Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1208

(01/2014)

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

Безопасность киберпространства – Кибербезопасность

Показатель риска в области кибербезопасности для укрепления доверия и безопасности при использовании электросвязи/информационно-коммуникационных технологий

Рекомендация МСЭ-Т X.1208

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	**X.1200–X.1229**
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

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

Рекомендация МСЭ-Т X.1208

Показатель риска в области кибербезопасности для укрепления доверия и безопасности при использовании электросвязи/информационно-коммуникационных технологий

Резюме

В Рекомендации МСЭ-Т X.1208 описывается методика использования показателей кибербезопасности при расчете меры риска для организаций, а также приводится перечень возможных таких показателей.

Рекомендация МСЭ-Т X.1208 предназначается для помощи организациям, реализующим или эксплуатирующим участок глобальной инфраструктуры информационно-коммуникационных технологий, для оценки их собственных возможностей и риска в области кибербезопасности. Эти руководящие указания имеют целью упростить принятие решения в рамках той или иной организации по снижению рисков и тому, куда можно/следует вкладывать ресурсы для повышения своей кибербезопасности.

В Рекомендации МСЭ-Т X.1208 не предлагается использование какого-либо индекса или какого-либо одного показателя для отражения возможностей организации в области кибербезопасности.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1208	24.01.2014 г.	17-я	11.1002/1000/11950

Ключевые слова

Показатель кибербезопасности, показатель риска в области кибербезопасности.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого следует 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

Рекомендация МСЭ-Т X.1208

Показатель риска в области кибербезопасности для укрепления доверия и безопасности при использовании электросвязи/ информационно-коммуникационных технологий

1 Сфера применения

В настоящей Рекомендации приведены руководящие принципы, призванные помочь организациям в разработке, выборе и идентификации данных, которые должны быть получены (на основе выбранных показателей), и показано, как эта информация может быть использована для расчета показателя риска в области кибербезопасности (CSIR). Следует отметить, что организация может генерировать показатель риска в области кибербезопасности по какому-либо конкретному набору показателей кибербезопасности (CSI), а департаменты организации могут также генерировать такой показатель по собственному конкретному набору показателей кибербезопасности. Показатель кибербезопасности имеет целью обеспечить возможность для оценки уровня компетентности какой-либо организации в вопросах кибербезопасности в какой-либо определенный момент времени, а при повторении данного процесса в другие моменты времени этот показатель позволяет оценить прогресс в реализации программы кибербезопасности какой-либо организации в динамике.

В настоящей Рекомендации также приводится перечень возможных показателей кибербезопасности и описывается методика, которую следует применять для расчета показателя риска в области кибербезопасности с использованием вышеупомянутых показателей.

Настоящая Рекомендация направлена на оказание помощи организациям, реализующим или эксплуатирующим участок глобальной инфраструктуры информационно-коммуникационных технологий, в оценке их собственных возможностей в области кибербезопасности и расчете показателя риска в области кибербезопасности. Данные руководящие указания имеют целью упростить процесс принятия решений в рамках организаций по повышению кибербезопасности и снижению рисков в этой области. Кроме того, они дают организациям представление о том, куда можно/следует вкладывать ресурсы для повышения своей кибербезопасности.

Настоящая Рекомендация не предназначена для использования в целях формирования показателя риска в области кибербезопасности на уровне страны. Кроме того, в ней не предлагается использование какого-либо индекса или какого-либо одного показателя для отражения возможностей организации в области кибербезопасности (см. п. 6.1).

ПРИМЕЧАНИЕ 1. – Не следует проводить сопоставление рассчитываемого показателя риска в области кибербезопасности между разными организациями, поскольку предполагается, что каждая организация или сообщество должны выбрать набор показателей кибербезопасности, который они сочтут подходящим для них. Кроме того, предполагается, что они должны разработать методику измерения и критерии для устранения своих рисков и проблем. В некоторых случаях вместо объективных данных может использоваться субъективная информация. Поэтому ни в коем случае не рекомендуется сопоставлять показатель риска в области кибербезопасности для одной организации с аналогичным показателем для другой, так как этот показатель в значительной мере зависит от контекста.

ПРИМЕЧАНИЕ 2. – Описанные в настоящей Рекомендации показатели могут быть несовместимы с показателями, разработанными собственными отраслями промышленности в связи с различными целями этих отраслей.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 проверка (audit) [b-ITU-T X.800]: Независимый анализ и рассмотрение записей и действий системы для проверки на соответствие управляющих функций систем в целях обеспечения соблюдения установленных политических и эксплуатационных процедур, для обнаружения брешей в системе безопасности и для рекомендаций каких-либо указанных изменений в контроле, политике и процедурах.

3.1.2 бот (bot) [b-ITU-T X-Sup.8]: Автоматизированное программное обеспечение, которое используется для выполнения конкретных задач, предназначенных для достижения злонамеренных целей. Этот термин является синонимом термина "робот".

3.1.3 кибербезопасность (cybersecurity) [b-ITU-T X.1205]: Это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде. Общие задачи обеспечения безопасности включают следующее:

– доступность;

– целостность, которая может включать аутентичность и неотказуемость;

– конфиденциальность.

3.1.4 измерение (measurement) [b-ENISA]: Действие по измерению или процесс измерения, при котором определяется значение количественной переменной в сравнении со (стандартной) единицей измерения.

3.1.5 метрика (metric) [b-ENISA]: Система связанных измерений, позволяющих получить количественное выражение некоторых характеристик системы, компонента или процесса. Метрика состоит из двух или более мер.

3.1.6 корректировка (patch) [b-ITU-T X.1206]: Широко распространяемое средство для устранения уязвимости конкретного продукта в отношении безопасности. Метод обновления файла, который заменяет только изменяемые части, а не весь файл.

3.1.7 информация, позволяющая установить личность (personally identifiable information (PII)) [b-ITU-T X.1252]: Любая информация, a) которая идентифицирует или может использоваться для идентификации, обращения или установления местоположения лица, к которому такая информация относится; b) на основе которой может быть осуществлена идентификация или получение контактной информации частного лица; или c) которая прямо или косвенно связана либо может быть связана с физическим лицом.

3.1.8 риск (risk) [b-ISO/IEC 27000]: Влияние неопределенности на задачи.

3.1.9 управление риском (risk management) [b-ISO/IEC 27000]: Скоординированные действия по управлению и контролю в организации по отношению к риску.

3.1.10 сертификат безопасности (security certificate) [b-ITU-T X.810]: Набор относящихся к обеспечению безопасности данных, который выдан органом обеспечения безопасности или доверенной третьей стороной, в совокупности с информацией о безопасности, которая используется для предоставления услуг обеспечения целостности и аутентификации источника данных в отношении данных.

3.1.11 меры обеспечения безопасности (security controls) [b-NIST FIPS 199]: Управленческие, эксплуатационные и технические меры обеспечения (т. е. защитные меры или контрмеры), предписанные информационной системе для защиты конфиденциальности, целостности и доступности этой системы и ее информации.

3.1.12 инцидент безопасности (security incident) [b-ITU-T E.409]: Это любое неблагоприятное событие, в результате которого некий аспект безопасности может подвергнуться угрозе.

3.1.13 спам (spam) [b-ITU-T X.1242]: Электронная информация, переданная от отправителей к получателям при помощи оконечных устройств, таких как компьютеры, мобильные телефоны, телефоны и т. д., которая, как правило, не предусмотрена, нежелательна и опасна для получателей.

3.1.14 угроза (threat) [b-ISO/IEC 27000]: Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации.

3.1.15 уязвимость (vulnerability) [b-ITU-T X.1500]: Любое слабое место, которое может быть использовано для нарушения системы или информации, которая в ней содержится (в соответствии с Приложением A к [b-ITU-T X.800]).

3.1.16 слабое место (weakness) [b-ITU-T X.1500]: Недостаток или дефект, который, хотя и не признается сам по себе в качестве уязвимости, мог бы в какой-то момент стать уязвимостью или мог бы способствовать привнесению других уязвимостей.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 показатель кибербезопасности (cybersecurity indicator): Любой показатель из набора показателей, используемых для расчета или измерения состояния риска возможностей или компетентности в вопросах кибербезопасности в организации или сообществе.

ПРИМЕЧАНИЕ. – Выбранные показатели кибербезопасности – это показатели, которые выбраны по причине их актуальности, т. е. их определенной связи с проблемами риска.

3.2.2 показатель риска в области кибербезопасности (cybersecurity indicator of risk): Результат применения методики расчета показателя риска в области кибербезопасности.

3.2.3 набор показателей кибербезопасности (cybersecurity indicator suite): Выбранная совокупность показателей кибербезопасности, которая будет использоваться для расчета показателя риска в области кибербезопасности.

ПРИМЕЧАНИЕ. – Какого-либо одного уникального набора показателей кибербезопасности не существует.

3.2.4 показатель (indicator): Является синонимом термина "метрика", приведенного в п. 3.1.5.

3.2.5 система управления информационной безопасностью (information security management system): Часть системы общего управления на основе метода определения деловых рисков, предназначенная для создания реализации, функционирования, контроля, анализа, поддержания и повышения информационной безопасности; см. п. 3.2.1 [b-ISO/IEC 27000].

ПРИМЕЧАНИЕ. – Система управления включает организационную структуру, политику, деятельность по планированию, обязанности, практические методы, процедуры, процессы и ресурсы.

3.2.6 программа (programme): Набор скоординированных действий, направленных на достижение четкой цели деятельности.

3.2.7 управляющая программа (program): Набор кодированных инструкций, которые позволяют машине, в частности компьютеру, выполнять требуемую последовательность операций.

3.2.8 источник угрозы (threat source): Это либо намерение и метод, в основе которых лежит умышленное использование уязвимости, либо ситуация и метод, которые могут случайно привести к использованию уязвимости.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

AS	Autonomous System	Автономная система
BSA	Business Software Alliance	Ассоциация производителей программного обеспечения
C&A	Certified and Accredited	Сертифицированный и аккредитованный
CIS	Center for Internet Security	Центр безопасности интернета

CSI	Cybersecurity indicator		Показатель кибербезопасности
CSIR	Cybersecurity indicator of Risk		Показатель риска в области кибербезопасности
CVE	Common Vulnerabilities and Exposures		Общеизвестные уязвимости и незащищенность
CYBEX	Cybersecurity information Exchange		Обмен информацией о кибербезопасности
DB	Database		База данных
DDoS	Distributed Denial-of-Service		Распределенный отказ в обслуживании
DHCP	Dynamic Host Configuration Protocol		Протокол динамической конфигурации хост-компьютера
DoS	Denial-of-Service		Отказ в обслуживании
DNS	Domain Name System		Система наименований доменов
GDP	Gross Domestic Product	ВВП	Валовой внутренний продукт
ICT	Information and Communication Technology		Информационно-коммуникационные технологии
ID	Identifier		Идентификатор
IDS	Intrusion Detection System		Система обнаружения проникновений
IP	Internet Protocol		Протокол Интернет
IPS	Intrusion Prevention System		Система предотвращения проникновений
ISMS	Information Security Management System		Система управления информационной безопасностью
IT	Information Technology	ИТ	Информационные технологии
PCA	Principal Components Analysis		Анализ главных компонентов
PII	Personally Identifiable Information		Информация, позволяющая установить личность
SSL	Secure Socket Layer		Уровень защищенных разъемов
TLS	Transport Layer Security		Безопасность транспортного уровня
TTP	Trusted Third Party		Доверенная третья сторона

5 Условные обозначения

В настоящей Рекомендации термин "организация" предназначен для широкого толкования. Следует понимать, что здесь термин "организация" охватывает также понятие "сообщество". Однако термин "организация" никогда не следует рассматривать как эквивалент термина "страна".

6 Показатель кибербезопасности

6.1 Введение

Многочисленные усилия прилагаются к тому, чтобы измерить характеристики информационно-коммуникационных технологий (ИКТ), отследить выполнение и оценить влияние использования ИКТ на правительственные органы, операторов, научно-исследовательские и отраслевые организации. Примеры таких отраслевых показателей включают Глобальный рейтинг облачных вычислений [b-BSA] и метрики безопасности, опубликованные Центром безопасности интернета [b-CIS]. Показатели, приведенные в настоящей Рекомендации, сосредоточены на некоторых аспектах кибербезопасности.

Показатель риска в области кибербезопасности, описанный в настоящей Рекомендации, состоит из нескольких показателей кибербезопасности, объединенных в рамках меры риска, описывающей существующую ситуацию с рисками возможностей кибербезопасности и их эффективности, а также действенности реализации мер обеспечения безопасности в организации или сообществе.

Существует два отдельных условия, при которых может быть вычислена такая мера риска, как показатель риска в области кибербезопасности, – самостоятельная оценка своих возможностей кибербезопасности или набор показателей, рассчитанных некоторой внешней сторонней организацией. Настоящая Рекомендация предназначена для использования при проведении организациями самостоятельной оценки.

В настоящей Рекомендации показатели могут выбираться с учетом международных стандартов в области систем управления информационной безопасностью [b-ISO/IEC 27001], [b-ISO/IEC 27002], [b-ISO/IEC 27003], сетевой безопасностью. [b-ISO/IEC 27033-1], [b-ISO/IEC 27033-2], [b-ISO/IEC 27033-4] и других спецификаций [b-NIST SP 800-27], [b-NIST SP 800-30], [b-NIST SP 800-53]. Международные стандарты в области управления позволяют организациям разрабатывать, осуществлять и поддерживать согласованный набор политических принципов, процессов и систем для управления рисками своим информационным ресурсам, обеспечивая тем самым приемлемые риски информационной безопасности. Международные стандарты в области сетевой безопасности определяют и описывают концепции, связанные с сетевой безопасностью, и обеспечивают руководство по управлению такой безопасностью. В других спецификациях приводятся основные принципы управления по снижению рисков информационному ресурсу и способы управления рисками среды ИКТ организации.

Эти показатели могут быть разбиты на группы в соответствии с бизнес-функциями: управление инцидентами, управление уязвимостями, управление корректировками, безопасность приложений, управление конфигурацией и функции финансовой категории.

В настоящей Рекомендации не предлагается использование какого-либо индекса или какого-либо одного показателя для отражения возможностей организации в области кибербезопасности. Причина в том, что безопасность любой организации определяется безопасностью ее самого слабого звена, а использование индекса, отражающего возможности такой организации в области кибербезопасности, не позволяет надлежащим образом выявить потенциальное влияние, связанное с этим слабым звеном. Представление показателя риска в области кибербезопасности в виде единого номера может ввести в заблуждение его предполагаемых пользователей, а также породить ложные ожидания у тех, кто, как предполагается, будет использовать его в процессе принятия решений. Более конкретно, в случае агрегирования ряда показателей и приведения их к единому номеру (т. е. индексу) наличие и значение слабых мест какой-либо организации перестают быть очевидными. Таким образом, было бы нецелесообразно как применять этот индекс для указания на наличие у организации удовлетворительных возможностей в области кибербезопасности, так и рассматривать вопрос его использования для сопоставления возможностей разных организаций в этой области.

6.2 Общие принципы, касающиеся показателей кибербезопасности

В этом пункте описываются общие принципы, которые необходимо учитывать при разработке показателей кибербезопасности.

- При расчете показателя риска в области кибербезопасности предпочтение следует отдавать использованию согласованного во всемирном масштабе набора показателей.
- Показатели кибербезопасности необходимо выбирать так, чтобы их можно было использовать для измерения текущего состояния компетентности в вопросах кибербезопасности по отношению к угрозам либо для измерения хода реализации программы обеспечения информационной безопасности в организации или сообществе.
- Следует выбирать показатели кибербезопасности, позволяющие обеспечить точность и конфиденциальность первичных данных, которые должны быть собраны и использованы в качестве основы для расчета показателя риска в области кибербезопасности.
- Процессы сбора должны обеспечивать сохранение целостности первичных данных, которые должны быть использованы в качестве основы для расчета показателя риска в области кибербезопасности.

- Предпочтение следует отдавать использованию показателей, которые могут помочь лицам, определяющим политику, измерять качество реализации политики в области информационной безопасности и отслеживать ход выполнения программы в области кибербезопасности.
- Необходимо разрабатывать новые дополнительные показатели или своевременно обновлять существующие в условиях быстрого изменения услуг и технологий ИКТ.

6.3 Руководящие принципы, касающиеся выбора показателей кибербезопасности

При выборе показателей, которые должны использоваться для расчета показателя, возможно, необходимо выбирать те из них, которые способствуют выполнению целей и задач организации. Так, организации могут выбирать показатели на основе бизнес-функций с высоким приоритетом.

В частности, показатель кибербезопасности должен обеспечивать возможность:

- измерения основного влияния на результаты функционирования;
- его использования для решения проблем на уровне системы, на уровне программы и на обоих уровнях в зависимости от ситуации;
- измерения хода реализации программы обеспечения кибербезопасности, конкретных мер обеспечения безопасности, а также связанных с ними политики и процедур кибербезопасности;
- измерения аспектов, позволяющих определить эффективность и действенность реализации мер в рамках программы обеспечения кибербезопасности;
- измерения положительного или отрицательного влияния программы обеспечения кибербезопасности на миссию организации;
- измерения состояния выполнения политики в области кибербезопасности с возможностью получения результатов на уровне системы, на уровне программы или на обоих уровнях;
- измерения положительного и отрицательного влияния на повседневную жизнь пользователей.

Кроме того, следует выбирать показатель кибербезопасности, обеспечивающий возможность сбора точных и надежных данных. На протяжении всего процесса измерения необходимо обеспечивать доступность первичных данных, целостность используемых данных и защиту их конфиденциальности.

6.4 Классификация показателей

Существует три типа показателей в зависимости от их характера: показатели реализации, эффективности/действенности и влияния. Показатели реализации используются, чтобы продемонстрировать ход реализации программы обеспечения информационной безопасности, конкретных мер противодействия для обеспечения безопасности и связанных с ними политики и процедур. Они могут быть сгруппированы по двум подтипам: показатели реализации на уровне программы и показатели на уровне системы. Примеры показателей реализации, относящихся к уровню системы, включают процентную долю сотрудников службы безопасности информационных систем, которые прошли обучение мерам обеспечения безопасности.

Показатели эффективности/действенности могут использоваться для проверки того, обеспечивается ли надлежащая реализация процессов на уровне программы и мер обеспечения безопасности на уровне системы, функционируют ли они намеченным образом и удовлетворяют ли они требуемым целям и задачам. Эти показатели касаются двух аспектов результата реализации мер обеспечения безопасности – эффективности и действенности; эффективность охватывает надежность, а действенность – своевременность. Примеры показателей эффективности включают процентную долю инцидентов информационной безопасности, вызванных ненадлежащей конфигурацией управления доступом; примеры показателей действенности включают процентную долю компонентов систем, которые проходят своевременное техническое обслуживание.

Показатели влияния могут быть использованы для определения влияния информационной безопасности на миссию организации. Они могут использоваться для количественного выражения экономии, полученной с помощью программы обеспечения информационной безопасности или затрат, понесенных при устранении инцидента информационной безопасности, степени общественного доверия, завоеванного программой информационной безопасности, или других видов влияния информационной безопасности на миссию. Примеры показателей влияния включают процентную долю издержек организации на информационную безопасность к общим издержкам на информационную систему.

Кроме того, показатели могут группироваться в соответствии с бизнес-функциями: управление инцидентами, управление уязвимостями, управление корректировками, безопасность приложений, безопасность конфигурации, финансовые метрики, безопасность данных и сетей и т. д.

7 Процесс разработки показателя кибербезопасности

7.1 Введение

Набор показателей кибербезопасности следует рассматривать как один из важнейших инструментариев, который можно использовать для оценки действенности политики укрепления информационной безопасности и выражения существующего состояния информационной безопасности в организации.

7.2 Методика создания набора показателей кибербезопасности

Разработка набора показателей кибербезопасности является сложной задачей, и она должна осуществляться высококвалифицированными специалистами, обладающими знаниями в области экономики, кибербезопасности и статистики. При разработке перечня показателей кибербезопасности необходимо учитывать условия организации, а также различные аспекты риска, подлежащие измерению.

Разработчик показателей кибербезопасности должен учитывать, что тот или иной такой показатель, в отличие от показателей, основанных на больших выборках, может быть в значительной мере подвержен изменчивости, вызванной ограниченностью измеряемых выборок, например инцидентов, которые могут наблюдаться в незначительном масштабе. Следовательно, макроскопический анализ необходимо применять с предельной осторожностью.

Разработка набора показателей кибербезопасности и подготовка соответствующей информации к использованию включают следующие этапы:

- определение ключевых показателей, которые должны быть выбраны и использованы для расчета показателя риска в области кибербезопасности;
- определение источников данных;
- решение проблемы отсутствующих наблюдений;
- обеспечение возможности сравнения показателей друг с другом;
- преобразование показателей в значения измерения риска;
- использование набора значений измерения риска.

7.2.1 Выбор показателей для создания меры риска

Выбор показателей для создания меры риска зависит от того, что измеряется, а также от практической осуществимости сбора первичных данных.

ПРИМЕЧАНИЕ. – Хотя проведение какого-то измерения в данный момент может быть неосуществимо на практике, показатель тем не менее может быть тщательно рассмотрен в целях его выбора. Этот процесс может быть использован для определения нового вида деятельности, позволяющего собирать данные, с тем чтобы можно было надлежащим образом провести оценку риска.

Количество показателей может зависеть от миссии и задач организации или от типа используемых ею технологий. Для создания меры риска, соответствующей показателю риска в области кибербезопасности, рекомендуется использовать широкий набор показателей (например, от 10 до 30 показателей). Сочетание субъективных показателей и объективных измерений может повлиять на

правильность полученного расчета. Поэтому при создании показателя риска в области кибербезопасности рекомендуется не пропускать использования субъективных показателей. Однако в некоторых областях управления риском могут быть необходимые субъективные показатели, поэтому крайне важно иметь строгую формулировку того, как определять субъективный показатель. После того как показатели выбраны, может оказаться желательным сгруппировать их в различные категории в соответствии с их бизнес-функциями, такими как управление инцидентами, управление уязвимостями, управление корректировками и т. д. Благодаря этому показатели становятся более контролируемыми, а сравнение – более значимым.

Подробное описание процедуры разработки приведено в п. 7.3.

7.2.2 Источники данных

Степень доступности данных для показателей кибербезопасности может определять количество и качество показателей для расчета показателя риска в области кибербезопасности. Чрезмерная зависимость от одного источника данных может привести к ошибкам и пропускам. Поэтому крайне важно проверять данные путем их сравнения с другими источниками, прежде чем применять их для расчета показателя риска в области кибербезопасности.

7.2.3 Решение проблемы отсутствующих данных

При сборе измерений риска для показателя кибербезопасности могут иметь место случаи, когда данные отсутствуют или недоступны. В этих случаях данные могут быть оставлены незаполненными – в этом случае организация не присвоит никакого значения данному показателю, или же для оценки отсутствующих данных может быть использована экстраполяция. Если не заполнить данные, то это может привести к исключению аспектов показателя кибербезопасности. Экстраполяция может увеличить значение данных и тем самым привести к завышенным результатам расчетов. Существует компромисс между экстраполяцией и пропуском данных, который должен учитывать значение данных или важность показателей. Возможно, следует провести проверку чувствительности в целях определения того, насколько результаты вычислений чувствительны к изменению экстраполированного значения или в случае использования вместо незаполненных данных оценочного значения.

7.2.4 Преобразование данных

Стадия преобразования включает два этапа: преобразование абсолютных значений в относительные и преобразование относительных значений показателей в показатель риска в области кибербезопасности. Сравнимость абсолютных значений достигается в основном за счет их деления на общее количество элементов. Многие показатели уже могут предоставляться в преобразованном виде, следовательно, данный этап может и не требоваться.

7.3 Процесс разработки показателей кибербезопасности

Процесс разработки показателя кибербезопасности включает выбор показателей, которые соответствуют миссии и задачам организации или сообщества. Этот процесс состоит из пяти этапов: определение интересов заинтересованных сторон; определение целей и задач; анализ политики, руководящих принципов и процедур в области информационной безопасности; анализ реализации информационной безопасности; и выбор показателей.

Этап 1. Определение интересов заинтересованных сторон – включает определение заинтересованных сторон и их интересов. Главными заинтересованными сторонами являются руководитель организации, руководитель информационной службы, руководитель службы безопасности, специалист по безопасности информационной системы и сотрудники службы поддержки информационной системы. Итоговым результатом данного этапа является измерение всех интересов в сфере информационной безопасности. Каждой заинтересованной стороне может требоваться разный набор показателей, отражающих ее мнение в рамках ее области ответственности.

Этап 2. Определение целей и задач – включает определение целей и задач функционирования системы информационной безопасности. Они могут быть выражены в виде политики, требований, руководящих принципов и руководящих указаний. Цели и задачи программы обеспечения информационной безопасности могут быть получены из высокоуровневых целей и задач, направленных на поддержку миссии организации.

Этап 3. Анализ политики, руководящих принципов и процедур в области информационной безопасности – включает подробное описание того, как следует реализовывать меры обеспечения безопасности в рамках политики и процедур конкретной организации.

Этап 4. Анализ реализации информационной безопасности – включает анализ существующих показателей и хранилищ соответствующих данных, которые могут быть использованы для получения новых показателей.

Этап 5. Выбор показателей – включает выбор и разработку в соответствующих случаях трех видов показателей, описанных в п. 6.4. Этот этап включает выбор набора показателей, отслеживающих процесс реализации, эффективность/действенность и влияние на миссию, а также, если потребуется, разработку в соответствующих случаях новых показателей.

8 Возможные показатели кибербезопасности

В настоящем пункте описываются различные возможные показатели кибербезопасности, которые определены как основные показатели и могут применяться для создания набора показателей кибербезопасности для организации. Эти показатели могут быть распределены по трем категориям: базовые показатели, рекомендуемые показатели и необязательные показатели. Кроме того, показатели могут быть распределены по трем категориям в соответствии с характером показателя: показатели реализации, показатели эффективности/действенности и показатели влияния. В настоящей Рекомендации не определяется уровень требований, связанных с любым показателем. Предполагается, что организации определят уровень требований каждого показателя в соответствии с предлагаемой ими для использования политикой организации в области безопасности. Кроме того, организации могут – и им предлагается – разработать дополнительные показатели с учетом своей ситуации.

Рассматриваемые в этом пункте показатели (см. таблицы 8-1 – 8-30) предназначены для использования организацией; однако они могут быть также применены к сообществу путем агрегирования показателей организаций, которые являются частью какого-либо сообщества.

Существуют показатели, для которых в одних случаях более желательным является большее значение (чем больше, тем лучше), а в других – меньшее значение (чем меньше, тем лучше); имеются также случаи, в которых нельзя интуитивно понять, какое значение лучше – большее или меньшее.

Таблица 8-1 – Показатель 1: Управление уязвимостями (уровень программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Процентная доля уменьшенных уязвимостей с высоким уровнем воздействия
Цель	Организации следует своевременно устранять известные уязвимости
Индикатор	Процентная доля уязвимостей с высоким уровнем воздействия, которые были уменьшены в установленные организацией сроки после обнаружения
Формула	(Общее количество своевременно уменьшенных уязвимостей с высоким уровнем воздействия/Общее количество (выявленных уязвимостей) с высоким уровнем воздействия) × 100
Первичные данные	• Количество выявленных уязвимостей в течение определенного организацией периода времени. (Обратите внимание, что количество выявленных в течение определенного организацией периода времени уязвимостей с высоким уровнем воздействия должно рассчитываться на основе первичных данных) • Количество уменьшенных уязвимостей с высоким уровнем воздействия за этот период времени
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	

Таблица 8-1 – Показатель 1: Управление уязвимостями (уровень программы; чем больше, тем лучше)

Поле	Данные
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	Рекомендация МСЭ-Т X.1521, Система оценки общеизвестных уязвимостей, [b-ITU-T X.1521] и Рекомендация МСЭ-Т X.1520, Общеизвестные уязвимости и незащищенность, [b-ITU-T X.1520]

Таблица 8-2 – Показатель 2: Ведение журнала проверки (уровень системы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Процентная доля устройств в конечных точках, для которых ведется журнал проверки
Цель	Организации следует вести журнал проверки системы, чтобы расследовать ненадлежащую деятельность конечных точек
Индикатор	Процентная доля устройств в конечных точках, для которых ведется журнал проверки
Формула	(Общее количество устройств в конечных точках, имеющих журнал проверки/ Общее количество устройств в конечных точках) × 100
Первичные данные	• Количество устройств конечных пользователей, для которых ведется журнал проверки сервером централизованного журнала или устройством в конечной точке • Общее количество устройств в конечных точках
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-3 – Показатель 3: Реагирование на инциденты (уровень системы и уровень программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Реагирование на инциденты
Цель	Организации следует своевременно регистрировать инциденты по каждой категории инцидентов
Индикатор	Процентная доля инцидентов, зарегистрированных в установленные сроки, в разбивке по применимым категориям
Формула	(Количество своевременно зарегистрированных инцидентов/Общее количество зарегистрированных инцидентов) × 100 (по каждой категории)
Первичные данные	• Количество инцидентов, зарегистрированных в установленные организацией сроки • Общее количество зарегистрированных инцидентов
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность

Таблица 8-3 – Показатель 3: Реагирование на инциденты (уровень системы и уровень программы; чем больше, тем лучше)

Поле	Данные
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	Рекомендация МСЭ-Т X.1544, Перечень и классификация общеизвестных схем атак, [b-ITU-T X.1544]

Таблица 8-4 – Показатель 4: Среднее время уменьшения уязвимостей (уровень системы и уровень программы; чем меньше, тем лучше)

Поле	Данные
Идентификатор показателя	Среднее время уменьшения уязвимостей
Цель	Этот показатель служит признаком эффективности организации в устранении выявленных уязвимостей. Чем меньше времени требуется для уменьшения уязвимостей, тем больше вероятность того, что организация способна эффективно реагировать и уменьшить риск эксплуатации уязвимостей
Индикатор	Среднее время уменьшения уязвимостей измеряет среднее время уменьшения выявленных в организации уязвимостей
Формула	Сумма (Дата выполнения уменьшения – Дата обнаружения)/Подсчитанное число (Уменьшенные уязвимости)
Первичные данные	• Дата обнаружения уязвимостей • Дата уменьшения уязвимостей • Общее количество обнаруженных уязвимостей • Общее количество уменьшенных уязвимостей, которые были зарегистрированы
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	Рекомендация МСЭ-Т X.1521, Система оценки общеизвестных уязвимостей, [b-ITU-T X.1521] и Рекомендация МСЭ-Т X.1520, Общеизвестные уязвимости и незащищенность, [b-ITU-T X.1520]

Таблица 8-5 – Показатель 5: Развертывание программы корректировки безопасности (уровень системы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Программа корректировки безопасности
Цель	На устройствах в конечных точках следует развертывать программы корректировки безопасности в целях уменьшения уязвимостей

Таблица 8-5 – Показатель 5: Развертывание программы корректировки безопасности (уровень системы; чем больше, тем лучше)

Поле	Данные
Индикатор	Процентная доля устройств в конечных точках, на которых развернута система управления корректировками
Формула	(Общее количество устройств в конечных точках, использующих программу корректировки безопасности/Общее количество устройств в конечных точках) × 100
Первичные данные	• Общее количество устройств в конечных точках, использующих программу корректировки безопасности • Количество устройств в конечных точках
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-6 – Показатель 6: Среднее время корректировки (уровень системы и уровень программы; чем меньше, тем лучше)

Поле	Данные
Идентификатор показателя	Среднее время корректировки
Цель	Среднее время корректировки измеряет среднее время, которое занимает развертывание корректировки для систем организации. Чем быстрее могут быть развернуты корректировки, тем меньше среднее время корректировки и тем меньше время эксплуатации организацией систем, находящихся в заведомо уязвимых состояниях
Индикатор	Среднее время, которое занимает развертывание корректировки для систем организации
Формула	Сумма (Дата установки – Дата наличия)/Подсчитанное число (Выполненные корректировки)
Первичные данные	• Дата установки • Дата наличия корректировок • Общее число выполненных корректировок
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-7 – Показатель 7: Среднее время выполнения изменения конфигурации (уровень системы и уровень программы; чем меньше, тем лучше)

Поле	Данные
Идентификатор показателя	Среднее время выполнения изменения конфигурации
Цель	Среднее время выполнения изменения конфигурации измеряет среднее время, которое занимает выполнение изменения в системе организации. Чем быстрее изменение может быть развернуто, тем меньше время корректировки и тем меньше время осуществляемого организацией развертывания в системах, находящихся в заведомо уязвимых состояниях
Индикатор	Среднее время, которое занимает выполнение изменения конфигурации в системе организации
Формула	Сумма (Дата выполнения – Дата представления)/Подсчитанное число (Выполненные изменения)
Первичные данные	• Дата выполнения • Дата представления • Общее количество выполненных изменений
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-8 – Показатель 8: Охват оценкой риска (уровень системы и уровень программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Охват оценкой риска
Цель	Организации следует, по возможности, проводить оценку рисков в отношении приложений, используемых в системах организации
Индикатор	Процентная доля бизнес-приложений, в отношении которых когда-либо проводилась оценка рисков
Формула	Подсчитанное число (Приложения, прошедшие оценку рисков)/Подсчитанное число (Приложения) × 100
Первичные данные	• Количество приложений, которые прошли оценку рисков • Количество приложений
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-9 – Показатель 9: Охват программой обнаружения и устранения вредоносного программного обеспечения (уровень системы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Программа обнаружения и устранения вредоносного программного обеспечения
Цель	На устройствах конечных пользователей следует развернуть антивирусную программу для устранения последствий имеющегося в них вредоносного программного обеспечения, включая вирусы
Индикатор	Процентная доля устройств в конечных точках, на которых развернута программа обнаружения и устранения вредоносного программного обеспечения
Формула	(Общее количество устройств в конечных точках, на которых развернута программа обнаружения и устранения вредоносного программного обеспечения/Общее количество устройств в конечных точках) × 100
Первичные данные	• Общее количество устройств в конечных точках, на которых развернута программа обнаружения и устранения вредоносного программного обеспечения • Количество устройств в конечных точках
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-10 – Показатель 10: Охват планированием действий в чрезвычайных ситуациях (уровень программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Проверка плана на случай непредвиденных обстоятельств
Цель	Организации следует провести проверку плана на случай непредвиденных обстоятельств для информационных систем
Показатель	Процентная доля информационных систем, для которых проведена проверка плана действий на случай непредвиденных обстоятельств
Формула	(Количество систем конечных точек, для которых проведена проверка плана действий на случай непредвиденных обстоятельств/Общее количество систем конечных точек) × 100
Первичные данные	• Количество информационных систем, для которых проведена проверка плана действий на случай непредвиденных обстоятельств • Количество систем конечных точек
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-11 – Показатель 11: Оценка безопасности (уровень программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Процентная доля информационных систем с утверждениями оценки безопасности
Цель	Система конечных точек организации должна пройти сертификацию и аккредитацию до того, как она будет развернута, чтобы обеспечить условия полной безопасности и подотчетности для персонала, средств и продуктов
Показатель	Процентная доля новых систем конечных точек, прошедших сертификацию и аккредитацию до того, как они были развернуты
Формула	(Количество информационных систем, прошедших сертификацию и аккредитацию/ Общее количество информационных систем) × 100
Первичные данные	• Количество новых систем конечных точек, прошедших сертификацию и аккредитацию • Количество систем конечных точек
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-12 – Показатель 12: Обязательство в отношении безопасности (уровень программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Обязательство в отношении безопасности или кодекс поведения
Цель	Сотрудники, которым разрешается доступ к информационным системам, должны подписать обязательство в отношении безопасности до получения доступа к системе конечных точек организации
Показатель	Процентная доля сотрудников безопасности информационных систем, подписавших обязательство в отношении безопасности
Формула	(Количество сотрудников, получивших доступ к системе и подписавших правила поведения/Общее количество сотрудников, которым разрешен доступ к системе конечных точек) × 100
Первичные данные	• Количество сотрудников, получивших доступ к системе после подписания обязательства в отношении безопасности • Количество сотрудников, получивших доступ к системе
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Реализация
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-13 – Показатель 13: Управление удаленным доступом с использованием шлюза безопасности (уровень системы/программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Пункты защищенного удаленного доступа
Цель	Организация должна развернуть шлюз безопасности, чтобы обеспечить защищенный удаленный доступ для защиты своих внутренних ресурсов
Показатель	Процентная доля пунктов защищенного удаленного доступа
Формула	(Количество пунктов удаленного доступа, использующих шлюз безопасности/ Общее количество пунктов удаленного доступа в организации) × 100
Первичные данные	• Количество пунктов защищенного удаленного доступа, использующих шлюз безопасности • Количество пунктов защищенного удаленного доступа
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-14 – Показатель 14: Управление удаленным доступом с использованием функции безопасности для предотвращения проникновений или обнаружения проникновений (уровень системы/программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Пункты защищенного удаленного доступа
Цель	Организация должна реализовать функцию безопасности для обнаружения или предотвращения проникновений, чтобы защитить свои внутренние ресурсы
Показатель	Процентная доля пунктов защищенного удаленного доступа
Формула	(Количество пунктов удаленного доступа, в которых реализована функция безопасности для обнаружения или предотвращения проникновений/ Общее количество пунктов удаленного доступа) × 100
Первичные данные	• Количество пунктов защищенного удаленного доступа, в которых реализована функция безопасности для обнаружения или предотвращения проникновений • Количество пунктов удаленного доступа
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-15 – Показатель 15: Управление беспроводным доступом (уровень системы/программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Пункты защищенного беспроводного доступа
Цель	Организация должна обеспечить пункты защищенного беспроводного доступа для защиты внутренней сети от несанкционированного доступа
Показатель	Процентная доля пунктов защищенного беспроводного доступа
Формула	(Количество пунктов защищенного беспроводного доступа/Общее количество пунктов беспроводного доступа) × 100
Первичные данные	• Количество пунктов защищенного беспроводного доступа • Количество пунктов беспроводного доступа
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-16 – Показатель 16: Защита от противозаконных действий персонала (уровень системы/уровень программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Проверка защиты от противозаконных действий персонала
Цель	Организация должна разрешить уполномоченному персоналу пользоваться доступом к системам конечных точек
Показатель	Процентное отношение лиц, прошедших проверку, прежде чем им был предоставлен доступ к системам конечных точек организации
Формула	(Количество лиц, прошедших проверку/Общее количество лиц, имеющих доступ) × 100
Первичные данные	• Количество лиц, прошедших проверку • Количество лиц
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Реализация
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-17 – Показатель 17: Защита информации, позволяющей установить личность (PII) (уровень системы/программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Процентная доля защищенной критичной информации, позволяющей установить личность
Цель	Организация должна обеспечить защиту критичной информации организации, позволяющей установить личность, путем кодирования
Показатель	Процентная доля защищенной критичной информации, позволяющей установить личность
Формула	(Количество закодированной критичной информации, позволяющей установить личность/Общее количество критичной информации, позволяющей установить личность) × 100
Первичные данные	• Количество защищенной информации, позволяющей установить личность • Общее количество информации, позволяющей установить личность
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность и реализация
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-18 – Показатель 18: Защита резервных данных (уровень системы/программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Норма контроля целостности резервных данных
Цель	Организация должна обеспечить защиту целостности резервных данных
Показатель	Процентная доля резервных данных, целостность которых защищена
Формула	(Объем резервных данных, целостность которых защищена/Общий объем резервных данных) × 100
Первичные данные	• Объем резервных данных, целостность которых защищена • Общий объем резервных данных
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность и реализация
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-19 – Показатель 19: Охват сертифицированной системой управления безопасностью (например, ISMS) (уровень системы/программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Охват системой управления
Цель	Конечная точка организации должна быть охвачена сертифицированной системой управления безопасностью (например, ISMS)
Показатель	Процентная доля систем конечных точек, охваченных системой управления информационной безопасностью
Формула	(Количество систем конечных точек, охваченных сертифицированной системой управления безопасностью (например, ISMS)/Общее количество систем конечных точек) × 100
Первичные данные	• Количество систем конечных точек, охваченных сертифицированной системой управления безопасностью (например, ISMS) • Общее количество систем конечных точек
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность и реализация
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-20 – Показатель 20: Развертывание сервера со средствами защиты (уровень системы/уровень программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Развертывание сервера со средствами защиты
Цель	Сетевые услуги организации должны обмениваться информацией путем использования защищенного туннеля для удаленного доступа
Показатель	Процентная доля сетевых услуг, использующих защищенный туннель, например TLS, SSL или защищенный командный процессор
Формула	(Количество сетевых услуг, использующих защищенный туннель/Общее количество сетевых услуг) × 100
Первичные данные	• Количество сетевых услуг, использующих безопасный канал • Общее количество сетевых услуг
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность и реализация
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	
ПРИМЕЧАНИЕ. – Существует много способов реализации сервера со средствами защиты (упоминаемого в названии показателя) для обеспечения защищенного тоннеля между конечными точками. Эти серверы включают серверы, которые защищены с помощью SSL/TLS или защищенного командного процессора.	

Таблица 8-21 – Показатель 21: Доля получаемого спама (программа; чем меньше, тем лучше)

Поле	Данные
Идентификатор показателя	Доля получаемого спама
Цель	Организация должна использовать фильтр спама, чтобы блокировать электронные сообщения, содержащие спам, не позволяя им доходить до сотрудников
Показатель	Процентная доля сотрудников, получивших за определенный период времени больше электронных сообщений, содержащих спам, чем это определено для данной организации
Формула	(Количество сотрудников, получивших определенное количество электронных сообщений, содержащих спам/Общее количество сотрудников) × 100
Первичные данные	• Количество сотрудников, получивших за определенный период времени больше электронных сообщений, содержащих спам, чем это определено для данной организации • Количество сотрудников
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность и реализация
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-22 – Показатель 22: Программа повышения осведомленности организации (чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Программа повышения осведомленности организации
Цель	Сотрудники должны принять участие в программе повышения осведомленности
Показатель	Процентная доля сотрудников, принявших участие в программе повышения осведомленности
Формула	(Количество сотрудников, принявших участие в программе повышения осведомленности/Общее количество сотрудников) × 100
Первичные данные	• Количество сотрудников, принявших участие в программе повышения осведомленности • Количество сотрудников
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Эффективность/действенность и реализация
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-23 – Показатель 23: Обучение мерам обеспечения безопасности (уровень программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Обучение мерам обеспечения безопасности
Цель	Работники организации должны пройти обучение мерам обеспечения безопасности, чтобы правильно реагировать на инциденты безопасности
Показатель	Процентное отношение сотрудников, прошедших обучение мерам обеспечения безопасности за период времени, определенный для данной организации
Формула	(Количество сотрудников, прошедших обучение мерам обеспечения безопасности/ Общее количество сотрудников) × 100
Первичные данные	• Количество сотрудников, прошедших обучение мерам обеспечения безопасности • Количество сотрудников
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Влияние/реализация
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-24 – Показатель 24: Роль и обязанность в области кибербезопасности (уровень программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Роль и обязанность в области кибербезопасности
Цель	Организация должна набрать и организовать работу сотрудников, занимающихся деятельностью, связанной с кибербезопасностью
Показатель	Процентная доля сотрудников, занимающихся деятельностью, связанной с кибербезопасностью
Формула	(Количество сотрудников, занимающихся вопросами кибербезопасности/ Общее количество сотрудников, занятых в ИТ) × 100
Первичные данные	• Количество сотрудников, занимающихся деятельностью, связанной с кибербезопасностью • Общее количество сотрудников, занятых в ИТ
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Влияние/реализация
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-25 – Показатель 25: Заражение вредоносным программным обеспечением (уровень программы и уровень системы; чем меньше, тем лучше)

Поле	Данные
Идентификатор показателя	Устройства в конечных точках, зараженные вредоносным программным обеспечением
Цель	Устройства в конечных точках сотрудников должны быть защищены от различного вредоносного программного обеспечения
Показатель	Процентная доля компьютеров сотрудников, зараженных вирусом или вредоносным программным обеспечением или подвергшихся атакам с использованием хакерских технологий
Формула	(Общее количество устройств в конечных точках, зараженных вредоносным программным обеспечением/Общее количество устройств в конечных точках) × 100
Первичные данные	• Количество устройств в конечных точках, зараженных вирусом или вредоносным программным обеспечением или подвергшихся атакам с использованием хакерских технологий • Общее количество устройств в конечных точках в организации
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Влияние и эффективность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-26 – Показатель 26: Утечка информации, позволяющей установить личность (уровень программы)

Поле	Данные
Идентификатор показателя	Утечка информации, позволяющей установить личность
Цель	Организация должна защитить информацию, позволяющую установить личность, от утечки за пределы организаций
Показатель	Процентная доля единиц информации, позволяющей установить личность, которые подверглись утечке за определенный период времени в результате зарегистрированных инцидентов с PII. ПРИМЕЧАНИЕ. – Разработчики этого показателя должны определить собственную единицу PII
Формула	(Количество единиц информации, позволяющей установить личность, которые подверглись утечке за определенный организацией период времени в результате зарегистрированных инцидентов с PII/Общее количество единиц информации, позволяющей установить личность) × 100
Первичные данные	• Количество единиц информации, позволяющей установить личность, которые подверглись утечке за определенный организацией период времени в результате зарегистрированных инцидентов с PII • Общее количество единиц информации, позволяющей установить личность
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Влияние
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-27 – Показатель 27: Бюджет на цели обеспечения безопасности как процентная доля от бюджета на ИКТ (уровень программы)

Поле	Данные
Идентификатор показателя	Процентная доля бюджета организации на кибербезопасность от бюджета на ИКТ
Цель	Организация должна обеспечить бюджет для кибербезопасности в пределах определенной плановой цифры
Показатель	Процентная доля бюджета организации на кибербезопасность от бюджета на ИКТ; предполагается, что бюджет на кибербезопасность будет включен в бюджет на ИТ
Формула	(Бюджет на кибербезопасность/Общий бюджет на ИКТ) × 100
Первичные данные	• Сумма бюджета на кибербезопасность • Сумма общего бюджета на ИКТ
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Влияние
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-28 – Показатель 28: Доля санкционированных устройств (чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Доля санкционированных устройств по отношению ко всем устройствам организации
Цель	Организация должна отслеживать/контролировать/предотвращать/корректировать доступ к сети, осуществляемый устройствами (компьютерами, сетевыми компонентами, принтерами, любыми устройствами с IP-адресами), на основе перечня ресурсов, устройствам которого разрешено подключение к сети
Показатель	Доля санкционированных устройств по отношению ко всем устройствам организации
Формула	(Количество санкционированных устройств/Количество устройств) × 100
Первичные данные	• Количество санкционированных устройств • Количество устройств
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Влияние
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица 8-29 – Показатель 29: Доля санкционированного программного обеспечения (чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Доля санкционированных программных средств по отношению ко всем программным средствам организации
Цель	Организация должна отслеживать/контролировать/предотвращать/корректировать установку и работу программного обеспечения на компьютерах на основе перечня утвержденных программных средств
Показатель	Доля санкционированных программных средств по отношению ко всем программным средствам организации
Формула	(Количество санкционированных программных средств/Общее количество программных средств) × 100
Первичные данные	• Количество санкционированных программных средств • Общее количество программных средств
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Влияние
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	Рекомендация МСЭ-Т X.1528, Перечень общеизвестных платформ, [b-ITU-T X.1528] и стандарт [ИСО/МЭК 19770-2], Информационные технологии. Управление программными средствами. Часть 2: Идентификационный маркер программного обеспечения, [b-ISO/IEC 19770-2]

Таблица 8-30 – Показатель 30: Безопасность прикладного программного обеспечения (чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Доля прикладного программного обеспечения организации, которое защищено от основных атак на программное обеспечение прикладного уровня (например, по первым 25 позициям перечня CWE), по отношению ко всем прикладным программным средствам организации
Цель	Организация должна обнаруживать и блокировать атаки на программное обеспечение прикладного уровня и осуществлять оповещение или направлять электронное сообщение административному персоналу предприятия в течение 24 часов с момента обнаружения и блокирования
Показатель	Доля прикладного программного обеспечения организации, которое защищено от основных атак на программное обеспечение прикладного уровня, по отношению ко всем прикладным программным средствам организации
Формула	(Количество прикладных программ организации, которые защищены от основных атак на программное обеспечение прикладного уровня/Количество всех прикладных программных средств) × 100
Первичные данные	• Количество прикладных программ организации, которые защищены от основных атак на программное обеспечение прикладного уровня • Количество всех прикладных программных средств
Частотность	• Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	• Влияние
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	Рекомендация МСЭ-Т X.1524, Перечень общеизвестных слабых мест, [b-ITU-T X.1524] и Рекомендация МСЭ-Т X.1544, Перечень и классификация общеизвестных схем атак, [b-ITU-T X.1544]

Дополнение I

Примеры показателей, характеризующих меры и метрики риска информационной безопасности

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

В настоящем дополнении приводится два примерных набора показателей, характеризующих меры и метрики риска информационной безопасности, которые могли бы использоваться для расчета показателя кибербезопасности.

В [b-NIST SP 800-55] приводятся потенциальные типы измерений риска на уровне системы и уровне программы, которые могут быть сгруппированы следующим образом.

- Меры риска уровня системы:
  - управление доступом;
  - проверка и подотчетность;
  - идентификация и аутентификация;
  - техническое обслуживание;
  - оценка риска.
- Меры риска уровня программы:
  - расходы на безопасность, управление уязвимостями;
  - информированность и обучение;
  - сертификация, аккредитация и оценка безопасности;
  - управление конфигурацией;
  - планирование действий в чрезвычайных ситуациях;
  - физическая среда.
- Меры риска уровня программы и уровня системы:
  - реагирование на инциденты;
  - защита носителей;
  - планирование;
  - личная безопасность;
  - создание систем и связи;
  - целостность системы и информации.

Кроме того, в [b-NRI] Всемирного экономического форума (ВЭФ) приведено несколько показателей, при этом в [b-WEF] используется сертификат уровня защищенных разъемов (SSL) или сертификат безопасности транспортного уровня (TLS), предоставляемый конкретным поставщиком.

Дополнение II

Классификация показателей по характеру

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

Для обеспечения более широкого принятия настоящей Рекомендации организациями было бы целесообразно определить минимальные наборы измерений, которые могут быть получены и использованы без особых затрат.

Так, например, можно было бы начать с легко внедряемого показателя 24 (роль и обязанность в области кибербезопасности), представленного в п. 8, поскольку его измерение предполагает только подсчет числа сотрудников. Некоторые другие показатели требуют дополнительного внедрения других инструментов и/или баз данных, чтобы сделать эти показатели поддающимися измерению. Например, показатель 1 (управление уязвимостями) требует наличия инструментов и соответствующих баз данных для управления уязвимостями. Следовательно, организации, желающие использовать этот показатель, должны оценить выгоду от вложения инвестиций для обеспечения доступности такой информации по отношению к соответствующим затратам. Точно так же показатель 2 требует, чтобы в организации уже была задействована функция управления средствами ИКТ. Другой класс показателей требует наличия в организации некоторых средств, чтобы сделать эти показатели поддающимися измерению. Например, показатель 4 (среднее время уменьшения уязвимостей) требует знания даты возникновения инцидента, что было бы трудно сделать в условиях отсутствия средств проверки и анализа.

В настоящем дополнении содержится описание классификации показателей по их характеру: показатели, легко поддающиеся измерению; показатели, поддающиеся измерению с использованием инструментов и/или баз данных, которые обычно имеются в организации; и показатели, поддающиеся измерению в случае принятия организацией решения о расширении возможности измерения.

Таблица II.1 – Классификация показателей по характеру

Характер показателей	Номер показателя	Идентификатор показателя
Показатели, легко поддающиеся измерению	Показатель 12: Обязательство в отношении безопасности	Обязательство в отношении безопасности, или кодекс поведения
	Показатель 16: Защита от противозаконных действий персонала	Проверка защиты от противозаконных действий персонала
	Показатель 24: Роль и обязанность в области кибербезопасности	Роль и обязанность в области кибербезопасности
	Показатель 27: Бюджет на цели обеспечения безопасности как процентная доля от бюджета на ИКТ	Процентная доля бюджета организации на обеспечение информационной безопасности от бюджета на ИКТ
Показатели, которые могут быть измерены с развертыванием инструментов и/или баз данных для измерения, которые обычно имеются в организации	Показатель 1: Управление уязвимостями	Процентная доля уменьшенных высоких уязвимостей
	Показатель 2: Ведение журнала проверки	Процентная доля устройств в конечных точках, для которых ведется журнал проверки
	Показатель 3: Реагирование на инциденты	Реагирование на инциденты
	Показатель 8: Охват оценки риска	Охват оценки риска
	Показатель 9: Охват программой обнаружения и устранения вредоносного программного обеспечения	Охват программой обнаружения и устранения вредоносного программного обеспечения

Таблица II.1 – Классификация показателей по характеру

Характер показателей	Номер показателя	Идентификатор показателя
	Показатель 21: Доля получаемого спама	Доля получаемого спама
	Показатель 22: Программа повышения осведомленности организации	Программа повышения осведомленности организации
	Показатель 23: Обучение мерам обеспечения безопасности	Обучение мерам обеспечения безопасности
	Показатель 28: Доля санкционированных устройств	Доля санкционированных устройств по отношению ко всем устройствам организации
	Показатель 29: Доля санкционированного программного обеспечения	Доля санкционированных программных средств по отношению ко всем программным средствам организации
	Показатель 30: Безопасность прикладного программного обеспечения	Доля прикладного программного обеспечения организации, которое защищено от основных атак на программное обеспечение прикладного уровня (например, по первым 25 позициям перечня CWE), по отношению ко всем программным средствам организации
Показатели, которые, вероятно, требуют дальнейшего развития возможностей измерения в рамках организации	Показатель 4: Среднее время ослабления уязвимостей	Среднее время ослабления уязвимостей
	Показатель 5: Развертывание программы корректировки безопасности	Программа корректировки безопасности
	Показатель 6: Среднее время корректировки	Среднее время корректировки
	Показатель 7: Среднее время выполнения изменения конфигурации	Среднее время выполнения изменения конфигурации
	Показатель 10: Охват планирования действий в чрезвычайных ситуациях	Проверка плана на случай непредвиденных обстоятельств
	Показатель 11: Оценка безопасности	Процентная доля информационных систем с утверждениями оценки безопасности
	Показатель 13: Управление удаленным доступом с использованием шлюза безопасности	Пункты защищенного удаленного доступа
	Показатель 14: Управление удаленным доступом с использованием функции безопасности для предотвращения проникновений или обнаружения проникновений	Пункты защищенного удаленного доступа
	Показатель 15: Управление беспроводным доступом	Пункты защищенного беспроводного доступа
	Показатель 17: Защита информации, позволяющей установить личность (PII)	Процентная доля защищенной критичной информации, позволяющей установить личность
	Показатель 18: Защита резервных данных	Норма контроля целостности резервных данных

Таблица II.1 – Классификация показателей по характеру

Характер показателей	Номер показателя	Идентификатор показателя
	Показатель 19: Охват сертифицированной системой управления безопасностью	Охват системой управления
	Показатель 20: Развертывание сервера со средствами защиты	Развертывание сервера со средствами защиты
	Показатель 25: Заражение вредоносным программным обеспечением	Устройства в конечных точках, зараженные вредоносным программным обеспечением
	Показатель 26: Утечка информации, позволяющей установить личность	Утечка информации, позволяющей установить личность

Дополнение III

Экспериментальные показатели

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

В настоящем дополнении приводится описание ряда экспериментальных показателей (см. таблицы III.1 – III.6), которые могут быть пригодны для использования организациями.

Таблица III.1 – Показатель III-1: Среднее время обнаружения инцидента (уровень системы и уровень программы; чем меньше, тем лучше)

Поле	Данные
Идентификатор показателя	Среднее время обнаружения инцидента
Цель	Организации следует обнаруживать инциденты как только они происходят и измерять среднее время обнаружения инцидента, чтобы подтвердить эффективность организации в обнаружении инцидентов безопасности. В целом чем быстрее организация может обнаружить какой-либо инцидент, тем меньше ущерб, который он может причинить
Индикатор	Среднее количество времени в часах, которое проходит между временем возникновения и временем обнаружения для заданного набора инцидентов
Формула	Сумма (Время обнаружения – Время возникновения инцидента)/Подсчитанное число (инциденты)
Первичные данные	Время обнаружения инцидента, для каждого инцидента. Общее количество инцидентов, о которых представлены отчеты
Частотность	Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица III.2 – Показатель III-2: Резервирование линий (система; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Процентная доля сетевых линий с резервированием
Цель	Организация должна создать резервную линию в основной сети, чтобы гарантировать готовность и непрерывность услуг организации
Показатель	Процентная доля сетевых линий с резервированием
Формула	(Количество резервных линий/Общее количество сетевых линий) × 100
Первичные данные	Количество резервных линий для маршрутизаторов, систем наименований доменов (DNS), протокола динамической конфигурации хост-компьютера (DHCP), брандмауэра или базы данных (DB). Количество линий без резервирования
Частотность	Еженедельно, ежемесячно, ежеквартально, ежегодно

Таблица III.2 – Показатель III-2: Резервирование линий (система; чем больше, тем лучше)

Поле	Данные
Тип	Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица III.3 – Показатель III-3: Заражение ботами (уровень системы; чем меньше, тем лучше)

Поле	Данные
Идентификатор показателя	Процентная доля устройств конечных пользователей, зараженных ботами
Цель	Организация должна уменьшить присутствие ботов в сети организации
Показатель	Процентная доля устройств конечных пользователей, зараженных известными ботами в организации. Предполагается, что организация использует систему обнаружения заражения ботами
Формула	(Общее количество устройств конечных пользователей, зараженных известными ботами/Общее количество устройств конечных пользователей) × 100
Первичные данные	Количество устройств конечных пользователей, зараженных ботами
Частотность	Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица III.4. Показатель III-4: Меры распределенного отказа в обслуживании (DDoS) (уровень системы; чем меньше, тем лучше)

Поле	Данные
Идентификатор показателя	Меры DDoS
Цель	Организация должна защитить свои информационные системы от DDoS (или атак распределенного отказа в обслуживании (DoS)) за период времени, определенный для данной организации
Показатель	Процентная доля систем организации, остающихся в состоянии неготовности на протяжении установленного периода времени в результате атак DDoS (DoS)

Таблица III.4. Показатель III-4: Меры распределенного отказа в обслуживании (DDoS) (уровень системы; чем меньше, тем лучше)

Поле	Данные
Формула	(Количество систем организации, остающихся в состоянии неготовности на протяжении установленного периода времени в результате атак DDoS за период времени, определенный для данной организации/Общее количество веб-сайтов, которые имеет организация) × 100
Первичные данные	Количество веб-сайтов, остающихся недоступными на протяжении установленного периода времени в результате атак DDoS в пределах периода времени, определенного для данной организации. Общее количество веб-сайтов
Частотность	Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица III.5 – Показатель III-5: Характеристика ведения журнала проверки (уровень системы и уровень программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Процентная доля инцидентов компьютерной безопасности, видимые признаки которых зафиксированы в журнале проверки
Цель	Организации следует оценивать эффективность журналов проверки
Показатель	Процентная доля инцидентов компьютерной безопасности, видимые признаки которых зафиксированы в журнале проверки
Формула	(Зарегистрированные инциденты, видимые признаки которых остались в журналах/Общее количество зарегистрированных инцидентов) × 100
Первичные данные	Количество зарегистрированных инцидентов, видимые признаки которых были обнаружены в журналах проверки (либо в централизованном журнале, либо в журналах, полученных от конечных точек). Общее количество зарегистрированных инцидентов
Частотность	Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Таблица III.6 – Показатель III-6: Характеристика смягчения последствий инцидента (уровень системы и уровень программы; чем больше, тем лучше)

Поле	Данные
Идентификатор показателя	Процентная доля инцидентов компьютерной безопасности, обнаруженных в сертифицированных и аккредитованных системах (конечные точки или группы конечных точек)
Цель	Организации следует оценивать эффективность процедур сертификации и аккредитации
Показатель	Процентная доля инцидентов компьютерной безопасности, обнаруженных в сертифицированных и аккредитованных системах
Формула	(Зарегистрированные инциденты, обнаруженные в сертифицированных и аккредитованных системах/Общее количество зарегистрированных инцидентов) × 100
Первичные данные	Количество зарегистрированных инцидентов, обнаруженных в сертифицированных и аккредитованных системах. Общее количество зарегистрированных инцидентов
Частотность	Еженедельно, ежемесячно, ежеквартально, ежегодно
Тип	Эффективность/действенность
Уровень требований	
Применимо к	Организациям (сообществу путем агрегирования)
Справочные документы по методам CYBEX	

Библиография

[b-ITU-T E.409] Рекомендация МСЭ-Т E.409 (2004 г.), *Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи*.

[b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.) | ISO/IEC 7498-2 (1989), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ*.

[b-ITU-T X.810] Рекомендация МСЭ-Т X.810 (1995 г.) | ISO/IEC 10181-1:1996, *Информационные технологии – Взаимосвязь открытых систем – Структура безопасности для открытых систем: обзор*.

[b-ITU-T X.1205] Рекомендация МСЭ-Т X.1205 (2008 г.), *Обзор кибербезопасности.*

[b-ITU-T X.1206] Рекомендация МСЭ-Т X.1206 (2008 г.), *Независимая от производителя структура автоматического сообщения связанной с безопасностью информации и распространения обновлений*.

[b-ITU-T X.1242] Рекомендация МСЭ-Т X.1242 (2009 г.), *Система фильтрации спама в службе коротких сообщений (SMS) на основе определяемых пользователем правил*.

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности*.

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

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

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

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

[b-ITU-T X.1528] Рекомендация МСЭ-Т X.1528 (2012 г.), *Перечень общеизвестных платформ*.

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

[b-ITU-T X-Sup.8] Рекомендации МСЭ-Т серии X − Добавление 8 (2010 г.), МСЭ-Т X.1205 − *Добавление, касающееся передовых методов противодействия угрозам бот-сетей*.

[b-ISO/IEC 19770-2] ISO/IEC 19770-2:2009, *Information technology – Software asset management – Part 2: Software identification tag*.

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[b-ISO/IEC 27003] ISO/IEC 27003:2010, *Information technology – Security techniques – Information security management system implementation guidance*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2009, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/IEC 27033-2] ISO/IEC 27033-2:2012, *Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security*.

[b-ISO/IEC 27033-4] ISO/IEC 27033-4: 2014, *Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways*.

[b-NIST SP 800-27] NIST SP 800-27 Revision A (2004), *Engineering Principles for IT Security (A Baseline for Achieving Security), Revision A*.

[b-NIST SP 800-30] NIST SP 800-30 Revision 1 (2012), *Guide for Conducting Risk Assessments*.

[b-NIST SP 800-53] NIST SP 800-53 Revision 4 (2013), *Security and Privacy Controls for Federal Information Systems and Organizations*.

[b-NIST SP 800-55] NIST SP 800-55 Revision 1 (2008), *Performance Measurement Guide for Information Security*.

[b-NIST FIPS 199] NIST FIPS PUB 199 (2004), *Standards for Security Categorization of Federal Information and Information Systems*.

[b-ENISA] ENISA (V6_2, 2011), *Measurement Frameworks and Metrics for Resilient Networks and Services: technical report*.

[b-NRI] World Economic Forum (2013), *Networked Readiness Index*.

[b-WEF] World Economic Forum (2013), *Secure Internet servers*. (Sources: The World Bank, World Development Indicators Online; national sources).

[b-CIS] Center for Internet Security (2010), *The CIS security metrics*.

[b-Nelson] Nelson, C. E. (2010), *Security metrics: An overview*, ISSA Journal, Vol. 8, No. 8.

[b-BSA] BSA (2013), *BSA Global Cloud Computing Scorecard*. http://cloudscorecard.bsa.org/2013/

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2014 г.