Международный союз электросвязи

МСЭ-Т X.1544

(04/2013)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Обмен информацией, касающейся кибербезопасности – Обмен информацией о событии/инциденте/эвристических правилах

Перечень и классификация общеизвестных схем атак

Рекомендация МСЭ-Т X.1544

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.1544

Перечень и классификация общеизвестных схем атак

Резюме

Рекомендация МСЭ-Т X.1544 представляет собой основанную на XML/XSD спецификацию для определения, описания и составления перечня схем атак. Схемы атак являются высокоэффективным средством, позволяющим получать и представлять информацию о подходах, используемых нарушителем защиты. Эти схемы являются описаниями общеизвестных методов использования программного обеспечения. Они выводятся из схем проектных решений, применяемых деструктивным, а не конструктивным образом, и составляются на основе углубленного анализа конкретных примеров реального использования. Цель перечня и классификации общеизвестных схем атак (CAPEC) состоит в том, чтобы обеспечить общедоступный каталог схем атак, наряду с комплексной схемой и классификационной таксономией.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1544	26.04.2013 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 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/.

СОДЕРЖАНИЕ

Введение

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

CAPEC дает возможность:

- стандартизировать получение и описание схем атак;
- собирать известные схемы атак в общий перечень, который может согласованным и эффективным образом использоваться сообществом;
- классифицировать схемы атак, с тем чтобы пользователи могли легко определять во всем перечне то подмножество, которое подходит к их условиям;
- с помощью явных ссылок увязать схемы атак и перечни общеизвестных слабых мест (CWE), в которых такие атаки могут быть эффективными.

Рекомендация МСЭ-Т X.1544 была разработана с учетом важности подержания, в максимально возможной степени, технической совместимости с "Требованиями и Рекомендацией по совместимости CAPEC" версии 1.0, опубликованной корпорацией MITRE 30 августа 2012 года (https://capec.mitre.org/compatible/requirements_v1.0.html).

Рекомендация МСЭ-Т X.1544

Перечень и классификация общеизвестных схем атак

1 Сфера применения

Настоящая Рекомендация предназначена для структурированного обмена общедоступными схемами атак, наряду с комплексной схемой и классификационной таксономией.

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.

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

3 Определения

3.1 Термины, определенные в других документах

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

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

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

3.1.2 уязвимость (vulnerability) [ITU-T X.1500]: Любое слабое место в программном обеспечении, которое могло бы использоваться для нарушения целостности системы или содержащейся в ней информации.

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 CAPEC.

3.2.2 случай атаки (attack instance): Конкретная подробно описанная атака против приложения или системы, целью которой являются уязвимые или слабые места в этой системе.

3.2.3 схема атаки (attack pattern): Обобщение общих подходов в случае атаки, наблюдаемой в неконтролируемых ситуациях в отношении приложений или систем (например, введение запроса SQL, атака через посредника, перехват сеанса связи и т. д.).

ПРИМЕЧАНИЕ. − Одна схема атаки потенциально может включать много различных случаев атак, которые с ней ассоциируются.

3.2.4 средство (capability): Инструментальное средство оценки, динамичной проверки безопасности приложений (DAST), тестирования на предмет несанкционированного доступа, использования структуры, моделирования угроз, база данных, веб-сайт, инструкция или услуга, которые обеспечивают информацию о случаях и схемах атак.

3.2.5 отображать/отображение (map/mapping): Описание связей между элементами схем атак в репозитории и пунктами CAPEC, относящимися к этим элементам.

3.2.6 владелец (owner) [на основе b-ITU-T X.1520]: Хранитель (реальное физическое лицо или компания), несущий ответственность за данное средство (определенное в настоящей Рекомендации).

3.2.7 репозиторий (repository): Явная или неявная совокупность элементов схем атак, обеспечивающая работу средства, например база данных схем атак, подборка случаев атак в инструментальном средстве DAST или веб-сайт.

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

3.2.9 версия анализа (review version): Датированная версия CAPEC, которая используется для определения совместимости средства с CAPEC.

3.2.10 элемент безопасности (security element): Запись в базе данных, проба оценки, случай атаки, использование, полезная нагрузка, и т. д., относящиеся к конкретной схеме атаки.

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

3.2.12 инструментальное средство (tool): Программное приложение или устройство, которое тестирует защитные свойства приложения или системы с помощью моделирования, эмуляции или описания характеристик потенциальных атак, направленных против этой системы, например инструментальное средство оценки, динамичной проверки безопасности приложений (DAST), тестирования на предмет несанкционированного доступа, использования структуры, моделирования угроз.

3.2.13 пользователь (user) [на основе b-ITU-T X.1520]: Пользователь или потенциальный пользователь соответствующего средства (определенного в настоящей Рекомендации).

3.2.14 слабое место (weakness): Недостаток или несовершенство в коде, проекте, архитектуре или развертывании программного обеспечения, которые в некоторый момент могут стать уязвимыми или могут приводить к появлению других уязвимостей.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

CAPEC	Common Attack Pattern Enumeration and Classification	Перечень и классификация общеизвестных схем атак
CCR	Coverage Claim Representation	Представление требования о покрытии
CIA	Confidentially, Integrity or Availability	Конфиденциальность, целостность или наличие
CWE	Common Weakness Enumeration	Перечень общеизвестных слабых мест
DAST	Dynamic Application Security testing Tool	Инструментальное средство динамичной проверки безопасности приложений
GUI	Graphical User Interface	Графический интерфейс пользователя
IDS	Intrusion Detection System	Система обнаружения проникновений
POC	Point Of Contact	Контактное лицо

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 (размещено по адресу: http://www.itu.int/oth/T0A0F000004/en).

6 Требования высокого уровня

В следующих далее пунктах определяются понятия, функции и ответственность, связанные с надлежащим использованием идентификаторов CAPEC для обмена данными между отдельными средствами проверки безопасности (инструментальные средства, репозитории и услуги), с тем чтобы обеспечить возможность совместного использования этих средств проверки безопасности и упростить сравнение инструментальных средств и услуг проверки безопасности.

Необходимые условия

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

6.2 Средство должно обеспечивать дополнительную ценность или информацию, помимо той, которая обеспечивается самими данными CAPEC (т. е. название, описание, риски, ссылки и соответствующая информация о слабых местах).

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

6.4 Средство – в производственной или общедоступной версии – должно быть доступным для населения или определенного круга потребителей.

6.5 Для обеспечения совместимости с CAPEC владелец средства должен предоставить организации по анализу заполненную "Форму оценки требований совместимости с CAPEC".

6.6 Владелец средства должен предоставить организации по анализу свободный доступ к репозиторию, для того чтобы эта организация могла убедиться в том, что репозиторий удовлетворяет всем связанным с точностью отображения требованиям.

6.7 Владелец средства должен предоставить организации по анализу возможность использовать репозиторий для определения любой схемы атак, которую следует добавить к CAPEC.

6.8 Владелец средства должен согласиться соблюдать все обязательные требования совместимости с CAPEC, которые включают обязательные требования для данного конкретного типа средства.

Функциональные возможности

6.9 В целях совместимости с CAPEC средство должно предоставлять пользователям возможность определять местоположение элементов безопасности, используя идентификаторы CAPEC ("поиск по CAPEC").

6.10 В целях совместимости с CAPEC, если средство представляет пользователю элементы безопасности, то оно должно позволять ему получить соответствующие идентификаторы CAPEC ("вывод идентификаторов CAPEC").

6.11 В целях совместимости с CAPEC отображение средства должно точно связывать элементы безопасности с соответствующими идентификаторами CAPEC ("точность отображения").

6.12 В целях совместимости с CAPEC документация, касающаяся средства, должна надлежащим образом описывать CAPEC, совместимость с CAPEC, а также порядок использования относящихся к CAPEC функциональных возможностей в данном средстве ("документация по CAPEC").

6.13 В целях совместимости с CAPEC общедоступная информация, касающаяся средства, должна содержать подробное перечисление идентификаторов CAPEC, которые владелец средства считает средством покрытия в качестве части своих функциональных возможностей ("покрытие CAPEC").

6.14 В целях совместимости с CAPEC следует, чтобы общедоступный веб-сайт, касающийся средства, обеспечивал для средства покрытие CAPEC в качестве документа(ов) XML с представлением требования о покрытии (CCR) CAPEC.

6.15 Средство должно указывать датированную используемую версию CAPEC ("использование версии").

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

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

6.18 От средства не требуется выполнения следующего:

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

Прочее

6.19 Если средство удовлетворяет не всем применимым требованиям, изложенным выше (пункты 6.1−6.18), то владелец средства не должен объявлять о том, что оно совместимо с CAPEC.

7 Точность

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

7.1 Репозиторий должен характеризоваться точностью на уровне 100 процентов.

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

7.3 По истечении периода анализа владельцу средства следует исправлять 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 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 нет.

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

8 Документация

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

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

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

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

8.4 Если документация включает индекс, то следует, чтобы он включал ссылки на относящуюся к CAPEC документацию согласно термину " CAPEC".

9 Использование версии CAPEC

Пользователи должны знать, какая версия CAPEC используется в репозитории средства в отношении его отображения в CAPEC. Владелец средства может указать срок действия отображения, используя соответствующую версию CAPEC или указав дату обновления отображения.

9.1 В средстве должна указываться версия CAPEC или дата обновления, которые использовались при создании или обновлении отображения, с помощью, по крайней мере, одного из следующих механизмов: журналы регистрации изменений, перечни новых свойств, справочные файлы или некоторые другие механизмы. Средство является "обновленным" относительно этой версии или даты.

9.2 Каждая новая версия средства должна быть обновленной относительно версии CAPEC, которая была выпущена не более четырех (4) месяцев до того, как данное средство стало доступно его пользователям. Если средство не удовлетворяет этому требованию, то оно считается "устаревшим".

9.3 Владельцу средства следует открыто сообщить о том, как быстро он обновит репозиторий средства после того, как на веб-сайте CAPEC станет доступной новая версия CAPEC или обновленный CAPEC.

10 Отзыв совместимости с CAPEC

10.1 Если организация по анализу проверила, что средство совместимо с CAPEC, но впоследствии обнаружила, что установленные требования не соблюдаются, то она может отозвать свое утверждение.

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

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

10.2.1 Организация по анализу может толковать выражение "намеренно недостоверные" по своему усмотрению.

10.3 Организации по анализу не следует рассматривать вопрос об отзыве совместимости с CAPEC в отношении данного конкретного средства чаще одного раза в шесть (6) месяцев.

Предупреждение и оценка

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

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

10.5 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.

10.6 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

10.7 Организация по анализу может отложить дату отзыва.

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

10.9 Если организация по анализу считает, что действия владельца средства в отношении требований совместимости с CAPEC являются намеренно недостоверными, то следует, чтобы период действия отзыва составлял не менее одного года.

10.10 Организация по анализу может открыто сообщить о причинах отзыва.

10.11 Владелец средства может разместить на том же сайте общедоступное заявление в отношении отзыва.

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

11 Организация по анализу

11.1 Организация по анализу должна проанализировать средство на предмет совместимости с CAPEC относительно конкретной версии CAPEC, т. е. анализируемой версии.

11.2 Организация по анализу должна четко определить анализируемую версию, которая была использована для определения совместимости для данного средства.

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

11.4 Организация по анализу должна проанализировать каждый элемент в репозитории средства на предмет точности отображения CAPEC.

11.5 Организации по анализу следует анализировать средство на точность отображения не реже одного раза в год.

11.6 Организация по анализу обязана предоставлять копию формы заявления о совместимости с CAPEC по запросу любого действительного владельца средства, желающего начать процесс обеспечения совместимости с CAPEC.

11.7 Организация по анализу обязана предоставлять копию формы оценки требований совместимости с CAPEC по запросу любого владельца средства, который представил заполненную форму заявления о совместимости с CAPEC.

Приложение A

Специфические для типа требования

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

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

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

A.1.1 Если таким средством является инструментальное средство оценки, динамичной проверки безопасности приложений (DAST), тестирования на предмет несанкционированного доступа, использования структуры, моделирования угроз или какой-либо продукт, сводящий воедино результаты оценки одного или нескольких из этих типов статей, то оно должно удовлетворять требованиям, предъявляемым к инструментальным средствам, пункты A.2.1–A.2.8.

A.1.2 Если таким средством является услуга (например, услуга оценки безопасности, тестирования на предмет несанкционированного доступа или услуга в области обучения или профессиональной подготовки), то она должна удовлетворять требованиям, предъявляемым к услугам обеспечения безопасности, пункты A.3.1–A.3.5.

A.1.3 Если таким средством является онлайновая база данных известных атак, ресурс на базе веб-сети или информационный сайт, то они должны удовлетворять требованиям, предъявляемым к онлайновым средствам, пункты A.4.1–A.4.3.

A.2 Требования, предъявляемые к инструментальным средствам

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

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

A.2.3 В общедоступной документации должны четко перечисляться идентификаторы CAPEC, которые владелец средства считает эффективным инструментальным средством при его установке ("покрытие требований о совместимости с CAPEC").

A.2.4 Общедоступный веб-сайт, касающийся средства, может обеспечивать для средства покрытие требований о совместимости с CAPEC в качестве документа(ов) XML с представлением требования о покрытии (CCR) CAPEC.

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

A.2.6 Инструментальному средству или владельцу средства следует предоставить пользователю перечень всех идентификаторов CAPEC, связанных с задачами данного инструментального средства.

A.2.7 Следует, чтобы инструментальное средство обеспечивало пользователю возможность выбирать набор задач, предоставив ему файл, содержащий перечень идентификаторов CAPEC.

A.2.8 Следует, чтобы интерфейс инструментального средства предоставлял пользователю возможность просматривать, выбирать и отменять выбор набора задач, используя идентификаторы отдельных CAPEC.

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

A.3 Требования, предъявляемые к услугам обеспечения безопасности

Услуги обеспечения безопасности могут использовать в работе инструментальные средства, совместимые с CAPEC, однако они не могут предоставить своим клиентам прямой доступ к этим инструментальным средствам. Поэтому для клиентов было бы сложным определять и сравнивать возможности различных услуг. Требования, предъявляемые к услугам обеспечения безопасности, позволяют устранить это потенциальное ограничение.

A.3.1 Услуга обеспечения безопасности должна иметь возможность использовать идентификаторы CAPEC, для того чтобы сообщить пользователю, какие элементы безопасности протестированы или покрываются данной предлагаемой услугой ("поиск по CAPEC") путем выполнения одного или нескольких из следующих действий: предоставление пользователю перечня идентификаторов CAPEC, определяющих элементы, протестированные или покрываемые этой услугой, предоставление пользователю отображения между элементами данной услуги и идентификаторами CAPEC, реагирование на введенный пользователем перечень идентификаторов CAPEC, определяя какие из идентификаторов CAPEC протестированы или покрываются 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 идентификаторы CAPEC для этих элементов ("вывод идентификаторов CAPEC") путем совершения одного или нескольких из следующих действий: предоставление пользователю возможности включения идентификаторов CAPEC непосредственно в отчет, предоставление пользователю отображения между элементами безопасности и идентификаторами CAPEC, или же используя какой-либо иной механизм.

A.3.3 В общедоступной документации должны четко перечисляться идентификаторы CAPEC, которые владелец средства считает услугой обеспечения безопасности, эффективно покрывающейся в его предложении ("покрытие требований о совместимости с CAPEC").

A.3.4 Общедоступный веб-сайт, касающийся средства, может обеспечивать для средства покрытие требований о совместимости с CAPEC в качестве документа(ов) XML с представлением требования о покрытии (CCR) CAPEC.

A.3.5 Любые требуемые отчеты или отображения, предоставляемые услугой, должны удовлетворять требованиям к среде передачи, указанным в Приложении B.

A.3.6 Если данная услуга предоставляет пользователю прямой доступ к продукту, определяющему элементы безопасности, то данный продукт должен быть совместим с CAPEC.

A.4 Требования, предъявляемые к онлайновым средствам

A.4.1 Онлайновое средство должно предоставлять пользователю возможность находить соответствующие элементы безопасности в репозитории онлайнового средства ("поиск по CAPEC") путем обеспечения одной из следующих функций: поиск с возвратом идентификаторов CAPEC для соответствующих элементов, отображение, связывающее каждый элемент безопасности с соответствующим(и) идентификатором (ами) CAPEC, 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 пункте A.4.1 требований, предъявляемых к онлайновым средствам.

Примеры создания ссылок:

http://www.example.com/cgi-bin/db-search.cgi?capecid=XXX
http://www.example.com/capec/xxx.html

A.4.1.2 Если сайт является общедоступным и не требует входа в систему, то следует, чтобы программа CGI принимала метод "GET".

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

A.4.3 В общедоступной документации должны четко перечисляться идентификаторы CAPEC, которые владелец средства считает покрываемыми в репозитории онлайнового средства ("покрытие требований о совместимости с CAPEC").

A.4.4 Общедоступный веб-сайт, касающийся средства, может обеспечивать для средства покрытие требований о совместимости с CAPEC в качестве документа(ов) XML с представлением требования о покрытии (CCR) CAPEC.

A.4.5 Если онлайновое средство не предоставляет подробной информации в отношении отдельных элементов безопасности, то это онлайновое средство должно обеспечивать отображение, связывающее каждый элемент с соответствующим(и) идентификатором(ами) CAPEC.

Приложение B

Требования, предъявляемые к среде передачи

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

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

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

B.3 Электронные документы (HTML, текстовый процессор, 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 CAPEC"), 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 CAPEC, связанных с этими элементами ("вывод идентификаторов CAPEC").

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

B.4 Графический интерфейс пользователя

B.4.1 Графический интерфейс пользователя (GUI) должен предоставлять пользователю функцию поиска, позволяющую ему вводить идентификаторы CAPEC и получать соответствующие элементы ("поиск по CAPEC").

B.4.2 Если GUI предоставляет подробную информацию по какому-либо отдельному элементу, то он должен содержать перечень идентификаторов CAPEC, отображаемых в данном элементе ("вывод идентификаторов CAPEC"). В ином случае, GUI должен предоставлять пользователю отображение в формате, удовлетворяющем требованиям к электронным документам, которые изложены в пункте B.3.1.

B.4.3 GUI должен предоставлять пользователю возможность экспортировать данные, относящиеся к CAPEC, или получать доступ к этим данным в альтернативном формате, удовлетворяющем требованиям к электронным документам, которые изложены в пункте B.3.1.

Библиография

[b-ITU-T X.1520] Рекомендация МСЭ-Т X.1520 (2011 г.), *Общеизвестные уязвимости и незащищенность.*

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, 2013 г.