Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1524

(03/2012)

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

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

Перечень общеизвестных слабых мест

Рекомендация МСЭ-Т X.1524

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.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

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

Рекомендация МСЭ-Т X.1524

Перечень общеизвестных слабых мест

Резюме

В Рекомендации МСЭ-Т X.1524 по использованию перечня общеизвестных слабых мест (CWE) представлено структурированное средство обмена сведениями о слабых местах в области информационной безопасности, обеспечивающее одинаковые общие наименования для широко известных проблем в коммерческом программном обеспечении или программном обеспечении с открытым исходным кодом, которое используется в сетях связи, устройствах конечных пользователей или же в любых других типах информационно-коммуникационных технологий (ИКТ), где может применяться программное обеспечение. Цель CWE состоит в том, чтобы обеспечить более эффективное обсуждение, описание, отбор и использование инструментальных средств и услуг по защите программного обеспечения, которые могут обнаруживать эти слабые места в кодах источников и операционных системах, а также улучшить понимание слабых мест программного обеспечения, связанных с его архитектурой и проектированием, и управление этими слабыми местами. В настоящей Рекомендации определяется применение CWE для создания механизма совместного использования средств, услуг, баз данных и других возможностей защиты программного обеспечения, а также для сравнения средств и услуг по его защите. CWE также содержит полезную контекстную информацию о возможных рисках, воздействии, постоянную информацию, а также подробную техническую информацию о том, какое значение данное слабое место может иметь для той или иной системы программного обеспечения.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1524	02.03.2012 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/.

СОДЕРЖАНИЕ

Введение

В Рекомендации по перечню общеизвестных слабых мест (CWE) описывается использование CWE − структурированного средства обмена единообразными измеримыми наборами слабых мест в программном обеспечении в целях установления общих наименований широко известных проблем. Цель CWE состоит в том, чтобы предоставить возможности для более эффективного обсуждения, описания, отбора и использования средств и услуг по защите программного обеспечения, которые могут обнаруживать эти слабые места в кодах источников и операционных системах, а также улучшить понимание слабых мест программного обеспечения, связанных с его архитектурой и проектированием, и управление этими слабыми местами.

Перечень CWE предназначен для того, чтобы охватить причины всех общеизвестных видов уязвимости и незащищенности, связанных со слабыми местами в архитектуре, проектировании, кодировании или развертывании программного обеспечения. Хотя CWE предназначен для включения в него тщательно проработанной информации, основное внимание уделяется определению слабых мест, которые могут стать причиной уязвимости и незащищенности. Орган по проведению анализа определяет соответствие в использовании идентификаторов CWE, как то определено в настоящей Рекомендации.

В CWE используются результаты работы, проводимой сообществом специалистов по кибербезопасности, например описание множества разнообразных реальных уязвимостей, приведенное в Рекомендации МСЭ-Т X.1520 − Общеизвестные уязвимости и незащищенности (CVE). Для разработки конкретных и емких определений элементов перечня CWE и структур дерева классификации использовались многие источники и примеры. Кроме того, созданы соответствующие отображения между наименованиями CWE и CVE, так что для каждого идентификатора CWE имеется список конкретных наименований CVE, принадлежащих к данной категории слабых мест программного обеспечения из перечня CWE. При создании перечня CWE и дерева классификации принимались меры к обеспечению максимально полного охвата соответствующих концептуальных, коммерческих и технических областей.

Настоящая Рекомендация в техническом отношении эквивалентна версии 1.0 "Требований и Рекомендаций в отношении совместимости с CWE и эффективности" от 28 июля 2011 года https://cwe.mitre.org/compatible/requirements_v1.0.html.

Рекомендация МСЭ-Т X.1524

Перечень общеизвестных слабых мест

1 Сфера применения

В настоящей Рекомендации по использованию перечня общеизвестных слабых мест (CWE) представлено "структурированное средство" для глобального обмена информацией о слабых с точки зрения безопасности местах в архитектуре, проектировании, кодировании или развертывании программного обеспечения, из-за которых системы программного обеспечения могут оказаться небезопасными, ненадежными и уязвимыми к атакам. Эти виды слабых мест программного обеспечения могут быть обнаружены с помощью инструментальных средств защиты, услуг по экспертной оценке и некоторых видов анализа мер безопасности. Это "структурированное средство", нередко называемое "совместимостью с CWE", определяет правильность применения CWE. Слабое место в системе информационной безопасности − это ошибка в программном обеспечении, вследствие которой может возникнуть уязвимость, которая может быть напрямую использована хакером для получения доступа в систему или сеть. Присвоение идентификаторов CWE не входит в сферу охвата настоящей Рекомендации. Список репозиториев идентификаторов CWE и соответствующей контекстной информации приводится в Дополнении I.

Перечень CWE, использование которого определяется в настоящей Рекомендации, предназначен для того, чтобы охватить причины всех общеизвестных видов уязвимости и незащищенности, связанных со слабыми местами в архитектуре, проектировании, кодировании или развертывании программного обеспечения. Хотя CWE предназначен для включения в него тщательно проработанной информации, основное внимание уделяется определению, изучению и описанию коренных причин слабых мест и уязвимостей, с тем чтобы разработчики могли их избежать, чтобы можно было проверить их наличие и чтобы группы разработчиков могли ими управлять, а также чтобы инструментальные средства и услуги по защите постоянно сообщали о них.

Настоящая Рекомендация в техническом отношении эквивалентна версии 1.0 "Требований и Рекомендаций в отношении совместимости с CWE и эффективности" от 28 июля 2011 года https://cwe.mitre.org/compatible/requirements_v1.0.html.

2 Справочные документы

Нет.

3 Определения

3.1 Термины, определенные в других документах

Нет.

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 правильные идентификаторы CWE.

3.2.2 средство (capability): Инструментальное средство оценки, интегрированная среда разработки (IDE), средство смыслового анализа кода, компилирующая программа проверки кода, база данных, веб-сайт, инструкция или услуга, предоставляющая информацию о слабых местах на уровне внедрения, проектирования или архитектуры, способных привести к возникновению в таком программном обеспечении уязвимости в плане безопасности, которой могут воспользоваться.

3.2.3 форма оценки требований к совместимости CWE (CWE compatibility requirements evaluation form): Эта форма оценки содержит серию вопросов к владельцу средства с целью документально подтвердить его соответствие требованиям к совместимости, изложенным в настоящей Рекомендации, с помощью текста, изображений или ссылок на веб-сайты, а также содержит инструкции по поводу представления заполненной формы или обращения к органу по проведению анализа за разъяснениями относительно заполнения формы оценки.

3.2.4 форма оценки требований к эффективности в отношении CWE (CWE effectiveness requirements evaluation form): Эта форма оценки содержит серию вопросов к владельцу средства с целью документально подтвердить его соответствие требованиям к эффективности, изложенным в настоящей Рекомендации, с помощью текста, изображений или ссылок на веб-сайты, а также содержит инструкции по поводу представления заполненной формы, обращения с просьбой о проведении теста или обращения к органу по проведению анализа за разъяснениями относительно заполнения формы оценки.

3.2.5 тестирование на эффективность (effectiveness testing): Процесс определения эффективности средства с точки зрения CWE.

3.2.6 отображать/отображение (map/mapping): Описание отношений между элементами слабых мест в репозитории и названиями CWE, относящимися к этим элементам.

3.2.7 владелец (owner): Хранитель (физическое или юридическое лицо), несущий ответственность за соответствующее средство.

3.2.8 репозиторий (repository): Явная или неявная совокупность элементов слабых мест в системе безопасности программного обеспечения, поддерживающая средство, например база данных слабых мест в системе безопасности, набор образцов в анализаторе кода или веб-сайт.

3.2.9 анализ (review): Процесс определения того, является ли то или иное средство совместимым с CWE.

3.2.10 орган по проведению анализа (review authority): Организация, осуществляющая анализ или тестирование на соответствие и уполномоченная предоставлять статус "совместимого с CWE" или "эффективного в отношении CWE".

В Дополнении II приводится список органов по проведению анализа.

3.2.11 версия анализа (review version): Датированная версия CWE, используемая для определения совместимости с CWE или эффективности в отношении CWE того или иного средства.

3.2.12 элемент безопасности (security element): Запись в базе данных, проба оценки, сигнатура и т. д., относящаяся к конкретному слабому месту в системе безопасности.

3.2.13 задача (task): Проба средства, проверка, сигнатура и т. д., которая выполняет некоторые действия, производящие информацию о безопасности (т. е. элемент безопасности).

3.2.14 результаты теста (test results): Данные об итогах тестирования эффективности.

3.2.15 инструментальное средство (tool): Программное приложение или устройство, которое изучает компьютерную программу, двоичный код или иной искусственный объект и производит информацию о слабых местах в системе безопасности, например анализатор безопасности исходного кода, средство оценки качества кода, компилирующая программа проверки кода или среда разработки.

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

3.2.17 уязвимость (vulnerability): Любое слабое место в программном обеспечении, которое может быть использовано для нарушения системы или содержащейся в ней информации (на основе [b-ITU-T X.1500]).

3.2.18 слабое место (weakness): Дефект или изъян в коде, проектировании, архитектуре или развертывании программного обеспечения, способный в определенный момент стать уязвимостью или приводить к возникновению других уязвимостей.

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
CCR	Coverage Claim Representation	Изложение заявленного охвата
CGI	Common Gateway Interface	Общий интерфейс шлюза
CWE	Common Weakness Enumeration	Перечень общеизвестных слабых мест
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	Информационно-коммуникационные технологии (ИКТ)
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

Нет.

6 Требования высокого уровня

В нижеследующих пунктах определяются концепции, функции и обязанности, связанные с надлежащим использованием идентификаторов CWE для обмена данными между отдельными средствами выявления слабых мест в системе безопасности (инструментальными средствами, репозиториями и услугами) с целью совместного использования этих средств выявления слабых мест в системе безопасности и облегчения сопоставления различных инструментальных средств и услуг по выявлению слабых мест в системе безопасности.

6.1 Владелец средства должен являться действительным юридическим лицом, т. е. организацией или отдельным 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 CWE (т. е. название, описание, риски, ссылки и сопутствующая информация о слабых местах).

6.3 Владелец средства должен предоставить органу по проведению анализа техническое контактное лицо, обладающее достаточной квалификацией, для того чтобы давать ответы на вопросы, касающиеся точности отображения и любой функциональной возможности средства, относящейся к CWE, а также координировать тестирование средства с целью оценки эффективности выявления CWE с его помощью.

6.4 Средство должно быть доступно общественности или кругу потребителей в рабочей или общедоступной версии, например ранее размещенной на общедоступном веб-сайте, предлагаемой для использования в качестве открытого источника, представленной для продажи или в качестве услуги, прилагаемой к контракту.

6.5 Для подтверждения совместимости с CWE средства его владелец должен предоставить органу по проведению анализа заполненную "Форму оценки требований к совместимости с CWE".

6.6 Владелец средства должен предоставить органу по проведению анализа свободный доступ к репозиторию средства, чтобы этот орган мог убедиться в том, что репозиторий средства удовлетворяет всем установленным требованиям к точности отображения.

6.7 Владелец средства должен предоставить возможность органу по проведению анализа использовать репозиторий для определения любых слабых мест, которые следует добавить к CWE.

6.8 Для обеспечения эффективности в отношении CWE средство должно быть совместимым с CWE.

6.9 Для обеспечения эффективности в отношении CWE владелец средства должен предоставить органу по проведению анализа заполненную "Форму оценки требований к эффективности в отношении CWE".

6.10 Для обеспечения эффективности в отношении CWE владелец средства должен предоставить органу по проведению анализа результаты тестирования эффективности в рамках своей "Формы оценки требований к эффективности в отношении CWE", с тем чтобы этот орган мог убедиться в том, что данное средство удовлетворяет всем установленным требованиям в отношении эффективности.

6.11 Владелец средства должен согласиться соблюдать все обязательные требования совместимости с CWE и эффективности в отношении CWE, которые включают обязательные требования для данного конкретного типа средства.

6.12 Для обеспечения совместимости с CWE средство должно позволять пользователям определять местоположение элементов системы безопасности, используя идентификаторы CWE ("поиск по идентификаторам CWE").

6.13 Если средство представляет пользователю элементы безопасности, то для обеспечения совместимости с CWE оно должно позволять пользователю получить соответствующие идентификаторы CWE ("вывод идентификаторов CWE").

6.14 Для обеспечения совместимости с CWE отображение средства должно точно связывать элементы безопасности с соответствующими идентификаторами CWE ("точность отображения").

6.15 Для обеспечения совместимости с CWE документация, касающаяся средства, должна надлежащим образом описывать CWE, совместимость с CWE, а также то, как в этом средстве используются функциональные возможности, относящиеся к CWE ("документация по CWE").

6.16 Для обеспечения совместимости с CWE в касающейся средства общедоступной документации должны быть прямо перечислены идентификаторы CWE, которые, по мнению владельца средства, охватываются средством в рамках его функциональных возможностей ("охват идентификаторов CWE").

6.17 Для обеспечения совместимости с CWE на общедоступном веб-сайте средства следует отразить охват средством идентификаторов CWE в виде XML-документа (документов) с изложением заявленного охвата (CCR) идентификаторов CWE.

6.18 Для обеспечения эффективности в отношении CWE на веб-сайте средства должны быть опубликованы результаты анализа данных средством набора тестов в отношении идентификаторов CWE (входящих в перечень охватываемых данным средством идентификаторов CWE) ("результаты теста CWE").

6.19 Средство должно указывать используемую в нем датированную версию CWE ("используемая версия").

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

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

6.22 От средства не требуется выполнения следующего:

- использования тех же описаний или ссылок, как CWE;
- включения каждого идентификатора CWE в его репозиторий.

6.23 Если средство удовлетворяет не всем применимым вышеперечисленным требованиям (пп. 6.1−6.22), то владелец средства не должен объявлять о том, что оно соответствует настоящей Рекомендации в части, относящейся к совместимости с CWE или эффективности в отношении CWE.

7 Точность

Совместимость с CWE облегчает обмен данными и их корреляцию только в том случае, если отображение средства является точным. Поэтому средства, совместимые с CWE, должны удовлетворять нижеследующим минимальным требованиям точности.

7.1 Репозиторий должен иметь процент точности на уровне 100 процентов.

7.2 Во время анализа владелец средства должен исправить любые ошибки отображения, выявленные органом по проведению анализа.

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 репозитория средства или в течение шести (6) месяцев, в зависимости от того, какой период короче.

7.4 Владельцу средства следует подготовить и подписать заявление о том, что, по имеющимся у него сведениям, ошибок в отображении не имеется.

7.5 Если соответствующее средство основывается на другом совместимом с CWE средстве или использует это средство (средство-"источник") и владельцу средства становится известно о наличии ошибок отображения в средстве-источнике, то владелец средства должен сообщить об этих ошибках владельцу средства-источника.

8 Эффективность

Эффективность направлена на обеспечение прозрачности для потенциальных пользователей какого-либо средства в отношении того, что могут быть обнаружены соответствующие слабые места в программном обеспечении. Знание о способности средства выявлять слабые места с учетом различных уровней сложности представляет для пользователей интерес в тех случаях, когда они намереваются использовать это средство или опираются на результаты использования этого средства другими. Поэтому средства, эффективные в отношении CWE, должны отвечать нижеследующим минимальным требованиям к эффективности.

8.1 В соответствующем разделе "Формы оценки требований к эффективности в отношении CWE" владелец средства должен указать, какие идентификаторы CWE, по его утверждению, данное средство способно обнаружить. Это можно сделать с помощью XML-документа (документов) с изложением заявленного охвата (CCR) идентификаторов CWE.

8.2 Для указанных им идентификаторов CWE владелец средства должен запросить соответствующие наборы тестов, что позволит ему использовать средство для анализа наборов тестов на выявление всех слабых мест, соответствующих указанным идентификаторам CWE.

8.3 В согласованный срок владелец средства должен представить результаты анализа наборов тестов с помощью своего средства.

8.4 Результаты должны содержать список всех проанализированных файлов с наборами тестов и номера строк всех выявленных слабых мест с указанием соответствующего идентификатора CWE.

8.5 Владелец средства должен подготовить и подписать заявление о согласии на размещение результатов тестирования своего средства на веб-сайте CWE.

8.6 Для проведения тестов на эффективность средства в отношении иного набора идентификаторов CWE владелец средства должен представить пересмотренную "Форму оценки требований к эффективности в отношении CWE", содержащую обновленный перечень идентификаторов CWE, которые, по утверждению владельца средства, оно способно обнаружить. Это можно сделать с помощью обновленного XML-документа (документы) с изложением заявленного охвата (CCR) идентификаторов CWE.

9 Документация

К документации, предоставляемой владельцем средства вместе со своим средством, применяются следующие требования.

9.1 Документация должна включать краткое описание CWE и совместимости с CWE, которое может быть основано на дословно цитированных частях документов с веб-сайта CWE органа по проведению анализа.

9.2 В документации должно содержаться описание того, как пользователь может найти отдельные элементы безопасности в репозитории средства, используя идентификаторы CWE.

9.3 В документации должно содержаться описание того, как пользователь может получить идентификаторы CWE из отдельных элементов в репозитории средства.

9.4 Если документация включает индекс, то он должен включать ссылки на относящуюся к CWE документацию с указанием аббревиатуры "CWE".

10 Используемая версия CWE

Пользователи должны знать, какая версия CWE используется в репозитории средства применительно к его отображению в CWE. Владелец средства может указать срок действия отображения, указав при этом номер версии CWE или дату обновления отображения.

10.1 Средство должно содержать указание на номер версии CWE или дату обновления, использованной при создании или обновлении отображения, с помощью по крайней мере одного из следующих механизмов: журналов регистрации изменений, перечней новых признаков, справочных файлов или некоторых других механизмов. Средство является "обновленным" по отношению к этой версии или дате обновления.

10.2 Каждая новая версия средства должна быть обновленной по отношению к версии CWE, которая была выпущена не ранее чем за четыре (4) месяца до того, как данное средство стало доступно для пользователей. Если средство не удовлетворяет этому требованию, то оно считается "устаревшим".

10.3 Владельцу средства следует открыто сообщать своим пользователям или предполагаемым пользователям, как скоро он собирается обновить репозиторий средства после размещения новой версии CWE или обновления на веб-сайте CWE.

11 Отзыв совместимости с CWE

Ниже описываются функции органа по проведению анализа на предмет отзыва совместимости с CWE.

11.1 Если орган по проведению анализа проверил, что средство совместимо с CWE или эффективно в отношении CWE, однако впоследствии обнаружил, что установленные требования не соблюдаются, то он может отозвать свое утверждение.

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

11.2 Орган по проведению анализа должен определить, являются ли действия или требования владельца средства "намеренно недостоверными".

11.2.1 Орган по проведению анализа может интерпретировать выражение "намеренно недостоверные" по своему усмотрению.

11.3 Органу по проведению анализа не следует рассматривать вопрос об отзыве совместимости с CWE в отношении данного конкретного средства чаще одного раза в шесть (6) месяцев.

11.4 Орган по проведению анализа должен предоставить владельцу средства и техническому контактному лицу предупреждение об отзыве не позднее чем за два (2) месяца до планируемой даты отзыва.

11.4.1 Если орган по проведению анализа считает, что действия или требования владельца средства являются намеренно недостоверными, то он может не соблюдать период предупреждения.

11.5 Если владелец средства считает, что установленные требования соблюдены, то он может ответить на предупреждение об отзыве, сообщив соответствующие подробные данные, объясняющие, почему соответствующее средство удовлетворяет данным требованиям.

11.6 Если в течение периода предупреждения владелец средства вносит изменения в соответствующее средство с целью обеспечения его соответствия данным требованиям, то органу по проведению анализа следует прекратить действия по отзыву в отношении данного средства.

11.7 Орган по проведению анализа может отложить дату отзыва.

11.8 Орган по проведению анализа должен открыто сообщить на своем веб-сайте CWE о том, что подтверждения совместимости с CWE или эффективности в отношении CWE отозваны.

11.9 Если орган по проведению анализа считает, что действия владельца в отношении требований совместимости с CWE или эффективности в отношении CWE являются намеренно недостоверными, то отзыв должен длиться не менее одного года.

11.10 Орган по проведению анализа может открыто сообщить о причинах такого отзыва.

11.11 Владелец средства может разместить на этом же веб-сайте публичное заявление по вопросу об отзыве.

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

12 Орган по проведению анализа

12.1 Орган по проведению анализа должен проанализировать средство на предмет совместимости с CWE или эффективности в отношении CWE применительно к конкретной версии CWE, т. е. версии анализа.

12.2 Орган по проведению анализа должен четко определить версию анализа, которая была использована для определения совместимости или эффективности данного средства.

12.3 Орган по проведению анализа должен четко определить версию документа с требованиями к совместимости с CWE или эффективности в отношении CWE, которая была использована для определения совместимости или эффективности данного средства.

12.4 Орган по проведению анализа должен проанализировать каждый элемент в репозитории средства на предмет точности отображения CWE.

12.5 Органу по проведению анализа следует анализировать средство на предмет точности отображения не реже одного раза в год.

Приложение A

Специфические для типа требования

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Поскольку самые различные средства используют CWE, некоторые типы средств могут иметь те или иные характерные особенности, требующие особого внимания в отношении совместимости с CWE.

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

A.1.1 Если таким средством является инструментальное средство оценки, анализатор безопасности исходного или двоичного кода, средство оценки качества кода, компилирующая программа проверки кода, среда разработки или какой-либо продукт, сводящий воедино результаты оценки одним или несколькими типами таких средств, то оно должно удовлетворять требованиям, предъявляемым к инструментальным средствам, A.2.1−A.2.8.

A.1.2 Если таким средством является услуга (например, услуга оценки безопасности, услуга обучения или профессиональной подготовки либо услуга анализа кода и разработки), то оно должно удовлетворять требованиям, предъявляемым к услугам безопасности, A.3.1−A.3.5.

A.1.3 Если таким средством является онлайновая база данных по вопросам безопасности или слабых мест в прикладном программном обеспечении, сетевой ресурс или информационный сайт, то оно должно удовлетворять требованиям, предъявляемым к онлайновым средствам, A.4.1−A.4.3.

A.2 Требования, предъявляемые к инструментальным средствам

Ниже излагаются особые требования, предъявляемые к инструментальным средствам.

A.2.1 Инструментальное средство должно позволять пользователю использовать идентификаторы CWE для установления местоположения соответствующих задач в данном инструментальном средстве ("поиск по идентификаторам CWE") путем обеспечения по крайней мере одной из следующих функций: функции "нахождения" или "поиска", отображения между названиями задач этого инструментального средства и идентификаторами CWE или другого механизма, признанного достаточным органом по проведению анализа.

A.2.2 В отношении любого отчета, определяющего отдельные элементы безопасности, инструментальное средство должно позволять пользователю определять соответствующие идентификаторы CWE для этих элементов ("вывод идентификаторов CWE") путем совершения по крайней мере одного из следующих действий: включения идентификаторов CWE непосредственно в отчет, предоставления отображения между названиями задач данного инструментального средства и идентификаторами CWE или использования какого-либо другого механизма, признанного достаточным органом по проведению анализа.

A.2.3 В общедоступной документации должны прямо перечисляться идентификаторы CWE, которые, по мнению владельца средства, данное инструментальное средство фактически способно выявлять в программном обеспечении ("заявленный охват совместимости с CWE").

A.2.4 Информация о заявленном охвате совместимости с CWE может быть отражена на общедоступном веб-сайте средства в виде XML-документа (документов) с изложением заявленного охвата (CCR) идентификаторов CWE.

A.2.5 Любые требуемые отчеты или отображения должны удовлетворять требованиям к среде передачи, предусмотренным в Приложении B.

A.2.6 Инструментальному средству или владельцу средства следует предоставить для пользователя перечень всех идентификаторов CWE, связанных с задачами данного инструментального средства.

A.2.7 Инструментальное средство должно позволять пользователю выбрать набор задач, предоставив ему файл, содержащий перечень идентификаторов CWE.

A.2.8 Интерфейс инструментального средства должен позволять пользователю просматривать, выбирать и отменять выбор набора задач, используя отдельные идентификаторы CWE.

A.2.9 Если инструментальное средство не имеет задачи, связанной с каким-либо идентификатором CWE, указанным пользователем в требованиях A.2.5 или A.2.6 к инструментальному средству, то инструментальное средство должно уведомить пользователя о том, что оно не может выполнить соответствующую задачу.

A.2.10 Владелец средства должен гарантировать, что 1) уровень ложных позитивных результатов составляет 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 что 2) уровень ложных негативных результатов составляет менее 100 процентов, т. е. если имеет место какая-либо проблема с артефактами системы, связанная с каким-либо конкретным элементом безопасности, то инструментальное средство иногда сообщает о такой проблеме.

A.3 Требования, предъявляемые к услугам безопасности

Услуги безопасности могут использовать в своей работе инструментальные средства, совместимые с CWE и эффективные в отношении CWE, однако они не могут предоставить своим клиентам прямой доступ к этим инструментальным средствам. Поэтому клиентам может быть трудно определить и сравнить возможности различных услуг. Требования, предъявляемые к услугам безопасности, позволяют устранить это потенциальное ограничение.

A.3.1 Услуга безопасности должна иметь возможность использовать идентификаторы CWE для того, чтобы сообщить пользователю, какие элементы безопасности тестируются, обнаруживаются или охватываются предлагаемой услугой ("поиск по идентификаторам CWE") путем совершения одного или нескольких из следующих действий: предоставления пользователю перечня идентификаторов CWE, определяющих элементы, которые тестируются, обнаруживаются или охватываются этой услугой, предоставления пользователю отображения между элементами данной услуги и идентификаторами CWE, реагирования на введенный пользователем перечень идентификаторов CWE, определяя при этом, какие из идентификаторов CWE тестируются, обнаруживаются или охватываются этой услугой, или используя какой-либо другой механизм.

A.3.2 В отношении любого отчета, определяющего отдельные элементы безопасности, данная услуга должна позволять пользователю определять соответствующие идентификаторы CWE для этих элементов ("вывод идентификаторов CWE") путем совершения одного или нескольких из следующих действий: предоставления пользователю возможности включения идентификаторов CWE непосредственно в отчет, предоставления пользователю отображения между элементами безопасности и идентификаторами CWE или использования какого-либо другого механизма.

A.3.3 В общедоступной документации должны прямо перечисляться идентификаторы CWE, которые, по мнению владельца средства, эффективно охватываются предлагаемой услугой безопасности ("заявленный охват совместимости с CWE").

A.3.4 Информация о заявленном охвате совместимости с CWE может быть отражена на общедоступном веб-сайте средства в виде XML-документа (документов) с изложением заявленного охвата (CCR) идентификаторов CWE.

A.3.5 Любые требуемые отчеты или отображения, предоставленные услугой, должны удовлетворять требованиям, предъявляемым к среде передачи, предусмотренным в Приложении B.

A.3.6 Если данная услуга предоставляет пользователю прямой доступ к какому-либо продукту, определяющему элементы безопасности, то данный продукт должен быть совместимым с CWE и эффективным в отношении CWE.

A.3.7 Владелец средства должен гарантировать, что 1) уровень ложных позитивных результатов составляет 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 что 2) уровень ложных негативных результатов составляет менее 100 процентов, т. е. если имеет место какая-либо проблема с артефактами системы, связанная с каким-либо конкретным элементом безопасности, то инструментальное средство иногда сообщает о такой проблеме.

A.4 Требования, предъявляемые к онлайновым средствам

Ниже излагаются особые требования, предъявляемые к онлайновым средствам.

A.4.1 Онлайновое средство должно позволять пользователю найти соответствующие элементы безопасности в репозитории онлайнового средства ("поиск по идентификаторам CWE") путем обеспечения одной из следующих функций: функции поиска с возвратом идентификаторов CWE для соответствующих элементов, отображения, связывающего каждый элемент с соответствующим(и) идентификатором(ами) CWE, или использование какого-либо другого механизма.

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

Примеры:

http://www.example.com/cgi-bin/db-search.cgi?cweid=XXX

http://www.example.com/cwe/xxx.html

A.4.1.2 Если данный веб-сайт является общедоступным и не требует регистрации при входе, то CGI-программа должна принимать метод "GET".

A.4.2 В отношении любого отчета, определяющего отдельные элементы безопасности, онлайновое средство должно позволять пользователю определять соответствующие идентификаторы CWE для этих элементов ("вывод идентификаторов CWE") путем совершения по крайней мере одного из следующих действий: предоставления пользователю возможности включения идентификаторов CWE непосредственно в отчет, предоставления пользователю отображения между элементами безопасности и идентификаторами CWE или использования какого-либо другого механизма.

A.4.3 В общедоступной документации должны прямо перечисляться идентификаторы CWE, которые, по мнению владельца средства, охватывает репозиторий данного онлайнового средства ("заявленный охват совместимости с CWE").

A.4.4 Информация о заявленном охвате совместимости с CWE может быть отражена на общедоступном веб-сайте средства в виде XML-документа (документов) с изложением заявленного охвата (CCR) идентификаторов CWE.

A.4.5 Если онлайновое средство не предоставляет подробную информацию в отношении отдельных элементов безопасности, то это онлайновое средство должно обеспечить отображение, связывающее каждый элемент с соответствующим(и) идентификатором(ами) CWE.

Приложение B

Требования, предъявляемые к среде передачи

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

B.1 Среда распространения, используемая средством, совместимым с CWE, должна использовать один из медиаформатов, описанных в настоящем Приложении.

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

B.3 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 идентификаторам CWE"), например необработанный ASCII-текст, HTML или PDF.

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

B.3.3 Документ должен включать отображение элементов на идентификаторы CWE, содержащее перечень соответствующих страниц для каждого элемента.

B.4 Графический интерфейс пользователя (GUI)

Ниже излагаются особые требования, предъявляемые к графическому интерфейсу пользователя.

B.4.1 GUI должен предоставлять пользователю функцию поиска, позволяющую ему вводить идентификаторы CWE и осуществлять поиск соответствующих элементов ("поиск по идентификаторам CWE").

B.4.2 Если GUI предоставляет подробную информацию по какому-либо отдельному элементу, то он должен предоставлять перечень идентификаторов CWE, отображающих данный элемент ("вывод идентификаторов CWE"). В ином случае GUI должен обеспечивать пользователю отображение в формате, удовлетворяющем требованию B.3.1, предъявляемому к электронным документам.

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

Дополнение I

Список репозиториев идентификаторов CWE и соответствующей контекстной информации

(Данное Дополнение является неотъемлемой частью настоящей Рекомендации.)

Корпорация MITRE	cwe.mitre.org/data

Дополнение II

Список органов по проведению анализа

(Данное Дополнение является неотъемлемой частью настоящей Рекомендации.)

1 Корпорация MITRE, для контактов: cwe@mitre.org.

Библиография

[b-ITU-T X.1500] Рекомендация МСЭ-Т X.1500 (2011 г.), *Методы обмена информацией о кибербезопасности*.

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	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

Отпечатано в Швейцарии
Женева, 2012 г.