Международный союз электросвязи

МСЭ-Т

X.1521

(03/2016)

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 3.0

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
Рекомендации, связанные с PKI	X.1340–X.1349
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	**X.1520–X.1539**
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

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

Рекомендация МСЭ-Т X.1521

Система оценки общеизвестных уязвимостей 3.0

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	Уникальный идентификатор*
1.0	МСЭ-Т X.1521	20.04.2011 г.	17-я	11.1002/1000/11062
2.0	МСЭ-Т X.1521	23.03.2016 г.	17-я	11.1002/1000/12614

Ключевые слова

Система оценки общеизвестных уязвимостей, CVSS, CYBEX, показатели.

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Введение

Система оценки общеизвестных уязвимостей (CVSS) – это открытая структура представления информации о характеристиках и степени серьезности уязвимостей в программном обеспечении. Система CVSS состоит из трех групп показателей – базовые показатели, временны́е показатели и показатели среды. Базовые показатели отражают неизменные характеристики, присущие уязвимости, временны́е показатели – характеристики уязвимости, которые меняются со временем, а показатели среды – характеристики, которые зависят от среды пользователя. Базовые показатели оцениваются по шкале от 0,0 до 10,0 при этом получившаяся оценка может быть затем уточнена оценками временны́х показателей и показателей среды. Оценка по CVSS может быть также представлена в виде векторной строки – сжатого текстового представления значений, на основе которых формируется оценка. В настоящей Рекомендации дается официальная спецификация CVSS версии 3.0 (CVSS v3.0).

CVSS v3.0 содержит коренные усовершенствования по сравнению с CVSS v2.0 и несовместима с последней. В ходе использования CVSS v2.0 был выявлен ряд ограничений, присущих этой спецификации. Они, в частности, связаны с оценкой уязвимостей в виртуальной среде, представлением "косвенных" уязвимостей, таких как межсайтовый скриптинг, невозможностью отразить взаимозависимости между приложениями в пределах одной системы и отражением действий пользователей, не являющихся злоумышленниками. Более подробная информация об усовершенствованиях в версии 3.0 приводится в Дополнении I, пункт 2.

В ходе работы над преодолением этих ограничений рабочая группа по CVSS пришла к выводу о невозможности сохранения обратной совместимости с CVSS v2.0. Признавая, что отсутствие совместимости приведет к некоторым проблемам с существующими системами, использующими CVSS v2.0, составители тем не менее убеждены, что преимущества версии 3.0 достаточно значительны, чтобы компенсировать эти неудобства. Пользователям и поставщикам, которые в настоящее время оценивают и обрабатывают уязвимости по CVSS v2.0, настоятельно рекомендуется перейти на CVSS v3.0.

Спецификация CVSS v2.0 останется доступной для архивных целей, но утратит силу. Разработчикам инструментальных средств и процессов настоятельно рекомендуется внедрить спецификацию CVSS версии 3.0, сохранив поддержку версии 2.0 для обработки имеющихся уязвимостей, уже получивших оценку по CVSS v2.0.

Рекомендация МСЭ-Т X.1521

Система оценки общеизвестных уязвимостей 3.0

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 3" от 10 июня 2015 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.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используется следующий термин, определенный 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 для субъекта рассматривать объект, изменять его или устанавливать с ним связь. Доступ обеспечивает возможность обмена информацией между субъектом и 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	Attack Complexity		Сложность атаки
AR	Availability Requirement		Важность требования доступности
ARP	Address Resolution Protocol		Протокол разрешения адресов
AV	Attack Vector		Вектор атаки
C	Confidentiality Impact		Воздействие на конфиденциальность
CIA	Confidentiality, Integrity, and Availability		Конфиденциальность, целостность и доступность
CPU	Central Processing Unit		Центральный процессор
CR	Confidentiality Requirement		Важность требования конфиденциальности
CVE	Common Vulnerability Exposure		Общеизвестные уязвимости и незащищенность
CVSS	Common Vulnerability Scoring System		Система оценки общеизвестных уязвимостей
CWE	Common Weakness Enumeration		Перечень общеизвестных слабых мест
DMA	Direct Memory Access		Прямой доступ к памяти
DNS	Domain Name System		Система наименований доменов
DOM	Document Object Model		Объектная модель документа
DoS	Denial-of-Service		Отказ в обслуживании
E	Exploit code maturity		Зрелость кода эксплойта
I	Integrity impact		Воздействие на целостность
ICT	Information and Communication Technologies	ИКТ	Информационно-коммуникационные технологии
ID	IDentifier		Идентификатор
IP	Internet Protocol		Протокол Интернет/IP-протокол
IR	Integrity Requirement		Важность требования целостности
ISC	Impact Sub Score		Частная оценка воздействия
IT	Information Technology	ИТ	Информационные технологии
LAN	Local Area Network	ЛВС	Локальная вычислительная сеть
MA	Modified Availability		Уточненное воздействие на доступность
MAC	Modified Attack Complexity		Уточненная сложность атаки
MAV	Modified Attack Vector		Уточненный вектор атаки
MC	Modified Confidentiality impact		Уточненное воздействие на конфиденциальность
MI	Modified Integrity		Уточненное воздействие на целостность
MPR	Modified Privileges Required		Уточненная потребность в привилегиях
MS	Modified Scope		Уточненная область действия

MUI	Modified User Interaction		Уточненное взаимодействие с пользователем
NIST	National Institute of Standards		Национальный институт стандартов и технологий
OS	Operating System	ОС	Операционная система
OSI	Open Systems Interconnection		Взаимосвязь открытых систем
PCI DSS	Payment Card Industry Data Security Standard		Стандарт безопасности данных индустрии платежных карт
PR	Privileges Required		Потребность в привилегиях
RC	Report Confidence		Достоверность сообщения
RL	Remediation Level		Уровень устранения
RPC	Remote Procedure Call		Дистанционный вызов процедуры
S	Scope		Область действия
SCAP	Security Content Automation Protocol		Протокол автоматизации управления данными безопасности
SQL	Structured Query Language		Язык структурированных запросов
TCP	Transmission Control Protocol		Протокол управления передачей
UI	User Interaction		Взаимодействие с пользователем
USB	Universal Serial Bus		Универсальная последовательная шина
VM	Virtual Machine		Виртуальная машина
XSS	Cross Site Scripting		Межсайтовый скриптинг

5 Условные обозначения

Нет.

6 О системе оценки общеизвестных уязвимостей

Система оценки общеизвестных уязвимостей (CVSS) – это открытая структура представления информации о характеристиках и степени серьезности уязвимостей в программном обеспечении. Система CVSS состоит из трех групп показателей – базовых показателей, временны́х показателей и показателей среды. Базовые показатели отражают неизменные характеристики, присущие уязвимости, временны́е показатели – характеристики уязвимости, которые меняются со временем, а показатели среды – характеристики, которые зависят от среды пользователя. Базовые показатели оцениваются по шкале от 0 до 10, при этом получившаяся оценка может быть затем уточнена оценками временны́х показателей и показателей среды. Оценка по CVSS может быть также представлена в виде векторной строки – сжатого текстового представления значений, на основе которых формируется оценка. В настоящей Рекомендации дается официальная спецификация CVSS версии 3.0 (CVSS v3.0).

6.1 Введение

Уязвимости программного, аппаратного и микропрограммного обеспечения связаны с серьезным риском для любой организации, эксплуатирующей компьютерную сеть. Классификация уязвимостей и защита от них могут представлять трудность. Система оценки общеизвестных уязвимостей (CVSS) позволяет выделить основные характеристики уязвимости и дать количественную (числовую) оценку степени ее серьезности, а также текстовое представление этой оценки. Количественная оценка затем может быть преобразована в качественную (низкая, средняя, высокая или критическая), чтобы помочь организациям надлежащим образом определить качество и приоритет процессов управления уязвимостями.

Говоря вкратце, CVSS дает три важных преимущества. Во-первых, она обеспечивает стандартизованную оценку уязвимостей. Пользуясь общим алгоритмом оценки уязвимостей на всех ИТ-платформах, организация может проводить единую политику управления уязвимостями с определением максимально допустимых сроков проверки наличия и устранения конкретной уязвимости. Во-вторых, она представляет собой открытую систему. Произвольная оценка, присвоенная уязвимости какой-либо третьей стороной, может дезориентировать пользователей. В CVSS четко видны отдельные характеристики, на основе которых формируется оценка. И наконец, CVSS позволяет приоритезировать риски. При расчете оценки среды уязвимость ставится в контекст конкретной организации, что помогает получить лучшее представление о риске, который влечет за собой эта уязвимость для организации.

В настоящей Рекомендации изложена официальная спецификация CVSS v3.0.

6.1.1 Показатели

Система CVSS состоит из трех групп показателей (базовые показатели, временны́е показатели и показатели среды), каждая из которых содержит набор показателей, как проиллюстрировано на рисунке 1.

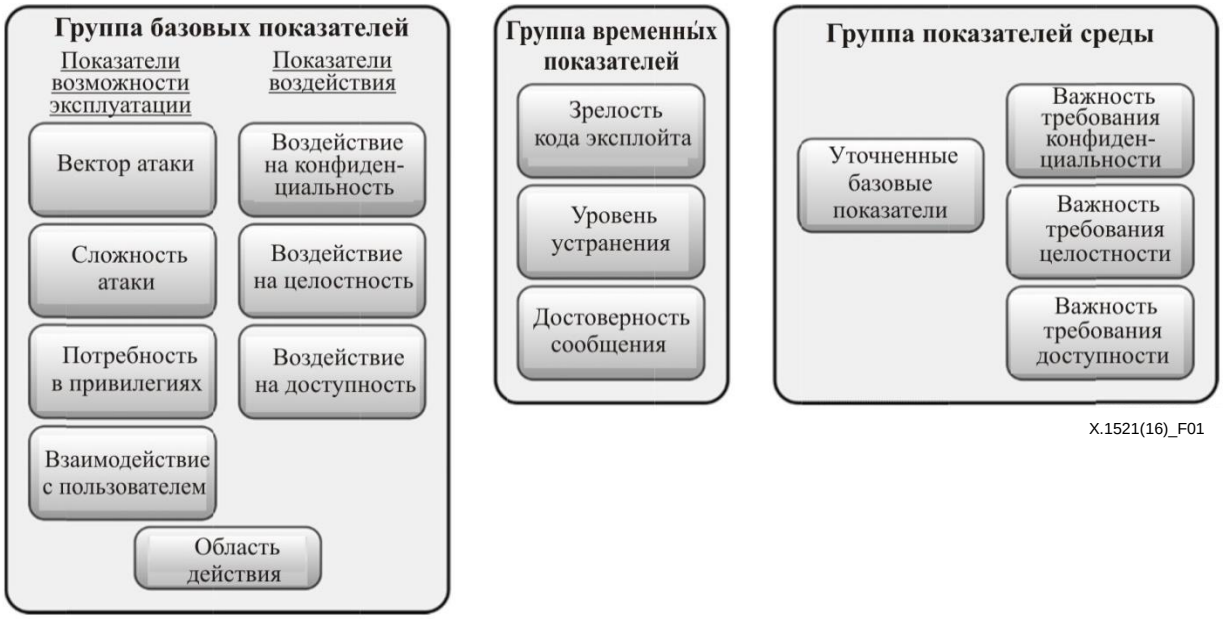


Рисунок 1 − Группа показателей системы CVSS v3.0

Группа базовых показателей отражает присущие уязвимости характеристики, которые не изменяются со временем и не зависят от пользовательской среды. Она содержит два набора показателей – показатели возможности эксплуатации и показатели воздействия.

Показатели возможности эксплуатации характеризуют простоту эксплуатации уязвимости и необходимые для этого технические средства. Таким образом, они отражают характеристики *уязвимого объекта*, который формально именуется *уязвимым компонентом*. Показатели же воздействия характеризуют непосредственные результаты успешной эксплуатации уязвимости и отражают последствия для *подвергающегося воздействию объекта*, который формально именуется *атакуемым компонентом*.

Обычно в роли уязвимого компонента выступает прикладная программа, модуль, драйвер и т. д. (или даже устройство), а атакуемым компонентом может быть прикладная программа, устройство или сетевой ресурс. Возможность измерять воздействие уязвимости на другие объекты, помимо уязвимого компонента, – ключевая особенность CVSS v3.0. Эта характеристика отражена в показателе "область действия", который более подробно рассматривается ниже.

Группа временны́х показателей отражает характеристики уязвимости, которые могут меняться со временем, но не зависят от пользовательской среды. Например, наличие простого в использовании средства поиска и эксплуатации уязвимостей повышает оценку по системе CVSS, а появление официального исправления ее снижает.

Показатели среды отражают характеристики уязвимости, которые относятся к конкретной среде пользователя и свойственны только ей. На основании этих показателей осуществляющий оценку уязвимостей аналитик может предусматривать меры и средства безопасности, позволяющие ослабить последствия эксплуатации уязвимости, а также повышать или понижать уровень значимости уязвимой системы в соответствии с риском для организации.

Ниже следует подробное рассмотрение каждого из этих показателей.

6.1.2 Процесс оценки

На основании присвоенных аналитиком значений базовых показателей по базовой формуле рассчитывается оценка в диапазоне от 0,0 до 10,0, как представлено на рисунке 2.

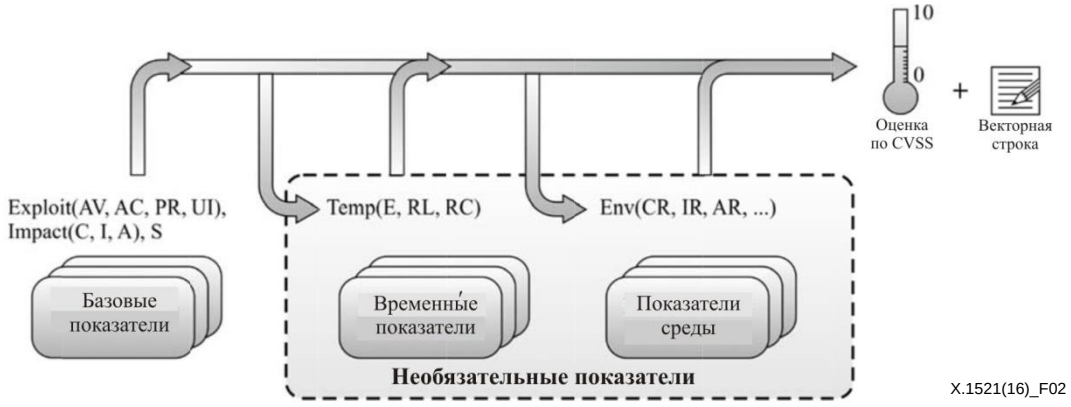


Рисунок 2 − Показатели и формулы CVSS

В базовой формуле используются в свою очередь две подформулы – формула частной оценки возможности эксплуатации и формула частной оценки воздействия. Формула частной оценки возможности эксплуатации основывается на базовых показателях возможности эксплуатации, а формула частной оценки воздействия – на базовых показателях воздействия.

Далее базовую оценку можно скорректировать путем вычисления оценок временны́х показателей и показателей среды, чтобы точнее отразить тот риск, который уязвимость представляет для пользовательской среды. Однако вычисление таких оценок не является обязательным.

Как правило, базовые и временны́е показатели определяются аналитиками, подготавливающими бюллетени с описанием уязвимостей, разработчиками продуктов в области безопасности или разработчиками приложений, потому что они обычно располагают наиболее точной информацией о характеристиках уязвимости. В то же время показатели среды определяются организациями, являющимися конечными пользователями, поскольку они лучше, чем кто бы то ни было, могут оценить потенциальное воздействие уязвимости в рамках собственной вычислительной среды.

При оценке уязвимости по системе CVSS на основе показателей формируется также векторная строка – текстовое представление значений показателей. Векторная строка представляет собой текстовую строку особого формата, которая содержит значения, присвоенные каждому показателю, и должна всегда приводиться вместе с оценкой уязвимости.

Формулы оценки и векторная строка более детально рассматриваются ниже.

Следует отметить, что все показатели должны оцениваться исходя из предположения, что злоумышленник уже нашел и идентифицировал уязвимость. Иными словами, аналитику нет нужды рассматривать способы, которыми была идентифицирована уязвимость. Кроме того, хотя оценкой уязвимостей будет скорее всего заниматься множество разных групп лиц (например, разработчики программного обеспечения, аналитики – составители бюллетеней с описанием уязвимостей, разработчики продуктов в сфере безопасности и т. д.), следует иметь в виду, что данная система оценки задумана как независимая от конкретного лица и организации.

6.2 Базовые показатели

6.2.1 Показатели возможности эксплуатации

Как уже отмечалось выше, показатели возможности эксплуатации отражают характеристики *уязвимого объекта*, который формально именуется *уязвимым компонентом*. Поэтому каждый из таких показателей, перечисленных ниже, должен оцениваться применительно к уязвимому компоненту и отражать те свойства уязвимости, которые ведут к успешной атаке.

6.2.1.1 Показатель "вектор атаки" (Attack Vector, AV)

Этот показатель отражает контекст, в котором возможна эксплуатация уязвимости. Его значение (а следовательно, и базовая оценка) будет тем выше, чем дальше (логически и физически) может находиться злоумышленник, способный эксплуатировать уязвимый компонент. Предполагается, что уязвимость, доступную через интернет, способно эксплуатировать большее число потенциальных злоумышленников, чем уязвимость, требующую физического доступа к устройству, и поэтому уязвимости первого типа следует присвоить более высокую оценку. Перечень возможных значений представлен в таблице 1.

Таблица 1 − Вектор атаки

Значение показателя	Описание
Сетевой (Network, N)	В случае уязвимости, эксплуатация которой возможна при доступе через сеть, уязвимый компонент привязан к сетевому стеку, а маршрут проникновения злоумышленника пролегает через уровень 3 (сетевой уровень) модели взаимосвязи открытых систем (OSI). Такие уязвимости часто называются "уязвимостями с возможностью дистанционной эксплуатации", то есть эксплуатации через один или несколько сетевых пролетов (например, через границы уровня 3 с маршрутизаторов). Примером сетевой атаки может служить инициирование злоумышленником отказа в обслуживании (DoS путем передачи особым образом сформированного TCP-пакета через общедоступный интернет (например, CVE-2004-0230)
Соседский (Adjacent, A)	В случае уязвимости, эксплуатация которой возможна со стороны соседей по сети, уязвимый компонент также привязан к сетевому стеку, но атака ограничена той же совместно используемой физической (например, Bluetooth, IEEE 802.11) или логической (например, локальной IP-подсетью) сетью и не может быть произведена через границы уровня 3 модели OSI (например, маршрутизатор). Примером "соседской" атаки является флуд-атака по протоколу разрешения адресов (ARP) (IPv4) или протоколу обнаружения соседей (IPv6), вызывающая отказ в обслуживании в местном сегменте локальной вычислительной сети (ЛВС). См. также CVE-2013-6014
Локальный (Local, L)	В случае уязвимости, которая может эксплуатироваться при локальном доступе, уязвимый компонент не привязан к сетевому стеку, а маршрут проникновения злоумышленника пролегает через возможности чтения/записи/выполнения. В одних случаях злоумышленник эксплуатирует уязвимость, войдя локально в систему, в других он/она может полагаться на взаимодействие с пользователем (UI) для выполнения вредоносного файла
Физический (Physical, P)	В случае уязвимости, которая может эксплуатироваться при физическом доступе, злоумышленнику для достижения своей цели необходимо физическое взаимодействие с уязвимым компонентом. Это физическое взаимодействие может быть кратковременным (как, например, при атаке типа Evil maid[1]) или постоянным. Примерами такой атаки могут служить атака методом холодной перезагрузки, позволяющая злоумышленнику получить доступ к ключам шифрования диска после получения физического доступа к системе, или атаки с прямым доступом в память через периферийные устройства Firewire/USB

[1] Описание атаки типа Evil maid см. по адресу: https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html.

6.2.1.2 Показатель "сложность атаки" (Attack Complexity, AC)

Этот показатель отражает необходимые для эксплуатации уязвимости условия, находящиеся вне контроля злоумышленника. Как описано ниже, такие условия могут включать сбор дополнительной информации о целевом объекте атаки, определенные настройки конфигурации системы или исключительные ситуации в процессе вычислений. Важная особенность этого показателя состоит в том, что он исключает необходимость взаимодействия с пользователем для эксплуатации уязвимости (такие условия отражены в показателе "взаимодействие с пользователем"). Показатель "сложность атаки" имеет наивысшее значение для наименее сложных атак. Перечень возможных значений представлен в таблице 2.

Таблица 2 − Сложность атаки

Значение показателя	Описание
Низкая (Low, L)	Не существует специальных условий доступа и особых обстоятельств. Злоумышленник может рассчитывать на успешное повторение атаки в отношении уязвимого компонента
Высокая (High, H)	Успех атаки зависит от условий, находящихся вне контроля злоумышленника. Иными словами, успешная атака не может быть выполнена произвольно, а требует от злоумышленника приложения заметных усилий для подготовки или реализации такой атаки в отношении уязвимого компонента[2]. Например, успех атаки может зависеть от любого из следующих условий: • злоумышленник должен собрать некоторую информацию о целевом объекте атаки – например, о настройках конфигурации, порядковых номерах, совместно используемых секретных ключах и т. д.; • злоумышленник должен подготовить целевую среду для повышения надежности эксплуатации – например, для повторной эксплуатации, нацеленной на получение выигрышного результата в условиях состязания, или для преодоления прогрессивных методов защиты от эксплуатации; • злоумышленник должен расположиться на логическом сетевом пути между целевым объектом и ресурсом, который был запрошен этим объектом, для чтения и/или изменения передаваемых по сети данных (например, атака через посредника)

6.2.1.3 Показатель "потребность в привилегиях" (Privileges Required, PR)

Этот показатель описывает уровень привилегий, которым должен обладать злоумышленник, чтобы *получить возможность* успешной эксплуатации уязвимости. Данный показатель имеет наивысшее значение, если привилегии не требуются. Перечень возможных значений представлен в таблице 3.

Таблица 3 − Потребность в привилегиях

Значение показателя	Описание
Отсутствует (None, N)	Злоумышленник может не иметь авторизации перед атакой и, соответственно, не нуждается в доступе к каким-либо настройкам или файлам для ее осуществления
Низкая (Low, L)	Злоумышленник должен быть авторизован и располагать ограниченными привилегиями, предоставляющими базовые пользовательские возможности, которые в нормальном случае распространяются только на настройки и файлы самого пользователя. Как вариант, при низком уровне привилегий злоумышленник может быть в состоянии воздействовать только на некритичные ресурсы
Высокая (High, H)	Злоумышленник должен быть авторизован и располагать привилегиями, предоставляющими значительный (например, административный) контроль над уязвимым компонентом, который может затрагивать настройки и файлы в масштабе всего компонента

[2] Следует обратить внимание на отсутствие здесь каких-либо комментариев относительно требуемого количества усилий. Считается лишь, что для эксплуатации уязвимости необходимо приложить некоторые дополнительные усилия.

6.2.1.4 Показатель "взаимодействие с пользователем" (User Interaction, UI)

Этот показатель отражает необходимость участия другого пользователя, помимо злоумышленника, для успешной компрометации уязвимого компонента. Данный показатель определяет, возможна ли эксплуатация уязвимости по желанию одного только злоумышленника или же требуется взаимодействие с другим пользователем либо инициированным им процессом. Показатель имеет наивысшее значение, если взаимодействие с пользователем не требуется. Перечень возможных значений представлен в таблице 4.

Таблица 4 − Взаимодействие с пользователем

Значение показателя	Описание
Отсутствует (None, N)	Существует возможность эксплуатации уязвимой системы без взаимодействия с каким-либо пользователем
Требуется (Required, R)	Для успешной эксплуатации этой уязвимости требуются те или иные действия со стороны пользователя. Например, успешная эксплуатация возможна только при установке приложения системным администратором

6.2.2 Показатель "область действия"

Важной характеристикой, учтенной в CVSS v3.0, является возможность воздействия уязвимости в программном компоненте на ресурсы за рамками привилегий, которыми наделен этот компонент. Ее отражает показатель "область действия авторизации" (Authorization Scope), или просто "область действия".

Формально область действия описывает набор привилегий, определенный субъектом авторизации в вычислительной системе (например, приложением, операционной системой или изолированной программной средой) при предоставлении доступа к вычислительным ресурсам (таким как файлы, центральный процессор, память и т. д.). Эти привилегии присваиваются на основе определенного метода идентификации и авторизации. В некоторых случаях авторизация может быть простой или нестрого регулироваться заранее заданными правилами либо стандартами. Например, в случае трафика Ethernet, передаваемого на сетевой коммутатор, последний принимает поступающий на его порты трафик и является субъектом авторизации, регулирующим поток трафика на другие порты.

Когда уязвимость программного компонента с одной областью действия авторизации способна воздействовать на ресурсы с другой областью действия авторизации, происходит смена области действия.

Интуитивно можно представить смену области действия как проникновение за пределы изолированной программной среды. Примером может служить уязвимость в виртуальной машине, позволяющая злоумышленнику удалять файлы в операционной системе хоста (а возможно и в собственной виртуальной машине). В этом примере есть два различных субъекта авторизации: один определяет и контролирует привилегии виртуальной машины и ее пользователей, другой определяет и контролирует привилегии для системы хоста, в которой эта машина работает.

Смены области действия не происходит, например, в случае уязвимости в Microsoft Word, которая дает злоумышленнику возможность компрометации всех системных файлов ОС хоста, поскольку привилегии пользовательского экземпляра Word и системные файлы хоста контролирует один и тот же субъект.

Значение базового показателя выше, если происходит смена области действия. Перечень возможных значений представлен в таблице 5.

Таблица 5 − Область действия

Значение показателя	Описание
Не меняется (Unchanged, U)	Эксплуатируемая уязвимость может воздействовать только на ресурсы под контролем того же субъекта авторизации. В этом случае уязвимый и атакуемый компоненты совпадают
Меняется (Changed, C)	Эксплуатируемая уязвимость может воздействовать на ресурсы за рамками привилегий, предусмотренных уязвимым компонентом. В этом случае уязвимый и атакуемый компоненты различаются

6.2.3 Показатели воздействия

Показатели воздействия характеризуют свойства атакуемого компонента. Независимо от того, влияет ли успешная эксплуатация уязвимости на один или несколько компонентов, показатели воздействия оцениваются по компоненту, для которого наступают наихудшие последствия, наиболее прямо и предсказуемо связанные с успешной атакой. Иными словами, аналитикам следует ограничить рассмотрение воздействия разумным конечным результатом, которого, по их мнению, гарантированно достигнет злоумышленник.

Если смена области действия не происходит, показатели воздействия должны отражать воздействие на конфиденциальность, целостность и доступность (CIA) применительно к уязвимому компоненту. В случае же смены области действия такие показатели должны отражать воздействие на конфиденциальность, целостность и доступность (CIA) применительно либо к уязвимому компоненту, либо к атакуемому компоненту в зависимости от того, для какого из них последствия являются наихудшими.

6.2.3.1 Показатель "воздействие на конфиденциальность" (Confidentiality Impact, C)

Этим показателем измеряется воздействие успешной эксплуатации уязвимости на конфиденциальность информационных ресурсов, находящихся в ведении программного компонента. Под конфиденциальностью понимается ограничение доступа к информации и ее раскрытия только авторизованными пользователями, а также предотвращение доступа к информации или ее раскрытия неавторизованным пользователям. Перечень возможных значений представлен в таблице 6. Значение этого показателя тем больше, чем выше степень потери конфиденциальности атакуемым компонентом.

Таблица 6 − Воздействие на конфиденциальность

Значение показателя	Описание
Сильное (High, H)	Полная потеря конфиденциальности, приводящая к тому, что все ресурсы атакуемого компонента становятся доступными злоумышленнику. Как вариант, злоумышленник получает доступ лишь к некоторой информации для ограниченного пользования, но раскрытие этой информации оказывает прямое и серьезное воздействие на конфиденциальность. Например, злоумышленник крадет пароль администратора или закрытые ключи шифрования данных веб-сервера
Слабое (Low, L)	Некоторая потеря конфиденциальности. Возможен доступ к некоторой информации для ограниченного пользования, но злоумышленник не имеет контроля над тем, какую именно информацию он получит, или масштабы потерь невелики либо их характер некритичен. Раскрытие информации не влечет за собой прямых серьезных потерь для атакуемого компонента
Отсутствует (None, N)	Потерь конфиденциальности в атакуемом компоненте нет

6.2.3.2 Показатель "воздействие на целостность" (Integrity Impact, I)

Этим показателем измеряется воздействие успешной эксплуатации уязвимости на целостность системы. Под целостностью понимается достоверность и точность информации. Перечень возможных значений представлен в таблице 7. Значение этого показателя тем выше, чем больше масштабы последствий для атакуемого компонента.

Таблица 7 − Воздействие на целостность

Значение показателя	Описание
Сильное (High, H)	Полная потеря целостности или защиты. Например, злоумышленник может изменять любые/все файлы, защищаемые атакуемым компонентом. Как вариант, могут быть изменены лишь некоторые файлы, но их вредоносное изменение будет иметь прямые серьезные последствия для атакуемого компонента
Слабое (Low, L)	Возможно изменение данных, но злоумышленник не имеет контроля над последствиями изменения или масштабы изменения ограничены. Изменение данных не имеет прямых серьезных последствий для атакуемого компонента
Отсутствует (None, N)	Потерь целостности в атакуемом компоненте нет

6.2.3.3 Показатель "воздействие на доступность" (Availability Impact, A)

Этим показателем измеряется влияние успешной эксплуатации уязвимости на доступность атакуемого компонента. В отличие от показателей "воздействие на конфиденциальность" и "воздействие на целостность", которые отражают соответственно потерю конфиденциальности и целостности данных (информации, файлов), используемых атакуемым компонентом, показатель "воздействие на доступность" отражает потерю доступности самого этого компонента, например сетевой службы (веб-сервера, базы данных, электронной почты). Поскольку под доступностью понимается возможность доступа к информационным ресурсам, атаки, которые используют полосу пропускания сети, рабочие циклы процессора или дисковое пространство, влияют на доступность атакуемого компонента. Перечень возможных значений представлен в таблице 8. Значение этого показателя тем выше, чем больше масштабы последствий для атакуемого компонента.

Таблица 8 − Воздействие на доступность

Значение показателя	Описание
Сильное (High, H)	Полная потеря доступности. Злоумышленник способен вызвать полный отказ в доступе к ресурсам атакуемого компонента; этот отказ является либо устойчивым (длится, пока злоумышленник продолжает атаку), либо постоянным (сохраняется даже после завершения атаки). Как вариант, злоумышленник способен вызвать некоторое снижение доступности, но такая потеря доступности имеет прямые серьезные последствия для атакуемого компонента (например, злоумышленник не может прервать существующие соединения, но может помешать установлению новых; злоумышленник может многократно эксплуатировать уязвимость, которая в каждом случае успешной атаки приводит к утечке лишь небольшого объема памяти, но после многократной эксплуатации делает полностью недоступной некоторую службу)
Слабое (Low, L)	Происходит снижение производительности или перебои в доступности ресурса. Хотя возможна многократная эксплуатация уязвимости, злоумышленник не способен вызвать полный отказ в обслуживании законных пользователей. Ресурсы атакуемого компонента либо частично доступны все время, либо полностью доступны только какую-то часть времени, но в целом прямые серьезные последствия для атакуемого компонента отсутствуют
Отсутствует (None, N)	Воздействие на доступность атакуемого компонента отсутствует

6.3 Временны́е показатели

Временны́е показатели отражают текущее состояние методов эксплуатации или доступность кода эксплойта, наличие каких-либо исправлений или обходных приемов, а также уверенность в правильности описания уязвимости.

6.3.1 Показатель "зрелость кода эксплойта" (Exploit Code Maturity, E)

Этим показателем измеряется вероятность атаки с использованием конкретной уязвимости. Обычно он оценивается исходя из текущего состояния методов эксплуатации, доступности кода эксплойта или активной эксплуатации этой уязвимости на практике. Если легкий в использовании код эксплойта является общедоступным, то число потенциальных злоумышленников возрастает за счет неквалифицированных злоумышленников, что увеличивает серьезность уязвимости. Изначально реальная эксплуатация уязвимости может допускаться только теоретически. Затем может последовать публикация кода, доказывающего правильность концепции эксплойта, функционального кода эксплойта или достаточного объема технических деталей, необходимых для эксплуатации уязвимости. Кроме того, код, демонстрирующий правильность концепции, со временем может развиться в код, обеспечивающий систематическую успешную эксплуатацию уязвимости. В некоторых особо серьезных случаях этот код может доставляться с помощью сетевых червей или вирусов или других автоматизированных инструментов атак.

Перечень возможных значений представлен в таблице 9. Чем легче эксплуатировать уязвимость, тем выше оценка уязвимости.

Таблица 9 − Зрелость кода эксплойта

Значение показателя	Описание
Не определено (Not Defined, X)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле расчета оценки данный показатель будет пропущен
Высокая (High, H)	Существующий функциональный автономный код или эксплойт не требуется (запуск производится вручную), и детали широко известны. Код эксплойта работает в любой ситуации или его активная доставка осуществляется автономным агентом (например, червем или вирусом). Подключенные к сети системы с высокой вероятностью могут подвергнуться попыткам сканирования или эксплуатации. Эксплойт достиг того уровня развития, при котором существуют надежные, широкодоступные и простые в использовании автоматические инструменты
Функциональная (Functional, F)	Доступен функциональный код эксплойта, применимый в большинстве ситуаций, где существует уязвимость
Доказана правильность концепции (Proof-of-Concept, P)	Доступен код эксплойта, доказывающий правильность концепции, или существует демонстрация атаки, неприменимая в большинстве систем. Код или метод действуют не во всех ситуациях, и для их использования может потребоваться существенное изменение, внесенное квалифицированным злоумышленником
Непроверенная (Unproven, U)	Код эксплойта не доступен или эксплуатация возможна лишь теоретически

6.3.2 Показатель "уровень устранения" (Remediation Level, RL)

Важным фактором, учитываемым при установлении приоритета, является уровень устранения уязвимости. Обычно когда информация об уязвимости публикуется впервые, для нее еще не существует исправления. Пока не будет выпущено официальное исправление или обновление, вре́менное устранение уязвимости могут обеспечить обходные приемы или оперативные исправления. Каждая из указанных выше поэтапных мер уменьшает значение временно́го показателя, отражая снижение остроты проблемы по мере ее окончательного устранения. Перечень возможных значений представлен в таблице 10. Чем менее официальным и постоянным является исправление, тем выше оценка уязвимости.

Таблица 10 − Уровень устранения

Значение показателя	Описание
Не определено (Not Defined, X)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле расчета оценки данный показатель будет пропущен
Недоступно (Unavailable, U)	Решение либо недоступно, либо его невозможно применить
Обходной прием (Workaround, W)	Доступно неофициальное решение, которое предоставлено третьей стороной. В некоторых случаях пользователи затронутой технологии создают собственное исправление, или принимают меры для нахождения обходного приема, или каким-либо другим способом уменьшают влияние уязвимости
Вре́менное исправление (Temporary Fix, T)	Доступно официальное вре́менное исправление. Например, разработчик выпустил оперативное исправление или временное программное средство либо опубликовал обходной прием
Официальное исправление (Official Fix, O)	Доступно полноценное решение от разработчика, который либо выпустил официальное исправление, либо предоставил обновление

6.3.3 Показатель "достоверность сообщения" (Report Confidence, RC)

Этим показателем измеряется степень достоверности информации о существовании уязвимости и доверия к известным техническим деталям. Иногда публикуется только информация о существовании уязвимости без указания конкретных деталей. Например, воздействие может признаваться нежелательным, но его первопричина может быть неизвестна. Позднее уязвимость может быть подтверждена (не всегда с полной уверенностью) данными исследований, указывающими на ее локализацию. Наконец, уязвимость может быть окончательно подтверждена автором или разработчиком затронутой технологии. Острота проблемы уязвимости выше, если о ее существовании достоверно известно. Этот показатель отражает также уровень технических знаний, доступных потенциальным злоумышленникам. Перечень возможных значений представлен в таблице 11. Чем больше уязвимость подтверждена разработчиком или другими заслуживающими доверия источниками, тем выше оценка.

Таблица 11 − Достоверность сообщения

Значение показателя	Описание
Не определено (Not Defined, X)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле расчета оценки данный показатель будет пропущен
Подтверждена (Confirmed, C)	Имеются подробные сообщения или уязвимость функционально воспроизводима (например, существуют функциональные эксплойты). Доступен исходный код, позволяющий независимо проверить утверждения, приведенные в исследованиях, либо автор или разработчик затронутого кода подтвердил наличие уязвимости
Разумная (Reasonable, R)	Опубликованы существенные подробности, но исследователи либо не уверены до конца в первопричине, либо не имеют доступа к исходному коду, чтобы окончательно подтвердить все взаимодействия, которые могут привести к рассматриваемому результату. Вместе с тем есть разумная уверенность в том, что ошибка воспроизводима и можно проверить как минимум один случай воздействия (например, существует код, демонстрирующий правильность концепции эксплойта). Примером может служить подробный обзор исследований некоторой уязвимости с пояснением (возможно, намеренно запутанным или "оставленным читателю в качестве упражнения "), которое позволяет уверенно воспроизвести заявленные результаты

Таблица 11 − Достоверность сообщения

Значение показателя	Описание
Неизвестна (Unknown, U)	Имеются сообщения о фактах воздействия на системы, указывающие на существование уязвимости. Сообщения свидетельствуют о том, что причина уязвимости неизвестна, либо расходятся в указании причин или описании воздействий уязвимости. Авторы сообщений не уверены в истинном характере уязвимости, и существуют большие сомнения в достоверности сообщений или возможности присвоить статическую базовую оценку ввиду описанных выше расхождений. Примером может служить сообщение об ошибке, в котором говорится о происходящем от случая к случаю, но невоспроизводимом аварийном завершении работы с признаками порчи содержимого памяти, что указывает на вероятность отказа в обслуживании, а возможно, и на более серьезные последствия

6.4 Показатели среды

Эти показатели позволяют аналитику адаптировать оценку по системе CVSS в зависимости от важности затронутого ИТ-ресурса для организации-пользователя, которая выражается через дополнительные/альтернативные меры и средства безопасности, конфиденциальность, целостность и доступность. Эти показатели служат уточненным эквивалентом базовых показателей, и значения им присваиваются исходя из места, занимаемого компонентом в инфраструктуре организации.

6.4.1 Показатели важности требований безопасности (CR, IR, AR)

Эти показатели позволяют аналитику адаптировать оценку по системе CVSS в зависимости от важности затронутого ИТ-ресурса для организации-пользователя, которая выражается через конфиденциальность, целостность и доступность. Это означает, что если какой-либо ИТ-ресурс отвечает за бизнес-функцию, для которой наиболее важна доступность, аналитик может присвоить доступности большее значение [вес] по сравнению с конфиденциальностью и целостностью. Показатель важности каждого требования безопасности имеет три возможных значения – "низкая" (Low), "средняя" (Medium) или "высокая" (High).

Их совокупное влияние на оценку среды определяется соответствующими уточненными базовыми показателями воздействия. Иными словами, эти показатели требований безопасности изменяют оценку среды путем изменения взвешенных значений показателей воздействия на конфиденциальность, целостность и доступность. Например, если показатель "важность требования конфиденциальности" (Confidentiality Requirement, CR) имеет значение "высокая", то вес показателя "уточненное воздействие на конфиденциальность" (Modified Confidentiality impact, MC) увеличивается. Соответственно если показатель "важность требования конфиденциальности" имеет значение "низкая", то вес показателя "уточненное воздействие на конфиденциальность" уменьшается. Наконец, если показатель "важность требования конфиденциальности" имеет значение "средняя", то вес показателя "уточненное воздействие на конфиденциальность" нейтрален. Те же правила применяются и к требованиям целостности и доступности.

Следует отметить, что требование конфиденциальности не влияет на оценку среды, если для (уточненного базового) показателя "воздействие на конфиденциальность" установлено значение "отсутствует" (None). Кроме того, если повысить важность требования конфиденциальности со средней до высокой, это не изменит оценку среды в ситуации, когда (уточненным базовым) показателям воздействия присвоено значение "сильное" (High), так как в этом случае уточненная частная оценка воздействия (часть уточненной базовой оценки, которая определяет воздействие) уже имеет максимальное значение 10,0.

Перечень возможных значений представлен в таблице 12. В целях краткости для всех трех показателей используется одна и та же таблица. Чем важнее требование безопасности, тем выше оценка (напоминаем, что стандартным значением является "средняя").

Таблица 12 − Важность требований безопасности

Значение показателя	Описание
Не определено (Not Defined, X)	Присвоение этого значения показателю не влияет на оценку и указывает на то, что в формуле данный показатель будет пропущен
Высокая (High, H)	Потеря [конфиденциальности | целостности | доступности] с высокой вероятностью оказывает катастрофическое неблагоприятное воздействие на организацию или частных лиц, связанных с организацией (например, сотрудников и/или клиентов)
Средняя (Medium, M)	Потеря [конфиденциальности | целостности | доступности] с высокой вероятностью оказывает серьезное неблагоприятное воздействие на организацию или частных лиц, связанных с организацией (например, сотрудников и/или клиентов)
Низкая (Low, L)	Потеря [конфиденциальности | целостности | доступности] с высокой вероятностью оказывает лишь ограниченное неблагоприятное воздействие на организацию или частных лиц, связанных с организацией (например, сотрудников и/или клиентов)

6.4.2 Уточненные базовые показатели

Эти показатели позволяют аналитику адаптировать оценку по системе CVSS с учетом изменений в анализируемой среде. Иными словами, если в среде произведены изменения общего характера, которые влияют на возможность эксплуатации, область действия или воздействие уязвимости в затронутом программном обеспечении, эти изменения можно отразить в уточненном соответствующим образом показателе среды.

Совокупное влияние всех этих показателей на оценку среды определяется соответствующими уточненными базовыми показателями. Иными словами, эти показатели изменяют оценку среды за счет присваивания других значений базовым показателям до учета показателя важности требований безопасности. Например, в конфигурации по умолчанию уязвимый компонент может запускать службу, прослушивающую трафик, с привилегиями администратора, в случае компрометации которой злоумышленник может получить возможность сильного (High) воздействия на конфиденциальность, целостность и доступность. Однако в анализируемой среде та же служба на базе интернета может работать с ограниченными привилегиями; в этом случае уточненным показателям воздействия на конфиденциальность, целостность и доступность может быть присвоено значение "слабое" (Low).

В целях краткости упоминаются только названия уточненных базовых показателей. Каждый уточненный показатель среды имеет те же значения, что и соответствующий базовый показатель, плюс значение "не определено" (Not Defined).

Целью уточненного показателя является учет мер, принятых в конкретной среде. Допустимо использовать уточненные показатели для описания ситуаций, в которых значение базового показателя повышается. Например, в конфигурации по умолчанию компоненту могут требоваться высокие привилегии (PR: High) для доступа к определенной функции, а в анализируемой среде привилегии могут не требоваться вовсе (PR: None). Чтобы отразить большую серьезность ситуации в анализируемой среде, аналитик может присвоить показателю MPR (уточненная потребность в привилегиях) значение "нет" (None).

Перечень возможных значений представлен в таблице 13.

Таблица 13 − Уточненные базовые показатели

Уточненный базовый показатель	Соответствующие значения
Уточненный вектор атаки (Modified Attack Vector, MAV)	Те же, что и у соответствующего базового показателя (см. выше "Базовые показатели"), плюс присваиваемое по умолчанию значение "не определено" (Not Defined)
Уточненная сложность атаки (Modified Attack Complexity, MAC)	
Уточненная потребность в привилегиях (Modified Privileges Required, MPR)	
Уточненное взаимодействие с пользователем (Modified User Interaction, MUI)	
Уточненная область действия (Modified Scope, MS)	
Уточненное воздействие на конфиденциальность (Modified Confidentiality, MC)	
Уточненное воздействие на целостность (Modified Integrity, MI)	
Уточненное воздействие на доступность (Modified Availability, MA)	

6.5 Качественная шкала оценки серьезности

Для некоторых целей полезно иметь текстовое представление количественных оценок базовых показателей, временны́х показателей и показателей среды. Все количественные оценки могут быть сопоставлены с качественными оценками[3], определенными в таблице 14.

Таблица 14 − Качественная шкала оценки серьезности

Качественная оценка (уровень серьезности)	Оценка по CVSS
Нет (None)	0,0
Низкий (Low)	0,1–3,9
Средний (Medium)	4,0–6,9
Высокий (High)	7,0–8,9
Критический (Critical)	9,0–10,0

Например, базовой оценке 4,0 по системе CVSS соответствует "средний" (Medium) уровень серьезности. Использование этих качественных оценок серьезности необязательно, и при публикации оценок по системе CVSS указывать их не требуется. Они призваны помочь организациям в надлежащем определении качества и приоритета процессов управления уязвимостями.

6.6 Векторная строка

Векторная строка CVSS v3.0 – это текстовое представление набора показателей CVSS. Она широко применяется для записи или передачи информации о показателях в краткой форме.

Векторная строка в версии 3.0 начинается с метки "CVSS:" и числового представления текущей версии системы, "3.0". Информация о показателях приводится в виде набора показателей, где каждому

[3] Следует отметить, что это сопоставление между количественными и качественными оценками применимо независимо от того, какие группы показателей используются – только базовые или все перечисленные выше.

показателю предшествует косая черта (/), отделяющая элементы набора друг от друга. Каждый элемент набора состоит из сокращенного названия показателя, двоеточия (:) и соответствующего сокращенного значения показателя. Краткие формы определены в данной спецификации выше (в скобках после названия и значения каждого показателя) и сведены в приведенной ниже таблице.

Порядок следования показателей в векторной строке может быть произвольным, хотя в таблице 15 дается предпочтительный порядок. Векторная строка должна включать все базовые показатели. Временны́е показатели и показатели среды необязательны, и для опущенных показателей предполагается значение "не определено" (Not Defined, X). При желании показатели со значением "не определено" можно явно включить в векторную строку. Программы для чтения векторных строк CVSS v3.0 должны допускать следование показателей в любом порядке и интерпретировать не указанные временны́е показатели и показатели среды как имеющие значение "не определено". Включение одного и того же показателя в векторную строку более одного раза не допускается.

Таблица 15 − Базовый вектор, временно́й вектор и вектор среды

Группа показателей	Полное и сокращенное название показателя	Возможные значения	Обязательный или нет
Базовые показатели	Вектор атаки (Attack Vector, AV)	[N, A, L, P]	Да
	Сложность атаки (Attack Complexity, AC)	[L, H]	Да
	Потребность в привилегиях (Privileges Required, PR)	[N, L, H]	Да
	Взаимодействие с пользователем (User Interaction, UI)	[N, R]	Да
	Область действия (Scope, S)	[U, C]	Да
	Воздействие на конфиденциальность (Confidentiality, C)	[H, L, N]	Да
	Воздействие на целостность (Integrity, I)	[H ,L, N]	Да
	Воздействие на доступность (Availability, A)	[H, L, N]	Да
Временны́е показатели	Зрелость кода эксплойта (Exploit code maturity, E)	[X, H, F, P, U]	Нет
	Уровень устранения (Remediation Level, RL)	[X, U, W, T, O]	Нет
	Достоверность сообщения (Report Confidence, RC)	[X, C, R, U]	Нет
Показатели среды	Важность требования конфиденциальности (Confidentiality Req., CR)	[X, H, M, L]	Нет
	Важность требования целостности (Integrity Req., IR)	[X, H, M, L]	Нет
	Важность требования доступности (Availability Req., AR)	[X, H, M, L]	Нет
	Уточненный вектор атаки (Modified Attack Vector, MAV)	[X, N, A, L, P]	Нет
	Уточненная сложность атаки (Modified Attack Complexity, MAC)	[X, L, H]	Нет
	Уточненная потребность в привилегиях (Modified Privileges Required, MPR)	[X, N, L, H]	Нет

Таблица 15 − Базовый вектор, временно́й вектор и вектор среды

Группа показателей	Полное и сокращенное название показателя	Возможные значения	Обязательный или нет
	Уточненное взаимодействие с пользователем (Modified User Interaction, MUI)	[X, N, R]	Нет
	Уточненная область действия (Modified Scope, MS)	[X, U, C]	Нет
	Уточненное воздействие на конфиденциальность (Modified Confidentiality, MC)	[X, N, L, H]	Нет
	Уточненное воздействие на целостность (Modified Integrity, MI)	[X, N, L, H]	Нет
	Уточненное воздействие на доступность (Modified Availability, MA)	[X, N, L, H]	Нет

Например, уязвимость со значениями базовых показателей "вектор атаки: сетевой, сложность атаки: низкая, потребность в привилегиях: высокая, взаимодействие с пользователем: отсутствует, область действия: не меняется, воздействие на конфиденциальность: слабое, воздействие на целостность: слабое, воздействие на доступность: отсутствует" и без указанных временных показателей или показателей среды даст следующий вектор:

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N.

Та же уязвимость с добавлением значений показателей "возможность эксплуатации: функциональная, уровень устранения: не определено" и с перечислением показателей в порядке, отличном от рекомендуемого, даст следующий вектор:

CVSS:3.0/S:U/AV:N/AC:L/PR:H/UI:N/C:L/I:L/A:N/E:F/RL:X.

6.7 Определение XML-схемы CVSS v3.0

Определение XML-схемы (XSD) для системы CVSS задает структуру XML-файла со значениями показателей CVSS. Оно будет полезно тем, кто хотел бы хранить или передавать такие данные в формате XML. XSD-файл доступен по адресу: https://www.first.org/cvss/cvss-v3.0.xsd.

6.8 Формулы CVSS v3.0

Ниже приведены формулы CVSS v3.0.

6.8.1 Базовая оценка

Формула базовой *оценки* есть функция от формул частных оценок воздействия и возможности эксплуатации. Базовая оценка определяется следующим образом:

If (*Impact sub score* <= 0)	0 *else*,
Scope Unchanged[4] *(оценка не изменяется)*	*Roundup*(*Minimum* [(*Impact* + *Exploitability*), 10]);
Scope Changed (оценка изменяется)	*Roundup*(*Minimum* [1,08 × (*Impact* + *Exploitability*), 10]).

[4] Функция Round up (округление) определяется как наименьшее значение, заданное с точностью до одного знака после запятой, большее или равное входному значению. Например, Round up(4,02) = 4,1, а Round up(4,00) = 4,0.

Частная оценка воздействия (ISC) определяется как:

Scope Unchanged $6{,}42 \times ISC_{Base}$;

Scope Changed $7{,}52 \times [ISC_{Base} - 0{,}029] - 3{,}25 \times [ISC_{Base} - 0{,}02]^{15}$,

где:

$$ISC_{Base} = 1 - \left[\left(1 - Impact_{Conf}\right) \times \left(1 - Impact_{Integ}\right) \times \left(1 - Impact_{Avail}\right)\right],$$

а частная оценка возможности эксплуатации определяется как:

$$8{,}22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction.$$

6.8.2 Временна́я оценка

Временна́я оценка (Temporal score) определяется следующим образом:

$$Roundup\ (BaseScore \times ExploitCodeMaturity \times RemediationLevel \times ReportConfidence).$$

6.8.3 Оценка среды

Оценка среды (Environmental score) определяется следующим образом:

If (*Modified Impact Sub score* <= 0)	0 else,
If Modified Scope is Unchanged	*Round up*(*Round up* (*Minimum* [× (M.Impact + M.Exploitability),10]) × Exploit Code Maturity × Remediation Level × Report Confidence);
If Modified Scope is Changed	*Round up*(*Round up* (*Minimum* [1,08 × (M.Impact + M.Exploitability × Exploit Code Maturity × Remediation Level × Report Confidence).

Уточненная частная оценка воздействия определяется следующим образом:

If Modified Scope is Unchanged	$6{,}42 \times \left[ISC_{Modified}\right]$;
If Modified Scope is Changed	$7{,}52 \times \left[ISC_{Modified} - 0{,}029\right] - 3{,}25 \times \left[ISC_{Modified} - 0{,}02\right]^{15}$,

где:

$$ISC_{Modified} = Minimum\left[\left[1 - \left(1 - M.I_{Conf} \times CR\right) \times \left(1 - M.I_{Integ} \times IR\right) \times \left(1 - M.I_{Avail} \times AR\right)\right], 0{,}915\right].$$

Частная оценка возможности эксплуатации определяется как

$$8{,}22 \times M.AttackVector \times M.AttackComplexity \times M.PrivilegeRequired \times M.UserInteraction.$$

6.8.4 Уровни показателей

Значения показателей определены в таблице 16.

Таблица 16 − Значения показателей

Показатель	Значение показателя	Числовое значение
Вектор атаки (Attack Vector)/ уточненный вектор атаки (Modified Attack Vector)	Сетевой (Network)	0,85
	Соседский (Adjacent Network)	0,62
	Локальный (Local)	0,55
	Физический (Physical)	0,2
Сложность атаки (Attack Complexity)/ уточненная сложность атаки (Modified Attack Complexity)	Низкая (Low)	0,77
	Высокая (High)	0,44
Потребность в привилегиях (Privileges Required)/ уточненная потребность в привилегиях (Modified Privileges Required)	Отсутствует (None)	0,85
	Низкая (Low)	0,62 (0,68, если показатель "область действия" (Scope)/"уточненная область действия" (Modified Scope) имеет значение "меняется" (Changed))
	Высокая (High)	0,27 (0,50, если показатель "область действия" (Scope)/ "уточненная область действия" (Modified Scope) имеет значение "меняется" (Changed))
Взаимодействие с пользователем (User Interaction)/ уточненное взаимодействие с пользователем (Modified User Interaction)	Отсутствует (None)	0,85
	Требуется (Required)	0,62
Воздействие на C, I, A/ уточненное воздействие на C, I, A	Сильное (High)	0,56
	Слабое (Low)	0,22
	Отсутствует (None)	0
Зрелость кода эксплойта (Exploit Code Maturity)	Не определено (Not Defined)	1
	Высокая (High)	1
	Функциональная (Functional)	0,97
	Доказана правильность концепции (Proof-of-Concept)	0,94
	Непроверенная (Unproven)	0,91

Таблица 16 − Значения показателей

Показатель	Значение показателя	Числовое значение
Уровень устранения (Remediation Level)	Не определено (Not Defined)	1
	Недоступно (Unavailable)	1
	Обходной прием (Workaround)	0,97
	Вре́менное исправление (Temporary Fix)	0,96
	Официальное исправление (Official Fix)	0,95
Достоверность сообщения (Report Confidence)	Не определено (Not Defined)	1
	Подтверждена (Confirmed)	1
	Разумная (Reasonable)	0,96
	Неизвестна (Unknown)	0,92
Важность требований безопасности – важность требований C, I, A (CR)	Не определено (Not Defined)	1
	Высокая (High)	1,5
	Средняя (Medium)	1
	Низкая (Low)	0,5

6.8.5 Замечания о формулах и вычислении оценок в CVSS v3.0

Формула CVSS v3.0 обеспечивает математическую аппроксимацию всех возможных комбинаций показателей, ранжированных по уровню серьезности (таблица подстановки значений показателей уязвимости). Для получения формулы CVSS v3.0 специальная группа по этой проблеме (SIG) составила таблицу подстановки, присвоив значения показателей по системе CVSS v3.0 реальным уязвимостям и уровням серьезности (низкий, средний, высокий, критический). Определив приемлемые диапазоны числовых значений для каждого уровня серьезности, SIG в сотрудничестве с Deloitte & Touche LLP скорректировала параметры формулы, чтобы установить соответствие между комбинациями показателей CVSS v3.0 и предлагаемыми SIG оценками степени серьезности.

Учитывая ограниченное количество возможных числовых значений (101 значение в диапазоне от 0,0 до 10,0), разные комбинации значений показателей могут давать одну и ту же итоговую оценку. Кроме того, некоторые числовые оценки могут опускаться, потому что соответствующие вес и расчетные формулы определяются по уровням серьезности, сопоставленным с комбинациями показателей. Наконец, при некоторых комбинациях значений показателей могут возникать отклонения от желаемого порогового уровня серьезности. Это неизбежно, и простой поправки на этот случай не существует, поскольку изменение значения одного показателя или параметра формулы может привести к другим отклонениям – возможно, еще более существенным.

По общему согласию, как и в CVSS v2.0, допустимое отклонение было установлено равным 0,5. Это означает, что все комбинации значений показателей, на основе которых определяется вес и производятся расчеты, будут давать числовую оценку в пределах ±0,5 от присвоенного им уровня серьезности. Например, комбинация, для которой предусмотрен высокий (High) уровень серьезности, может давать числовую оценку в диапазоне от 6,6 до 9,3. Наконец, в целях обратной совместимости в CVSS v3.0 сохраняется диапазон значений от 0,0 до 10,0.

Дополнение I

Руководство пользователя CVSS v3.0

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Введение

Данное руководство служит дополнением к официальной спецификации CVSS v3.0. В нем приводится дополнительная информация, описываются значимые изменения по сравнению с версией 2.0, а также даются руководящие указания по вычислению оценок и сводка соответствующих алгоритмов.

Система оценки общеизвестных уязвимостей (CVSS) позволяет выделить основные характеристики уязвимости и дать количественную (числовую) оценку степени ее серьезности, а также текстовое представление этой оценки. Количественная оценка затем может быть преобразована в качественную (низкая, средняя, высокая или критическая), чтобы помочь организациям надлежащим образом определить качество и приоритет процессов управления уязвимости.

CVSS дает три важных преимущества.

- Она обеспечивает стандартизованную оценку уязвимостей. Пользуясь общим алгоритмом оценки уязвимостей на всех ИТ-платформах, организация может проводить единую политику управления уязвимостями с определением максимально допустимых сроков проверки наличия и устранения конкретной уязвимости.
- Она представляет собой открытую систему. Произвольная оценка, присвоенная уязвимости какой-либо третьей стороной, может дезориентировать пользователей. В CVSS четко видны отдельные характеристики, на основе которых формируется оценка.
- CVSS помогает приоритезировать риски. При вычислении оценки среды уязвимость ставится в контекст конкретной организации, что помогает получить лучшее представление о риске, который влечет за собой эта уязвимость для организации.

С момента первого выпуска в 2004 году система CVSS получила широкое распространение. В сентябре 2007 года система CVSS v2.0 была принята в качестве составной части Стандарта безопасности данных индустрии платежных карт (PCI DSS). Чтобы обеспечить соответствие стандарту PCI DSS, продавцы, обрабатывающие кредитные карты, обязаны продемонстрировать, что ни в одной из используемых ими вычислительных систем не имеется ни одной уязвимости, оценка которой по CVSS больше или равна 4,0. В 2007 году Национальный институт стандартов и технологий (NIST) включил CVSS v2.0 в состав своего протокола автоматизации управления данными безопасности[5] (SCAP). В апреле 2011 года система CVSS v2.0 была официально принята в качестве международного стандарта оценки уязвимостей (Рекомендация МСЭ-Т X.1521[6]).

I.2 Изменения в CVSS v3.0

Учитывая широкое распространение, которое получила система CVSS v2.0, был выявлен целый ряд возможностей для ее усовершенствования, что послужило побудительным мотивом к разработке версии 3.0. Соответствующие изменения подробно описываются ниже.

I.2.1 Область действия, уязвимый компонент и атакуемый компонент

При использовании CVSS v2.0 разработчики сталкивались с трудностями при оценке уязвимостей, которые приводили к полной компрометации их программного обеспечения, но лишь частично воздействовали на операционную систему хоста. В версии 2.0 уязвимости оценивались относительно операционной система хоста, что побудило одного из разработчиков приложений внедрить по соглашению дополнительное значение показателя воздействия – "частичное+" (Partial+)[7]. В CVSS v3.0 эта проблема решена за счет изменения контекста оценки показателей воздействия и введения нового

---

[5] См. http://scap.nist.gov/.

[6] См. https://www.itu.int/rec/T-REC-X.1521-201104-I/en.

[7] Например, см. http://www.oracle.com/technetwork/topics/security/cvssscoringsystem-091884.html.

показателя "область действия" (Scope), который более подробно обсуждается ниже. Поэтому одним из важных концептуальных изменений, внесенных в CVSS v3.0, стала возможность оценки уязвимостей, существующих в одном программном компоненте (который формально именуется *уязвимым компонентом*), но воздействующих на другой программный, аппаратный или сетевой компонент (который формально именуется *атакуемым компонентом*), как показано на рисунке I.1[8].

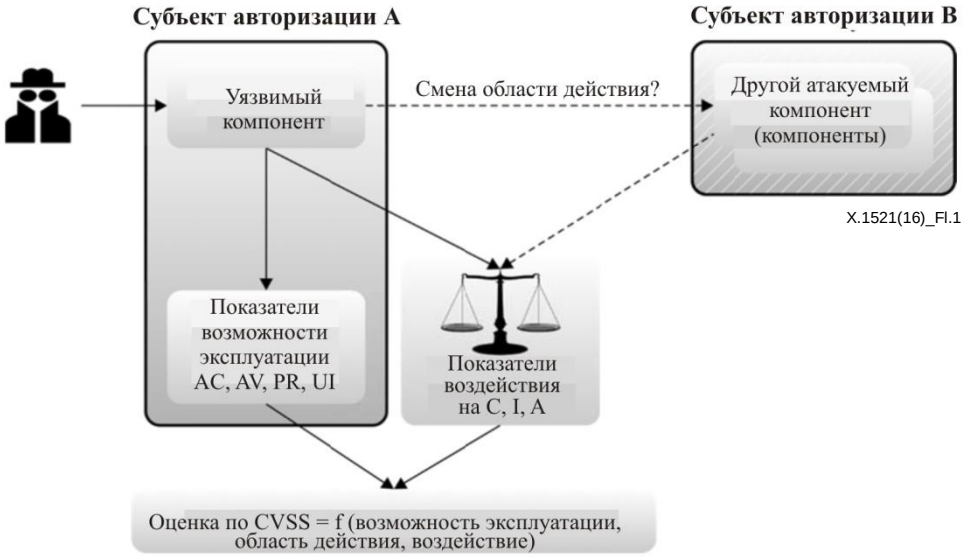


Рисунок I.1 − Изменение области действия

Для примера рассмотрим уязвимость в виртуальной машине, которая компрометирует операционную систему хоста. Уязвимым компонентом в данном случае является виртуальная машина, а атакуемым – операционная система хоста. Поскольку эти два компонента независимо управляют привилегиями на доступ к вычислительным ресурсам, они представляют собой разные субъекты авторизации. На рисунке I.1 виртуальной машиной управляет субъект A, а ОС хоста – субъект B. Когда эксплуатация уязвимости затрагивает два субъекта, в системе CVSS считается, что произошла *смена области действия*. Эта ситуация отражена в новом показателе – "область действия" (Scope).

Как показано на рисунке I.1, при оценке уязвимостей по CVSS v3.0 показатели возможности эксплуатации оцениваются относительно уязвимого компонента, то есть компонента, в программном коде которого содержится ошибка. При этом показатели воздействия оцениваются относительно атакуемого компонента. В некоторых случаях уязвимый и атакуемый компоненты могут совпадать, и тогда смены области действия не происходит. Однако бывает и так, что воздействие испытывает как уязвимый компонент, так и атакуемый. В этих случаях происходит смена области действия, и показатели воздействия должны отражать воздействие на конфиденциальность, целостность и доступность (CIA) применительно либо к уязвимому компоненту, либо к атакуемому компоненту в зависимости от того, для какого из них последствия являются наихудшими.

В случае уязвимости, которая дает возможность кражи файла паролей, самым непосредственным ее результатом является потеря конфиденциальности локального системного файла, хотя впоследствии злоумышленник может предпринимать дальнейшие шаги для несанкционированного доступа к учетным записям. Исходя из этого область действия не меняется. В случае же уязвимости, которая позволяет злоумышленнику переписать ARP-таблицу маршрутизатора, воздействие имеет двоякий характер: во-первых, воздействие на системный файл маршрутизатора (воздействие на целостность уязвимого компонента), а во-вторых, воздействие на интернет-службы, обслуживаемые маршрутизатором (воздействие на доступность затрагиваемых систем). Поскольку оценка должна отражать наиболее серьезные последствия, оценка показателя воздействия может отражать либо

[8] Следует отметить, что уязвимый компонент – это всегда программное обеспечение (операционная система хоста, интернет-приложение, драйвер устройства и т. д.), а атакуемым компонентом может быть либо другое программное обеспечение, либо устройство, либо сетевой ресурс.

потерю целостности уязвимого компонента, либо потерю доступности интернет-служб в зависимости от того, какое из этих двух последствий серьезнее[9].

I.2.2 Вектор атаки

Показатель "вектор доступа" (Access Vector) из версии 2.0 был переименован в "вектор атаки" (Attack Vector), но по-прежнему, как правило, отражает степень удаленности злоумышленника от уязвимого компонента. Иными словами, чем дальше находится злоумышленник от уязвимого компонента (в смысле логической и физической удаленности в сети), тем выше будет базовая оценка. Кроме того, теперь в этом показателе проводится разграничение между локальными атаками, требующими локального доступа к системе (например, атака на настольное приложение), и физическими атаками, требующими физического доступа к платформе для эксплуатации уязвимости (например, атака через физический интерфейс Firewire или USB либо атака с выходом из изолированной программной среды).

I.2.3 Сложность атаки

В показателе "сложность доступа" (Access Complexity) из версии 2.0 смешивались два различных аспекта: находящиеся вне контроля злоумышленника программные, аппаратные или сетевые факторы, которые должны присутствовать для успешной эксплуатации уязвимости (например, условия состязания в программе или конкретная конфигурация приложения), и требование взаимодействия с пользователем (например, необходимость запуска вредоносного исполняемого файла пользователем). Поэтому показатель "сложность доступа" был разделен на два показателя – "сложность атаки" (Attack Complexity), (который отражает первый аспект) и "**взаимодействие с пользователем**" (User Interaction), который отражает второй аспект).

I.2.4 Потребность в привилегиях

Новый показатель "**потребность в привилегиях**" (**Privileges Required**) вводится взамен показателя "аутентификация" (Authentication), который использовался в CVSS v2.0. Вместо определения *количества* отдельных процессов аутентификации в системе, которые должен пройти злоумышленник, показатель "потребность в привилегиях" отражает *уровень доступа*, необходимый для успешной атаки. Значения "высокая", "низкая" и "отсутствует" этого показателя отражают степень, в которой злоумышленнику необходимы привилегии для эксплуатации уязвимости.

I.2.5 Показатели воздействия

Показателям **воздействия на конфиденциальность, целостность и доступность** вместо значений "отсутствует" (None), "частичное" (Partial) и "полное" (Complete), которые использовались в версии 2.0, присваиваются теперь значения "отсутствует" (None), "слабое" (Low) и "сильное" (High). Вместо общей *процентной доли* систем, на которые воздействует атака, новые показатели отражают общую *степень* воздействия атаки. Например, хотя уязвимость Heartbleed[10] привела к потере лишь небольшого количества информации, ее воздействие было весьма серьезным. В CVSS v2.0 это воздействие получило бы оценку "частичное" (Partial), а в CVSS v3.0 оно надлежащим образом оценивается как "сильное" (High).

Кроме того, в приведенном выше примере показатели воздействия теперь отражают последствия для атакуемого компонента, который может совпадать, а может и не совпадать с компонентом, содержащим эксплуатируемую уязвимость.

I.2.6 Временны́е показатели

Влияние временны́х показателей в CVSS v3.0 понижено по сравнению с версией 2.0. Показатель "возможность эксплуатации" (Exploitability) получил новое название "зрелость кода эксплойта" (Exploit Code Maturity), лучше отражающее его суть.

---

9 Дополнительную информацию см. в документе с примерами, прилагаемом к настоящему руководству.

10 См. http://heartbleed.com/.

I.2.7 Показатели среды

Показатели среды "распределение целей" (Target Distribution) и "возможность сопутствующего ущерба" (Collateral Damage Potential) были заменены рядом уточненных показателей, учитывающих реализованные в среде пользователя меры и средства безопасности, ослабляющие воздействие успешно эксплуатированной уязвимости, или, наоборот, слабые места, которые усиливают воздействие этой уязвимости.

I.2.8 Качественная шкала оценки серьезности

В некоторых организациях были созданы системы, сопоставляющие количественные оценки по системе CVSS v2.0 с качественными оценками. В CVSS v3.0 предусмотрено стандартное отображений числовых значений оценок в качественные оценки уровней серьезности "нет" (None), "низкий" (Low), "средний" (Medium), "высокий" (High) и "критический" (Critical), как описано в официальной спецификации CVSS v3.0. Использование этих качественных оценок серьезности необязательно, и при публикации оценок по системе CVSS указывать их не требуется.

Организациям, использующим количественные оценки по системе CVSS v3.0, которые желают использовать *альтернативную* систему качественной оценки серьезности, следует во избежание недоразумений применять другие формулировки качественных оценок или четко указать, что их качественные оценки не соответствуют спецификации CVSS v3.0.

I.2.9 Сводный перечень изменений

Одно из важных следствий описанных выше изменений состоит в том, что оценки по системе CVSS версий 2.0 и 3.0 не всегда могут быть сопоставимы. Например, содержащаяся в приложении уязвимость, способная привести к его полной компрометации, по версии 2.0 была бы оценена с присвоением показателям воздействия на конфиденциальность, целостность и доступность значения "частичное" (Partial). В версии 3.0 эквивалентным показателям воздействия той же уязвимости было бы присвоено значение "сильное" (High).

Сводный перечень изменений по сравнению с версией 2.0 представлен в таблице I.1.

Таблица I.1 – Изменения в CVSS версии 3.0 по сравнению с версией 2.0

Версия 2.0	Версия 3.0
Уязвимости оценивались по общему воздействию на платформу хоста	Уязвимости теперь оцениваются по воздействию на атакуемый компонент
Не учитывались ситуации, в которых уязвимость одного приложения влияет на другие приложения в той же системе	Введен новый показатель "область действия" (Scope) для учета уязвимостей, при которых *подвергающийся воздействию объект* (атакуемый компонент), отличается от *объекта, содержащего уязвимость* (уязвимого компонента)
В показателе "вектор доступа" (Access Vector) не различались атаки, требующие локального доступа, и физические атаки на аппаратное обеспечение	Введен показатель "вектор атаки" (Attack Vector), для которого предусмотрены отдельные значения "локальный" (Local) и "физический" (Physical)
Показатель "сложность доступа" (Access Complexity) порой объединял такие факторы, как конфигурация системы и взаимодействие с пользователем	Взамен введены два показателя: "сложность атаки" (Attack Complexity), учитывающий сложность системы, и "взаимодействие с пользователем" (User Interaction), учитывающий необходимость участия пользователей для совершения успешной атаки
На практике оценки показателя "аутентификация" (Authentication) были смещены в сторону двух из трех возможных вариантов и неэффективно отражали нужный аспект уязвимости	Взамен введен новый показатель "потребность в привилегиях" (Privileges Required), который отражает наивысший уровень привилегий, необходимый злоумышленнику, а не количество процессов аутентификации, которое должен пройти злоумышленник

Таблица I.1 – Изменения в CVSS версии 3.0 по сравнению с версией 2.0

Версия 2.0	Версия 3.0
Показатели воздействия отражали процентную долю воздействия, оказанного на уязвимое приложение	Показатели воздействия отражают степень воздействия и принимают теперь значения "отсутствует" (None), "слабое" (Low) и "сильное" (High)
Полезность показателей среды "распределение целей" (Target Distribution) и "возможность сопутствующего ущерба" (Collateral Damage Potential) не была установлена	Показатели "распределение целей" (Target Distribution) и "возможность сопутствующего ущерба" (Collateral Damage Potential) были заменены рядом уточненных показателей, отражающих факторы, которые ослабляют воздействие
В CVSS v2.0 отсутствовала возможность оценки нескольких уязвимостей, используемых в одной атаке	Хотя соответствующий формальный показатель не предусмотрен, но ниже, в подразделе "Построение цепочек уязвимостей", даны руководящие указания по оценке нескольких уязвимостей
Не были предусмотрены официальные критерии качественной оценки	Диапазоны числовых значений сопоставлены с качественной шкалой оценки серьезности с пятью градациями

I.3 Руководство по оценке

Ниже дается ряд рекомендаций аналитикам по оценке уязвимостей с использованием системы CVSS v3.0.

I.3.1 Оценка по CVSS в рамках жизненного цикла эксплойта

Аналитикам, когда им станет ясно, в какое время необходимо провести оценку воздействия уязвимостей, следует ограничить рассмотрение воздействия разумным конечным результатом, которого, по их мнению, гарантированно достигнет злоумышленник. Возможность оказания такого воздействия должна быть подкреплена как минимум частной оценкой возможности эксплуатации. Однако обоснование может также содержать подробную информацию из описания уязвимости. Для примера рассмотрим две уязвимости.

Уязвимость 1 состоит в том, что не прошедший аутентификацию удаленной злоумышленник может передать на веб-сервер простейших запрос специального вида, который приведет к раскрытию веб-сервером пароля учетной записи корневого пользователя/администратора в открытой текстовой форме. Из частной оценки возможности эксплуатации и описания уязвимости аналитик знает только то, что злоумышленник обладает достаточным уровнем доступа для отправки запроса специального вида на веб-сервер в целях эксплуатации уязвимости. Оценка воздействия должна ограничиваться этим; хотя злоумышленник *может* быть в состоянии воспользоваться этой удостоверяющей информацией для запуска кода с привилегиями администратора, неизвестно, есть ли у него доступ к приглашению для входа в систему или возможность выполнять команды с данной удостоверяющей информацией. Получение доступа к этому паролю влечет за собой лишь прямую серьезную потерю конфиденциальности:

Базовая оценка: 7.5 [CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N].

Уязвимость 2 состоит в том, что локальный пользователь с низким уровнем привилегий может послать в операционную систему простейший запрос специального вида, который приведет к раскрытию ею пароля учетной записи корневого пользователя/администратора в открытой текстовой форме. Из частной оценки возможности эксплуатации и описания уязвимости аналитик знает, что злоумышленник имеет доступ к операционной системе и может войти в нее локально как пользователь с низким уровнем привилегий. Получение доступа к этому паролю влечет за собой прямую серьезную потерю конфиденциальности, целостности и доступности, поскольку разумно допустить, что пользователь в этом случае способен выполнять команды от имени учетной записи корневого пользователя/администратора (предполагая, что злоумышленник может выйти из своей учетной записи и войти в качестве корневого пользователя):

Базовая оценка: 7.8 [CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H].

I.3.2 Отличие воздействия на конфиденциальность и целостность от воздействия на доступность

Показатели "воздействие на конфиденциальность" и "воздействие на целостность" описывают воздействие на *данные*, используемые службой. Например, это может быть вредоносное изменение содержимого веб-сайта или кража системных файлов. Показатель "воздействие на доступность" описывает воздействие на *работу* службы. Иными словами, показатель "воздействие на доступность" говорит о функционировании и качестве работы самой службы, а не о доступности ее данных. Рассмотрим уязвимость в интернет-службе (такой, как веб-служба, электронная почта или система наименований доменов (DNS)), которая позволяет злоумышленнику изменить или удалить все файлы веб-сайта в каталоге. Такая уязвимость окажет воздействие только на целостность, но не на доступность, потому что веб-служба по-прежнему работает надлежащим образом, но при этом возвращает измененное содержимое.

I.3.3 Локальные уязвимости, эксплуатируемые удаленными злоумышленниками

В CVSS v2.0 рекомендация по оценке № 5 гласила: "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)". Эта рекомендация иногда вела к недоразумениям в случаях, когда злоумышленник мог обманом побудить пользователя загрузить вредоносный документ с удаленного веб-сервера, эксплуатируя уязвимость в подсистеме синтаксического разбора файлов. В таких ситуациях аналитики, использующие CVSS v2.0, должны были бы рассматривать эти уязвимости как сетевые и присвоить им векторные строки вроде AV:N/AC:M/Au:N/C:P/I:P/A:P или AV:N/AC:M/Au:N/C:C/I:C/A:C.

В системе CVSS v3.0 эта рекомендация была усовершенствована за счет более ясного определения значений "сетевой" (Network) и "соседский" (Adjacent) показателя "вектор атаки" (Attack Vector). В частности аналитикам следует присваивать этому показателю значения "сетевой" или "соседский" только в том случае, если уязвимость привязана к сетевому стеку. В случае уязвимостей, требующих взаимодействия с пользователем для загрузки или приема вредоносного контента (который может также доставляться локально, например через USB-накопители), этому показателю следует присваивать значение "локальный".

Например, уязвимость в подсистеме синтаксического разбора документов, для успешной эксплуатации которой не нужна сеть, как правило, следует оценивать путем присвоения значения "локальный", независимо от метода распространения вредоносного документа (будь то ссылка на веб-сайт или распространение через USB-накопитель).

I.3.4 Уязвимости типа "межсайтовый скриптинг"

В CVSS v2.0 необходимо было следовать специальным указаниям, чтобы получить ненулевые оценки для уязвимостей типа "межсайтовый скриптинг" (XSS), поскольку уязвимости оценивались относительно содержавшей их операционной системы хоста. Обычно XSS-уязвимостям давалась оценка, описывающая частичное воздействие на целостность из-за изменения отклика веб-сервера клиенту: AV:N/AC:M/Au:N/C:N/I:P/A:N. Так было даже в случае XSS-уязвимостей объектной модели документа (DOM), которые эксплуатировались целиком на клиентской стороне (например когда доставленный с сервера код JavaScript производил синтаксический разбор строки запроса, переданной на сервер), хотя бы и в результате взаимодействия с сервером.

Это был один из ключевых сценариев, в расчете на который был введен показатель "область действия" (Scope). С его помощью удалось учесть случаи, когда воздействие испытывает не уязвимый компонент (например, веб-сервер или доставляемый им код JavaScript), а другой компонент, привилегиями которого управляет отдельный субъект авторизации (например, среда клиентского браузера). Поэтому в CVSS v3.0 уязвимости типа "межсайтовый скриптинг" не приходится ограничивать незначительным или вовсе отсутствующим воздействием на сервер, и теперь их можно оценивать по воздействию на клиентскую сторону. Отраженная XSS-уязвимость, с помощью которой злоумышленник может доставить жертве вредоносную ссылку и запустить в ее браузере код JavaScript, может быть оценена следующим образом:

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N.

I.3.5 Атака через посредника

В CVSS v3.0 явно предусмотрена оценка атак через посредника (Man in the Middle). В то время как в CVSS v2.0 этот тип атак конкретно не рассматривался, в версии 3.0 он учитывается с помощью показателя "сложность атаки" (Attack Complexity).

I.3.6 Аппаратные уязвимости

Хотя система CVSS предназначена главным образом для оценки уязвимостей в программном обеспечении и их воздействия на программное обеспечение, CVSS версии 3.0 теперь лучше подходит для оценки воздействия на аппаратные компоненты и сети.

I.3.7 Построение цепочек уязвимостей

Система CVSS предназначена для классификации и оценки отдельных уязвимостей. Вместе с тем важно учесть потребности сообщества специалистов по анализу уязвимостей, предусмотрев метод оценки случаев, в которых в ходе одной атаки эксплуатируется сразу несколько уязвимостей для компрометации хоста или приложения. Оценка нескольких уязвимостей применительно к такой ситуации называется построением цепочки уязвимостей. Следует отметить, что этот показатель не является официальным, а включен сюда в качестве ориентира для использования аналитиками по оценке таких атак.

При оценке цепочки уязвимостей в обязанности аналитика входит определение видов объединенных в цепочку уязвимостей, на основе которых формируется итоговая оценка для цепочки. Аналитику следует перечислить эти отдельные уязвимости и их оценки, а также указать итоговую оценку для цепочки. Например, это можно сделать в уведомлении о раскрытии уязвимостей, опубликованном на веб-странице.

Кроме того, аналитик может указать и другие виды уязвимостей, которые могут быть объединены в цепочку с оцениваемыми уязвимостями. В частности, аналитик может перечислить обобщенные виды (или классы) взаимосвязанных уязвимостей, которые часто объединяются в цепочку, или дать более подробные описания необходимых условий их эксплуатации. Например, можно описать, как определенные виды уязвимостей с внедрением SQL-кода могут стать предпосылками к атаке типа "межсайтовый скриптинг" (XSS) или как конкретный вид переполнения буфера может обеспечить получение привилегий локального доступа. Перечисление обобщенных видов или классов уязвимостей предоставляет минимальную информацию, необходимую для предупреждения других пользователей, не сообщая при этом злоумышленникам о новых возможностях эксплуатации уязвимостей.

Как вариант, аналитик может определить (в форме машиночитаемого и пригодного для синтаксического разбора списка уязвимостей с идентификаторами общеизвестных уязвимостей и незащищенности (CVE) или перечня общеизвестных слабых мест (CWE)) полный список конкретных взаимосвязанных уязвимостей, которые на практике объединяются (или с высокой вероятностью могут быть объединены) в цепочку с одной или несколькими уязвимостями в оцениваемой цепочке для эксплуатации ИТ-системы. В случае если эксплуатация уязвимости возможна только при выполнении других необходимых условий (таких как предварительная эксплуатация некоторой другой уязвимости), допустимо объединить две или более оценки по системе CVSS для описания цепочки уязвимостей исходя из наименее ограничительной частной оценки возможности эксплуатации и наибольшей частной оценки воздействия. В следующем примере для описания цепочки уязвимостей используются частные оценки возможности эксплуатации, области действия и воздействия.

Уязвимость A описывается векторной строкой AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H, и как видно из нее для эксплуатации этой уязвимости требуется локальный пользователь с низким уровнем привилегий. В свою очередь уязвимость B описывается векторной строкой AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L и предоставляет непривилегированному удаленному злоумышленнику возможность выполнять код в системе со значением показателя воздействия "слабое" (Low) при условии взаимодействия с локальным пользователем для реализации атаки. Поэтому имея A и B, цепочку уязвимостей C = B > A можно описать векторной строкой AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H, которая сочетает в себе возможность эксплуатации уязвимости B, неизменную область действия в обоих случаях и воздействие уязвимости A, потому что в случае возможности эксплуатации уязвимости B и получении возможности выполнять код от лица локального пользователя удовлетворяются необходимые условия для последующей эксплуатации уязвимости A, оказывающей воздействие.

I.4 Словарь терминов

Субъект авторизации (authority) – вычислительная среда с определенными границами, предоставляющая привилегии для доступа к ресурсам и управляющая ими. Примерами субъектов авторизации могут служить приложение базы данных, операционная система и изолированная программная среда.

Итоговая оценка для цепочки (chained score) – базовая оценка, получаемая в результате оценивания цепочки из двух или более уязвимостей.

Цепочка уязвимостей (chained vulnerabilities) – см. термин "построение цепочек уязвимостей".

Компонент (component) – относится либо к программному, либо к аппаратному компоненту.

Программный компонент (software component) – программа или программный модуль, содержащий команды, предназначенные для выполнения компьютером. Примеры: операционная система, интернет-приложение, драйвер устройства.

Аппаратный компонент (hardware component) – физическое вычислительное устройство.

Атакуемый компонент (impacted component) – компонент (или компоненты), испытывающий последствия эксплуатации уязвимости. Атакуемый компонент может совпадать с уязвимым компонентом, а может отличаться от него; в последнем случае говорят о смене области действия.

Привилегии (privileges) – набор предоставляемых пользователю или пользовательскому процессу прав (обычно на чтение, запись и выполнение), определяющих его доступ к вычислительным ресурсам.

Ресурсы (resources) – программный или сетевой объект, к которому осуществляет доступ вычислительное устройство или который изменяется либо используется вычислительным устройством. Примеры: файлы на компьютере, память, рабочие циклы процессора или полоса пропускания сети.

Область действия (scope) – набор привилегий, определенный и управляемый субъектом авторизации при предоставлении доступа к вычислительным ресурсам.

Уязвимость (vulnerability) – слабое место или дефект в программном (или аппаратном) компоненте.

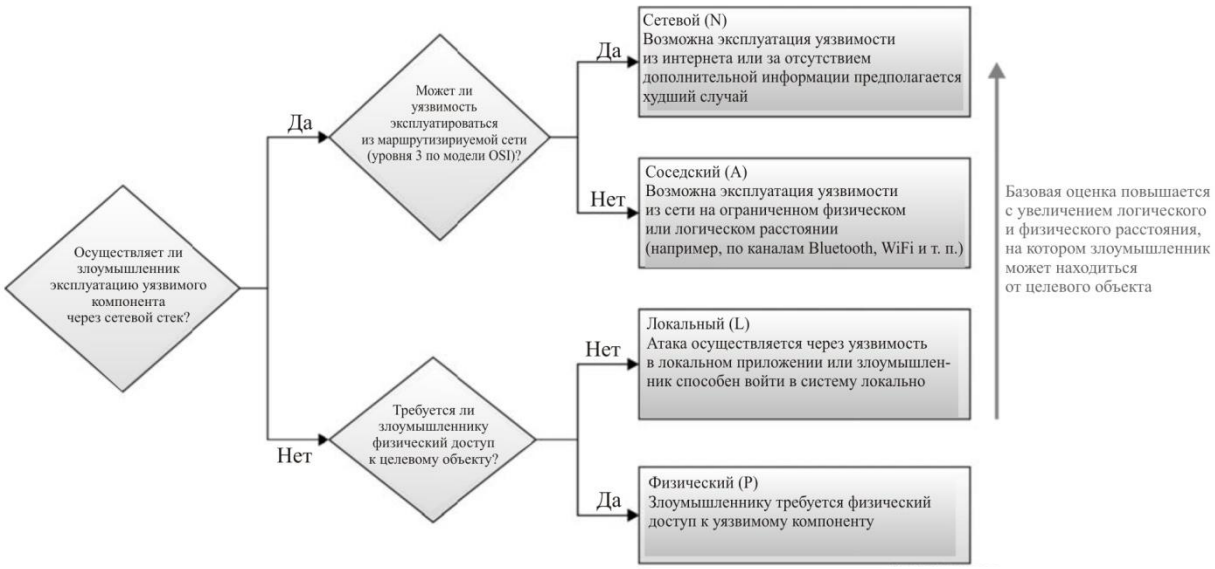
Построение цепочек уязвимостей (vulnerability chaining) – последовательная эксплуатация нескольких уязвимостей в целях атаки на ИТ-систему, при которой для эксплуатации одной или более уязвимостей на конце цепочки требуется успешная эксплуатация предшествующих по цепочек уязвимостей. См. также определение на веб-сайте по адресу: http://cwe.mitre.org/documents/glossary/#Chain.

Уязвимый компонент (vulnerable component) – программный (или аппаратный) компонент, в котором существует уязвимость и в который необходимо внести исправление.

I.5 Сводка алгоритмов оценки

В этом разделе приведена сводка кратких алгоритмов оценки уязвимостей по системе CVSS v3.0. Она дается в дополнение к сведениям, приведенным в спецификации.

I.5.1 Показатель "вектор атаки"

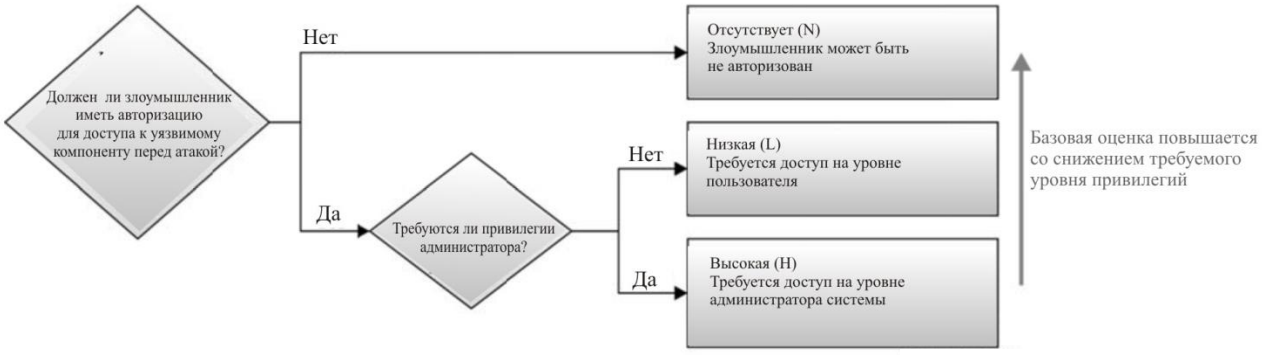


X.1521(16)_FI.2

I.5.2 Показатель "сложность атаки"

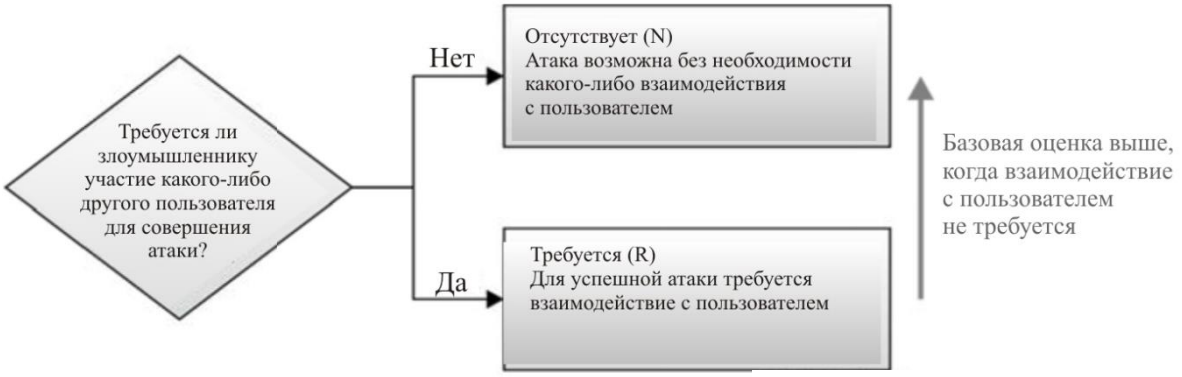
X.1521(16)_FI.3

I.5.3 Показатель "потребность в привилегиях"



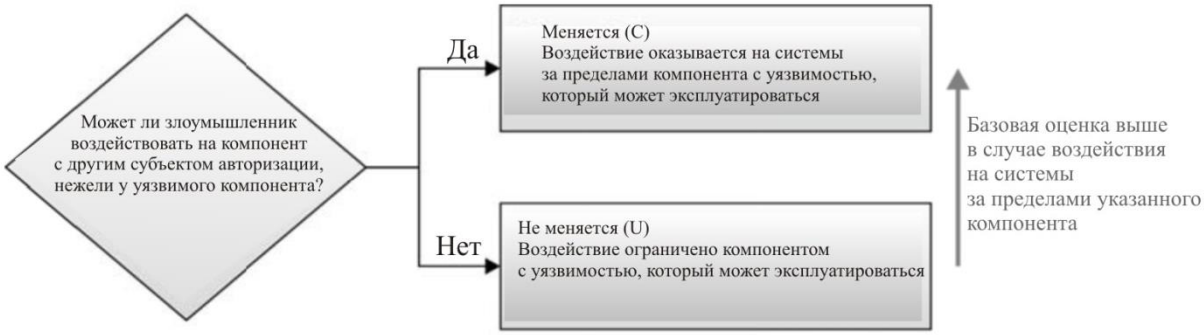
X.1521(16)_FI.4

I.5.4 Показатель "взаимодействие с пользователем"



X.1521(16)_FI.5

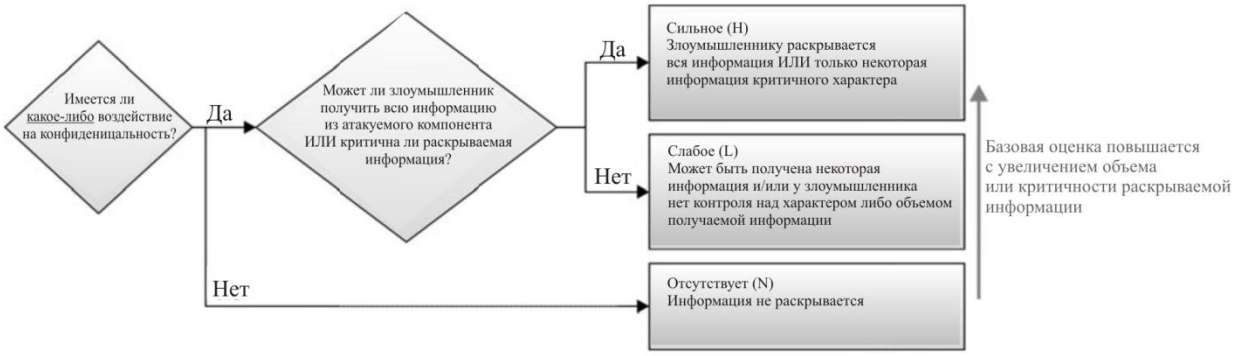
I.5.5 Показатель "область действия"



X.1521(16)_FI.6

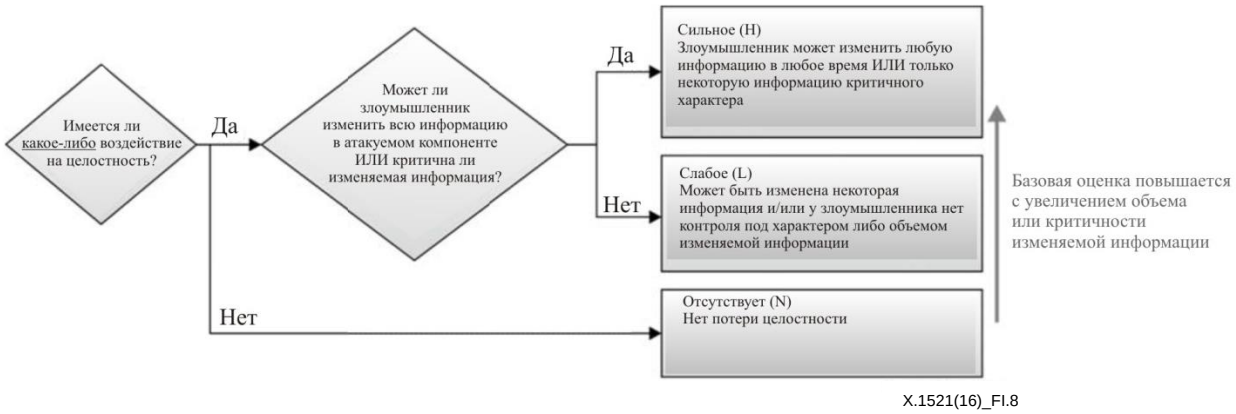
ПРИМЕЧАНИЕ. – Следует иметь в виду, что если смены области действия не происходит, показатели воздействия на конфиденциальность, целостность и доступность (CIA) отражают последствия уязвимого компонента. В противном случае они отражают последствия для компонента, который испытывает наиболее серьезное воздействие.

I.5.6 Показатель "воздействие на конфиденциальность"



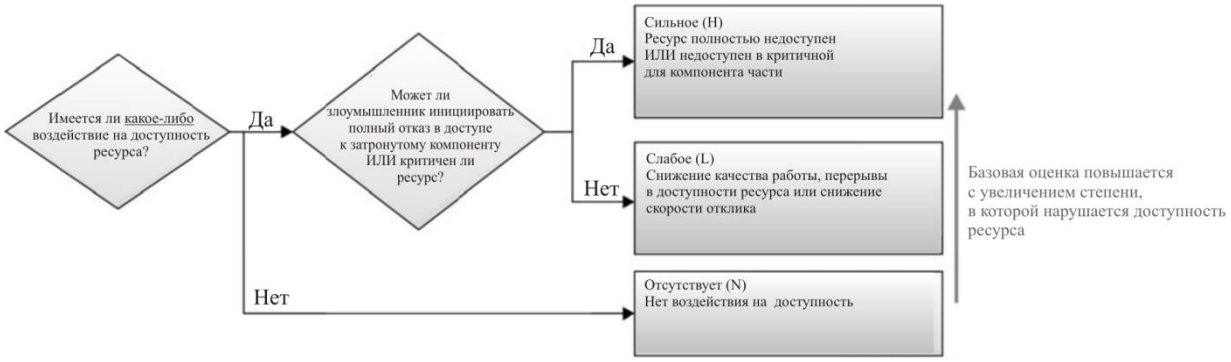
X.1521(16)_FI.7

I.5.7 Показатель "воздействие на целостность"



X.1521(16)_FI.8

I.5.8 Показатель "воздействие на доступность"



X.1521(16)_FI.9

Дополнение II

Ресурсы и ссылки

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Ниже приведены полезные ссылки на дополнительные документы по CVSS v3.0.

Ресурс	Место размещения
Спецификация	Включает описание показателей, формулы и правила формирования векторной строки; доступно по адресу: http://www.first.org/cvss/specification-document
Руководство пользователя	Включает более подробное рассмотрение CVSS v3.0, сводку алгоритмов оценки и словарь терминов; доступно по адресу: http://www.first.org/cvss/user-guide
Документ с примерами	Включает практические примеры оценки по системе CVSS v3.0; доступно по адресу: https://www.first.org/cvss/examples
Логотип CVSS v3.0	Изображения в высоком и низком разрешениях доступны по адресу: http://www.first.org/cvss/identity
Калькулятор CVSS v3.0	Базовая реализация формул CVSS v3.0 доступна по адресу: http://www.first.org/cvss/calculator/3.0
XML-схема	Определение схемы доступно по адресу: https://www.first.org/cvss/cvss-v3.0.xsd

Библиография

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

[b-ITU-T X.1524] Рекомендация МСЭ-Т X.1524 (2012 г.), *Перечень общеизвестных слабых мест.*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
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	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
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 межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2017 г.