Международный союз электросвязи

МСЭ-Т X.1521

(04/2011)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

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

Система оценки общеизвестных уязвимостей

Рекомендация МСЭ-Т X.1521

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.1521

Система оценки общеизвестных уязвимостей

Резюме

В Рекомендации МСЭ-Т X.1521 по системе оценки общеизвестных уязвимостей (CVSS) определена открытая структура представления информации о характеристиках и воздействиях уязвимостей информационно-коммуникационных технологий (ИКТ), имеющихся в коммерческом программном обеспечении или в программном обеспечении с открытым исходным кодом, которое используется на сетях связи, в устройствах конечных пользователей или в любых других видах ИКТ, способных выполнять программы. Цель этой Рекомендации состоит в том, чтобы предоставить менеджерам по ИКТ, поставщикам бюллетеней с описаниями уязвимостей, разработчикам средств защиты, разработчикам приложений и исследователям возможность общаться, используя общий язык оценки уязвимостей ИКТ.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1521	20.04.2011 г.	17-я

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Введение

Менеджеры по ИКТ должны выявлять и оценивать уязвимости, имеющиеся во множестве различных аппаратных и программных платформ. Далее, им приходится устанавливать приоритеты этих уязвимостей и устранять те из них, которые представляют наибольший риск. При наличии множества подлежащих исправлению уязвимостей, которые оценивались по разным шкалам, менеджеры по ИКТ вынуждены полагаться на собственные методы, для того чтобы каким-то образом сравнить различные уязвимости и получить по ним информацию, позволяющую принять меры.

В связи с тем, что в CVSS стандартизованы методы описания уязвимостей, пользователи CVSS могут задействовать временны́е показатели и показатели среды для обеспечения связанной с контекстом информации, которая более точно отражает риск для их уникальной среды. Благодаря этому пользователи CVSS, старающиеся снизить риски, которые связаны с независящими от разработчика уязвимостями в рамках их уникальной среды, могут принимать более обоснованные решения.

Настоящая Рекомендация технически соответствует "Системе оценки общеизвестных уязвимостей (CVSS) версии 2" от 20 июня 2007 года и совместима с этой системой, которая представлена на веб-сайте: http://www.first.org/cvss.

Рекомендация МСЭ-Т X.1521

Система оценки общеизвестных уязвимостей

1 Сфера применения

В настоящей Рекомендации определен стандартизованный подход к представлению информации о характеристиках и воздействиях уязвимостей ИКТ, опирающийся на систему временны́х показателей и показателей среды. В этом подходе применяется контекстная информация, чтобы более точно отразить риск для уникальной среды каждого пользователя.

Настоящая Рекомендация технически соответствует "Системе оценки общеизвестных уязвимостей (CVSS) версии 2" от 20 июня 2007 года и совместима с этой системой, которая представлена на веб-сайте: http://www.first.org/cvss.

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.

[CVSS Guide] CVSS (2007), *A complete Guide to the Common Vulnerability Scoring System Version 2.0*. <http://www.first.org/cvss/cvss-guide.pdf>

3 Определения

3.1 Термины, определенные в других документах

3.1.1 уязвимость (vulnerability) [b-ITU-T X.1500]: Любое слабое место, которое может быть использовано для нарушения целостности системы или информации, которая в ней содержится.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 доступ (access): Возможность субъекта рассматривать объект, изменять его или устанавливать с ним связь. Доступ обеспечивает возможность обмена информацией между субъектом или объектом.

3.2.2 доступность (availability): Надежный и своевременный доступ к данным и ресурсам, осуществляемый авторизованными физическими лицами.

3.2.3 конфиденциальность (confidentiality): Принцип безопасности, служащий для обеспечения того, чтобы информация не раскрывалась неавторизованным субъектам.

3.2.4 целостность (integrity): Принцип безопасности, обеспечивающий, чтобы информация и системы не подвергались изменению по злому умыслу или случайно.

3.2.5 риск (risk): Относительное воздействие, которое обычно оказывается эксплуатацией уязвимости на среду пользователя.

3.2.6 угроза (threat): Вероятность или частота возникновения опасного события.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

A	Availability Impact		Воздействие на доступность
AC	Access Complexity		Сложность доступа
AR	Availability Requirement		Требование доступности
Au	Authentication		Аутентификация
AV	Access Vector		Вектор доступа
C	Confidentiality Impact		Воздействие на конфиденциальность
CDP	Collateral Damage Potential		Возможность сопутствующего ущерба
CR	Confidentiality Requirement		Требование конфиденциальности
CVSS	Common Vulnerability Scoring System		Система оценки общеизвестных уязвимостей
DMA	Direct Memory Access		Прямой доступ к памяти
DNS	Domain Name System		Система наименований доменов
E	Exploitability Impact		Воздействие на возможность эксплуатации
I	Integrity Impact		Воздействие на целостность
ICT	Information and Communication Technologies	ИКТ	Информационно-коммуникационные технологии
IM	Instant Messaging		Мгновенный обмен сообщениями
IR	Integrity Requirement		Требование целостности
JVN	Japan Vulnerability Notes		Сайт-портал Japan Vulnerability Notes
NVD	National Vulnerability Database		Национальная база данных об уязвимостях
RC	Report Confidence		Достоверность сообщения
RL	Remediation Level		Уровень устранения
RPC	Remote Procedure Call		Дистанционный вызов процедуры
SLA	Service Level Agreement		Соглашение об уровне обслуживания
TD	Target Distribution		Распределение целей
USB	Universal Serial Bus		Универсальная последовательная шина

5 Условные обозначения

Нет.

6 Использование CVSS

В настоящее время менеджерам по ИКТ требуется выявлять и оценивать уязвимости, имеющиеся во множестве различных аппаратных и программных платформ. Им необходимо устанавливать приоритеты этих уязвимостей и устранять те из них, которые представляют наибольший риск. Однако, при наличии множества подлежащих исправлению уязвимостей, каждая из которых оценивается по разным шкалам, менеджерам по ИКТ трудно получить из этого огромного объема данных об уязвимостях информацию, позволяющую принять меры. Система оценки общеизвестных уязвимостей (CVSS) является открытой структурой, позволяющей решить данную проблему. Она обеспечивает следующие преимущества:

- Стандартизованные оценки уязвимости: если организация нормирует оценки уязвимости по всем своим программным и аппаратным платформам, она может использовать единую политику управления уязвимостями. Данная политика может быть сходна с соглашением об уровне обслуживания (SLA), в котором установлено, как быстро должна быть валидирована эксплуатация конкретной уязвимости и как быстро она должна быть устранена.
- Открытую структуру: если уязвимости присвоена какая-либо произвольная оценка, это может поставить пользователей в затруднительное положение. Возникает вопрос: на основании каких свойств присвоена эта оценка, и чем она отличается от совсем недавно выданной оценки? Благодаря CVSS каждый может выяснить индивидуальные характеристики уязвимости, использованные для получения оценки.
- Установленный приоритет риска: при вычислении оценки среды уязвимость становится связанной с контекстом. То есть теперь оценки уязвимости отражают фактический риск для той или иной организации. Пользователи сознают, насколько серьезна данная уязвимость по отношению к другим уязвимостям.

6.1 Описание CVSS

Как показано на рисунке 1, система CVSS состоит их трех групп, в каждую из которых входит ряд показателей: группы базовых показателей, группы временны́х показателей и группы показателей среды.

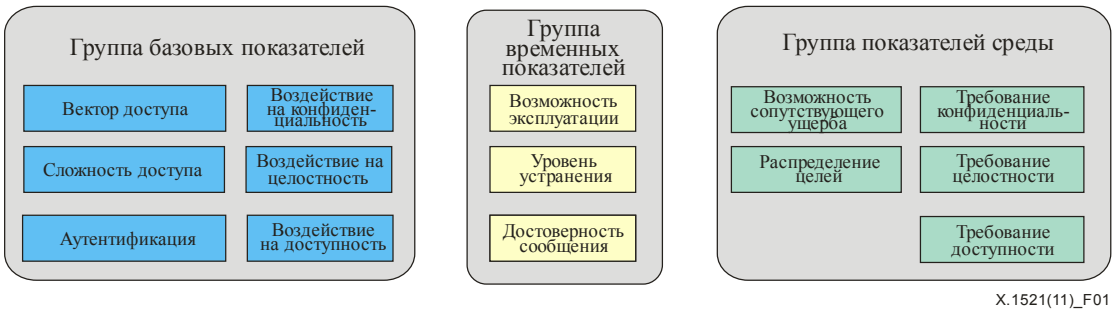

Рисунок 1 – Группы показателей системы CVSS

Ниже приведено описание этих групп показателей:

- Базовые показатели: отражают основные внутренние характеристики уязвимости, которые не изменяются во времени и не зависят от среды пользователей. Базовые показатели рассматриваются в пункте 6.5.
- Временны́е показатели: отражают характеристики уязвимости, которые изменяются во времени, но не зависят от среды пользователей. Временны́е показатели рассматриваются в пункте 6.6.
- Показатели среды: отражают характеристики уязвимости, которые относятся к конкретной среде пользователя и характерны только для нее. Показатели среды рассматриваются в пункте 6.7.

Группа базовых показателей CVSS предназначена для определения и представления основных характеристик уязвимости. Данный объективный метод описания уязвимостей дает пользователям четкое и интуитивно понятное представление об уязвимости. Кроме того, пользователи могут задействовать временны́е показатели и показатели среды для обеспечения связанной с контекстом информации, которая более точно отражает риск для их уникальной среды. Благодаря этому пользователи, старающиеся снизить риски, которые связаны с уязвимостями, могут принимать более обоснованные решения.

6.2 Работа CVSS

Как показано на рисунке 2, ниже, после того как базовым показателям присвоены значения, с помощью базовой формулы вычисляется оценка, находящаяся в пределах от 0 до 10, а также создается вектор. Этот вектор способствует обеспечению "открытого" характера структуры. Вектор – это тестовая строка, в которой содержатся присвоенные каждому показателю значения. Он используется для точного представления информации о том, как получена оценка по каждой уязвимости. Поэтому вместе с оценкой уязвимости всегда следует указывать вектор. Более подробное объяснение, касающееся векторов, представлено в пункте 7.4.

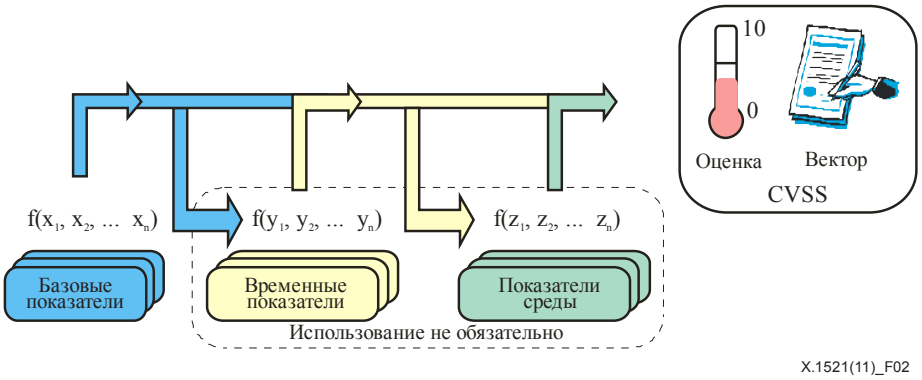

Рисунок 2 – Показатели и формулы CVSS

При желании можно улучшить базовую оценку путем присвоения значений временны́м показателям и показателям среды. Это целесообразно осуществить для того, чтобы обеспечить дополнительный контекст уязвимости путем более точного отражения риска, который представляет эта уязвимость для среды пользователя, однако это не является обязательным требованием. В зависимости от поставленной цели, может быть достаточным обеспечение базовой оценки и вектора.

Если необходима временна́я оценка, используется временна́я формула, в которой временны́е показатели объединяются с базовой оценкой, и получается временна́я оценка, находящаяся в пределах от 0 до 10. Аналогичным образом, если необходима оценка среды, используется формула среды, в которой показатели среды объединяются с временно́й оценкой, и получается оценка среды, находящаяся в пределах от 0 до 10. Подробное описание базовой и временно́й формул, а также формулы среды приведено в пункте 8.2.

6.3 Оценка CVSS

Как правило, базовые и временны́е показатели определяются аналитиками, осуществляющими подготовку бюллетеней с описанием уязвимостей, разработчиками продуктов в области безопасности или разработчиками приложений, потому что они обычно лучше осведомлены о характеристиках уязвимости, чем пользователи. В то же время показатели среды определяются пользователями, поскольку они лучше, чем кто бы то ни было, могут оценить потенциальное воздействие уязвимости в рамках своей собственной среды.

6.4 Пользователи CVSS

CVSS используется многими организациями, и каждая получает оценку своим способом. Ниже приведен ряд примеров:

- Поставщики бюллетеней с описанием уязвимости: как некоммерческие, так и коммерческие организации публикуют базовые и временны́е оценки и векторы CVSS в своих бесплатных бюллетенях с описанием уязвимости. В этих бюллетенях содержится много информации, в том числе дата обнаружения, затронутые системы и координаты разработчиков для получения рекомендаций относительно корректировки.
- Разработчики программных приложений: разработчики программных приложений предоставляют своим клиентам базовые оценки и векторы CVSS. Это позволяет разработчикам надлежащим образом информировать о серьезности уязвимостей их продуктов и помогает их клиентам эффективно управлять своими рисками ИКТ.

- Организации-пользователи: CVSS используется многими организациями частного сектора для принятия более обоснованных решений, связанных с управлением уязвимостями. Эти организации используют сканеры или технологии мониторинга, чтобы первыми локализовать уязвимости хост-компьютеров и приложений. Они объединяют эти данные с базовыми и временны́ми оценками, а также оценками среды CVSS, чтобы получить информацию о риске, более тесно связанную с контекстом, и устранить те уязвимости, которые представляют самый большой риск для их систем.
- Сканирование уязвимостей и управление уязвимостями: организации, осуществляющие управление уязвимостями, сканируют сети с целью обнаружения уязвимостей ИКТ. Они предоставляют базовые оценки CVSS для каждой уязвимости на каждом хост-компьютере. Организации-пользователи используют этот поток важнейших данных для более эффективного управления своей инфраструктурой ИКТ путем уменьшения отказов и защиты от угроз ИКТ, обусловленных злым умыслом или случайностью.
- Управление (рисками) безопасности: фирмы, занимающиеся управлением рисками безопасности, используют оценки CVSS в качестве основы для расчета уровня риска или угрозы для организации. Эти фирмы используют сложные приложения, в которых нередко сопряжены топология сети организации, данные об уязвимости и базы данных о ресурсах, обеспечивая своим клиентам более обоснованный взгляд на уровень их риска.
- Исследователи: открытая структура CVSS позволяет исследователям осуществлять статистический анализ уязвимостей и их свойств.

6.5 Группы показателей: базовые показатели

Группа базовых показателей отображает характеристики уязвимости, которые не изменяются со временем и не зависят от среды пользователей. Показатели "вектор доступа" (Access Vector), "сложность доступа" (Access Complexity) и "аутентификация" (Authentication) оценивают, как получить доступ к уязвимости, и требуются ли для ее эксплуатации дополнительные условия. Эти три показателя воздействия измеряют возможное прямое воздействие уязвимости на ресурс ИКТ в случае эксплуатации уязвимости. При этом воздействие определяется независимо с точки зрения степени потери конфиденциальности, целостности и доступности. Это означает, например, что эксплуатация уязвимости могла бы вызвать частичную потерю целостности и доступности, но не привести к потере конфиденциальности.

6.5.1 Показатель "вектор доступа" (Access Vector, AV)

Этот показатель отражает то, как эксплуатируется уязвимость. Возможные значения этого показателя перечислены в таблице 1. Чем более удаленным от хост-компьютера может быть злоумышленник при атаке на хост-компьютер, тем выше оценка уязвимости.

Таблица 1 – Значения показателя "вектора доступа"

Значение показателя	Описание
Локальный (Local, L)	В случае уязвимости, которая может эксплуатироваться только при локальном доступе, злоумышленник должен иметь либо физический доступ к уязвимой системе, либо локальную учетная запись. Примерами уязвимостей с возможностью локальной эксплуатации могут служить атаки на внешние устройства, например, атаки Firewire/USB DMA, и локальное повышение привилегий (например, выполнение команды от имени суперпользователя (sudo)).
Соседняя сеть (Adjacent network, A)	В случае уязвимости, которая может эксплуатироваться при доступе из соседней сети, злоумышленник должен иметь доступ либо к домену многоадресной рассылки, либо к домену коллизий, относящимися к уязвимому программному обеспечению. Примерами локальных сетей являются локальные IP-подсети, Bluetooth, IEEE 802.11 и локальный сегмент Ethernet-сети.
Сетевой (Network, N)	В случае уязвимости, которая может эксплуатироваться при сетевом доступе, программное обеспечение ограничено сетевым стеком, а злоумышленник не должен иметь локальный сетевой доступ или локальный доступ. Такие уязвимости часто называют уязвимостями "с возможностью дистанционной эксплуатации". Примером такой сетевой атаки служит переполнение буфера RPC.

6.5.2 Показатель "сложность доступа" (Access complexity, AC)

Этим показателем измеряется сложность атаки, требующейся для эксплуатации уязвимости, если злоумышленник получил доступ к целевой системе. Например, рассмотрим переполнение буфера при использовании того или иного сервиса интернета: как только целевая система локализована, злоумышленник может в любой момент начать эксплуатацию уязвимости.

В то же время для эксплуатации других уязвимостей могут требоваться дополнительные действия. Например, уязвимость в почтовом клиенте может эксплуатироваться только после того, как пользователь скачает и откроет зараженное приложение. Возможные значения этого показателя перечислены в таблице 2. Чем ниже требуемая сложность, тем выше оценка уязвимости.

Таблица 2 – Значения показателя "сложность доступа"

Значение показателя	Описание
Высокая (High, H)	Существуют особые условия доступа, например: • В большинстве конфигураций злоумышленник должен иметь предварительно повышенные привилегии или обмануть, наряду с атакуемой системой, дополнительные системы (например, путем захвата DNS). • Атака основана на методах социальной инженерии, которые обычно легко обнаруживаются хорошо осведомленными людьми. Например, жертва должна выполнить некоторые подозрительные или нетипичные действия. • Уязвимая конфигурация на практике встречается очень редко. • При наличии условия состязания, окно является очень узким.
Средняя (Medium, M)	Условия доступа являются до некоторой степени особыми, например: • Злоумышленники ограничены группой систем или пользователей, которые имеют некоторый уровень авторизации, и, возможно, являются недоверенными. • Для успешного осуществления атаки должна быть заранее собрана некоторая информация. • Затронутая конфигурация не является стандартной и общеизвестной (например, уязвимость существует, когда сервер проводит аутентификацию учетной записи пользователя по одной специальной схеме, но не существует при использовании другой схемы). • Для атаки требуется небольшой объем навыков социальной инженерии, с помощью которых можно случайно обмануть осмотрительных пользователей (например, атаки фишинга, которые изменяют статусную строку веб-браузера и показывают ложную ссылку, которая должна быть в списке контактов какого-либо пользователя, прежде чем отправить IM-эксплойт).
Низкая (Low, L)	Не существует специальных условий доступа и особых обстоятельств, например: • Затронутому продукту, как правило, требуется доступ к большому количеству систем и пользователей, причем доступ может быть анонимным или недоверенным (например, соединенный с интернетом веб-сервер или почтовый сервер). • Затронутая конфигурация является стандартной или повсеместно распространенной. • Атаку можно провести вручную, обладая небольшим количеством навыков. Требуется немного дополнительной информации. • Условие состязания является легко выполнимым (т. е. формально это состязание, однако в нем легко победить).

6.5.3 Показатель "аутентификация" (Authentication, Au)

Этим показателем измеряется количество раз, которое злоумышленник должен аутентифицироваться в целевой системе, чтобы эксплуатировать уязвимость. Этот показатель не оценивает силу или сложность самого процесса аутентификации, а касается только необходимости для злоумышленника предъявить регистрационные данные, прежде чем уязвимость можно будет эксплуатировать. Возможные значения этого показателя перечислены в таблице 3. Чем меньше требуемое число случаев аутентификации, тем выше оценка уязвимости.

Таблица 3 – Значения показателя "аутентификация"

Значение показателя	Описание
Многократная (Multiple, M)	Для эксплуатации уязвимости злоумышленник должен аутентифицироваться два и более раз, даже если одни и те же регистрационные данные используются несколько раз. Примером может служить аутентификация злоумышленника в операционной системе, помимо предоставления регистрационных данных для доступа к приложению в данной системе.
Однократная (Single, S)	Для эксплуатации уязвимости злоумышленник должен войти в систему (например, через командную строку, сеанс удаленного рабочего стола или веб-интерфейс).
Отсутствует (None, N)	Для эксплуатации уязвимости аутентификация не требуется.

Этот показатель следует применять с учетом аутентификации, которую должен пройти злоумышленник до того, как провести атаку. Например, если почтовый сервер уязвим с помощью команд, которые можно исполнять до аутентификации пользователя, то этот показатель имеет значение "отсутствует" (None), потому что злоумышленник может провести атаку до того, как потребуются регистрационные данные. Если выполнение такой команды возможно только после успешной аутентификации, то показатель уязвимости должен иметь значение "Однократная" (Single) или "Многократная" (Multiple), в зависимости от того, какое число случаев аутентификации должно иметь место до того, как можно будет подать эту команду.

6.5.4 Показатель "воздействие на конфиденциальность" (Confidentiality impact, C)

Этим показателем измеряется воздействие успешной эксплуатации уязвимости на сохранение конфиденциальности. Под "конфиденциальностью" понимается ограничение доступа к информации и ее раскрытия только авторизованными пользователями, а также предотвращение доступа к информации или ее раскрытия неавторизованным пользователям. Возможные значения этого показателя перечислены в таблице 4. Чем больше воздействие на конфиденциальность, тем выше оценка уязвимости.

Таблица 4 – Значения показателя "воздействие на конфиденциальность"

Значение показателя	Описание
Отсутствует (None, N)	Отсутствует воздействие на конфиденциальность системы.
Частичное (Partial, P)	Имеется существенное раскрытие информации. Возможен доступ к некоторым системным файлам, но злоумышленник не имеет контроля над этой информацией, или же масштабы потерь невелики. Примером может служить уязвимость, которая вызывает разглашение лишь определенных таблиц в базе данных.
Полное (Complete, C)	Происходит полное раскрытие информации, что приводит к показу всех системных файлов. Злоумышленник может читать все системные данные (память, файлы и пр.).

6.5.5 Показатель "воздействие на целостность" (Integrity impact, I)

Этим показателем измеряется воздействие успешной эксплуатации уязвимости на целостность системы. Под "целостностью" понимается достоверность и гарантированная точность информации. Возможные значения этого показателя перечислены в таблице 5. Чем больше воздействие на целостность системы, тем выше оценка уязвимости.

Таблица 5 – Значения показателя "воздействие на целостность"

Значение показателя	Описание
Отсутствует (None, N)	Отсутствует воздействие на целостность системы.
Частичное (Partial, P)	Возможно изменение некоторых системных файлов или информации, но злоумышленник не имеет контроля над изменяемыми данными, или область его влияния ограничена. Например, системные файлы или файлы приложений могут быть перезаписаны или изменены, но злоумышленник не может выбрать файлы, которые будут изменены, или может изменять файлы в ограниченном контексте или масштабе.
Полное (Complete, C)	Целостность системы полностью нарушена. Защита системы полностью ослаблена, в результате чего система полностью взломана. Злоумышленник может изменять любые файлы целевой системы.

6.5.6 Показатель "воздействие на доступность" (Availability impact, A)

Этим показателем измеряется воздействие успешной эксплуатации уязвимости на доступность системы, Под "доступностью" понимается возможность доступа к информационным ресурсам. Атаки, при которых расходуется пропускная способность сети, рабочие циклы процессора или дисковое пространство, воздействуют на доступность системы. Возможные значения этого показателя перечислены в таблице 6. Чем больше воздействие на доступность системы, тем выше оценка уязвимости.

Таблица 6 – Значения показателя "воздействие на доступность"

Значение показателя	Описание
Отсутствует (None, N)	Отсутствует воздействие на доступность системы.
Частичное (Partial, P)	Происходит уменьшение производительности или сбои в доступности ресурса. Примером может служить сетевая атака типа флуд, которая позволяет ограничить число успешных соединений с сервисом интернета.
Полное (Complete, C)	Происходит полное отключение затронутой системы. Злоумышленник может сделать ресурс полностью недоступным.

6.6 Временны́е показатели

Угроза, связанная с уязвимостью, может изменяться со временем. Имеется три таких фактора, которые учитываются в CVSS: подтверждение технических деталей уязвимости, статус устранения уязвимости и доступность кода эксплуатации или метода эксплуатации. Так как временны́е показатели являются необязательными, каждый из них содержит одно значение, которое не влияет на оценку. Это значение используется в тех случаях, когда пользователь полагает, что конкретный показатель не применим, и хочет его пропустить.

6.6.1 Показатель "возможность эксплуатации" (Exploitability, E)

Этим показателем измеряется существующее состояние доступности кода или метода эксплуатации. Если легкий в использовании код эксплуатации является общедоступным, то число потенциальных злоумышленников возрастает за счет добавления неквалифицированных злоумышленников, что тем самым увеличивает серьезность уязвимости.

Изначально реальная эксплуатация уязвимости может допускаться только теоретически. Затем может последовать публикация кода доказательства правильности концепции, функционального кода эксплойта или достаточного объема технических деталей, необходимых для эксплуатации уязвимости. Кроме того, может произойти развитие доступного кода эксплойта, который из кода, демонстрирующего правильность концепции, превратится в код эксплойта, при котором возможна систематическая успешная эксплуатация уязвимости. В некоторых особо серьезных случаях доставка этого кода может быть осуществлена с помощью сетевых червей или вирусов. Возможные значения этого показателя перечислены в таблице 7. Чем легче эксплуатировать уязвимость, тем выше оценка уязвимости.

Таблица 7 – Значения показателя "воздействие на возможность эксплуатации"

Значение показателя	Описание
Непроверенная (Unproven, U)	Код эксплойта не доступен или эксплуатация возможна лишь теоретически.
Доказана правильность концепции (Proof-of-Concept, POC)	Доступен код эксплойта, доказывающий правильность концепции, или существует демонстрация атаки, которая не применима в большинстве систем. Код или метод действуют не во всех ситуациях, и для их использования может потребоваться существенное изменение, внесенное квалифицированным злоумышленником.
Функциональная (Functional, F)	Функциональный код эксплойта доступен и применим в большинстве ситуаций, где существует уязвимость.
Высокая (High, H)	Уязвимость можно эксплуатировать с помощью функционального мобильного автономного кода, или эксплойт не нужен (запуск вручную) и детали широко известны. Код эксплуатации работает в любой ситуации или его активная доставка осуществляется мобильным автономным агентом (например, червем или вирусом).
Не определено (Not Defined, ND)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле данный показатель будет пропущен.

6.6.2 Показатель "уровень устранения" (Remediation level, RL)

Важным фактором установления приоритета является уровень устранения уязвимости. Типичная уязвимость обычно не имеет корректировки, когда информация о ней публикуется впервые. Обходные приемы или модули оперативной коррекции могут обеспечить вре́менное устранение уязвимости до того момента, когда будет выпущена официальная корректировка или обновление. Каждая из указанных выше мер приводит к уменьшению временно́й оценки и отражает снижение срочности проблемы по мере ее окончательного устранения. Возможные значения этого показателя перечислены в таблице 8. Чем менее официальный характер носит исправление или чем более оно вре́менное, тем выше оценка уязвимости.

Таблица 8 – Значения показателя "уровень устранения"

Значение показателя	Описание
Официальное исправление (Official Fix, OF)	Доступно готовое решение от разработчика, который либо выпустил официальную корректировку, либо предоставил обновление.
Вре́менное исправление (Temporary Fix, TF)	Доступно официальное вре́менное исправление. Например, разработчик выпустил временный модуль оперативной коррекции, средство или опубликовал обходной прием.
Обходной прием (Workaround, W)	Доступно неофициальное решение, которое предоставлено третьей стороной. В некоторых случаях пользователи затронутой технологии создают собственную корректировку или принимают меры для нахождения обходного приема или каким-либо другим способом уменьшают влияние уязвимости.
Недоступно (Unavailable, U)	Решение либо недоступно, либо его невозможно применить.
Не определено (Not defined, ND)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле данный показатель будет пропущен.

6.6.3 Показатель "достоверность сообщения" (Report confidence, RC)

Этим показателем измеряется степень достоверности информации о существовании уязвимости и доверия к известным техническим деталям. Иногда публикуется только информации о существовании уязвимости без указания конкретных деталей. Позднее уязвимость может быть подкреплена свидетельствами и затем подтверждена, получив признание автора или разработчика затронутой технологии. Острота проблемы уязвимости выше, если о ее существовании достоверно известно. Этот показатель отражает также уровень технических знаний, доступных потенциальным злоумышленникам. Возможные значения этого показателя перечислены в таблице 9. Чем более подробно эксплуатация уязвимости валидирована разработчиком или другими надежными источниками, тем выше оценка.

Таблица 9 – Значения показателя "достоверность сообщения"

Значение показателя	Описание
Не подтверждена (Unconfirmed, UC)	Существует единственный неподтвержденный источник или несколько противоречивых сообщений. Достоверность степени валидации этих сообщений мала. Одним из примером является слух, появившийся в хакерских кругах.
Не подкреплена доказательствами (Uncorroborated, UR)	Существует множество неофициальных источников, в том числе, возможно, независимых компаний в области безопасности или исследовательских организаций. На этом этапе могут существовать противоречивые технические детали или некоторая иная затянувшаяся неопределенность.
Подтверждена (Confirmed, C)	Уязвимость признана разработчиком или автором затронутой технологии. Это значение также может быть присвоено уязвимости, если ее существование подтверждено каким-то внешним событием, например, публикацией функционального кода эксплойта или кода эксплойта, доказывающего правильность концепции, либо масштабной эксплуатацией.
Не определено (Not defined, ND)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле данный показатель будет пропущен.

6.7 Показатели среды

Различные среды могут оказывать огромное влияние на риск, который представляет собой наличие уязвимости для организации и заинтересованных сторон. Группа показателей среды CVSS отражает характеристики уязвимости, которые связаны со ИКТ-средой пользователя. Так как показатели среды являются необязательными, каждый из них содержит одно значение, которое не влияет на оценку. Это значение используется в тех случаях, когда пользователь полагает, что конкретный показатель не применим, и хочет его пропустить.

6.7.1 Показатель "возможность сопутствующего ущерба" (Collateral damage potential, CDP)

Этим показателем измеряется возможность человеческих жертв или утраты физических ресурсов путем повреждения или кражи имущества или оборудования. С его помощью могут также оцениваться экономические потери, связанные с производительностью или доходом. Возможные значения этого показателя перечислены в таблице 10. Чем больше возможность повреждения, тем выше оценка уязвимости.

Таблица 10 – Значения показателя "возможность сопутствующего ущерба"

Значение показателя	Описание
Отсутствует (None, N)	Отсутствует возможность человеческих жертв, утраты физических ресурсов, снижения производительности или дохода.
Низкая (Low, L)	Успешная эксплуатация этой уязвимости может нанести незначительный ущерб здоровью или имуществу. Либо же может иметь место незначительная потеря дохода или производительности в организации.
От низкой до средней (Low-medium, LM)	Успешная эксплуатация этой уязвимости может нанести умеренный ущерб здоровью или имуществу. Либо же может иметь место умеренная потеря дохода или производительности в организации.
От средней до высокой (Medium-high, MH)	Успешная эксплуатация этой уязвимости может нанести серьезный ущерб здоровью или имуществу, либо привести к гибели людей или утрате имущества. Либо же может иметь место серьезная потеря дохода или производительности в организации.
Высокая (High, H)	Успешная эксплуатация этой уязвимости может нанести непоправимый ущерб здоровью или имуществу и привести к гибели людей или утрате имущества. Либо же может иметь место катастрофическая потеря дохода или производительности в организации.
Не определено (Not defined, ND)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле данный показатель будет пропущен.

Очевидно, что каждая организация должна сама для себя определить точное значение понятий "незначительный, умеренный, серьезный и непоправимый (катастрофический)".

6.7.2 Показатель "распределение целей" (Target distribution, TD)

Этим показателем измеряется доля уязвимых систем от всех имеющихся систем. Он используется как зависящий от среды индикатор, чтобы приблизительно определить процентную долю систем, которые могут оказаться затронутыми данной уязвимостью. Возможные значения этого показателя перечислены в таблице 11. Чем больше доля уязвимых систем, тем выше оценка.

Таблица 11 – Значения показателя "распределение целей"

Значение показателя	Описание
Отсутствует (None, N)	Целевых систем нет, или цели настолько специализированы, что существуют только в лабораторных условиях. Фактически, риску подвержено 0% систем среды.
Низкое (Low, L)	В данной среде имеются цели, но в небольшом количестве. Риску подвержено от 1% до 25% всех систем среды.
Среднее (Medium, M)	В данной среде имеются цели, но в среднем количестве Риску подвержено от 26% до 75% всех систем среды.
Высокое (High, H)	В данной среде имеется большое количество целей. Риску подвержено от 76% до 100% всех систем среды.
Не определено (Not Defined, ND)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле данный показатель будет пропущен.

6.7.3 Показатели требований безопасности (CR, IR, AR)

Эти показатели позволяют аналитику адаптировать CVSS-оценку в зависимости от важности затронутого ресурса ИКТ для организации-пользователя, выраженной через конфиденциальность, целостность и доступность. Это означает, что если какой-либо ресурс ИКТ отвечает за бизнес-функцию, для которой наиболее важна доступность, аналитик может присвоить доступности большее значение, по сравнению с конфиденциальностью и целостностью. Каждое требование безопасности имеет три возможных значения: "низкое" (low), "среднее" (medium) или "высокое" (high).

Полное влияние на оценку среды определяется соответствующими базовыми показателями воздействия (следует отметить, что сами базовые показатели воздействия на конфиденциальность, целостность и доступность не изменяются). Это означает, что эти три показателя требований безопасности изменяют оценку среды путем изменения взвешенных значений (базовых) показателей воздействия на конфиденциальность, целостность и доступность. Например, если значение показателя "требование конфиденциальности" (confidentiality requirement, CR) равно "высокое" (high), то взвешенное значение показателя "воздействие на конфиденциальность" (confidentiality impact, C) увеличится. Соответственно, если значение показателя "требование конфиденциальности" равно "низкое" (low), то взвешенное значение показателя "воздействие на конфиденциальность" уменьшится. Если значение показателя "требование конфиденциальности" равно "среднее" (medium), то взвешенное значение показателя "воздействие на конфиденциальность" не изменится. Такие же правила применяются и к требованиям целостности и доступности.

Отметим, что требование конфиденциальности не влияет на оценку среды, если для (базового) показателя "воздействие на конфиденциальность" установлено значение "отсутствует" (none). Кроме того, увеличение значения показателя "требование конфиденциальности" со "среднее" до "высокое" не изменит оценку среды, если (базовым) показателям воздействия присвоены значения "полное" (complete), т.к. в этом случае часть оценки воздействия (часть базовой оценки, которая определяет воздействие), уже равна максимальному значению 10.

Возможные значения требований безопасности перечислены в таблице 12. Для краткости для всех трех показателей используется одна и та же таблица. Чем больше требование безопасности, тем выше оценка (помните, что стандартным значением является "среднее"). Эти показатели изменяют оценку на ±2,5.

Таблица 12 – Значения показателей требований безопасности

Значение показателя	Описание
Низкое (Low, L)	Потеря [конфиденциальности | целостности | доступности], вероятно, оказывает ограниченное неблагоприятное влияние на организацию или частных лиц, связанных с организацией (например, сотрудников и клиентов).
Среднее (Medium, M)	Потеря [конфиденциальности | целостности | доступности], вероятно, оказывает серьезное неблагоприятное влияние на организацию или частных лиц, связанных с организацией (например, сотрудников и клиентов).
Высокое (High, H)	Потеря [конфиденциальности | целостности | доступности], вероятно, оказывает катастрофическое неблагоприятное влияние на организацию или частных лиц, связанных с организацией (например, сотрудников и клиентов).
Не определено (Not defined, ND)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле данный показатель будет пропущен.

Во многих организациях ресурсам ИКТ присвоены коэффициенты критичности, исходя из положения в сети, бизнес-функции и возможности человеческих жертв или потери дохода. Например, правительство США относит каждый несекретный ресурс ИКТ к группе ресурсов, называемой "системой". Каждой "системе" должно быть присвоено три коэффициента "возможного воздействия", отражающих возможное воздействие, которому подвергнется организация в случае взлома "системы", в соответствии с тремя целевыми показателями: конфиденциальность, целостность и доступность. Таким образом, в правительстве США каждый несекретный ресурс ИКТ имеет низкий, средний или высокий коэффициент возможного воздействия по отношению к показателям безопасности, связанным с конфиденциальностью, целостностью и доступностью. Эта система оценок описана в публикации "Федеральные стандарты обработки информации" (FIPS) №199. CVSS соответствует этой общей модели FIPS 199, но в ней не требуется, чтобы организации использовали какую-либо конкретную систему для присвоения низких, средних или высоких коэффициентов.

6.8 Базовый вектор, временной вектор и вектор среды

По каждому показателю в векторе содержится сокращенное название показателя, за которым следует знак ":" (двоеточие), а затем – сокращенное значение показателя. Эти показатели перечислены в векторе в заранее установленном порядке, при этом для разделения показателей используется символ "/" (косая черта). Если временной показатель или показатель среды не используется, то ему присваивается значение "ND" (не определено). Базовый вектор, временной вектор и вектор среды представлены в таблице 13, ниже.

Таблица 13 – Базовый вектор, временной вектор и вектор среды

Значение показателя	Описание
Базовый вектор	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Временной вектор	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
Вектор среды	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

Например, уязвимость со значениями базовых показателей "вектор доступа: низкий, сложность доступа: средняя, аутентификация: отсутствует, воздействие на конфиденциальность: отсутствует, воздействие на целостность: частичное, воздействие на доступность: полное" (Access Vector: Low, Access Complexity: Medium, Authentication: None, Confidentiality Impact: None, Integrity Impact: Partial, Availability Impact: Complete) имеет следующий базовый вектор: "AV:L/AC:M/Au:N/C:N/I:P/A:C."

6.9 Руководящие указания по вычислению оценки

Ниже представлены руководящие указания, которые помогут аналитикам при вычислении оценок уязвимостей.

6.9.1 Общие положения

Рекомендация по оценке № 1: При оценке уязвимости следует устранить влияние других уязвимостей. Это означает, что каждую уязвимость следует оценивать независимо.

Рекомендация по оценке № 2: При вычислении оценки уязвимости следует принимать во внимание только прямое воздействие на целевой хост-компьютер. Например, рассмотрим уязвимость, связанную с межсайтовым выполнением сценариев: воздействие на систему пользователя могло бы быть значительно больше, чем воздействие на целевой хост–компьютер. В то же время это непрямое воздействие. Уязвимости, связанные с межсайтовым выполнением сценариев, следует оценивать как уязвимости, при которых отсутствует воздействие на конфиденциальность и доступность и имеется частичное воздействие на целостность.

Рекомендация по оценке № 3: Многие приложения, такие как приложения веб-серверов, могут выполняться с различными привилегиями, и при оценке воздействия делается предположение относительно того, какие привилегии используются. Поэтому уязвимости следует оценивать по наиболее широко используемым привилегиям. При выполнении приложений может и не соблюдаться передовой опыт безопасности, особенно для клиентских приложений, которые нередко выполняются с привилегиями корневого пользователя (администратора). Если аналитики не уверены, какой уровень привилегий является наиболее широко используемым, предполагается исходить из стандартной конфигурации.

Рекомендация по оценке № 4: При вычислении оценки уязвимости, которая имеет несколько способов эксплуатации (векторов атаки), аналитику следует выбрать тот метод эксплуатации, который оказывает самое большое воздействие, а не метод, который используется чаще или который легче реализовать. Например, если функциональный код эксплойта существует для одной платформы и не существует для другой платформы, то показателю "возможность эксплуатации" (Exploitability) следует присвоить значение "функциональная" (Functional). Если два отдельных варианта продукта разрабатываются параллельно (например, PHP 4.x и PHP 5.x), и исправление существует только для одного из этих вариантов, то показателю "уровень исправления" (Remediation Level) следует присвоить значение "недоступно" (Unavailable).

6.9.2 Базовые показатели

6.9.2.1 Вектор доступа

Рекомендация по оценке № 5: Если уязвимость может эксплуатироваться локально и через сеть, следует выбрать значение "сетевой" (Network). Если уязвимость может эксплуатироваться локально и из соседних сетей, но не из удаленных сетей, следует выбрать значение "соседняя сеть" (Adjacent Network). Если уязвимость может эксплуатироваться из соседних и удаленных сетей, то следует выбрать значение "сетевой" (Network).

Рекомендация по оценке № 6: Во многих клиентских приложениях и утилитах имеются локальные уязвимости, которые могут эксплуатироваться дистанционно: либо при активном участии пользователя, либо автоматически. Например, утилиты распаковки архивов и сканеры вирусов автоматически сканируют входящие сообщения электронной почты. Кроме того, уязвимости во вспомогательных приложениях (пакетах офисных приложений, приложениях для просмотра изображений, медиапроигрывателях и др.) эксплуатируются при пересылке по электронной почте или загрузке с веб-сайтов вредоносных файлов. Поэтому для таких уязвимостей показатель "вектор доступа" (Access Vector) аналитикам следует оценивать как "сетевой" (Network).

6.9.2.2 Аутентификация

Рекомендация по оценке № 7: Если уязвимость существует в схеме аутентификации (например, PAM, Kerberos) или в анонимном сервисе (например, общедоступный FTP-сервер), показатель следует оценивать как " отсутствует" (None), так как злоумышленник может эксплуатировать уязвимость, не предоставляя действительные регистрационные данные. При наличии стандартной учетной записи пользователя показатель "аутентификация" (Authentication) можно оценить как "однократная" (Single) или "многократная" (Multiple), в зависимости от случая, однако если регистрационные данные разглашены, показатель "возможность эксплуатации" (Exploitability) может иметь значение "высокая" (High).

Рекомендация по оценке № 8: Важно отметить, что показатель "аутентификация" (Authentication) отличается от показателя "вектор доступа" (Access Vector). В показателе "аутентификация" требования аутентификации учитываются с того момента, как осуществлен доступ в систему. В частности, для локально эксплуатируемых уязвимостей значение "однократная" (Single) или "многократная" (Multiple) следует присвоить данному показателю только в том случае, если необходима дополнительная аутентификация, помимо той аутентификации, которая требуется при регистрации в системе. Примером локальной эксплуатации уязвимости, требующей аутентификация, является эксплуатация уязвимости, затрагивающей ядро базы данных, при которой прослушиваются сокеты Unix-домена (или ряда других портов интерфейсов, не являющихся сетевыми). Если пользователь должен быть аутентифицирован как зарегистрированный пользователь базы данных, для того чтобы эксплуатировать уязвимость, то данному показателю следует присвоить значение "однократная" (Single).

6.9.2.3 Воздействие на конфиденциальность, целостность и доступность

Рекомендация по оценке № 9: Уязвимости, при которых обеспечивается доступ на корневом уровне, следует оценивать как полную потерю конфиденциальности, целостности и доступности, а уязвимости, которые предоставляют доступ с пользовательским уровнем привилегий, оцениваются как частичная потеря конфиденциальности, целостности и уязвимости. Например, нарушение целостности, которое позволяет злоумышленнику изменять файл паролей операционной системы, следует оценивать как полное нарушение конфиденциальности, целостности и доступности.

Рекомендация по оценке № 10: Уязвимости с частичной или полной потерей целостности также могут оказывать воздействие на доступность. Например, злоумышленник, имеющий возможность изменять записи, вероятно, может также удалять их.

6.10 Формулы

Формулы и алгоритмы для оценки групп базовых и временны́х показателей, а также показателей среды описаны ниже. Дополнительная информация о составлении и тестировании этих формул представлена по адресу: http://www.first.org/cvss. В Дополнении I приведены три примера со сценариями использования этих формул.

6.10.1 Базовая формула

Базовая формула является основой для вычисления CVSS и имеет следующий вид (версия 2.10):

```
BaseScore = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))
Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
Exploitability = 20*AccessVector*AccessComplexity*Authentication
f(impact) = 0 if Impact=0, 1.176 otherwise
AccessVector     = case AccessVector of
                       requires local access: 0.395
                       adjacent network accessible: 0.646
                       network accessible: 1.0
AccessComplexity = case AccessComplexity of
                       high: 0.35
                       medium: 0.61
                       low: 0.71
Authentication   = case Authentication of
                       requires multiple instances of authentication: 0.45
                       requires single instance of authentication: 0.56
                       requires no authentication: 0.704
ConfImpact       = case ConfidentialityImpact of
                       none:              0.000
                       partial:           0.275
                       complete:          0.660
IntegImpact      = case IntegrityImpact of
                       none:              0.000
                       partial:           0.275
                       complete:          0.660
AvailImpact      = case AvailabilityImpact of
                       none:              0.000
                       partial:           0.275
                       complete:          0.660
```

6.10.2 Временна́я формула

При использовании временно́й формулы временны́е показатели объединяются с базовой оценкой, и получается временна́я оценка, находящаяся в пределах от 0 до 10. Кроме того, полученная по этой формуле временна́я оценка не превышает базовую и не более чем на 33% меньше ее. Временна́я формула имеет следующий вид:

```
TemporalScore = round_to_1_decimal(BaseScore*Exploitability
              *RemediationLevel*ReportConfidence)
Exploitability   = case Exploitability of
                        unproven:             0.85
                        proof-of-concept:     0.90
                        functional:           0.95
                        high:                 1.00
                        not defined:          1.00

RemediationLevel = case RemediationLevel of
                        official-fix:         0.87
                        temporary-fix:        0.90
                        workaround:           0.95
                        unavailable:          1.00
                        not defined:          1.00

ReportConfidence = case ReportConfidence of
                        unconfirmed:          0.90
                        uncorroborated:       0.95
                        confirmed:            1.00
                        not defined:          1.00
```

6.10.3 Формула среды

При использовании формулы среды показатели среды объединяются с временно́й оценкой, и получается оценка среды, находящаяся в пределах от 0 до 10. Кроме того, полученная по этой формуле оценка не превышает временну́ю оценку. Формула среды имеет следующий вид:

```
EnvironmentalScore = round_to_1_decimal((AdjustedTemporal+
(10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)
AdjustedTemporal = TemporalScore recomputed with the BaseScores Impact
sub-equation replaced with the AdjustedImpact equation
AdjustedImpact = min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)
               *(1-AvailImpact*AvailReq)))
CollateralDamagePotential = case CollateralDamagePotential of
                                none:            0.0
                                low:             0.1
                                low-medium:      0.3
                                medium-high:     0.4
                                high:            0.5
                                not defined:     0.0

TargetDistribution        = case TargetDistribution of
                                none:            0.00
                                low:             0.25
                                medium:          0.75
                                high:            1.00
                                not defined:     1.00
ConfReq                    = case ConfReq of
                                low:             0.5
                                medium:          1.0
                                high:            1.51
                                not defined:     1.0
IntegReq                  = case IntegReq of
                                low:             0.5
                                medium:          1.0
                                high:            1.51
                                not defined:     1.0
AvailReq                  = case AvailReq of
                                low:             0.5
                                medium:          1.0
                                high:            1.51
                                not defined:     1.0
```

7 Дополнительные ресурсы

В Дополнении II представлен список ресурсов, которые могут быть полезны при реализации CVSS. В этом списке содержатся ссылки на бюллетени с описанием уязвимостей и на несколько калькуляторов CVSS. Бюллетени с описанием уязвимостей удобны при поиске подробной информации о конкретной уязвимости. Калькуляторы CVSS необходимы для вычисления собственных базовых и временны́х оценок или оценок среды.

Дополнение I

Примеры использования CVSS

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Ниже представлены примеры использования CVSS для трех различных уязвимостей.

I.1 Уязвимость CVE-2002-0392

Рассмотрим уязвимость CVE-2002-0392: Нарушение целостности данных в памяти при блочном кодировании на веб-сервере Apache. В июне 2002 года в механизме обработки веб-сервером Apache запросов, закодированных с помощью блочного кодирования, была обнаружена уязвимость. Организация-фонд Apache Foundation сообщила, что успешная эксплуатация этой уязвимости может в некоторых случаях привести к отказу в обслуживании, а в других случаях – позволить выполнить произвольный код с привилегиями веб-сервера.

Поскольку эту уязвимость можно эксплуатировать удаленно, показатель "вектор доступа" (Access Vector) принимает значение "сетевой" (Network). Показатель "сложность доступа" (Access Complexity) имеет значение "низкая" (Low), потому что для успешной эксплуатации не требуются дополнительные условия. Злоумышленник должен только подготовить сообщение-эксплойт для прослушивающего процесса веб-сервера Apache. Для эксплуатации данной уязвимости аутентификация не требуется (любой пользователь интернета может подключиться к веб-серверу), поэтому показатель "аутентификация" (Authentication) равен "отсутствует" (None).

В связи с тем, что уязвимость может эксплуатироваться различными методами с различными последствиями, необходимо вычислить оценки для каждого метода и использовать наибольше значение.

Если при эксплуатации уязвимости выполняется произвольный код с привилегиями веб-сервера, и вследствие этого изменяется веб-контент и возможно, просматривается информация локальных пользователей и информация о конфигурации (в том числе, параметры подключения и пароли для внутренних баз данных), то показатели "воздействие на конфиденциальность" (Confidentiality Impact) и "воздействие на целостность" (Integrity Impact) имеют значение "частичное" (Partial). Эти показатели вместе дают базовую оценку 6,4.

Если эксплуатация уязвимости вызывает отказ в обслуживании, то показатель "воздействие на доступность" (Availability Impact) имеет значение "полное" (Complete). Эти показатели вместе дают базовую оценку 7,8. Так как это самая высокая возможная базовая оценка для разных вариантов эксплуатации уязвимости, то именно она используется как базовая оценка данной уязвимости.

Таким образом, базовый вектор этой уязвимости имеет вид: AV:N/AC:L/Au:N/C:N/I:N/A:C.

Известно, что код эксплойта существует, поэтому показатель "возможность эксплуатации" (Exploitability) имеет значение "функциональная" (Functional). Фонд Apache выпустил корректировки для этой уязвимости (доступно для версий 1.3 и 2.0), поэтому показатель "уровень устранения" (Remediation Level) равен "официальное исправление" (Official-Fix). Понятно, что показатель "достоверность сообщения" (Report Confidence) имеет значение "подтверждена" (Confirmed). Эти показатели уточняют базовую оценку, и получается временна́я оценка, равная 6,4.

Исходя из того, что доступность более важна, чем обычно для целевых систем, в зависимости от значений показателей "возможность сопутствующего ущерба" (Collateral Damage Potential) и "распределение целей" (Target Distribution) оценка среды могла бы изменяться в интервале от 0,0 ("отсутствует" (None), "отсутствует" (None)) до 9,2 ("высокая" (High), "высокое" (High)). Эти результаты обобщены ниже.

```
-------------------------------------------------------
BASE METRIC                 EVALUATION              SCORE
-------------------------------------------------------
Access Vector               [Network]              (1.00)
Access Complexity           [Low]                  (0.71)
Authentication              [None]                 (0.704)
Confidentiality Impact      [None]                 (0.00)
Integrity Impact            [None]                 (0.00)
Availability Impact         [Complete]             (0.66)
-------------------------------------------------------
BASE FORMULA                                   BASE SCORE
-------------------------------------------------------
Impact = 10.41*(1-(1)*(1)*(0.34)) == 6.9
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore = ((0.6*6.9) + (0.4*10.0) - 1.5)*1.176 == (7.8)
-------------------------------------------------------
-------------------------------------------------------
TEMPORAL METRIC             EVALUATION              SCORE
-------------------------------------------------------
Exploitability              [Functional]           (0.95)
Remediation Level           [Official-Fix]         (0.87)
Report Confidence           [Confirmed]            (1.00)
-------------------------------------------------------
TEMPORAL FORMULA                            TEMPORAL SCORE
-------------------------------------------------------
round(7.8 * 0.95 * 0.87 * 1.00)                == (6.4)
-------------------------------------------------------
-------------------------------------------------------
ENVIRONMENTAL METRIC        EVALUATION              SCORE
-------------------------------------------------------
Collateral Damage Potential [None - High]       {0 - 0.5}
Target Distribution         [None - High]       {0 - 1.0}
Confidentiality Req.        [Medium]                (1.0)
Integrity Req.              [Medium]                (1.0)
Availability Req.           [High]                 (1.51)
-------------------------------------------------------
ENVIRONMENTAL FORMULA                ENVIRONMENTAL SCORE
-------------------------------------------------------
AdjustedImpact = min(10,10.41*(1-(1-0*1)*(1-0*1)
         *(1-0.66*1.51))                       == (10.0)
AdjustedBase =((0.6*10)+(0.4*10.0) - 1.5)*1.176
                                               == (10.0)
AdjustedTemporal == (10*0.95*0.87*1.0)          == (8.3)
EnvScore = round((8.3+(10-8.3)*{0-0.5})*{0-1})
                                          == (0.00 - 9.2)
-------------------------------------------------------
```

I.2 Уязвимость CVE-2003-0818

Рассмотрим уязвимость CVE-2003-0818: уязвимость при обработке целочисленных значений в библиотеке Microsoft Windows ASN.1. В сентябре 2003 года была обнаружена уязвимость, ориентированная на библиотеки ASN.1 во всех операционных системах Microsoft. Успешная эксплуатация этой уязвимости приводит к переполнению буфера, что позволяет злоумышленнику выполнить произвольный код с привилегиями (системного) администратора.

Эта уязвимость эксплуатируется дистанционно и не требует аутентификации, поэтому показатель "вектор доступа" (Access Vector) равен "сетевой" (Network) и показатель "аутентификация"(Authentication) равен "отсутствует" (None). Показатель "сложность доступа" (Access Complexity) имеет значение "низкая" (Low), потому что для успешной эксплуатации этой уязвимости не требуются дополнительный доступ или специальные условия. Каждый из показателей воздействия имеет значение "полное" (Complete), потому что существует возможность полного взлома системы. Эти показатели вместе дают максимальную базовую оценку 10,0.

Таким образом, базовый вектор этой уязвимости имеет вид: AV:N/AC:L/Au:N/C:C/I:C/A:C.

Для этой уязвимости существуют известные эксплойты, поэтому показатель "возможность эксплуатации" (Exploitability) имеет значение "функциональная" (Functional). В феврале 2004 года Microsoft выпустила корректировку MS04-007, поэтому показатель "уровень устранения" (Remediation Level) имеет значение "официальное исправление" (Official-Fix), и показатель "достоверность сообщения" (Report Confidence) имеет значение "подтверждена" (Confirmed). Эти показатели уточняют базовую оценку, и получается временна́я оценка, равная 8.3.

Исходя из того, что доступность менее важна, чем обычно для целевых систем, в зависимости от значений показателей "возможность сопутствующего ущерба" (Collateral Damage Potential) и "распределение целей" (Target Distribution) оценка среды могла бы изменяться в интервале от 0,0 ("отсутствует" (None), "отсутствует" (None)) до 9,0 ("высокая" (High), "высокое" (High)). Эти результаты обобщены ниже.

```
-------------------------------------------------------
BASE METRIC                 EVALUATION             SCORE
-------------------------------------------------------
Access Vector               [Network]             (1.00)
Access Complexity           [Low]                 (0.71)
Authentication              [None]                (0.704)
Confidentiality Impact      [Complete]            (0.66)
Integrity Impact            [Complete]            (0.66)
Availability Impact         [Complete]            (0.66)
-------------------------------------------------------
FORMULA                                       BASE SCORE
-------------------------------------------------------
Impact = 10.41*(1-(0.34*0.34*0.34)) == 10.0
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore =((0.6*10.0)+(0.4*10.0) - 1.5)*1.176  == (10.0)
-------------------------------------------------------

-------------------------------------------------------
TEMPORAL METRIC             EVALUATION             SCORE
-------------------------------------------------------
Exploitability              [Functional]          (0.95)
Remediation Level           [Official-Fix]        (0.87)
Report Confidence           [Confirmed]           (1.00)
-------------------------------------------------------
FORMULA                                   TEMPORAL SCORE
-------------------------------------------------------
round(10.0 * 0.95 * 0.87 * 1.00) ==                (8.3)
-------------------------------------------------------
-------------------------------------------------------
ENVIRONMENTAL METRIC        EVALUATION             SCORE
-------------------------------------------------------
Collateral Damage Potential [None - High]       {0 - 0.5}
Target Distribution         [None - High]       {0 - 1.0}
Confidentiality Req.        [Medium]               (1.0)
Integrity Req.              [Medium]               (1.0)
Availability Req.           [Low]                  (0.5)
-------------------------------------------------------
FORMULA                                ENVIRONMENTAL SCORE
-------------------------------------------------------
AdjustedImpact = 10.41*(1-(1-0.66*1)*(1-0.66*1)
         *(1-0.66*0.5))                          == (9.6)
AdjustedBase =((0.6*9.6)+(0.4*10.0) - 1.5)*1.176
                                                 == (9.7)
AdjustedTemporal == (9.7*0.95*0.87*1.0)          == (8.0)
EnvScore = round((8.0+(10-8.0)*{0-0.5})*{0-1})
                 ==                        (0.00 - 9.0)
-------------------------------------------------------
```

I.3 Уязвимость CVE-2003-0062

Рассмотрим уязвимость CVE-2003-0062: переполнение буфера в NOD32 Antivirus. NOD32 – это антивирусное программное приложение, разработанное компанией Eset. В феврале 2003 года в версиях Linux и Unix, предшествующих версии 1.013, была обнаружена уязвимость, связанная с переполнение буфера. Она могла позволить локальным пользователям выполнить произвольный код с привилегиями пользователя, запустившего NOD32. Чтобы вызвать переполнение буфера злоумышленник должен дождаться (или спровоцировать), пока другой пользователь (возможно, администратор) начнет сканировать каталог с очень большой длиной пути.

Поскольку уязвимость эксплуатируется только пользователем, который локально зарегистрирован в системе, показатель "вектор доступа" (Access Vector) равен "локальный" (Local). Показатель "сложность доступа" (Access Complexity) имеет значение "высокая"(High), потому что эта уязвимость не может произвольно эксплуатироваться злоумышленником. Существует дополнительный уровень сложности, потому что злоумышленник должен дождаться, пока другой пользователь запустит программу сканирования на вирусы. Показатель "аутентификация" (Authentication) равен "отсутствует" (None), потому что злоумышленнику не требуется аутентификация в какой-либо дополнительной системе. Если администратор запустит сканирование на вирусы и тем самым вызовет переполнение буфера, то возможен полный взлом системы. В связи с тем, что должен рассматриваться самый опасный случай, то каждый из трех показателей воздействия имеет значение "полное" (Complete). Эти показатели вместе дают базовую оценку 6,2.

Таким образом, базовый вектор этой уязвимости имеет вид: AV:L/AC:H/Au:N/C:C/I:C/A:C.

Был выпущен частичный код эксплойта, поэтому показатель "возможность эксплуатации" (Exploitability) имеет значение "доказана правильность концепции" (Proof-Of-Concept). Компания Eset выпустила обновление, поэтому показателю "уровень устранения" (Remediation Level) присвоено значение "официальное исправление" (Official-Fix), а показателю "достоверность сообщения" (Report Confidence) – "подтверждена" (Confirmed). Эти показатели уточняют базовую оценку, и получается временна́я оценка, равная 4,9.

Исходя из того, что конфиденциальность, целостность и доступность ориентировочно одинаково важны для целевых систем, в зависимости от значений показателей "возможность сопутствующего ущерба" (Collateral Damage Potential) и "распределение целей" (Target Distribution) оценка среды могла бы изменяться в интервале от 0,0 ("отсутствует" (None), "отсутствует" (None)) до 7,5 ("высокая" (High), "высокое" (High)). Эти результаты обобщены ниже.

```
-------------------------------------------------------
BASE METRIC                EVALUATION              SCORE
-------------------------------------------------------
Access Vector              [Local]                (0.395)
Access Complexity          [High]                 (0.35)
Authentication             [None]                 (0.704)
Confidentiality Impact     [Complete]             (0.66)
Integrity Impact           [Complete]             (0.66)
Availability Impact        [Complete]             (0.66)
-------------------------------------------------------
FORMULA                                       BASE SCORE
-------------------------------------------------------
Impact = 10.41 *(1-(0.34*0.34*0.34)) == 10.0
Exploitability = 20*0.35*0.704*0.395 == 1.9
f(Impact) = 1.176
BaseScore =((0.6*10)+(0.4*1.9) - 1.5)*1.176      == (6.2)
-------------------------------------------------------
-------------------------------------------------------
TEMPORAL METRIC            EVALUATION              SCORE
-------------------------------------------------------
Exploitability             [Proof-Of-Concept]     (0.90)
Remediation Level          [Official-Fix]         (0.87)
Report Confidence          [Confirmed]            (1.00)
-------------------------------------------------------
FORMULA                                    TEMPORAL SCORE
-------------------------------------------------------
round(6.2 * 0.90 * 0.87 * 1.00) ==                 (4.9)
-------------------------------------------------------
-------------------------------------------------------
ENVIRONMENTAL METRIC       EVALUATION              SCORE
-------------------------------------------------------
Collateral Damage Potential [None - High]       {0 - 0.5}
Target Distribution        [None - High]       {0 - 1.0}
Confidentiality Req.       [Medium]                (1.0)
Integrity Req.             [Medium]                (1.0)
Availability Req.          [Medium]                (1.0)
-------------------------------------------------------
FORMULA                                ENVIRONMENTAL SCORE
-------------------------------------------------------
AdjustedTemporal == 4.9
EnvScore = round((4.9+(10-4.9)*{0-0.5})*{0-1})
                                          == (0.00 - 7.5)
-------------------------------------------------------
```

Дополнение II

Дополнительные ресурсы

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Ниже представлен список ресурсов, которые могут быть полезны при реализации CVSS. Бюллетени с описанием уязвимостей удобны при поиске подробной информации о конкретной уязвимости. Калькуляторы CVSS необходимы для вычисления собственных базовых и временны́х оценок или оценок среды.

Бюллетени с описанием уязвимостей:

- Национальным институтом стандартов и технологий (NIST) ведется национальная база данных об уязвимостях (NVD) – веб-сайт бюллетеней с описанием уязвимостей, которые содержат базовые оценки CVSS. NIST бесплатно предоставляет эти веб-бюллетени, а также XML-каналы. Эти материалы представлены, соответственно, по адресам: http://nvd.nist.gov/nvd.cfm и http://nvd.nist.gov/download.cfm#XML.
- Подразделение IBM Internet Security Systems (ISS) публикует бюллетени с описанием уязвимостей X-Force и предоставляет их бесплатно. Эти бюллетени содержат базовую и временну́ю оценки CVSS и представлены по адресу: http://xforce.iss.net/xforce/alerts.
- Компания Qualys публикует справочные документы об уязвимостях, которые содержат базовую и временну́ю оценки CVSS. Эти документы представлены по адресу: http://www.qualys.com/research/alerts/.
- Бюллетени уязвимостей Cisco, содержащие базовую и временну́ю оценки CVSS, представлены по адресу: http://tools.cisco.com/MySDN/Intelligence/home.x. (Примечание. – Требуется учетная запись Cisco Connection Online).
- Компания Tenable Network Security публикует плагины для средства сканирования уязвимостей Nessus. Эти плагины, включающие базовую оценку CVSS, представлены по адресу: http://www.nessus.org/plugins/.
- JPCERT/CC и IPA ведут сайт-портал Japan Vulnerability Notes (JVN), на котором размещаются бюллетени с описанием уязвимостей, содержащие базовые оценки CVSS. JVN бесплатно предоставляет эти веб-бюллетени, а также XML-каналы. Эти материалы представлены, соответственно, по адресам: http://jvndb.jvn.jp/en/ и http://jvndb.jvn.jp/en/apis/.

Калькуляторы CVSS:

- Калькулятор NIST CVSSv2: http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2;
- Калькулятор Агентства по содействию развитию информационных технологий Японии: http://jvndb.jvn.jp/en/cvss/index.html.

Библиография

[b-1] Mike Schiffman, Gerhard Eschelbeck, David Ahmad, Andrew Wright, Sasha Romanosky, "*CVSS: A Common Vulnerability Scoring System*", National Infrastructure Advisory Council (NIAC), 2004.

[b-2] Microsoft Corporation. *Microsoft Security Response Center Security Bulletin Severity Rating System*. November 2002 [cited 16 March 2007]. Available from URL: http://www.microsoft.com/technet/security/bulletin/rating.mspx.

[b-3] United States Computer Emergency Readiness Team (US-CERT). *US-CERT Vulnerability Note Field Descriptions*. 2006 [cited 16 March 2007]. Available from URL: http://www.kb.cert.org/vuls/html/fieldhelp.

[b-4] SANS Institute. *SANS Critical Vulnerability Analysis Archive*. Undated (cited 16 March 2007).

[b-ITU-T X.1500] Recommendation X.1500 (2011), *Overview of Cybersecurity information exchange (CYBEX)*.

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.