsd:enumeration value="Modified"/>
      <xsd:enumeration value="Assigned"/>
```

```
  </xsd:restriction>
</xsd:simpleType>

<!--  ********************************************************************** -->
<!--  Complex Types -->
<!--  ********************************************************************** -->
<xsd:complexType name="ItemType">
  <xsd:sequence>
    <xsd:element name="status" type="statusEnumType" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="phase" type="specificPhaseType" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="desc" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="refs" type="refsType" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="votes" type="votesType" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="comments" type="commentsType" minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
  <!--Need to Verify Enumeration-->
  <xsd:attribute name="type" type="typeEnumType" use="required"/>
  <xsd:attribute name="name" type="xsd:token" use="required"/>
  <xsd:attribute name="seq" type="xsd:token" use="required"/>
</xsd:complexType>

<xsd:complexType name="commentsType">
  <xsd:sequence>
    <xsd:element name="comment" minOccurs="0" maxOccurs="unbounded">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="voter" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="votesType">
  <xsd:sequence>
    <xsd:element name="accept" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="modify" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="noop" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="recast" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
```

```
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="reject" minOccurs="0" maxOccurs="1">
        <xsd:complexType>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="count" type="xsd:token" use="required"/>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="reviewing" minOccurs="0" maxOccurs="1">
        <xsd:complexType>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="count" type="xsd:token" use="required"/>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="revote" minOccurs="0" maxOccurs="1">
        <xsd:complexType>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="count" type="xsd:token" use="required"/>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
    </xsd:sequence>
  </xsd:complexType>


  <xsd:complexType name="specificPhaseType">
    <xsd:simpleContent>
      <xsd:extension base="simplePhaseEnumType">
        <xsd:attribute name="date" type="xsd:token" use="optional"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>

  <xsd:complexType name="refsType">
    <xsd:annotation>
      <xsd:documentation>holds all hyperlink elements</xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
      <xsd:element name="ref" type="refType" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="refType">
    <xsd:annotation>
      <xsd:documentation>Holds individual hyperlink element</xsd:documentation>
    </xsd:annotation>
    <xsd:simpleContent>
      <xsd:extension base="xsd:string">
        <xsd:attribute name="source" type="xsd:token" use="required"/>
        <xsd:attribute name="url" type="xsd:anyURI" use="optional"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>

</xsd:schema>
```

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2012 г.