Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1525

(04/2015)

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

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

Система оценки общеизвестных слабых мест

Рекомендация МСЭ-Т X.1525

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 (1)	
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 (1)	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 (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	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-TX.1525

Система оценки общеизвестных слабых мест

Резюме

В Рекомендации МСЭ-Т X.1525 по системе оценки общеизвестных слабых мест (CWSS) определена открытая структура представления информации о характеристиках и воздействии слабых мест информационно-коммуникационных технологий (ИКТ) в ходе разработки возможностей программного обеспечения. Цель этой Рекомендации состоит в том, чтобы предоставить разработчикам программного обеспечения, менеджерам, специалистам по тестированию, разработчикам средств защиты, поставщикам услуг, специалистам по закупкам, разработчикам приложений и исследователям в области ИКТ возможность общаться, используя общий язык оценки слабых мест ИКТ, которые могут проявиться как уязвимости при использовании программного обеспечения.

Хронологическая справка

Издание	Рекомендация	Утверждена	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1525	17.04.2015	17-я	11.1002/1000/12357

* Для доступа к Рекомендации наберите URL http://handle.itu.int/ в вашем веб-браузере, а затем 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

Разработчики программного обеспечения нередко имеют дело с сотнями и тысячами отдельных отчетов об ошибках, касающихся слабых мест, которые обнаруживаются в их коде. В определенных обстоятельствах слабое место в программном обеспечении способно даже привести к возникновению уязвимости, которая может эксплуатироваться. В связи с большим объемом обнаруженных уязвимостей заинтересованные стороны нередко вынуждены определять, какие проблемы им следует изучать и устранять в первую очередь. Иными словами, специалисты должны иметь возможность обосновывать относительную значимость различных слабых мест и сообщать о ней. В настоящее время используется множество методов оценки, но при этом они являются либо узкоспециализированными, либо непригодными к применению для все еще неточной оценки безопасности программного обеспечения. Система оценки общеизвестных слабых мест (CWSS) предоставляет механизм упорядоченного, гибкого и открытого установления приоритета слабых мест программного обеспечения и при этом приспосабливает контекст к различным бизнес-доменам и предназначениям программного обеспечения. Она предусматривает совместную коллективную деятельность, направленную на удовлетворение потребностей всех заинтересованных в ней сторон, – правительственных, академических и отраслевых организаций.

Разработчики программного обеспечения, менеджеры, специалисты по тестированию, разработчики средств защиты, поставщики услуг, специалисты по закупкам, разработчики приложений и исследователи в области ИКТ должны определять и оценивать слабые стороны программного обеспечения, которые могут проявиться как уязвимости при его использовании. Они должны быть способны установить приоритеты этих слабых мест и определить те, которые должны быть устранены, исходя из того, какие из них представляют наибольший риск. При наличии множества подлежащих исправлению слабых мест, каждое из которых оценивается по разным шкалам, многочисленные члены сообщества ИКТ, менеджеры, специалисты по тестированию, специалисты по закупкам и разработчики вынуждены полагаться на собственные методы, для того чтобы каким-то образом сравнивать различные слабые места и получать по ним информацию, позволяющую принять меры.

В связи с тем, что в CWSS стандартизованы методы описания слабых мест, пользователи CWSS могут воспользоваться данными об области атаки и показателями среды, чтобы использовать связанную с контекстом информацию, которая более точно отражает риск для возможности программного обеспечения, с учетом уникального бизнес-контекста, в котором оно будет работать, и уникальной бизнес-возможности, которую оно должно предоставлять. Благодаря этому пользователи, старающиеся снизить риски, которые связаны со слабыми местами, могут принимать более обоснованные решения.

В Рекомендации по CWSS используются результаты работы, проводимой сообществом специалистов по кибербезопасности, например, описание множества разнообразных реальных общеизвестных уязвимостей, приведенное в [b-ITU-T X.1520] по общеизвестным уязвимостям и незащищенности (CVE), [b-ITU-T X.1520], а также система оценки, применяемая при обсуждении серьезности этих общеизвестных уязвимостей с использованием [b-ITU-T X.1521] по системе оценки общеизвестных уязвимостей (CVSS), [b-ITU-T X.1521]. Кроме того, в ней используется список слабых мест в архитектуре, проектировании, коде или развертывании программного обеспечения согласно перечню общеизвестных слабых мест (CWE). При создании CWSS обеспечивается возможность допущения приемлемых значений по умолчанию для областей, которые могут быть еще не известны, а также адаптации к деловым и техническим условиям.

Рекомендация по CWE является одной из того класса Рекомендаций МСЭ-Т, которые стали результатом деятельности существующего широкого и глобального сообщества разработчиков и пользователей, которое подготовило и развило открытую спецификацию, представляемую МСЭ-Т для принятия, при условии что любые изменения или обновления этой спецификации будут осуществляться таким образом, чтобы сохранить полную техническую эквивалентность и совместимость, что дискуссии по поводу изменений и улучшений будут осуществляться в рамках процессов с участием того же сообщества пользователей, и включает прямые ссылки на соответствующую конкретную версию, поддерживаемую сообществом пользователей. Таким образом, в момент принятия первоначальной редакции Рекомендации МСЭ-Т X.1525 будет проведена ее надлежащая проверка и дано подтверждение ее эквивалентности; по мере внесения изменений сообществом пользователей такие изменения, благодаря постоянному сотрудничеству с этим сообществом, будут своевременно отражаться в последующих редакциях Рекомендации.

Рекомендация МСЭ-Т X.1525 по системе оценки общеизвестных слабых мест (CWSS) разработана на основе сотрудничества с корпорацией MITRE, с учетом важности поддержания, по мере возможности, технической совместимости между Рекомендацией МСЭ-Т X.1525 по системе оценки общеизвестных слабых мест (CWSS) и версией 1.0.1 документа "Система оценки общеизвестных слабых мест (CWSS)" от 5 сентября 2014 года, размещенного по адресу: [https://cwe.mitre.org/cwss/cwss_v1.0.1.html]

Рекомендация МСЭ-Т X.1525

Система оценки общеизвестных слабых мест

1 Сфера применения

В настоящей Рекомендации представлен стандартизованный метод представления информации о характеристиках и воздействиях слабых мест в ходе разработки возможностей программного обеспечения ИКТ с использованием данных об области атаки и показателей среды для использования связанной с контекстом информации. CWSS более точно отражает риск для пользователя возможности программного обеспечения, с учетом уникального бизнес-контекста, в котором оно будет работать в интересах пользователя, и уникальной бизнес-возможности, которую программное обеспечение предоставляет пользователю.

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 Термины и определения

3.1 Термины, определенные в других документах

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

3.1.1 доступ (access) [b-ITU-T X.1521] – возможность субъекта рассматривать объект, изменять его или устанавливать с ним связь. Доступ обеспечивает возможность обмена информацией между субъектом и объектом.

3.1.2 доступность (availability) [b-ITU-T X.1521] – надежный и своевременный доступ к данным и ресурсам, осуществляемый авторизованными физическими лицами.

3.1.3 случай атаки (attack instance) [b-ITU-T X.1544] – конкретная подробно описанная атака против приложения или системы, целью которой являются уязвимые или слабые места в этой системе.

3.1.4 конфиденциальность (confidentiality) [b-ITU-T X.1521] – принцип безопасности, служащий для обеспечения того, чтобы информация не раскрывалась неавторизованным субъектам.

3.1.5 целостность (integrity) [b-ITU-T X.1521] – принцип безопасности, обеспечивающий, чтобы информация и системы не подвергались изменению по злому умыслу или случайно.

3.1.6 риск (risk) [b-ITU-T X.1521] – относительное воздействие, которое обычно оказывается эксплуатацией уязвимости на среду пользователя.

3.1.7 угроза (threat) [b-ITU-T X.1521] – вероятность или частота возникновения опасного события.

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

3.1.9 слабое место (weakness) [b-ITU-T X.1524] – дефект или изъян в коде, проектировании, архитектуре или развертывании программного обеспечения, способный в определенный момент стать уязвимостью или приводить к возникновению других уязвимостей.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяется следующий термин.

3.2.1 этикетка (vignette) – этикетка обеспечивает совместно используемую формализованную возможность определения какой-либо конкретной среды, функций программного обеспечения в данной среде, а также приоритетов организации в отношении безопасности программного обеспечения.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AI	Authentication Instances		Случаи аутентификации
AL	Acquired Privilege Layer		Уровень приобретенной привилегии
AP	Acquired Privilege		Приобретенная привилегия
AS	Authentication Strength		Сложность аутентификации
ASLR	Address Space Layout Randomization		Рандомизация распределения адресного пространства
AV	Access Vector		Вектор доступа
BI	Business Impact		Воздействие на деятельность
BVC	Business Value Context		Контекст бизнес-ценности
CD	Compact Disc		Компакт-диск
CIO	Chief Information Officer		Руководитель информационной службы
CSO	Chief Security Officer		Руководитель службы безопасности
CSRF	Cross-Site Request Forgery		Подделка межсайтовых запросов
CVSS	Common Vulnerability Scoring System		Общая система оценки уязвимостей
CWE	Common Weakness Enumeration		Перечень общеизвестных слабых мест
CWRAF	Common Weakness Risk Analysis Framework		Структура анализа рисков общеизвестных слабых мест
CWSS	Common Weakness Scoring System		Система оценки общеизвестных слабых мест
DI	Likelihood of Discovery		Вероятность обнаружения
DNS	Domain Name System		Система наименований доменов
DS	Deployment Scope		Масштаб развертывания
EC	External Control Effectiveness		Эффективность внешнего контроля
EX	Likelihood of Exploit		Вероятность эксплуатации
FC	Finding Confidence		Доверие к результатам поиска
FTP	File Transfer Protocol		Протокол передачи файлов
HTML	HyperText Markup Language		Язык описания гипертекстовых документов
IC	Internal Control Effectiveness		Эффективность внутреннего контроля
ICT	Information Communication Technology	ИКТ	Информационно-коммуникационные технологии

IN	Level of Interaction		Уровень взаимодействия
IP	Internet Protocol		Протокол Интернет
NIST	National Institute of Standards and Technology		Национальный институт стандартов и технологий
OS	Operating System	ОС	Операционная система
OWASP	Open Web Applications Security Project		Открытый проект обеспечения безопасности веб-приложений
P	Prevalence		Распространенность
PCI DSS	Payment Card Industry Data Security Standard		Стандарт безопасности данных индустрии платежных карт
RL	Required Privilege Layer		Уровень требуемой привилегии
RP	Required Privilege		Требуемая привилегия
SAMATE	Software Assurance Metrics And Tool Evaluation		Оценка показателей и инструмента получения гарантий на программное обеспечение
SANS	SysAdmin, Audit, Networking, and Security		Системное администрирование, аудит, организация сетей и безопасность
SQL	Structured Query Language		Язык структурированных запросов
SSL	Secure Socket Layer		Уровень защищенных разъемов
TI	Technical Impact		Техническое воздействие
TLS	Transport Layer Security		Безопасность транспортного уровня
USB	Universal Serial Bus		Универсальная последовательная шина
XSS	Cross-Site Scripting		Межсайтовая атака с внедрением сценария

5 Соглашения

Отсутствуют.

6 Использование CWSS

В настоящее время разработчики программного обеспечения, менеджеры, специалисты по тестированию, разработчики средств защиты, поставщики услуг, специалисты по закупкам, разработчики приложений и исследователи в области ИКТ должны определять и оценивать слабые стороны программного обеспечения, которые могут проявиться как уязвимости при его использовании. Они должны быть способны установить приоритеты этих слабых мест и определить те, которые должны быть устранены, исходя из того, какие из них представляют наибольший риск. При наличии множества подлежащих исправлению слабых мест, каждое из которых оценивается по разным шкалам, многочисленные члены сообщества ИКТ, менеджеры, специалисты по тестированию, специалисты по закупкам и разработчики вынуждены полагаться на собственные методы, для того чтобы каким-то образом сравнивать различные слабые места и получать по ним информацию, позволяющую принять меры. Система оценки общеизвестных слабых мест (CWSS) является открытой структурой, позволяющей решить данную проблему. Она обеспечивает следующие преимущества:

- Количественные измерения: CWSS обеспечивает возможность количественного измерения неисправленных слабых мест, которые могут присутствовать в программном приложении.
- Общая структура: CWSS обеспечивает общую структуру для установления приоритетов ошибок безопасности ("слабых мест"), которые обнаружены в программных приложениях.

- Определяемая потребителем установка приоритетов: в сочетании со Структурой анализа рисков общеизвестных слабых мест (CWRAF) [b-CWRAF] CWSS может использоваться потребителями для определения наиболее важных типов слабых мест в их бизнес-доменах, для того чтобы их деятельность по получению информации и защите осуществлялась обоснованным образом в рамках более широкого процесса получения гарантий на программное обеспечение.

6.1 Описание CWSS

Как показано на рисунке 1, CWSS состоит из трех *групп показателей*: базовых результатов поиска, области атаки и среды. В каждой группе содержится несколько показателей, называемых также *параметрами*, которые используются для вычисления оценки CWSS для того или иного слабого места.

Рисунок 1 – Группы показателей CWSS

Ниже приведено описание этих групп показателей.

- Группа показателей базовых результатов поиска: охватывает внутренние риски, присущие слабому месту, доверие к точности результатов поиска, а также действенность средств контроля. Группа показателей базовых результатов поиска рассматривается в пункте 7.3.
- Группа показателей области атаки: барьеры, которые должен преодолеть злоумышленник, для того чтобы эксплуатировать слабое место. Группа показателей области атаки рассматривается в пункте 7.4.
- Группа показателей среды: характеристики слабого места, присущие конкретной среде или операционному контексту. Группа показателей среды рассматривается в пункте 7.5.

6.2 Разработка оценки CWSS

Каждому параметру в группе показателей базовых результатов поиска присваивается значение. Эти значения преобразуются в соответствующие им весовые коэффициенты и рассчитывается элемент оценки базовых результатов поиска, который может находиться в интервале от 0 до 100. Аналогичный метод применяется к группам показателей области атаки и среды; их элементы оценки могут находиться в интервале от 0 до 1. Наконец, эти три элемента перемножаются, и в результате получается оценка CWSS в интервале от 0 до 100, как показано ниже на рисунке 2.

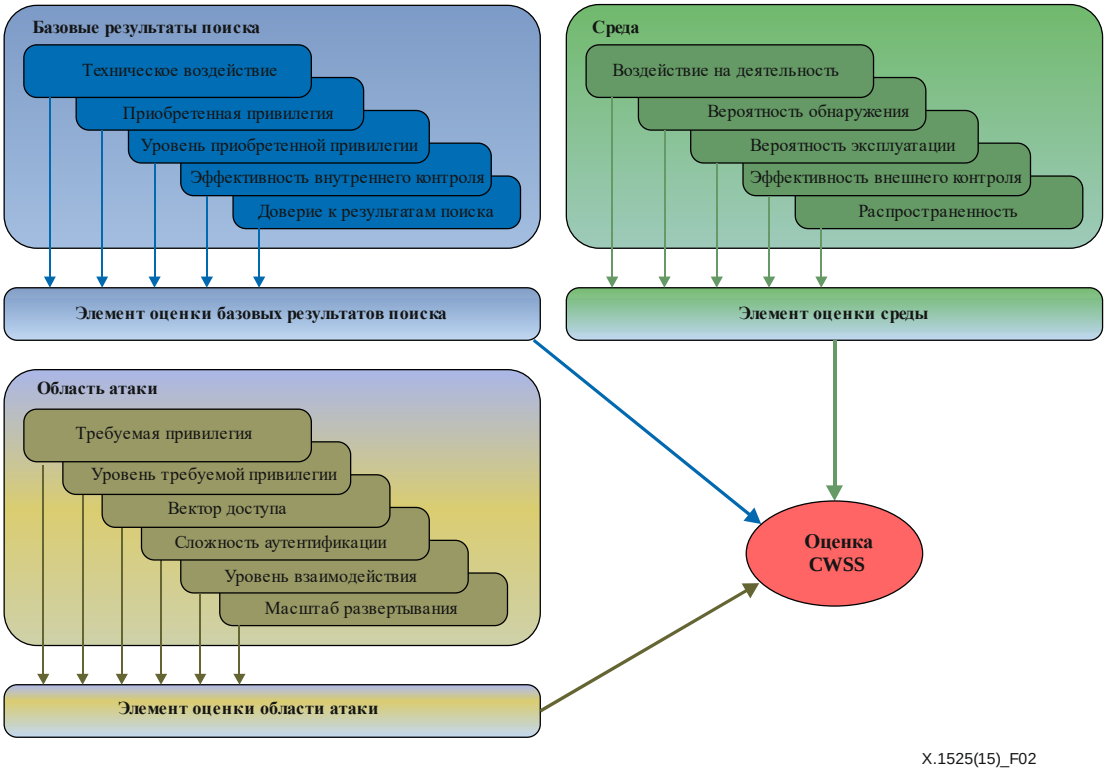

Рисунок 2 – Оценка CWSS

6.3 Оценка CWSS

Сообщество заинтересованных сторон взаимодействует с организацией MITRE с целью изучения нескольких различных методов оценки, которые, возможно, потребуется обеспечить в рамках CWSS. Существует четыре метода оценки:

Метод целевой оценки	Оцениваются отдельные слабые стороны, которые обнаруживаются при проектировании или реализации конкретного ("целевого") пакета программного обеспечения, например переполнение буфера имени пользователя в программе аутентификации в строке 1234 server.c пакета сервера FTP. Автоматизированные инструменты и консультанты по безопасности программного обеспечения используют целевые методы при оценке безопасности пакета программного обеспечения с точки зрения содержащихся в нем слабых мест.
Метод обобщенной оценки	Оцениваются классы слабых мест, не зависящие от какого-либо конкретного пакета программного обеспечения, в целях установления их взаимных приоритетов (например, "переполнения буфера имеют более высокий приоритет, чем утечки памяти"). Данный подход используется в списках Топ-25 CWE SANS, Топ-10 OWASP и в аналогичных исследованиях, а также в некоторых автоматических сканерах кодов. Обобщенные оценки могут существенно отличаться от целевых оценок, получаемых в результате полного анализа отдельных экземпляров класса слабых мест в конкретном пакете программного обеспечения. Например, класс переполнений буфера по-прежнему является весьма важным для многих разработчиков, но при этом отдельные ошибки переполнения буфера могут считаться менее важными, если они не могут быть непосредственно задействованы злоумышленником, и их воздействие уменьшено благодаря защитным механизмам на уровне операционной системы (ОС), таким как рандомизация распределения адресного пространства (ASLR).

Метод контекстно-адаптированной оценки	Оценки изменяются в соответствии с требованиями конкретного аналитического контекста, который может объединять приоритеты деятельности/миссии, угрозы среды, допустимый риск и т. д. Сбор этих требований осуществляется с использованием этикеток, которые увязывают присущие слабым местам характеристики с аспектами деятельности более высокого уровня. Данный метод может применяться и к целевой, и к обобщенной оценке.
Метод агрегированной оценки	Объединяются результаты нескольких оценок слабых сторон более низкого уровня и получается единая общая оценка (или "ранг"). Применение агрегирования, возможно, наиболее уместно в целевом методе, но при этом оно может использоваться и при обобщенной оценке, как в списке Топ-25 CWE SANS за 2010 год.

Следует отметить, что в настоящее время большинство обсуждений, касающихся CWSS, посвящено методу целевой оценки и структуре контекстно адаптированной оценки. Далее будет обсуждаться метод агрегированной оценки. Метод обобщенной оценки разрабатывается отдельно, главным образом в рамках списка Топ-25 за 2011 год и CWRAF.

Оценки CWSS могут рассчитываться автоматически, например, инструментом анализа кода, или же они могут рассчитываться вручную консультантом по безопасности программного обеспечения или разработчиком. В связи с тем что для автоматического анализа, по всей вероятности, недоступна определенная информация, например о рабочей среде приложения, оценка CWSS, возможно, могла бы осуществляться в несколько циклов: вначале инструмент автоматически рассчитывает оценки CWSS, а затем специалист-аналитик вручную добавляет дополнительную информацию и пересчитывает эти оценки.

6.4 Пользователи CWSS

Для достижения максимальной эффективности в CWSS обеспечивается несколько сценариев использования различными заинтересованными сторонами. Все они заинтересованы в согласованной системе оценки, позволяющей устанавливать приоритеты слабых мест программного обеспечения, которые могут создавать риски для продуктов, систем, сетей и услуг. Ниже приводится несколько примеров основных заинтересованных сторон.

- Разработчики программного обеспечения: разработчики нередко действуют в условиях сжатых сроков, обусловленных циклами выпусков и ограниченными ресурсами. Вследствие этого они не имеют возможности изучения и исправления каждого обнаруженного слабого места. Возможно, они решат сосредоточиться на самых острых проблемах, которые проще всего исправить. В случае автоматического поиска слабых мест они, возможно, захотят сосредоточиться на результатах, в отношении которых вероятность ложного срабатывания минимальна.
- Менеджеры по разработке программного обеспечения: менеджеры по разработке создают стратегии установления приоритетов и устранения целых классов слабых мест из всей базы кодов, или, по меньшей мере, из той части, которая представляется наиболее подверженной риску. Это может быть сделано с помощью настраиваемых списков "Топ-N". Они должны отдавать себе отчет о последствиях для безопасности, связанных с интеграцией стороннего программного обеспечения, которое может содержать собственные слабые места. Возможно, им потребуется обеспечить соблюдение отдельных требований безопасности и установление приоритетов для каждой линейки продуктов.

- Заказчики программного обеспечения: клиенты, в том числе сотрудники, осуществляющие заказ, хотят получить стороннее программное обеспечение с разумным уровнем гарантии того, что поставщик этого программного обеспечения принял меры осмотрительности с целью устранения или недопущения слабых мест, которые наиболее опасны для деятельности и миссии заказчика. Соответствующие заинтересованные стороны включают руководителей информационных служб (CIO), руководителей служб безопасности (CSO), системных администраторов и конечных пользователей программного обеспечения.
- Менеджеры по безопасности предприятия: менеджеры по безопасности предприятия стремятся свести к минимуму риски в рамках своего предприятия, как в отношении известных уязвимостей в сторонних продуктах, так и в отношении уязвимостей (или слабых мест) в программном обеспечении собственной разработки. Они могут использовать механизм оценки, который можно объединить с другими процессами управления безопасностью, например, использовать сочетание результатов сканирования сторонних уязвимостей (для известных уязвимостей стороннего программного обеспечения) и анализа настраиваемого приложения (для программного обеспечения собственной разработки, чтобы улучшить оценку общего риска для того или иного ресурса.
- Разработчики инструментов анализа кода и консультанты в этой области: разработчики и консультанты нередко имеют собственные настраиваемые методы оценки, однако они хотят предоставлять согласованный и проверенный сообществом механизм оценки для разных клиентов.
- Специалисты по оценке возможностей анализа кода: специалисты по оценке анализируют и измеряют возможности методов анализа кода (например, NIST SAMATE). Они могут использовать согласованный механизм оценки слабых мест для обеспечения отбора обнаруженных результатов поиска, а также для понимания серьезности эти результатов, не будучи зависимыми от узкоспециализированных методов оценки, которые могут значительно различаться по инструменту/способу.
- Другие заинтересованные стороны: другие заинтересованные стороны могут включать исследователей уязвимостей, сторонников безопасной разработки и специалисты по соблюдению требований (например, PCI DSS).

По состоянию на июнь 2014 года (на момент действия CWSS 0.8) существует всего несколько реальных реализаций CWSS. Основными пользователями являются разработчики инструментов анализа кода и консультанты по безопасности программного обеспечения.

7 Группы показателей

7.1 Параметры групп показателей

CWSS включает следующие параметры, организованные в соответствии с их группами показателей, как показано ниже в таблице 1. В последующих пунктах каждый параметр описывается более подробно.

Таблица 1 – Параметры групп показателей

Группа	Название	Резюме
Базовые результаты поиска	Техническое воздействие (TI)	Потенциальный результат, к которому может привести слабое место, при условии, что к этому слабому месту можно успешно получить доступ, и оно может успешно эксплуатироваться
	Приобретенная привилегия (AP)	Тип привилегий, получаемых злоумышленником, который может успешно эксплуатировать слабое место
	Уровень приобретенной привилегии (AL)	Операционный уровень, для которого злоумышленник получает привилегии за счет успешной эксплуатации слабого места
	Эффективность внутреннего контроля (IC)	Способность средств контроля сделать слабое место непригодным для эксплуатации злоумышленником
	Доверие к результатам поиска (FC)	Уверенность в том, что обнаруженная проблема является слабым местом, которое может быть использовано злоумышленником
Область атаки	Требуемая привилегия (RP)	Тип привилегий, которые уже должен иметь злоумышленник, для того чтобы получить доступ к коду/функциональной возможности, содержащим слабое место
	Уровень требуемой привилегии (RL)	Операционный уровень, для которого злоумышленник должен иметь привилегии, чтобы попытаться атаковать слабое место
	Вектор доступа (AV)	Канал, по которому злоумышленник должен обмениваться информацией, чтобы получить доступ к коду или функциональной возможности, содержащим слабое место
	Сложность аутентификации (AS)	Сложность программы аутентификации, которая обеспечивает защиту кода/функциональной возможности, содержащих слабое место
	Уровень взаимодействия (IN)	Действия, которые должно совершить лицо(а), являющееся объектом атаки, чтобы создать условия для ее успешного осуществления
	Масштаб развертывания (SC)	Присутствие слабого места либо во всех развертываемых экземплярах программного обеспечения, либо ограниченно в ряде платформ и/или конфигураций
Среда	Воздействие на деятельность (BI)	Потенциальное воздействие на деятельность или миссию в случае успешной эксплуатации слабого места
	Вероятность обнаружения (DI)	Вероятность того, что злоумышленник может обнаружить слабое место
	Вероятность эксплуатации (EX)	Вероятность того, что, в случае обнаружения слабого места, злоумышленник, обладающий требуемыми привилегиями/ аутентификацией/доступом, сможет его успешно эксплуатировать
	Эффективность внешнего контроля (EC)	Возможность контроля или смягчения последствий, не относящаяся к программному обеспечению, которая может затруднить доступ злоумышленника к слабому месту и его задействование злоумышленником
	Распространенность (P)	Частота появления слабого места данного типа в программном обеспечении

7.2 Значения для случаев неопределенности и для обеспечения гибкости

CWSS может использоваться в случаях, когда вначале имеется мало информации, однако постепенно качество информации может улучшиться. Предусматривается, что во многих сценариях использования оценка CWSS для отдельных результатов поиска слабых мест может часто меняться по мере получения дополнительной информации. Разные организации могут оценивать отдельные параметры в разные моменты времени.

По сути, у каждого параметра CWSS фактически имеются характеристики среды или временны́е характеристики, поэтому не имеет особого смысла заимствовать группы показателей тех же типов, которые используются в CVSS.

Большинство параметров имеет четыре общих для них значения, которые показаны в таблице 2 ниже.

Таблица 2 – Значения параметров для случаев неопределенности и для обеспечения гибкости

Значение	Использование
Неизвестно	Организация, вычисляющая оценку, не обладает достаточной информацией для присвоения значения параметру. Это может свидетельствовать о необходимости дальнейшего изучения. Например, автоматический сканнер кода может иметь возможность поиска определенных слабых мест, но не иметь возможности определения того, действует ли какой-либо механизм аутентификации. Использование значения "Неизвестно" подчеркивает, что оценка является неполной или приблизительной, и может потребоваться проведение дополнительного анализа. Тем самым упрощается моделирование неполной информации, и это позволяет контексту бизнес-ценности оказывать влияние на итоговые оценки, полученные с использованием неполной информации. Для всех параметров весовой коэффициент данного значения равен 0,5, что, как правило, приводит к более низкой оценке; добавление новой информации (например, замена значения "Неизвестно" в некоторых параметрах на другое) приведет к корректировке оценки в сторону повышения или понижения, в зависимости от новой информации
Не применяется	Этот параметр явным образом не учитывается при расчете оценки. По сути, это позволяет контексту бизнес-ценности определять, нужен ли тот или иной параметр для итоговой оценки. Например, в методе ориентированной на клиента оценки CWSS могут не учитываться меры по устранению, а в среде с высоким уровнем гарантии может требоваться изучение всех обнаруженных результатов поиска, даже при низком уровне доверия к их точности. Что касается совокупности результатов поиска слабых мест в отдельном пакете программного обеспечения, ожидается, что у всех результатов будет одинаковое ("Не применяется") значение параметра, который не учитывается
Количественное значение	Весовой коэффициент параметра может быть выражен количественно с использованием непрерывного диапазона значений от 0,0 до 1,0 вместо заданного набора дискретных значений параметра. Не все параметры можно количественно определить таким способом, однако этим предусматривается дополнительная возможность настройки показателей
Стандартное значение	Весовому коэффициенту параметра можно присвоить стандартное значение. Указание на стандартное значение параметра предусматривает изучение и возможное изменение в дальнейшем

7.3 Группа показателей базовых результатов поиска

Группа показателей базовых результатов поиска состоит из следующих параметров:

- техническое воздействие (TI);
- приобретенная привилегия (AP);
- уровень приобретенной привилегии (AL);
- эффективность внутреннего контроля (IC);
- доверие к результатам поиска (FC).

Сочетание значений параметров технического воздействия, приобретенной привилегии и уровня приобретенной привилегии дает пользователю некоторые выразительные возможности. Например,

пользователь может дать следующее описание: "Высокое" техническое воздействие с привилегиями "Администратора" на уровне "Приложения".

7.3.1 Техническое воздействие (TI)

Техническое воздействие – это потенциальный результат, к которому может привести слабое место, при условии, что к этому слабому месту можно успешно получить доступ и оно может успешно эксплуатироваться. Оно выражается в более детализирующих терминах, чем конфиденциальность, целостность и доступность.

Техническое воздействие следует оценивать по отношению к приобретенной привилегии (AP) и уровню приобретенной привилегии (AL).

Таблица 3 – Весовые коэффициенты технического воздействия

Значение	Код	Вес	Описание
Критическое	C	1,0	Полный контроль анализируемого программного обеспечения до такого уровня, когда невозможно осуществлять деятельность
Высокое	H	0,9	Существенный контроль анализируемого программного обеспечения или возможность получения доступа к важнейшей информации
Среднее	M	0,6	Умеренный контроль анализируемого программного обеспечения или возможность получения доступа к информации средней важности
Низкое	L	0,3	Минимальный контроль анализируемого программного обеспечения или возможность получения доступа только к относительно маловажной информации
Отсутствует	N	0,0	Полное отсутствие технического воздействия на анализируемое программное обеспечение. Иными словами, это не приведет к уязвимости
Стандартное значение	D	0,6	Весовой коэффициент для стандартного значения – это медиана весовых коэффициентов для значений "Критическое", "Высокое", "Среднее", "Низкое" и "Отсутствует"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Данный параметр может не применяться в среде с высокими требованиями к гарантии; пользователь, возможно, хочет изучить каждый интересующий результат поиска слабых мест, независимо от уровня доверия
Количествен-ное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов

В случае недостаточной точности этого набора значений пользователи CWSS могут использовать собственные количественные методы для получения элемента оценки. Один из таких методов включает использование Структуры анализа рисков общеизвестных слабых мест (CWRAF) [b-CWRAF] для определения этикетки и оценочной карты технического воздействия. Весовой коэффициент воздействия рассчитывается с использованием зависящих от этикетки рейтингов важности разных видов технического воздействия, обусловленного эксплуатацией слабого места, таких как изменение критичных данных, приобретение привилегий, потребление ресурсов и т. д.

7.3.2 Приобретенная привилегия (AP)

Приобретенная привилегия определяет тип привилегий, получаемых злоумышленником, который может успешно эксплуатировать слабое место.

Отметим, что для этого параметра используются те же значения, что и для параметра "Требуемая привилегия", но другие весовые коэффициенты.

В некоторых случаях значение параметра "приобретенная привилегия" может быть таким же, как у параметра "требуемая привилегия", что предполагает либо (1) "горизонтальное" расширение

привилегий (например, от одного непривилегированного пользователя другому), либо (2) расширение привилегий в рамках тестовой среды, например, когда пользователь, имеющий доступ только к протоколу передачи файлов (FTP), может выйти в программную оболочку.

Таблица 4 – Весовые коэффициенты приобретенной привилегии

Значение	Код (прим.)	Вес	Описание
Администратор	A	1,0	Злоумышленник получает доступ к объекту с привилегиями администратора, корневого пользователя, с системными или эквивалентными им привилегиями, что предполагает полный контроль анализируемого программного обеспечения; или же злоумышленник может расширить собственные привилегии (более низкого уровня) до привилегий администратора
Частично привилегированный пользователь	P	0,9	Злоумышленник получает доступ к объекту с некоторыми особыми привилегиями, но не достаточными, чтобы соответствовать привилегиями администратора; или же злоумышленник может расширить собственные привилегии (более низкого уровня) до привилегий частично привилегированного пользователя. Например, пользователь может иметь привилегии, позволяющие делать резервные копии, но не изменять конфигурацию программного обеспечения или устанавливать обновления
Обычный пользователь	RU	0,7	Злоумышленник получает доступ к объекту, являющемуся обычным пользователем без особых привилегий; или же злоумышленник может расширить собственные привилегии (более низкого уровня) до привилегий обычного пользователя
Ограниченная/ гостевая	L	0,6	Злоумышленник получает доступ к объекту с ограниченными или "гостевыми" привилегиями, которые могут существенно ограничивать допустимые действия; или же злоумышленник может расширить собственные привилегии (более низкого уровня) до гостевых привилегий. Примечание: данное значение не касается понятия "гостевой операционной системы" в виртуализованных хост-компьютерах
Отсутствует	N	0,1	Злоумышленник не может получить доступ к каким бы то ни было дополнительным привилегиям, помимо тех, которые у него уже имеются. (Следует отметить, что данное значение целесообразно использовать в ограниченных случаях, когда злоумышленник может выйти из тестовой среды или иной среды с ограниченными возможностями, но еще не может получить дополнительные привилегии и не может получить доступ как другие пользователи)
Стандартное значение	D	0,7	Медиана весовых коэффициентов для значений "Отсутствует", "Гостевой", "Обычный пользователь", "Частично привилегированный пользователь" и "Администратор"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Данный параметр может не применяться в среде с высокими требованиями к гарантии, предписывающими строгое выполнение мер по разделению привилегий, даже между пользователями, уже имеющими привилегии
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. Следует отметить, что количественные значения поддерживаются для полноты; однако в связи с тем, что привилегии и пользователи являются отдельными объектами, может существовать лишь ограниченное число случаев, в которых целесообразно использовать количественную модель
ПРИМЕЧАНИЕ. – Основные значения данного параметра мнемонически обозначаются как "ОПООАЧ" (Обычный пользователь, Отсутствует, Ограниченная, Администратор, Частично привилегированный).			

7.3.3 Уровень приобретенной привилегии (AL)

Уровень приобретенной привилегии определяет операционный уровень, для которого злоумышленник получает привилегии за счет успешной эксплуатации слабого места.

Таблица 5 – Весовые коэффициенты уровня приобретенной привилегии

Значение	Код (прим.)	Вес	Описание
Приложение	A	1,0	Злоумышленник приобретает привилегии, которые поддерживаются в самом анализируемом программном обеспечении. (Если анализируемое программное обеспечение является одной из важнейших частей базовой системы, например, ядром операционной системы, то, возможно, более целесообразно использовать значение "Система")
Система	S	0,9	Злоумышленник приобретает привилегии для базовой системы или физического хоста, которые используются для прогона анализируемого программного обеспечения
Сеть	N	0,7	Злоумышленник приобретает привилегии для доступа в сеть
Инфраструктура предприятия	E	1,0	Злоумышленник приобретает привилегии для одного из важнейших участков инфраструктуры предприятия, например, маршрутизатора, коммутатора, системы наименований доменов (DNS), контроллера домена, брандмауэра, сервера определения идентичности и т. д.
Стандартное значение	D	0,9	Медиана весовых коэффициентов для значений "Приложение", "Система", "Сеть" и "Инфраструктура предприятия"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Данный параметр может не применяться в среде с высокими требованиями к гарантии, предписывающими строгое выполнение мер по разделению привилегий, даже между пользователями, уже имеющими привилегии
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. Следует отметить, что количественные значения поддерживаются для полноты; однако в связи с тем, что уровни привилегии являются отдельными объектами, может существовать лишь ограниченное число случаев, в которых целесообразно использовать количественную модель
ПРИМЕЧАНИЕ. – Основные значения данного параметра мнемонически обозначаются как "СПСИ" (Система, Приложение, Сеть, Инфраструктура предприятия).			

7.3.4 Эффективность внутреннего контроля (IC)

Внутренний контроль – это средство контроля, механизм защиты или уменьшения влияния, который в явном виде встроен в программное обеспечение (через архитектуру или проектирование, или реализацию). Эффективность внутреннего контроля измеряет способность средств контроля сделать слабое место непригодным для эксплуатации злоумышленником. Например, программа проверки вводимых значений, ограничивающая длину вводимого значения 15 символами, может быть сравнительно эффективна в отношении межсайтовых атак с внедрением сценария (XSS) благодаря уменьшению размера эксплойта XSS, который могут попытаться использовать.

При наличии нескольких средств внутреннего контроля или нескольких ветвей кода, по которым можно достичь одного и того же слабого места, применяется следующий руководящий принцип:

- Для каждой ветви кода провести анализ каждого средства внутреннего контроля, существующего на этой ветви, и выбрать значение с наименьшим весовым коэффициентом (то есть самое действенное средство внутреннего контроля на ветви кода). Данное значение называется значением ветви кода.
- Осуществить сбор всех значений ветви кода.

- Выбрать значение ветви кода, имеющее наибольший весовой коэффициент (то есть наименее действенное средство контроля).

В данном методе каждая ветвь кода оценивается через самое действенное средство контроля на этой ветви (поскольку злоумышленнику потребуется обойти данное средство контроля), затем выбирается наименее защищенная ветвь кода (то есть самый легкий путь, по которому пойдет злоумышленник).

Таблица 6 – Весовые коэффициенты эффективности внутреннего контроля

Значение	Код	Вес	Описание
Отсутствует	N	1,0	Средства контроля отсутствуют.
Ограниченный	L	0,9	Имеются упрощенные методы или случайные ограничения, которые могут не позволить недостаточно подготовленному злоумышленнику эксплуатировать эту проблему
Умеренный	M	0,7	Механизм защиты широко используется, но имеет известные ограничения, которые опытный нарушитель может обойти, приняв некоторые меры. Например, использование кодирования объектов в языке описания гипертекстовых документов (HTML) для предотвращения атак XSS можно обойти, если поместить выходные данные в другой контекст, например, в атрибут метки в каскадной таблице стилей (CSS) или HTML
Косвенный (эшелонированная защита)	I	0,5	Средства контроля не обеспечивают реальной защиты от эксплуатации слабого места, но косвенным образом уменьшают воздействие, в случае если предпринята успешная атака, или иным образом затрудняют создание работоспособного эксплойта. Например, программа проверки может косвенным образом ограничивать размер вводимого значения, что может затруднить создание злоумышленником вредоносной нагрузки для атаки XSS или атаки с внедрением кода языка структурированных запросов (SQL)
Наилучший имеющийся	B	0,3	Контроль соответствует существующему передовому опыту, но ему могут быть присущи некоторые ограничения, позволяющие опытному злоумышленнику, имеющему четкую цель, преодолеть контроль, при этом может требоваться наличие других слабых мест. Например, метод двойного представления для защиты от подделки межсайтовых запросов (CSRF) считается одним из самых действенных среди имеющихся, но его можно обойти, использовав одновременно поведение определенных функциональных возможностей, которые могут считывать необработанные заголовки HTTP
Полный	C	0,0	Средство контроля абсолютно эффективно противодействует слабому месту, то есть отсутствуют ошибка и уязвимость, а также отрицательные последствия эксплуатации этой проблемы. Например, операция копирования в буфер, при которой всегда обеспечивается превышение размера буфера получателя над размером источника (вместе с любым косвенным увеличением первоначального размера источника), не вызовет переполнения буфера
Стандартное значение	D	0,6	Медиана весовых коэффициентов для значений "Полный", "Наилучший имеющийся", "Косвенный", "Умеренный", "Ограниченный" и "Отсутствует"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов

7.3.5 Доверие к результатам поиска (FC)

Доверие к результатам поиска – это уверенность в том, что обнаруженная проблема:

1) является слабым местом; и

2) может быть задействована или использована злоумышленником.

Таблица 7 – Весовые коэффициенты доверия к результатам поиска

Значение	Код	Вес	Описание
Подтверждено	T	1,0	Злоумышленник может получить доступ к слабому месту
Локально подтверждено	LT	0,8	Слабое место возникает в отдельной функции или компоненте, в дизайне которого используется безопасный вызов данной функции, однако возможность доступа злоумышленника к данной функции неизвестна или отсутствует. Например, служебная функция может создавать запрос к базе данных, не кодируя его вводимые значения, однако если она вызывается только с помощью строковых констант, то результат поиска является локально подтвержденным
Не подтверждено	F	0,0	Результат поиска является ошибочным (то есть результат не подтвержден и слабое место отсутствует) и/или отсутствует возможная роль злоумышленника
Стандартное значение	D	0,8	Медиана весовых коэффициентов для значений "Подтверждено", "Локально подтверждено" и "Не подтверждено"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Данный параметр может не применяться в среде с высокими требованиями к гарантии; пользователь, возможно, хочет изучить каждый интересующий результат поиска слабых мест, независимо от уровня доверия
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. Некоторые инструменты анализа кода включают точные измерения точности конкретных схем обнаружения

7.4 Группа показателей области атаки

Группа показателей области атаки состоит из следующих параметров:

- требуемая привилегия (RP);
- уровень требуемой привилегии (RL);
- вектор доступа (AV);
- сложность аутентификации (AS);
- уровень взаимодействия (IN);
- масштаб развертывания (SC).

7.4.1 Требуемая привилегия (RP)

Требуемая

привилегия определяет тип привилегий, которые уже должен иметь злоумышленник, для того чтобы получить доступ к коду/функциональной возможности, содержащим слабое место.

Таблица 8 – Весовые коэффициенты требуемой привилегии

Значение	Код (прим.)	Вес	Описание
Отсутствует	N	1,0	Не требуется привилегий. Например, поисковая система на базе веб может не требовать для объекта каких-либо привилегий при вводе поискового термина или просмотра результатов поиска
Ограниченная/ гостевая	L	0,9	Объект имеет ограниченные или "гостевые" привилегии, которые могут существенно ограничивать допустимые действия; объект может обладать способностью регистрироваться и создавать новую учетную запись без каких-либо конкретных требований или доказательства идентичности. Например, веб-блог может разрешать участникам создавать имя пользователя и представлять действительный адрес электронной почты до ввода комментариев. Примечание: данное значение не касается понятия "гостевой операционной системы" в виртуализованных хост-компьютерах
Обычный пользователь	RU	0,7	Объект является обычным пользователем, не имеющим конкретных привилегий
Частично привилегиро-ванный пользователь	P	0,6	Объект является действительным пользователем, имеющим ряд конкретных привилегий, но не достаточных, для того чтобы быть эквивалентными привилегиям администратора. Например, пользователь может иметь привилегии, позволяющие делать резервные копии, но не изменять конфигурацию программного обеспечения или устанавливать обновления
Администратор	A	0,1	Объект имеет привилегии администратора, корневого пользователя, СИСТЕМЫ или эквивалентные привилегии, что предполагает полный контроль над программным обеспечением или базовой ОС
Стандартное значение	D	0,7	Медиана весовых коэффициентов для значений "Отсутствует", "Ограниченный", "Обычный пользователь", "Частично привилегированный пользователь" и "Администратор"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Данный параметр может не применяться в среде с высокими требованиями к гарантии, предписывающими строгое выполнение мер по разделению привилегий, даже между пользователями, уже имеющими привилегии
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. Следует отметить, что количественные значения поддерживаются для полноты; однако в связи с тем, что привилегии и пользователи являются отдельными объектами, может существовать лишь ограниченное число случаев, в которых целесообразно использовать количественную модель
ПРИМЕЧАНИЕ. – Основные значения данного параметра мнемонически обозначаются как "ОПООАЧ" (Обычный пользователь, Отсутствует, Ограниченная, Администратор, Частично привилегированный).			

7.4.2 Уровень требуемой привилегии (RL)

Уровень требуемой привилегии определяет операционный уровень, для которого злоумышленник должен иметь привилегии, чтобы попытаться атаковать слабое место.

Таблица 9 – Весовые коэффициенты уровня требуемой привилегии

Значение	Код (прим.)	Вес	Описание
Приложение	A	1,0	Злоумышленник должен обладать привилегиями, которые поддерживаются в самом анализируемом программном обеспечении. (Если анализируемое программное обеспечение является одной из важнейших частей базовой системы, например ядром операционной системы, то, возможно, более целесообразно использовать значение "Система")
Система	S	0,9	Злоумышленник должен обладать привилегиями для базовой системы или физического хоста, которые используются для прогона анализируемого программного обеспечения
Сеть	N	0,7	Злоумышленник должен обладать привилегиями для доступа в сеть
Инфраструктура предприятия	E	1,0	Злоумышленник должен обладать привилегиями для одного из важнейших участков инфраструктуры предприятия, например маршрутизатора, коммутатора, DNS, контроллера домена, брандмауэра, сервера определения идентичности и т. д.
Стандартное значение	D	0,9	Медиана весовых коэффициентов для значений "Приложение", "Система", "Сеть" и "Инфраструктура предприятия"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Этот параметр может не применяться в среде с высокими требованиями к гарантии, предписывающими строгое выполнение мер по разделению привилегий, даже между пользователями, уже имеющими привилегии
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. Следует отметить, что количественные значения поддерживаются для полноты; однако в связи с тем, что привилегии и пользователи являются отдельными объектами, может существовать лишь ограниченное число случаев, в которых целесообразно использовать количественную модель
ПРИМЕЧАНИЕ. – Основные значения данного параметра мнемонически обозначаются как "СПСИ" (Система, Приложение, Сеть, Инфраструктура предприятия).			

7.4.3 Вектор доступа (AV)

Вектор доступа определяет канал, по которому злоумышленник должен обмениваться информацией, чтобы получить доступ к коду или функциональной возможности, содержащими слабое место. Следует отметить, что эти значения весьма схожи со значениями, используемыми в CVSS, за исключением того, что в CWSS проводится различие между физическим доступом и местным (оболочка/учетная запись) доступом.

Притом что между вектором доступа и уровнем требуемой привилегии существует тесная взаимосвязь, эти два параметра различны. Например, злоумышленник, имеющий "физический" доступ к маршрутизатору, может обладать способностью затронуть сеть или уровень предприятия.

Таблица 10 – Весовые коэффициенты вектора доступа

Значение	Код	Вес	Описание
Интернет	I	1,0	Злоумышленник должен иметь доступ в интернет, для того чтобы добраться до слабого места
Интранет	R	0,8	Злоумышленник должен иметь доступ к внутренней сети предприятия, которая защищена от прямого доступа из интернета, например с помощью брандмауэра, при этом без использования интернета внутренняя сеть доступна для большинства сотрудников предприятия
Частная сеть	V	0,8	Злоумышленник должен иметь доступ к частной сети, которая доступна узко определенному кругу доверенных сторон
Соседняя сеть	A	0,7	Злоумышленник должен иметь доступ к физическому интерфейсу с сетью, например домену широковещательной передачи или домену коллизий, относящимся к уязвимому программному обеспечению. К примерам локальных сетей относятся локальная подсеть на базе протокола Интернет (IP), Bluetooth, IEEE 802.11 и локальный сегмент Ethernet
Локальный	L	0,5	Злоумышленник должен иметь интерактивную локальную (оболочка) учетную запись, которая имеет прямой интерфейс с базовой операционной системой
Физический	P	0,2	Злоумышленник должен иметь физический доступ к системе, в которой работает программное обеспечение, или, в противном случае, он должен иметь возможность взаимодействия с системой через такие интерфейсы, как универсальная последовательная шина (USB), компакт-диск (CD), клавиатура, мышь и т. д.
Стандартное значение	D	0,75	Медиана весовых коэффициентов для соответствующих значений
Неизвестно	U	0,5	
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. Следует отметить, что количественные значения поддерживаются для полноты; однако, поскольку векторы доступа являются дискретными объектами, может существовать лишь ограниченное число случаев, в которых целесообразно использовать количественную модель

7.4.4 Сложность аутентификации (AS)

Сложность аутентификации охватывает сложность программы аутентификации, которая обеспечивает защиту кода/функциональной возможности, содержащих слабое место.

Если используется несколько программ аутентификации или если существует две и более ветвей кода, оценка должна выполняться следующим образом:

В случае нескольких программ аутентификации или нескольких ветвей кода, по которым можно достичь того же слабого места, применяется следующий руководящий принцип.

- Для каждой ветви кода проводится анализ каждой программы аутентификации, существующей на данной ветви кода, и выбирается значение с наименьшим весовым коэффициентом (то есть программа самой строгой аутентификации на данной ветви кода). Это значением называется значением ветви кода.
- Осуществляется сбор всех значений ветви кода.
- Выбирается значение ветви кода, имеющее наибольший весовой коэффициент (то есть имеющее самую слабую программу).

В данном методе каждая ветвь кода оценивается по самой строгой программе аутентификации данной ветви (поскольку злоумышленнику потребуется обойти данное средство контроля), затем выбирается наименее защищенная ветвь кода (то есть самый легкий путь, по которому пойдет злоумышленник).

Таблица 11 – Весовые коэффициенты сложности аутентификации

Значение	Код	Вес	Описание
Строгая	S	0,7	Слабое место обусловливает потребность в наиболее строгом из имеющихся методов для привязки данного объекта к реальной идентичности, например таком, как аппаратные жетон и/или многофакторная аутентификация
Средняя	M	0,8	Слабое место обусловливает потребность в аутентификации с использованием умеренно строгих методов, таких как применение сертификатов от недоверенных органов, аутентификации на основе знаний или одноразовых паролей
Слабая	W	0,9	Слабое место обусловливает потребность в методе простой, слабой аутентификации, который легко вскрывается с помощью спуфинга, словаря или атак с повтором, таких как неизменный пароль
Отсутствует	N	1,0	Слабое место не обусловливает потребности в какой бы то ни было аутентификации
Стандартное значение	D	0,85	Медиана весовых коэффициентов для значений "Строгая", "Средняя", "Слабая" и "Отсутствует"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Данный параметр может не применяться в среде с высокими требованиями к гарантии, предписывающими строгое выполнение мер по разделению привилегий, даже между пользователями, уже имеющими привилегии
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов

7.4.5 Уровень взаимодействия (IN)

Уровень взаимодействия охватывает действия, которые необходимо совершить лицу/лицам, являющемуся/являющимся объектом атаки, для того чтобы создать условия для ее успешного осуществления.

Таблица 12 – Весовые коэффициенты уровня взаимодействия

Значение	Код	Вес	Описание
Автоматическое	A	1,0	Взаимодействия с человеком не требуется
Типовое/ ограниченное	T	0,9	Злоумышленник должен убедить пользователя выполнить действие, которое является общим или рассматривается как "обычное" в рамках типового режима работы продукта. Например, щелчок по ссылке на веб-страницу или предварительный просмотр тела письма, пришедшего по электронной почте, являются общим поведением
Среднее	M	0,8	Злоумышленник должен убедить пользователя выполнить действие, которое осмотрительному знающему пользователю может показаться подозрительным. Например, пользователь должен принять предупреждение, в котором предполагается, что полезная нагрузка злоумышленника может содержать опасный контент
Уступающее	O	0,3	Злоумышленник не может напрямую контролировать объект атаки или воздействовать на него, а может лишь пассивно извлекать выгоду из ошибок и действий других
Высокое	H	0,1	Требуется весьма обширная психологическая атака, возможно включающая использование неосведомленности объекта атаки или неосторожности с его стороны
Взаимодействие отсутствует	NI	0,0	Не существует возможного взаимодействия, даже уступающего вместо того, чтобы вести к уязвимости, это будет, как правило, представлять

Таблица 12 – Весовые коэффициенты уровня взаимодействия

			слабое место как "ошибку". С учетом того что CWSS служит для безопасности, весовой коэффициент составляет 0
Стандартное значение	D	0,55	Медиана для значений "Автоматическое", "Ограниченное", "Среднее", "Уступающее", "Высокое" и "Взаимодействие отсутствует"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку

7.4.6 Масштаб развертывания (SC)

Масштаб развертывания определяет, присутствует ли слабое место во всех развертываемых экземплярах программного обеспечения или оно ограничено поднабором платформ и/или конфигураций. Например, ошибка числового решения может применяться только к программному обеспечению, которое запускается в среде определенной ОС и в 64-битовой архитектуре, а проблема обхода каталога может затрагивать только операционные системы, в которых символ "\" интерпретируется как разделитель каталогов.

Таблица 13 – Весовые коэффициенты масштаба развертывания

Значение	Код (прим. 1)	Вес	Описание
Полное	A	1,0	Присутствует во всех платформах или конфигурациях
Среднее	M	0,9	Присутствует в общих платформах или конфигурациях
Встречается редко	R	0,5	Присутствует только в редких платформах или конфигурациях
Потенциально достижимое	P	0,1	Потенциально достижимое (прим. 2), однако все ветви кода на текущий момент являются безопасными и/или слабое место находится в недоступном участке программы
Стандартное значение	D	0,7	Медиана весовых коэффициентов для значений РПСП
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. Пользователь может знать, какая процентная доля отправленного (или поддерживаемого) программного обеспечения содержит эту ошибку
ПРИМЕЧАНИЕ 1. – Основные значения данного параметра мнемонически обозначаются как "РПСП" (Встречается редко, Полное, Среднее, Потенциально достижимое).			
ПРИМЕЧАНИЕ 2. – Значения "Потенциально достижимое" и "Локально подтверждено" в определенной степени перекрываются в показателе "Доверие к результатам поиска" (FC).			

7.5 Группа показателей среды

Группа показателей среды состоит из следующих параметров:

- воздействие на деятельность (BI);
- вероятность обнаружения (DI);
- вероятность эксплуатации (EX);
- эффективность внешнего контроля (EC);
- распространенность (P).

7.5.1 Воздействие на деятельность (BI)

Воздействие на деятельность описывает потенциальное воздействие на деятельность или миссию в случае успешной эксплуатации слабого места.

ПРИМЕЧАНИЕ. – Поскольку связанные с деятельностью вопросы в значительной степени зависят от конкретной организации, в CWSS 1.0 не предпринимается попытки провести более детальную разбивку, например по показателю финансового, репутационного, физического, юридического или иного ущерба. Этот параметр может оцениваться количественно для поддержки моделей, определенных внешне.

Таблица 14 – Весовые коэффициенты воздействия на деятельность

Значение	Код	Вес	Описание
Критическое	C	1,0	Деятельность/миссия может оказаться невыполнимой
Высокое	H	0,9	Операции в рамках деятельности/миссии будут существенным образом затронуты
Среднее	M	0,6	Деятельность/миссия будет затронута, но без значительного ущерба для плановых операций
Низкое	L	0,3	Минимальное воздействие на деятельность/миссию
Отсутствует	N	0,0	Воздействие отсутствует
Стандартное значение	D	0,6	Медиана весовых коэффициентов для значений "Критическое", "Высокое", "Среднее", "Низкое" и "Отсутствует"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Данный параметр может не применяться в тех условиях, когда неактуален показатель воздействия на деятельность или когда воздействие оценивается и рассматриваться в аналитических процессах, не входящих в саму оценку CWSS
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. В некоторых организациях могут применяться специальные измерения бизнес-ценности актива, например такие, которые могут быть интегрированы в данное измерение

7.5.2 Вероятность обнаружения (DI)

Вероятность обнаружения – это вероятность того, что злоумышленник может обнаружить слабое место.

ПРИМЕЧАНИЕ. – Рассматривался вопрос об исключении этого параметра из CWSS 1.0, поскольку могут возникнуть трудности при его измерении и на него могут оказывать воздействие другие параметры, такие как "Приобретенная привилегия", "Техническое воздействие" и "Распространенность". Однако он был сохранен для отражения того факта, что некоторые разработчики будут использовать параметр "Вероятность обнаружения" при определении срочности разрешения какой-либо проблемы.

Таблица 15 – Весовые коэффициенты вероятности обнаружения

Значение	Код	Вес	Описание
Высокая	H	1,0	С высокой вероятностью злоумышленник сможет обнаружить слабое место быстро и с малыми усилиями, используя простые методы, без доступа к исходному коду или иным артефактам, упрощающим обнаружение слабого места
Средняя	M	0,6	Злоумышленник может выявить слабое место, но для этого потребуются определенные навыки, возможно доступ к исходному коду или реверсивное воспроизведение. Обнаружение проблемы может потребовать определенных затрат времени
Низкая	L	0,2	Маловероятно, что злоумышленник сможет обнаружить слабое место, не имея узкоспециальных навыков, доступа к исходному коду (или его эквиваленту) и без существенных затрат времени
Стандартное значение	D	0,6	Медиана для значений "Высокая", "Средняя" и "Низкая
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Этот параметр может не применяться, если эксперт предполагает, что злоумышленник обнаружит все слабые места
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов

7.5.3 Вероятность эксплуатации (EX)

Вероятность эксплуатации – это вероятность того, что, в случае обнаружения слабого места, злоумышленник, обладающий требуемыми привилегиями/аутентификацией/доступом, сможет его успешно эксплуатировать.

Таблица 16 – Весовые коэффициенты вероятности эксплуатации

Значение	Код	Вес	Описание
Высокая	H	1,0	С высокой вероятностью злоумышленник успешно поразит выбранное целью данное слабое место, имея надежный эксплойт, который легко можно развивать
Средняя	M	0,6	Злоумышленник вероятно успешно поразит выбранное целью данное слабое место, однако его шансы на успех могут изменяться или же для успешного осуществления потребуется несколько попыток
Низкая	L	0,2	Злоумышленник вероятно не поразит выбранное целью данное слабое место или имеет ограниченные шансы на успех
Отсутствует	N	0,0	Злоумышленник не имеет шансов на успех, то есть проблема является "ошибкой", так как отсутствует участие злоумышленника и отсутствуют выгоды для злоумышленника
Стандартное значение	D	0,6	Медиана для значений "Высокая", "Средняя" и "Низкая". Значение "Отсутствует" не учитывается, исходя из предположения, что с использованием этого значения будет оценено малое число результатов поиска слабых мест, а его включение в расчет медианы сократит весовой коэффициент до неинтуитивного уровня
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. Например, эксперт пожелает сделать допущение о том, что злоумышленники могут эксплуатировать любое слабое место, которое найдут, или готовы направить существенные ресурсы для обхода любых возможных барьеров в целях развития успеха
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов

Следует отметить, что на данный параметр влияет показатель воздействия слабого места, так как злоумышленники зачастую нацеливаются на слабые места, вызывающие наиболее серьезные последствия. В качестве альтернативы они могут нацеливаться на слабые места, которые легко задействовать. На этот параметр влияют также другие параметры, такие как эффективность внутреннего и внешнего контроля.

Может представляться, что влияние также оказывает распространенность, однако распространенность более тесно связана с вероятностью обнаружения.

7.5.4 Эффективность внешнего контроля (EC)

Эффективность внешнего контроля – это возможность контроля или смягчения последствий, не относящаяся к программному обеспечению, которая может затруднить доступ злоумышленника к слабому месту и его задействование злоумышленником. Например, рандомизация распределения адресного пространства (ASLR) и аналогичные методы снижают, но не ликвидируют шансы на успех атаки "переполнение буфера". Однако ASLR не реализуется напрямую в самом программном обеспечении.

В случае нескольких средств внешнего контроля или нескольких ветвей кода, по которым можно достичь того же слабого места, применяется следующий руководящий принцип:

- Для каждой ветви кода проводится анализ каждого средства внешнего контроля, существующего на данной ветви кода, и выбирается значение с наименьшим весовым коэффициентом (то есть самое действенное средство внешнего контроля на данной ветви кода). Это значение называется значением ветви кода.
- Осуществляется сбор всех значений ветви кода.

- Выбирается значение ветви кода, имеющее наибольший весовой коэффициент (то есть наименее действенное средство контроля).

В данном методе каждая ветвь кода оценивается по самому действенному средству контроля данной ветви (поскольку злоумышленнику потребуется обойти данное средство контроля), затем выбирается наименее защищенная ветвь кода (то есть самый легкий путь, по которому пойдет злоумышленник).

Таблица 17 – Весовые коэффициенты эффективности внешнего контроля

Значение	Код	Вес	Описание
Отсутствует	N	1,0	Средства контроля отсутствуют
Ограниченный	L	0,9	Имеются упрощенные методы или случайные ограничения, которые могут не позволить недостаточно подготовленному злоумышленнику эксплуатировать эту проблему
Умеренный	M	0,7	Механизм защиты широко используется, но имеет известные ограничения, которые опытный нарушитель может обойти, приняв некоторые меры
Косвенный (эшелонированная защита)	I	0,5	Средство контроля не обеспечивает реальной защиты от эксплуатации слабого места, но косвенным образом уменьшает воздействие, в случае если предпринята успешная атака, или иным образом затрудняют создание работоспособного эксплойта. Например, рандомизация распределения адресного пространства (ASLR) и аналогичные методы снижают, но не ликвидируют шансы на успех атаки "переполнение буфера". С учетом того что ответной реакцией является, как правило, выход из процесса, то результатом будет и отказ в обслуживании
Наилучший имеющийся	B	0,3	Контроль соответствует существующему передовому опыту, но ему могут быть присущи некоторые ограничения, позволяющие опытному злоумышленнику, имеющему четкую цель, преодолеть контроль, при этом может требоваться наличие других слабых мест. Например, в значительной части веб-сети используется безопасность транспортного уровня (TLS)/уровень защищенных разъемов (SSL 3), и более действенные методы в целом недоступны вследствие проблем совместимости
Полный	C	0,1	Средство контроля абсолютно эффективно противодействует слабому месту, то есть отсутствуют ошибка и уязвимость, а также отрицательные последствия эксплуатации этой проблемы. Например, тестовая среда может ограничивать операции по доступу к файлам одним рабочим каталогом, что защищает от эксплуатации обхода каталога. Весовой показатель, отличный от нуля, используется для того, чтобы отразить вероятность случайного удаления средства внешнего контроля в будущем, например при изменениях среды программного обеспечения
Стандартное значение	D	0,6	Медиана для значений "Полный", "Наилучший имеющийся", "Косвенный", "Умеренный", "Ограниченный" и "Отсутствует"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов

7.5.5 Распространенность (P)

Распространенность результата поиска определяет частоту появления слабого места данного типа в программном обеспечении.

ПРИМЕЧАНИЕ. – Следует заметить, что может рассматриваться вопрос об исключении данного параметра из будущих версий. Однако он слишком тесно связан с методами обобщенной оценки и CWRAF, чтобы быть исключенным из CWSS 1.0.

Этот параметр предназначен для использования в обобщенной оценке классов слабых мест, такой как разработка настраиваемых списков слабых мест "Топ-N". При оценке отдельного результата поиска слабого места в условиях автоматического сканирования для данного параметра вероятнее использование значения "Не применяется".

Таблица 18 – Весовые коэффициенты распространенности

Значение	Код	Вес (прим.)	Описание
Широкая	W	1,0	Слабое место обнаруживается в большинстве или всем программном обеспечении в связанной среде и может встречаться несколько раз в рамках того же программного пакета
Высокая	H	0,9	Слабое место встречается весьма часто, но оно не распространено широко
Общая	C	0,8	Слабое место встречается периодически
Ограниченная	L	0,7	Слабое место встречается редко или не встречается никогда
Стандартное значение	D	0,85	Медиана значений "Ограниченная", "Общая", "Высокая" и "Широкая"
Неизвестно	UK	0,5	Для присвоения значения данному параметру недостаточно информации. Может потребоваться дополнительный анализ. В будущем вероятен выбор иного значения, которое может затронуть оценку
Не применяется	NA	1,0	Данный параметр намеренно не учитывается при расчете оценки, потому что он не имеет значения для способа установления приоритетов слабых мест экспертом. При выполнении целевой оценки по конкретным результатам поиска слабых мест в приложении, как правило ожидается, что параметр "Распространенность" будет неактуальным, поскольку частоту появления слабого места определяют отдельное приложение и аналитические методы, и в случае наличия большего числа слабых мест многие методы агрегированной оценки будут вырабатывать более высокие оценки
Количественное значение	Q		Данный параметр можно количественно оценить с использованием настраиваемых весовых коэффициентов. Точные данные о распространенности могут иметься в ограниченных случаях использования, при условии что пользователь отслеживает данные о слабых местах на низком уровне детализации. Например, разработчик может отслеживать слабое место в рамках семейства продуктов или разработчик ревизии программы может измерять распространенность из анализируемого программного обеспечения по всей клиентской базе. В предыдущей версии CWSS распространенность вычислялась на основании необработанных данных голосования, собираемых по списку Топ-25 за 2011 год, в которых использовались дискретные значения (в интервале от 1 до 4), далее приводимые к интервалу 1–10
ПРИМЕЧАНИЕ. – Поскольку успешная атака на программное обеспечение может быть предпринята даже при наличии единственного слабого места, выбранные весовые показатели не обеспечивают существенного различия между ними.			

7.6 Формула оценки CWSS

Оценка CWSS 1.0 может лежать в интервале от 0 до 100. Она рассчитывается следующим образом:

```
BaseFindingSubscore * AttackSurfaceSubscore * EnvironmentSubscore
```

Элемент оценки базовых результатов поиска – BaseFindingSubscore – поддерживает значения в интервале от 0 до 100. Элементы оценки области атаки и среды – AttackSurfaceSubscore и EnvironmentSubscore – поддерживают значения в интервале от 0 до 1.

7.6.1 Элемент оценки базовых результатов поиска

Элемент оценки базовых результатов поиска – BaseFindingSubscore – рассчитывается следующим образом:

```
Base = [ (10 * TechnicalImpact + 5*(AcquiredPrivilege + AcquiredPrivilegeLayer) + 5*FindingConfidence) * f(TechnicalImpact) * InternalControlEffectiveness ] * 4.0
```

```
f(TechnicalImpact) = 0 if TechnicalImpact = 0; otherwise f(TechnicalImpact) = 1.
```

Максимальное возможное значение BaseFindingSubscore составляет 100.

Определение f(TechImpact) имеет эквивалент в CVSS. Оно используется для обеспечения того, что если Техническое воздействие составляет 0, то другие добавленные параметры непреднамеренно выработают отличную он нуля оценку.

Сочетание TechnicalImpact (Техническое воздействие) и AcquiredPrivilege/AcquiredPrivilegeLayer (Требуемая привилегия/Уровень требуемой привилегии) дает равный весовой коэффициент, каждый составляющий 40% от BaseFindingSubscore. (Каждый из них генерирует подзначение, максимально равное 10). Существует определенная корректировка параметра Доверие к результатам поиска в размере 20% от Базового (максимальное значение 5). Элемент InternalControlEffectiveness (Эффективность внутреннего контроля) может снизить оценку, возможно до 0 – в зависимости от действенности какого-либо средства внутреннего контроля, которое применялось для данной проблемы. После применения InternalControlEffectiveness возможный интервал результатов составляет 0–25, поэтому используется коэффициент 4.0 для корректировки BaseFindingSubscore в целях приведения его к интервалу 0–100.

7.6.2 Элемент оценки области атаки

Элемент оценки области атаки – AttackSurfaceSubscore – рассчитывается следующим образом:

```
[ 20*(RequiredPrivilege + RequiredPrivilegeLayer + AccessVector) + 20*DeploymentScope + 15*LevelOfInteraction + 5*AuthenticationStrength ] / 100.0
```

Сочетание требуемых привилегий/доступа составляет 60% от элемента оценки области атаки; масштаб развертывания составляет еще 20%; взаимодействие – 15% и аутентификация – 5%. Требования к аутентификации не имеют большого значения при том предположении, что требование убедительного доказательства идентичности не будет существенно сдерживать злоумышленника от попыток эксплуатации уязвимости.

Значения этого элемента образуют диапазон от 0 до 100 и далее выполняется их деление на 100.

7.6.3 Элемент оценки среды

Элемент оценки среды – EnvironmentalSubscore – рассчитывается следующим образом:

```
[ (10*BusinessImpact + 3*LikelihoodOfDiscovery + 4*LikelihoodOfExploit + 3*Prevalence) * f(BusinessImpact) * ExternalControlEffectiveness ] / 20.0
```

```
f(BusinessImpact) = 0 if BusinessImpact == 0; otherwise f(BusinessImpact) = 1
```

Элемент BusinessImpact (Воздействие на деятельность) составляет 50% оценки среды и может привести итоговую оценку к 0. Элемент ExternalControlEffectiveness (Эффективность внешнего контроля) всегда не равен нулю (для учета риска его случайного удаления при изменениях среды), однако в противном случае он может оказывать значительное воздействие на итоговую оценку. Сочетание элементов вероятности обнаружения и вероятности эксплуатации – LikelihoodOfDiscovery и LikelihoodOfExploit – составляет 35% оценки, а распространенность (Prevalence) – 15%.

7.6.4 Дополнительные характеристики формулы

Существует большое разнообразие видов оценок, которые могут быть представлены, хотя умножение большого числа различных параметров в сочетании с большим числом имеющих малые значения весовых коэффициентов означает, что диапазон потенциальных оценок смещен в сторону области меньших значений.

Поскольку значения параметра "Не применяется" имеют весовой коэффициент 1, возможный максимум оценки, полученной с помощью этой формулы, составляет 100,0. В крайне редких случаях, когда определенные параметры интерпретируются как параметр "Не применяется" (например, "Техническое воздействие", "Воздействие на деятельность" и "Эффективность внутреннего контроля"), минимальная возможная оценка может отличаться от нуля.

Если для большого числа параметров используются стандартные значения при получении одной оценки с использованием медианы весовых коэффициентов, определенных в CWSS 1.0, оценки будут находиться в области малых значений. Медиана весовых коэффициентов того или иного параметра необязательно отражает наиболее вероятное значение, которое может использоваться, поэтому в будущих версиях может измениться набор стандартных весовых коэффициентов. В идеальном случае формула будет обладать таким свойством, что использование большого числа стандартных значений создает оценку, относительно близкую к 50; набор нестандартных значений может корректировать итоговую оценку в большую или меньшую сторону, повышая, таким образом, точность.

Использование значений "Неизвестно" также создает оценки, лежащие в области малых значений. Это может быть полезной характеристикой, поскольку оценки будут выше при наличии более конкретной информации.

7.7 Векторы, примеры оценок и переносимость оценок CWSS

Используя коды, определенные для каждого параметра, оценку CWSS можно хранить в компактном машинно-анализируемом, удобочитаемом для человека формате, содержащем подробные данные о том, как была создана оценка. Это подобно созданию векторов CVSS.

В отличие от CVSS, не все параметры CWSS могут быть описаны в символьной форме с дискретными значениями. Любой параметр может быть оценен количественно с непрерывными весовыми коэффициентами, которые замещают исходно определенные стандартные дискретные значения с использованием значения "Q". Параметр "Воздействие", рассчитанный с использованием CWRAF, является выражением из 32-х отдельных технических воздействий и уровней, многие из которых не будут применимы к конкретному слабому месту. Интерпретирование каждого воздействия в качестве отдельного параметра примерно вдвое увеличит число параметров, требуемых для расчета оценки CWSS. Кроме того, использование в CWRAF контекста бизнес-ценности (BVC) в целях корректировки оценок для определяемых коммерческой деятельностью вопросов означает также, что оценка CWSS и ее вектор могут оказаться несовместимым, если они "транспортированы" в другие домены или виньетки.

Ввиду всего вышеизложенного вектор CWSS 1.0 должен содержать явный перечень весовых коэффициентов для каждого параметра, даже если он увеличивает размер представления вектора.

Формат одного параметра в векторе CWSS имеет вид:

FactorName:Value,Weight (Наименование параметра: Значение, Весовой коэффициент)

Например, "`P:NA,1.0`" определяет значение "Не применяется" для параметра "Распространенность" с весовым коэффициентом 1.0. Спецификатор "`AV:P,0.2`" обозначает значение "Физический" для параметра "Вектор доступа" с весовым коэффициентом 0.2.

Параметры разделяются символом прямой косой черты, например:

```
AV:I,1.0/RP:G,0.9/AS:N,1.0,
```

в которых содержится перечень значений и весовых коэффициентов для "AV" (Вектор доступа), "RP" (Уровень требуемой привилегии) и "AS" (Сложность аутентификации).

Если представлен вектор CWSS, не содержащий перечня актуальных весовых коэффициентов для данного значения, то в отчете о реализации следует сообщить о возможной ошибке или

несоответствии, попытаться вывести версию CWSS на основании параметров и значений вектора, пересчитать оценку CWSS на базе выведенной версии и сравнить ее с исходной оценкой. Если оценки расходятся, в отчете о реализации следует сообщить о возможной ошибке или несоответствии.

7.7.1 Пример: приложение, критически важное для деятельности

Рассмотрим слабое место, о котором поступило сообщение, где приложение является основным источником дохода компании, то есть оно имеет критически важное значение для деятельности. Приложение разрешает случайным пользователям интернета создавать учетные записи, используя только адрес электронной почты. Далее пользователь может эксплуатировать это слабое место для получения привилегий администратора приложения, однако атака не будет успешной, если администратор просматривает отчет о недавней деятельности пользователя, что является общепринятой практикой. Злоумышленник на сможет получить полный контроль над приложением, но сможет удалять пользователей и данные этого приложения. Предположим также, что средства контроля для защиты слабых мест отсутствуют, однако устранить эту проблему несложно, и для этого потребуется всего несколько строк кода.

Данная ситуация может быть записана в следующем векторе CWSS:

```
(TI:H,0.9/AP:A,1.0/AL:A,1.0/IC:N,1.0/FC:T,1.0/
RP:G,0.9/RL:A,1.0/AV:I,1.0/AS:N,1.0/IN:T,0.9/SC:A,1.0/
BI:C/0.9,DI:H,1.0/EX:H,1.0/EC:N,1.0/P:NA,1.0)
```

Вектор был разбит на несколько линий для удобочитаемости. Каждая строка представляет группу показателей.

Параметры и значения представлены в таблице 19, ниже.

Таблица 19 – Параметры и значения для примера приложения, критически важного для деятельности

Фактор	Значение
Техническое воздействие	Высокое
Приобретенная привилегия	Администратор
Уровень приобретенной привилегии	Приложение
Эффективность внутреннего контроля	Отсутствует
Доверие к результатам поиска	Подтверждено
Требуемая привилегия	Гостевая
Уровень требуемой привилегии	Приложение
Вектор доступа	Интернет
Сложность аутентификации	Отсутствует
Уровень взаимодействия	Типовой/ограниченный
Масштаб развертывания	Полное
Воздействие на деятельность	Критическое
Вероятность обнаружения	Высокая
Вероятность эксплуатации	Высокая
Эффективность внешнего контроля	Отсутствует
Распространенность	Не применяется

Оценка CWSS для этого вектора составляет 92,6 и получена следующим образом:

- BaseSubscore:
  - `[ (10 * TI + 5*(AP + AL) + 5*FC) * f(TI) * IC ] * 4.0`

- f(TI) = 1
- = [(10 * 0.9 + 5*(1.0 + 1.0) + 5*1.0) * 1 * 1.0] * 4.0
- = [(9.0 + 10.0 + 5.0) * 1.0] * 4.0
- = 24.0 * 4.0
- = 96.0

• AttackSurfaceSubscore:

- [20*(RP + RL + AV) + 20*SC + 15*IN + 5*AS] / 100.0
- = [20*(0.9 + 1.0 + 1.0) + 20*1.0 + 15*0.9 + 5*1.0] / 100.0
- = [58.0 + 20.0 + 13.5 + 5.0] / 100.0
- = 96.5 / 100.0
- = 0.965

• EnvironmentSubscore:

- [(10*BI + 3*DI + 4*EX + 3*P) * f(BI) * EC] / 20.0
- f(BI) = 1
- = [(10*1.0 + 3*1.0 + 4*1.0 + 3*1.0) * 1 * 1.0] / 20.0
- = [(10.0 + 3.0 + 4.0 + 3.0) * 1.0] / 20.0
- = 20.0 / 20.0
- = 1.0

Итоговая оценка:

```
96.0 * 0.965 * 1.0 = 92.64 == 92.6
```

7.7.2 Пример: вики с ограниченной критичностью для деятельности

Рассмотрим данный вектор CWSS. Предположим, что программным обеспечением является вики, используемая для отслеживания общественных мероприятий для предприятия средних размеров. Одной из наиболее важных характеристик является среднее техническое воздействие на администратора приложения со стороны постоянного пользователя приложения, однако это приложение не имеет критически важного значения для деятельности, поэтому общее воздействие на деятельность невелико. Следует отметить также, что значением большинства параметров среды установлено значение "Не применяется".

```
(TI:M,0.6/AP:A,1.0/AL:A,1.0/IC:N,1.0/FC:T,1.0/
RP:RU,0.7/RL:A,1.0/AV:I,1.0/AS:W,0.9/IN:A,1.0/SC:NA,1.0/
BI:L/0.3,DI:NA,1.0/EX:NA,1.0/EC:N,1.0/RE:NA,1.0/P:NA,1.0)
```

Вектор был разбит на несколько строк для удобочитаемости. Каждая строка представляет группу показателей.

Параметры и значения представлены в таблице 20, ниже.

Таблица 20 – Параметры и значения примера приложения с ограниченной критичностью для деятельности

Фактор	Значение
Техническое воздействие	Среднее
Приобретенная привилегия	Администратор
Уровень приобретенной привилегии	Приложение
Эффективность внутреннего контроля	Отсутствует
Доверие к результатам поиска	Подтверждено
Требуемая привилегия	Обычный пользователь
Уровень требуемой привилегии	Приложение
Вектор доступа	Интернет
Сложность аутентификации	Слабая
Уровень взаимодействия	Автоматическое
Масштаб развертывания	Не применяется
Воздействие на деятельность	Низкое
Вероятность обнаружения	Не применяется
Вероятность эксплуатации	Не применяется
Эффективность внешнего контроля	Отсутствует
Распространенность	Не применяется

Оценка CWSS для этого вектора составляет 51,1 и получена следующим образом:

- BaseSubscore:
  - `[ (10 * TI + 5*(AP + AL) + 5*FC) * f(TI) * IC ] * 4.0`
  - `f(TI) = 1`
  - `= [ (10 * 0.6 + 5*(1 + 1) + 5*1) * f(TI) * 1 ] * 4.0`
  - `= 84.0`
- AttackSurfaceSubscore:
  - `[ 20*(RP + RL + AV) + 20*SC + 15*IN + 5*AS ] / 100.0`
  - `= [ 20*(0.7 + 1 + 1) + 20*1.0 + 15*1.0 + 5*0.9 ] / 100.0`
  - `= [ 54.0 + 20.0 + 15.0 + 4.5 ] / 100.0`
  - `= 93.5 / 100.0`
  - `= 0.94 (0.935)`
- EnvironmentSubscore:
  - `[ (10*BI + 3*DI + 4*EX + 3*P) * f(BI) * EC ] / 20.0`
  - `f(BI) = 1`
  - `= [ (10*0.3 + 3*1.0 + 4*1.0 + 3*1.0) * f(BI) * 1 ] / 20.0`
  - `= [ (3.0 + 3.0 + 4.0 + 3.0) * 1.0 * 1.0 ] / 20.0`
  - `= [ 13.0 * 1.0 ] / 20.0`
  - `= 0.65`

Итоговая оценка:

`84.0 * 0.935 * 0.65 = 51.051 == 51.1`

7.7.3 Другие подходы к переносимости оценки CWSS

Взамен регистрации каждого отдельного весового коэффициента в векторе CWSS могут быть приняты иные методы.

Одна из возможностей заключается в расширении векторов CWSS для записи дополнительных метаданных, которые не затрагивают оценку, но отражают версию или содержат иную важную информацию. Часть метаданных необязательно должна включать весовые показатели как таковые.

Например, версия CWSS может быть записана с использованием наименования "параметра", например "V", вместе со значением, отражающим версию CWSS, например: "V:1.1". Это добавит примерно 4 байта к каждому вектору CWSS. Однако если версия кодируется в рамках вектора, то более не потребуется записывать присвоенные весовые коэффициенты (за исключением количественных значений), поэтому результирующие векторы могут оказаться значительно короче.

Другой подход может заключаться в прикреплении метаданных к совокупности оценок CWSS (таких как оценочная карта технического воздействия, если используется CWRAF), однако эти метаданные могут очень легко отделиться от оценок/векторов. По-прежнему будет необходимо представлять в векторе параметры, оцененные количественно, так как они могут изменяться для каждого результата поиска слабого мета.

Еще один подход заключается в том, что когда оценки CWSS передаются от одной стороне другой, принимающая сторона может пересчитать оценки на основе данных векторов CWSS, а затем сравнить пересчитанные оценки с исходными оценками. Разница в оценках будет указывать на то, что поставщик и принимающая сторона используют разные механизмы, возможно разные версии CWSS.

Библиография

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

[b-ITU-T X.1520] Рекомендация МСЭ-Т X.1520 (2014 год*), Общеизвестные уязвимости и незащищенность*.

[b-ITU-T X.1521] Рекомендация МСЭ-Т X.1521 (2011 год*), Система оценки общеизвестных уязвимостей.*

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

[b-ITU-T X.1544] Рекомендация МСЭ-Т X.1544 (2013 год), *Перечень и классификация общеизвестных схем атак*.

[b-CWRAF] Common Weakness Risk Analysis Framework <http://cwe.mitre.org/cwraf/>

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 протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2020 год