

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1526

(01/2014)

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

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

**Язык для открытого определения
уязвимостей и оценки состояния системы**

Рекомендация МСЭ-Т X.1526

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.399
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
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

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

Рекомендация МСЭ-Т X.1526

Язык для открытого определения уязвимостей и оценки состояния системы

Резюме

Рекомендация МСЭ-Т X.1526 о языке для открытого определения уязвимостей и оценки состояния системы (называемом также открытым языком описания уязвимостей и оценки, OVAL) включает три основных этапа процесса оценки: представление информации о конфигурации конечных точек для тестирования, анализ конечной точки на наличие определенного машинного состояния (уязвимость, конфигурация, состояние исправления и т. д.), и представление отчета о результатах этой оценки. Назначение OVAL заключается в обеспечении международного общего стандарта информационной безопасности для содействия созданию открытого и общедоступного контента безопасности и для стандартизации передачи этой информации между всеми существующими средствами и услугами безопасности. OVAL – это язык, используемый для кодирования подробных данных конечных точек, и также информация о репозиториях контента, которые ведутся во всем сообществе.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1526	26.04.2013 г.	17-я	11.1002/1000/11752
2.0	МСЭ-Т X.1526	24.01.2014 г.	17-я	11.1002/1000/12039

* Для доступа к Рекомендации наберите в адресном поле вашего веб-навигатора URL <http://handle.itu.int/>, после которого укажите уникальный идентификатор Рекомендации. Например:
<http://handle.itu.int/11.1002/1000/11830-en>.

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 извещения 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/>.

© МСЭ 2014

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

	Стр.
1 Сфера применения	1
2 Справочные документы	1
3 Определения	1
3.1 Термины, определенные в других документах	1
3.2 Термины, определенные в настоящей Рекомендации	1
4 Сокращения и акронимы	2
5 Соглашения по терминологии	2
6 Требования высокого уровня	3
7 Правильность	4
8 Документация	4
9 Действительность	4
10 Конкретные требования к функциональным возможностям	4
11 Требования к органу по проведению анализа	7
12 Отзыв	8
Библиография	9

Введение

В Рекомендации МСЭ-Т X.1526 описывается использование языка для открытого определения уязвимостей и оценки состояния системы (называемого также открытым языком описания уязвимостей и оценки, OVAL), который является международным общим стандартом информационной безопасности для содействия созданию открытого и общедоступного контента безопасности и для стандартизации передачи этой информации между всеми существующими средствами и услугами безопасности. OVAL включает язык, используемый для кодирования подробных данных о конечных точках, а также информацию о репозиториях контента, которые ведутся во всем сообществе. Этот язык стандартизует три основных этапа процесса оценки: представление информации о конфигурации конечных точек для тестирования, анализ конечной точки на наличие определенного машинного состояния (уязвимость, конфигурация, состояние исправления и т. д.) и представление отчета о результатах этой оценки. Репозитории являются сборниками общедоступного и открытого контента, в котором используется данный язык.

Сообщество OVAL разработало три схемы, написанные на 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 какого-либо конкретного машинного состояния, и схема "Результаты OVAL", предназначенная для представления отчетов о результатах оценки.

Контент, написанный на языке OVAL, размещается в одном из многочисленных репозиториях сообщества. Один такой репозиторий называется репозиторием OVAL. Это – центральное место встречи сообщества OVAL для обсуждения, анализа, хранения и распространения Определений OVAL. Каждое определение в репозитории OVAL указывает, имеется ли в конечной точке конкретная уязвимость программных средств, выпуск конфигурации, программа или исправление.

Сообщество информационной безопасности содействует разработке OVAL, участвуя в создании языка OVAL на Форуме разработчиков OVAL и составляя определения для репозитория OVAL через Форум сообщества OVAL. Совет OVAL, состоящий из представителей различных предприятий отрасли, академических организаций и государственных 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 со всего мира. Рекомендация МСЭ-Т X.1526 разработана с учетом важности поддержания, в максимальной возможной степени, технической совместимости Рекомендации МСЭ-Т X.1526 и [b-MITRE Adoption].

Язык для открытого определения уязвимостей и оценки состояния системы

1 Сфера применения

Рекомендация МСЭ-Т X.1526 предоставляет структурированное средство для глобального обмена общедоступным контентом безопасности и для стандартизации передачи этой информации между всеми существующими средствами и услугами безопасности. Язык для открытого определения уязвимостей и оценки состояния системы (называемый также открытым языком описания уязвимостей и оценки (OVAL)), включает язык, используемый для кодирования подробных данных о конечных точках, и также информацию о репозиториях контента, которые ведутся во всем сообществе.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ISO/IEC 19757-3] ISO/IEC 19757-3:2006, *Information technology – Document Schema Definition Language (DSDL) – Part 3: Rule-based validation – Schematron*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 орган по проведению анализа (review authority) [b-ITU-T X.1520]: Любая структура, выполняющая анализ.

ПРИМЕЧАНИЕ. – В настоящее время единственным органом по проведению анализа является MITRE.

3.1.2 пользователь (user) [b-ITU-T X.1520]: Потребитель или потенциальный потребитель функциональной возможности.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 средство авторской разработки (authoring tool): Продукт, помогающий в процессе создания новых файлов открытого языка описания уязвимостей и оценки (OVAL) (включая продукты, сводящие существующие Определения OVAL в единый файл).

3.2.2 метод оценки (assessment method): Конкретный метод, который используется продуктом или услугой для оценки определения открытого языка описания уязвимостей и оценки (OVAL). OVAL поддерживает оценку с помощью:

- 1) запроса к базе данных о настройках текущей конфигурации конечной точки;
- 2) оценки состояния датчиком, расположенным в хост-узле; или
- 3) оценки состояния датчиком дистанционного сканирования.

3.2.3 функциональная возможность (capability): Конкретная функция или функции продукта, услуги или репозитория.

3.2.4 тестирование на правильность (correctness testing): Процесс определения, правильно ли продукт, услуга или репозиторий приняли открытый язык описания уязвимостей и оценки (OVAL).

3.2.5 блок оценки определения (definition evaluator): Продукт, который использует определение открытого языка описания уязвимостей и оценки (OVAL), для того чтобы направлять ход оценки, и который производит Результаты OVAL (полные результаты) в качестве выходных данных.

3.2.6 репозиторий определений (definition repository): Репозиторий Определений открытого языка описания уязвимостей и оценки (OVAL), доступных для сообщества (бесплатно или за плату).

3.2.7 конечная точка (endpoint) (на основе определения, приведенного в [b-IETF RFC 5209]): Любое вычислительное устройство, которое может быть подключено к сети, например компьютерная система, сервер, сетевое устройство, мобильное устройство и т. д. "Таким устройствам до присоединения к сети, как правило, соответствует какой-либо конкретный адрес уровня канала передачи, а после присоединения к сети, возможно, какой-либо IP-адрес".

3.2.8 владелец (owner) (на основе определения, приведенного в [b-ITU-T X.1520]): Хранитель (реальное физическое лицо или компания), несущий ответственность за данную функциональную возможность (определенную в настоящей Рекомендации).

3.2.9 продукт (product): Приложение, устройство безопасности или база данных по безопасности, имеющие одну и более функциональных возможностей.

3.2.10 репозиторий (repository) (на основе определения, приведенного в [b-ITU-T X.1520]): Явная или неявная совокупность элементов безопасности, обеспечивающая функциональную возможность (определенную в настоящей Рекомендации), например база данных уязвимостей, архив инструкций, набор сигнатур в системе обнаружения проникновений (IDS) или веб-сайт.

3.2.11 потребитель результатов (results consumer): Продукт, который принимает результаты открытого языка описания уязвимостей и оценки (OVAL) в качестве входных данных и который либо отображает эти результаты пользователю, либо использует их для совершения некоторых действий (например, восстановление, управление информацией о безопасности (SIM)).

3.2.12 производитель характеристик системы (system characteristics producer): Продукт, генерирующий действительный документ, который содержит характеристики системы открытого языка описания уязвимостей и оценки (OVAL) на основе данных системы.

3.2.13 результаты теста (test results): Данные об итогах тестирования на правильность.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

CCE	Common Configuration Enumeration	Перечень общеизвестных конфигураций
CPE	Common Platform Enumeration	Перечень общеизвестных платформ
CVE	Common Vulnerabilities and Exposures	Общеизвестные уязвимости и незащищенность
ID	Identifier	Идентификатор
IDS	Intrusion Detection System	Система обнаружения проникновений
OVAL	Open Vulnerability and Assessment Language	Открытый язык описания уязвимостей и оценки
SIM	Security Information Management	Управление информацией о безопасности
XML	Extensible Markup Language	Расширяемый язык разметки

5 Соглашения по терминологии

В настоящей Рекомендации такие ключевые слова, как "требуемый" ("required"), "должен" ("shall"), "не должен" ("shall not"), "следует" ("should"), "не следует" ("should not"), "рекомендуемый" ("recommended"), "может" ("may") и "не обязательный" ("optional") толкуются в соответствии с "Руководством для авторов" МСЭ-Т.

6 Требования высокого уровня

Следующие элементы определяют понятия, роли и ответственности, связанные с пятью различными функциональными возможностями, ориентированными на какое-либо отличное использование языка OVAL, которые составляют надлежащее использование языка OVAL. Эти функциональные возможности позволяют каждому члену сообщества OVAL легко понять, как данный продукт использует язык OVAL и как он может удовлетворить их потребности.

Следующие требования относятся ко всем функциональным возможностям, реализующим обеспечение OVAL, независимо от конкретной функциональной возможности, которую планируется реализовать. Если продукт, услуга или репозиторий удовлетворяет всем применимым требованиям, то владелец соответствующей функциональной возможности получит официальное подтверждение правильности принятия OVAL.

Необходимые условия

6.1 Владелец функциональной возможности должен быть действительным юридическим лицом, т. е. организацией или отдельным лицом, имеющим действительный номер телефона, адрес электронной почты и почтовый адрес.

6.2 Владелец функциональной возможности должен согласиться соблюдать все обязательные требования принятия OVAL, которые включают обязательные требования для данной конкретной функциональной возможности.

6.3 Владелец функциональной возможности должен предоставить органу по проведению анализа техническое лицо для контактов, обладающее достаточной квалификацией, для того чтобы отвечать на вопросы, касающиеся любого функционального назначения продукта, услуги или репозитория, относящихся к OVAL, и координировать подготовку продукта, услуги или репозитория для тестирования на правильность.

6.4 Владелец функциональной возможности должен предоставить органу по проведению анализа заполненную "Форму вопросника по принятию OVAL". Эта форма направляется после удовлетворительного завершения процесса заявления. Более подробную информацию см. в разделе "Как заявить ваш продукт, репозиторий или услугу как принявшие OVAL" по адресу: <http://oval.mitre.org/adoption/requirements.html>.

6.5 Владелец функциональной возможности должен предоставить органу по проведению анализа свободный доступ к элементам, необходимым для тестирования на правильность, в том числе к результатам тестирования и/или репозиторию, для того чтобы определить их соответствие всем установленным требованиям.

6.6 Владелец функциональной возможности должен сотрудничать с органом по проведению анализа для обеспечения ему доступа к соответствующему продукту, репозиторию или услуге в целях тестирования на правильность.

6.7 В качестве одного из условий получения официального подтверждения правильности принятия OVAL владелец функциональной возможности должен согласиться оказывать поддержку органу по проведению анализа в осуществлении им тестирования, во время которого будет произведен обмен файлами соответствующих типов с другими организациями, пытающимися доказать правильность их продукта, услуги или репозитория. Управлять этим процессом будет орган по проведению анализа, что потребует разумных усилий со стороны всех участвующих сторон.

6.8 Соответствующий продукт должен нести в себе дополнительную ценность или информацию, сверх той, которая содержится в самом OVAL. Поэтому направление на единственный источник Определений OVAL, созданный еще кем-либо, или предоставление ссылок на него само по себе не считается достаточным для официального подтверждения правильности принятия OVAL.

6.9 Продукт, услуга или репозиторий должны быть доступны для населения или группы потребителей.

6.10 Продукт, услуга или репозиторий должны четко указывать схему(ы) и версию, с которой они совместимы.

Разное

6.11 Если соответствующая функциональная возможность удовлетворяет не всем применимым требованиям, перечисленным выше (пп. 6.1–6.10), то владелец этой функциональной возможности не должен открыто сообщать о том, что в ней принят OVAL.

7 Правильность

Принятие OVAL лишь упрощает функциональную совместимость, если использование OVAL соответствующей функциональной возможностью является правильным. Поэтому функциональные возможности принявших OVAL, должны отвечать минимальным требованиям к правильности, описание которых приводится ниже.

7.1 Владелец функциональной возможности должен располагать средствами, позволяющими пользователю представить ошибки правильности, выявленные им при использовании OVAL, а также в любом контенте OVAL, производимом продуктом, услугой или репозиторием.

7.2 Владелец функциональной возможности должен иметь план по устранению любых ошибок правильности, о которых ему было сообщено.

7.3 Владелец функциональной возможности должен устранять любые ошибки правильности, о которых ему было сообщено, в пределах разумного периода времени после первого сообщения о данной ошибке.

8 Документация

К документации, предоставляемой вместе с продуктом, услугой или репозиторием лица, принявшего OVAL, применяются следующие требования.

8.1 Документация на продукт должна включать краткое описание OVAL и принятия OVAL, которое может включать дословно цитируемые части документов с веб-сайта OVAL.

8.2 В документации на продукт должны быть четко указаны любые схемы компонентов или отдельные тесты, которые он не поддерживает. Например, если какой-либо продукт применяется для официального подтверждения правильности принятия OVAL как блок оценки определения и этот продукт не поддерживает тестирования конкретной функции серийного продукта, то в документации на продукт, услугу или репозиторий должна быть указана эта функциональная несовместимость.

8.4 В документации на продукт, услугу или репозиторий должна быть четко указана процедура, которой должен придерживаться пользователь при представлении ошибок правильности, выявленных им в любом контенте OVAL, производимом этим продуктом.

8.5 Если документация, относящаяся к продукту, услуге или репозиторию, включает индекс, то она должна включать ссылки на документацию, связанную с OVAL, под термином "OVAL".

9 Действительность

Лица, принимающие OVAL, должны работать с действительными документами. Это помогает обеспечить правильное форматирование информации и соответствие структуры документа языку OVAL.

9.1 Продукт, услуга или репозиторий должны проверять весь контент OVAL (как произведенный, так и потребленный), используя валидацию на основе схемы XML консорциума W3C, на соответствие версии языка OVAL, с которой заявлена совместимость.

9.2 Продукт, услуга или репозиторий должны сообщать пользователю о любых ошибках, выявленных при проверке на базе схемы XML консорциума W3C.

9.3 Продукт, услуга или репозиторий должны быть проверены на соответствие всему контенту OVAL (как произведенному, так и потребленному), используя проверку на базе языка Schematron на его соответствие версии языка OVAL, которой, как было заявлено, он соответствует.

9.4 Продукт, услуга или репозиторий должны сообщать пользователю о любых ошибках валидации на базе языка Schematron.

10 Конкретные требования к функциональным возможностям

Следующие требования относятся к конкретным функциональным возможностям принятия и применяются только к продуктам, услугам или репозиториям, в отношении которых добиваются получения официального подтверждения правильности принятия OVAL для данной конкретной функциональной возможности.

Средство авторской разработки	Продукт, помогающий в процессе создания новых файлов OVAL (включая продукты, сводящие существующие Определения OVAL в единый файл).
Блок оценки Определения	Продукт, который использует Определение OVAL, для того чтобы направлять ход оценки, и который производит Результаты OVAL (полные результаты) в качестве выходных данных.
Репозиторий Определений	Репозиторий Определений OVAL, доступных для сообщества (бесплатно или за плату).
Потребитель Результаты	Продукт, который принимает Результаты OVAL в качестве входных данных и который либо отображает эти результаты пользователю, либо использует их для совершения некоторых действий (восстановление, управление информацией о безопасности (SIM) и т. д.).
Производитель характеристик системы	Продукт, генерирующий действительный документ, который содержит характеристики системы OVAL на основе данных системы.

Производитель характеристик системы

Данные требования применяются ко всем продуктам или услугам, предназначенным для генерирования информации о конкретной машине в формате схемы характеристик системы OVAL.

10.1 Продукт или услуга должны использовать уникальный идентификатор (ID) элемента (уникальный в рамках файла) для каждого конкретного элемента характеристик системы, которые они собирают.

10.2 Продукт или услуга должны генерировать элементы характеристик системы, содержащие точные значения конфигурации системы, собранные в то время, когда этот продукт или услуга были применены к конечной точке.

10.3 Продукт или услуга, использующие документ Определений OVAL, для того чтобы генерировать элементы характеристик системы, должны включать раздел collected_objects с объектом характеристик системы для каждого объекта, собранного во входном документе Определений OVAL.

Репозиторий определений

Данные требования применяются ко всем репозиториям, предназначенным для сбора информации в формате схемы Определения OVAL.

10.4 Все Определения, Тесты, Объекты, Состояния и Переменные OVAL должны содержать уникальный ID по отношению ко всем другим Определениям, Тестам, Объектам, Состояниям и Переменным OVAL в сообществе OVAL.

10.5 Каждый репозиторий должен использовать свою собственную часть уникального постоянного пространства имен идентификатора во всем контенте OVAL.

10.6 Все Определения, Тесты, Объекты, Состояния и Переменные OVAL должны сохранять тот же ID на протяжении всего периода своего существования. Это позволяет пользователям обращаться к этим элементам на основе постоянного ID. Существующий элемент не должен переписываться для какой-либо другой цели, поскольку пользователь может обращаться к нему в своем собственном контенте.

10.7 Каждое обновление или изменение Определения, Теста, Объекта, Состояния или Переменной OVAL в репозитории должно иметь результатом прирост номера версии соответствующего элемента. Точно также каждый элемент, обращающийся к обновленному или измененному элементу, тоже должен приращивать свою версию. Такое каскадирование обновлений версий элементов, на которые делается ссылка, не требуется за пределами Определений OVAL, на которые делается ссылка, поскольку Определения OVAL образуют логический блок.

10.8 Метаданные Определения OVAL должны соответствовать контенту Определения OVAL (например, затронутым семейством не должно быть семейство "platform A", если при тестировании рассматривается семейство "platform white"). Кроме того, метаданные должны отражать весь контент Определения OVAL, что означает тот факт, что если Определение OVAL будет применяться более чем к одному семейству, для каждого затронутого семейства могут потребоваться разделы метаданных.

10.9 Репозиторий, который содержит Определение OVAL для охвата конкретной уязвимости, должен включать, по мере доступности, в качестве ссылки название общеизвестных уязвимостей и незащищенностей (CVE).

10.10 Репозиторий, который содержит Определение OVAL для проверки состояния конкретной конфигурации, должен включать, по мере доступности, в качестве ссылки ID перечня общеизвестных конфигураций (CCE).

10.11 Репозиторий, который содержит Определение OVAL для проверки конкретной платформы, должен включать, по мере доступности, в качестве ссылки название перечня общеизвестных платформ (CPE).

10.12 Владелец функциональной возможности должен документально оформить процесс, с помощью которого пользователь может извлечь обновления контента.

Средство авторской разработки

Данные требования применяются ко всем продуктам или услугам, предназначенным для оказания помощи в создании или изменении контента OVAL.

10.13 Средство авторской разработки должно обеспечивать поисковый интерфейс, который дает пользователю возможность поиска Определений, Тестов, Объектов, Состояний и Переменных OVAL по ID.

10.14 Средство авторской разработки должно побуждать повторное использование существующих Определений, Тестов, Объектов, Состояний и Переменных OVAL.

10.15 Средство авторской разработки должно обеспечивать пользователю возможность инициирования валидации в документе, написанном для языка OVAL, и сообщать ему обо всех ошибках, выявленных с использованием схемы XML W3C и языка Schematron.

10.16 Средство авторской разработки должно обеспечивать пользователю возможность импортировать и редактировать существующий контент OVAL.

10.17 Средство авторской разработки должно обеспечивать пользователю возможность экспортировать контент, созданный этим средством, в качестве действительных документов языка OVAL.

10.18 Средство авторской разработки должно сообщать пользователю о дублированном контенте.

10.19 Средство авторской разработки должно обеспечивать ценность и возможности, превышающие возможности редактора XML.

Блок оценки определения

Данные требования применяются ко всем продуктам или услугам, предназначенным для оценки конкретной конечной точки, используя в качестве входных данных информацию, предоставленную в формате схемы Определений OVAL. После того, как оценка завершена, ее результаты должны быть доступны в формате схемы Результатов OVAL.

10.20 Пользователь должен иметь возможность определить, какие Определения OVAL оцениваются.

10.21 Пользователь должен иметь возможность изучить детали каждого оцениваемого Определения OVAL. Это требование обеспечивает открытость Определений OVAL для пользователя, что позволяет ему видеть, как проходит тестирование конкретного выпуска.

10.22 Если продукт или услуга во время работы не использует Определения OVAL, то владелец функциональной возможности должен документально оформить процесс, с помощью которого пользователь может представить Определения OVAL этому владельцу функциональной возможности для интерпретации данным продуктом. Это включает указание того, насколько быстро определения, представленные владельцу функциональной возможности, станут доступными для данного продукта.

10.23 Продукты и услуги должны быть способны интерпретировать всю логику в пределах каждого Определения OVAL и последующих Тестов OVAL в соответствии с заявленными логическими операторами.

10.24 Продукты и услуги должны определить результат оценки целевой конечной точки на основе подробных данных, указанных в Определении OVAL.

10.25 Пользователь должен иметь возможность определить результат всех Определений OVAL, использованных при оценке целевой конечной точки.

10.26 Продукты и услуги должны генерировать точные, предсказуемые и повторяющиеся результаты при использовании конкретного набора Определений OVAL и информации о состоянии конечной точки.

10.27 Результаты, генерированные продуктами или услугами, должны быть доступны в полном формате Результатов OVAL. Это позволяет другим продуктам или услугам, желающим использовать подробную информацию оценки, получать эту информацию по желанию. Неполные результаты также могут быть доступны, однако требуются полные результаты.

10.28 Если Определение OVAL оценивается в одной конечной точке более одного раза и всякий раз выявляются разные значения для переменных, то файл с Результатами OVAL должен включать единственные значения переменных экземпляра для каждого отдельного случая.

10.29 Продукты и услуги должны использовать результат "не оценен" для всех Определений OVAL, являющихся частью исходного файла Определений OVAL, однако этот результат не сообщается. Это удовлетворяет требованию п. 10.25 для данного Определения OVAL.

10.30 Любое использование или перевод Определения OVAL на внутренний язык соответствующего продукта или услуги должен отражать ту же логику, что и первичное Определение OVAL.

Потребитель результатов

Данные требования применяются ко всем продуктам или услугам, предназначенным для использования информации в формате схемы Результатов OVAL.

10.31 Для каждой конечной точки, определенной в используемом файле Результатов OVAL, пользователь должен иметь возможность определить конкретные Определения OVAL, по которым сообщается информация.

10.32 Пользователь должен иметь возможность изучить подробные данные используемого файла Результатов OVAL. Этот процесс должен быть таким же простым, как и процедура открытия пользователем файла XML. Суть этого требования заключается в обеспечении того, чтобы используемые Результаты OVAL были открыты для пользователя, что позволит ему изучать сообщаемые данные.

10.33 Если продукт или услуга в процессе работы не использует файлы Результатов OVAL, то владелец должен документально оформить процесс, с помощью которого пользователь может представить Результаты OVAL владельцу функциональной возможности для интерпретации соответствующим продуктом или услугой. Это включает указание того, насколько быстро файлы, представленные владельцу функциональной возможности, будут доступны для данного продукта или услуги.

11 Требования к органу по проведению анализа

Орган по проведению анализа должен соблюдать следующие требования, касающиеся принятия OVAL.

11.1 Орган по проведению анализа должен четко определять версию принятия, версию документа требований и версию языка OVAL, которая использовалась для определения формального соблюдения требований принятия OVAL для каждого продукта, услуги или репозитория.

11.2 Орган по проведению анализа должен определять и публиковать примеры материалов тестов.

11.3 Орган по проведению анализа должен публиковать информацию о порядке участия в тестировании на правильность, с тем чтобы организации могли подготовиться как можно раньше.

11.4 Орган по проведению анализа должен сообщать контактное лицо для организации тестирования на правильность функциональных возможностей, заявленных как поддерживающие OVAL, по которым заполнена "Форма вопросника о принятии OVAL".

11.5 Орган по проведению анализа может провести повторное тестирование продукта, услуги или репозитория, получивших официальное подтверждение принятия OVAL, по усмотрению органа по проведению анализа.

11.6 Орган по проведению анализа должен предоставлять копию "Формы заявления о принятии OVAL" по запросу любого действительного владельца функциональной возможности, желающего начать процесс принятия OVAL.

11.7 Орган по проведению анализа должен предоставлять копию "Формы вопросника о принятии OVAL" по запросу любого владельца функциональной возможности, представившего заполненную "Форму заявления о принятии OVAL".

12 Отзыв

Если орган по проведению анализа засвидетельствовал, что продукт, услуга или репозиторий правильно приняли OVAL, однако позднее выяснилось, что установленные требования более не соблюдаются, то он может отозвать свое утверждение, и соответствующие продукт, услуга или репозиторий более не будут признаваться как правильно принявшие OVAL. Ниже приводятся требования, которым должен следовать орган по проведению анализа, для того чтобы отозвать свое подтверждение.

12.1 Орган по проведению анализа должен предоставить владельцу функциональной возможности предупреждение об отзыве не позднее чем за два (2) месяца до даты планируемого отзыва.

12.2 Орган по проведению анализа может отложить дату отзыва.

12.3 Если орган по проведению анализа полагает, что действия или заявления владельца функциональной возможности являются заведомо неверными, то он может не учитывать период предупреждения. Орган по проведению анализа может интерпретировать фразу "заведомо неверными" по своему усмотрению.

12.4 Если орган по проведению анализа полагает, что действия владельца функциональной возможности в отношении требований принятия являются заведомо неверными, то отзыв должен длиться не менее одного года.

12.5 Орган по проведению анализа должен определить конкретные требования, которые не соблюдаются.

12.6 Если владелец функциональной возможности полагает, что установленные требования соблюдены, он может ответить на предупреждение об отзыве, сообщив конкретные подробные данные, объясняющие, почему соответствующие продукт, услуга или репозиторий удовлетворяет данным требованиям.

12.7 Если в течение периода предупреждения владелец вносит изменения в соответствующие продукт, услугу или репозиторий с целью обеспечения его соответствия установленным требованиям, орган по проведению анализа должен прекратить действия по отзыву в отношении этих продукта, услуги или репозитория.

12.8 Орган по проведению анализа должен открыто сообщать о том, что официальное подтверждение правильности принятия OVAL в отношении соответствующих продукта, услуги или репозитория отозвано.

12.9 Орган по проведению анализа может открыто сообщать о причинах такого отзыва.

Библиография

- [b-ITU-T X.1520] Рекомендация МСЭ-Т X.1520 (2014 г.), *Общеизвестные уязвимости и незащищенность*.
- [b-IETF RFC 5209] IETF RFC 5209 (2008), *Network Endpoint Assessment (NEA): Overview and Requirements*.
- [b-MITRE Adoption] MITRE Corporation, Requirements and Recommendation for OVAL Adoption and Use, Ver. 1.1 (22 August 2013).
<http://oval.mitre.org/adoption/Requirements_and_Recommendations_for_OVAL_Adoption_and_Use_v1.1.pdf>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	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	Оконечное оборудование, субъективные и объективные методы оценки
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