Н. Г. Милославская, А. И. Толстой

МЕЖДУНАРОДНЫЙ СТАНДАРТ ИСО/МЭК 27004: 2009 ОБ ОЦЕНКЕ ДЕЯТЕЛЬНОСТИ ПО УПРАВЛЕНИЮ ИБ В ОРГАНИЗАЦИИ

Введение

Международная организация по стандартизации ISO (ИСО) и Международная электротехническая комиссия IEC (МЭК) формируют специализированную систему всемирной стандартизации. На текущий момент мировое сообщество проделало существенную работу в направлении стандартизации систем управления информационной безопасностью (СУИБ) и отдельных процессов управления ИБ. Основоположником такой стандартизации стала серия стандартов ИСО 9000, предъявляющих требования к системам менеджмента качества, соблюдение которых позволяет контролировать качество выпускаемой продукции или предоставляемых услуг. При разработке стандартов на СУИБ многое было взято за основу именно из стандартов серии ИСО 9000, например основной подход — процессный подход и использование циклической модели «планирование — реализация — оценка — совершенствование» (PDCA) для непрерывного совершенствования как самой системы, так и отдельных ее процессов. Также с 1999 г. начала разрабатываться серия стандартов ИСО/МЭК 27000 «Информационные технологии. Методы обеспечения безопасности». На основе ИСО/МЭК 27001:2005, 27002:2005 и ИСО 9000 в 2009 г. был принят стандарт ИСО/МЭК 27004:2009 «Information technology. Security techniques. Information security management. Measurement» («Информационная технология. Методы и средства обеспечения безопасности. Менеджмент ИБ. Измерение»), посвященный оценке деятельности организации по управлению ее ИБ [1]. В статье приводится авторизированный перевод основных положений данного стандарта с целью их популяризации на русском языке.

1. Измерение, показатель и метрика безопасности

Широко распространен принцип управления, согласно которому деятельность не может быть управляема, если она не может быть измерена. Этот принцип распространяется и на область ИБ. Оценки уровня ИБ организации и функционирования СУИБ в настоящее время еще являются достаточно молодой областью исследований, в которой существует много нерешенных проблем. Для получения таких оценок используются в основном три понятия: измерение (англ. *measurement*), показатели (англ. *measures*) и метрики безопасности (англ. *security metrics*). Хотя все они часто применяются как взаимозаменяемые (особенно второе и третье), поскольку получаются при непосредственном сборе необработанной информации (англ. *raw data*) от функционирующих систем, для определения того, что понимается под каждым из этих терминов, предпринимаются разные действия (в основном заключающиеся в сборе и специальном анализе необработанной информации). Метрики безопасности обычно являются результатом применения метода измерения к одному или нескольким объектам измеряемой системы для получения количественного значения показателя [2]. Метрика — это показатель (или единица показателя), являющийся средством, способствующим принятию решений и улучшающим исполнение деятельности и ее учетность посредством сбора, анализа и составления отчетов по соответствующим данным, относящимся к исполнению этой деятельности. Показатель — это число или символ, присваиваемый объекту в процессе измерения с целью охарактеризовать его атрибут, или количественная оценка степени, в которой продукт или процесс владеет этим атрибутом [3, 4].

2. Основные положения стандарта ИСО/МЭК 27004:2009

Стандарт ИСО/МЭК 27004:2009 предназначен для помощи организациям в оценке результативности деятельности по управлению ИБ в рамках их СУИБ за счет предоставления

единого руководства по использованию механизмов получения оценки в результате измерений и введения показателей. На основе полученных показателей, их анализа и принятия соответствующих решений по устранению выявленных проблем организациям удастся повысить результативность функционирования их СУИБ. Эта информация крайне важна для обоснования всех решений, связанных с СУИБ, при внедрении СУИБ и принятии решений о необходимости внесения изменений в существующую СУИБ для ее дальнейшего совершенствования.

В стандарте содержится общее руководство по разработке и использованию показателей и их сбору для оценки результативности внедренной в организации СУИБ, а также по областям контроля — отдельным элементам управления ИБ (англ. *controls*), определенным в ИСО/МЭК 27001, включая политику осуществления контрольных мероприятий, управление рисками ИБ, задачи контроля, сами мероприятия, процессы и процедуры, а также поддержку процесса их пересмотра, помощи в определении необходимости изменения или усовершенствования процессов СУИБ и самих областей контроля для СУИБ.

Стандарт подробно описывает процесс сбора *базовых показателей*, использование операции агрегирования полученных измерений, математического вычисления *производных (от двух и более базовых) показателей* и применения аналитических методов и методов принятия решений для выявления «индикаторов» совершенствования СУИБ.

Отправной точкой для разработки показателей и процедур их сбора является правильное понимание организацией рисков ИБ, с которыми она сталкивается. Выбранные и используемые показатели должны относиться к непосредственному функционированию СУИБ и быть связаны с показателями основных бизнес-процессов организации. Сам процесс измерения показателей определяется как процесс получения информации о СУИБ и элементах управления ИБ с использованием выбора показателей, самих измерений и вычислений, аналитической модели и критерией принятия решений.

Организация должна определить цели проведения измерений показателей СУИБ, принимая во внимание следующие факторы: роль обеспечения ИБ в основной деятельности организации и возникающие при этом риски ИБ; применимые требования нормативно-правовых актов и договорных обязательств; структура организации; стоимость и ожидаемая выгода от использования результатов измерения эффективности СУИБ; критерии принятия организацией рисков ИБ; необходимость сравнения нескольких СУИБ внутри организации.

Для регулярного проведения измерений в организации должна быть разработана и принята соответствующая программа, позволяющая достичь целей оценки уровня ИБ, обеспечиваемого функционированием СУИБ, и по полученным результатам оценки принять решения по усовершенствованию процессов управления ИБ и самой СУИБ и внедрить их в соответствии с моделью PDCA (рис. 1). Такая программа включает описание показателей и процесса их измерения, проведение измерений, анализ данных и составление отчетных материалов по полученным результатам, а также оценку и совершенствование самой программы. Должны быть установлены процедуры сбора (через определенные интервалы с помощью одобренных метода измерения, формулы вычислений и аналитической модели), хранения (как и где) и проверки данных (на соответствие установленному перечню и возможным значениям), их анализа (по выбранными методиками анализа данных, на соответствие критериям отбора измерений и критериям оценки проведения измерений), а также составления отчетов по результатам проведенных измерений (с заданными периодичностью, форматами и методами). Процедуры измерений должны быть скоординированы с функционированием СУИБ.

Рис. 1. Входные и выходные данные процесса измерения показателей СУИБ

Структура программы оценки уровня ИБ разрабатывается с учетом размера и сложности СУИБ организации. Программа должна обеспечить получение повторяемых, объективных и действительно полезных результатов измерений, основываясь на модели оценки уровня ИБ (рис. 2). Эта модель представляет собой структуру, объединяющую информационную потребность измерения соответствующих объектов с их атрибутами. Объектами измерений могут быть запланированные или уже реализованные процессы, процедуры, проекты и ресурсы. Данная модель описывает, как установленные атрибуты могут быть оценены количественно и преобразованы в показатели, которые являются основой для принятия решений об усовершенствовании СУИБ.

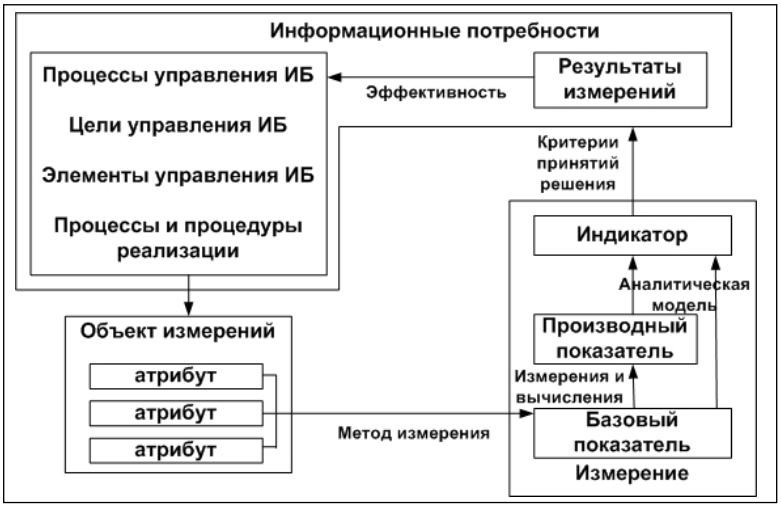

Рис. 2. Модель оценки уровня ИБ

3. Основные понятия стандарта ИСО/МЭК 27004:2009

Базовый показатель — самый простой из всех, которые могут быть получены. Он определяется на основе применения метода измерения к выбранным атрибутам объекта измерения. Объект измерения может иметь несколько атрибутов, но лишь некоторые из них могут быть ценны для определения базового показателя. Один атрибут может использоваться несколькими разными базовыми показателями. Примерами объектов измерений являются: результативность элементов управления ИБ, реализованных в СУИБ; статут конкретных информационных активов, защищенных данными элементами, например устройства, приложения и ИС, как это определено в ИСО/МЭК 27001:2005; результативность процессов управления ИБ, реализованных в СУИБ; поведение персонала, ответственного за реализацию СУИБ; действия подразделений организации, ответственных за ИБ; продукты и сервисы, включая сервисы третьих лиц, и т. п. Для каждого базового показателя должен быть определен метод его измерения, который используется для количественной оценки объекта измерения посредством преобразования атрибутов в численные значения, присваиваемые базовому показателю.

Производный показатель является объединением двух или более базовых показателей. Один базовый показатель может использоваться в качестве исходных данных для нескольких производных показателей.

Метод измерения — это логическая последовательность операций, применяемых для количественной оценки атрибута с учетом специальной шкалы (масштаба). Операция может включать, например, такие действия, как подсчет числа значимых происшествий или наблюдение за определенный отрезок времени. Метод измерения может использовать объекты измерений и их атрибуты, полученные из различных источников, например из результатов анализа и оценки рисков ИБ; из опросников и интервью с сотрудниками; отчетов внутренних и/или внешних аудитов ИБ; записей о событиях, например из журналов регистрации, статистических данных и результатов технического аудита ИБ; отчетов об инцидентах ИБ, особенно тех, которые приводят к ущербу; из результатов тестов, например тестов на проникновение, социальной инженерии и т. д. или записей от относящихся к ИБ организации процедур и программ, например результатов обучения сотрудников вопросам обеспечения ИБ. Метод измерения может быть субъективным или объективным. Субъективные методы основаны на количественной оценке с участием человека, в то время как объективные используют количественное выражение, основанное на таких действиях, как подсчет, выполняемый человеком или средствами автоматизации. Метод измерения количественно определяет атрибуты как значения в рамках соответствующей шкалы, состоящей из своих единиц измерения. Для каждого метода измерения должен быть установлен и документирован свой процесс верификации, который гарантирует то, что только верный метод был применен к атрибуту объекта измерений и таким образом получен базовый показатель. Метод измерения должен быть постоянным во времени, поэтому значения, присваиваемые базовым показателям в разное время, сопоставимы, а также сравнимы показатели, присваиваемые производному показателю и индикатору.

Формула вычисления — это алгоритм или формула, используемые для объединения базовых показателей для вывода производного показателя. Масштаб (шкала) и единица измерения производного показателя зависят от масштабов и единиц измерения базовых показателей, из которых он состоит, а также от того, как они объединяются. Формула вычисления может включать несколько методик, например усреднение базовых показателей, применение весовых коэффициентов или присвоение качественных значений базовым показателям. Для каждого производного показателя должна быть определена формула вычисления, которая применяется к двум или более значениям, присваиваемым базовым показателям. Одна формула вычисления должна соответствовать, по крайней мере, одной информационной потребности.

Индикатор является показателем, обеспечивающим оценку или расчет атрибутов, выведенных из аналитической модели с учетом определенных *информационных потребностей* (т. е. потребностей в информации). Индикаторы получаются путем применения аналитической модели к базовым и/или производным показателям и интерпретируются на основе критерия принятия решений. Шкала и метод измерения влияют на выбор аналитических методов, используемых для расчета показателей. Для каждого индикатора должен быть определен свой формат, который позволяет изобразить его визуально и описать словесно и соответствует потребностям заинтересованных сторон.

Для каждого индикатора должна быть определена *аналитическая модель*, которая используется для преобразования одного или нескольких значений, присваиваемых базовому и/или производному показателю, в значение, присваиваемое индикатору. Эта модель сочетает соответствующие показатели таким образом, что они порождают выходные данные, понятные заинтересованным сторонам. При определении аналитической модели должны быть установлены критерии принятия решений, применяемые к индикатору.

Должны быть установлены и документированы соответствующие каждому индикатору *критерии принятия решений*, выведенные из целей обеспечения ИБ и содержащие осуществимые указания для заинтересованных сторон. Эти указания должны соответствовать продвижению вперед и быть отправной точкой для начала действий по усовершенствованию в зависимости от значения индикатора. Критерии устанавливают цель, на основании которой измеряется успех ее достижения, и содержат указания по интерпретации индикатора по отношению к его близости к выполнению цели. Цели должны быть определены для каждого оцениваемого аспекта, касающегося результативности процессов СУИБ и контрольных мероприятий для нее, достижения поставленных целей и эффективности СУИБ. Установление критериев может быть облегчено, если доступны исторические данные, относящиеся к разработанному или выбранному показателю. Тенденции, наблюдаемые в прошлом, обеспечат понимание диапазонов результативности, которые существовали ранее, и ими можно руководствоваться при создании реалистичных критериев принятия решений. Критерии могут быть рассчитаны как статистические контрольные или доверительные интервалы или основаны на концептуальном понимании ожидаемого поведения, планах и эвристиках.

Результаты измерений получаются с учетом интерпретации применимым показателей на основе определенных критериев принятия решений. Они должны рассматриваться в контексте общих целей оценки СУИБ. Эти критерии используются для определения необходимости принятия мер или проведения дальнейших исследований, а также описывают уровень доверия к результатам измерений. Критерии могут применяться к ряду показателей, например для проведения анализа тенденций на основе индикаторов, полученных в разные моменты времени. Результаты измерений должны быть легки в понимании, своевременно передаваться заинтересованным сторонам, быть объективными, сопоставимыми и воспроизводимыми. Они должны быть полезны для усовершенствования деятельности по обеспечению ИБ и должны отвечать информационным потребностям. Процедуры их получения должны быть хорошо определены, легко и правильно выполнимы.

Для каждого базового и/или производного показателя должны быть определены и документированы *заинтересованные стороны*: клиент измерений — руководство или другая заинтересованная сторона, запрашивающая или требующая информацию об эффективности СУИБ, элементов или групп элементов управления ИБ; рецензент измерений — лицо или подразделение организации, которое утверждает применимость разработанной концепции измерений к оценке эффективности СУИБ, элементов или групп элементов управления ИБ; владелец информации — лицо или подразделение организации, владеющее информацией об объекте измерений и его атрибутах и ответственное за измерения; сборщик информации — лицо или подразделение организации, отвечающее за сбор, фиксацию и хранение данных; информатор — лицо или подразделение

организации, отвечающее за анализ данных и информирующее о результатах измерений. Результаты измерений должны быть доведены до сведения всех заинтересованных сторон.

Действия, необходимые для разработки показателей и методов их получения, должны быть определены и документированы, включая следующее: определение области измерения показателей, скоординированной с областью действия СУИБ; идентификация информационных потребностей; выбор объектов измерений и их атрибутов; разработка концепций и формул измерения; применение концепций и формул измерения; установление процессов и средств сбора и анализа данных; определение подходов к реализации измерений и их документированию. При этом должны учитываться все виды ресурсов — финансовых, людских и инфраструктурных.

4. Пример описания измерения оценок

В качестве примера приведем описание измерения оценки обучения персонала по вопросам СУИБ [1].

Наименование измерения	Персонал, прошедший обучение по вопросам СУИБ.
Порядковый номер	Проставляется организацией.
Цель измерения	Оценить контроль соответствия ПолИБ организации.
Задачи контроля/процесса	Обучение, информирование и компетентность.
Задачи контроля/процесса 1	Организация должна обеспечить обучение всего персонала, наделенного обязанностями, связанными с СУИБ, выполнению задач по поддержанию записей об обучении, тренингах, навыках, опыте и квалификации.
Задачи контроля/процесса 2	Опционально: дальнейший контроль посредством группирования в одном показателе, если это возможно (запланировано или реализовано).
Объект измерений	База данных сотрудников.
Атрибуты	Записи об обучении.
Базовый показатель	Число сотрудников, участвовавших в ежегодном обучении по вопросам СУИБ согласно плану обучения. Число сотрудников, которым еще требуется ежегодное обучение по вопросам ИБ.
Метод измерения	Подсчет логов/регистраций с фильтром по области/строке «Ежегодное обучение» со значением «Выполнено».
Тип метода измерения	Объективный.
Шкала	Числовая.
Тип шкалы	Отношение.
Единица измерения	Сотрудник.

Производный показатель	Процент сотрудников, участвовавших в ежегодном обучении по вопросам СУИБ.
Формула измерения	(Число сотрудников, участвовавших в обучении вопросам СУИБ/число сотрудников, которым еще требуется ежегодное обучение по вопросам ИБ) * 100
Индикатор	Использование цветового кодирования и цветных идентификаторов. Гистограмма, изображающая соблюдение в течение нескольких отчетных периодов по отношению к пороговым значениям (красный, желтый, зеленый, с цветными идентификаторами), определенная аналитической моделью. Число отчетных периодов, которые должны быть рассмотрены в рамках гистограммы, определяется организацией.
Аналитическая модель	«Красный» — 0–60 %; «желтый» — 60–90 %; «зеленый» — 90–100 %. Если за квартал не достигнут прогресс по крайней мере в 10 %, то «желтый» автоматически переводится в «красный».
Критерий принятия решений	«Красный» — требуется вмешательство, должен быть проведен анализ для выявления причин несоблюдения или низкой результативности; «желтый» — индикатор должен быть внимательно отслежен для его возможного постепенного перевода в «красный»; «зеленый» — не требуется никаких действий.
Результаты измерений	Определяется организацией
Интерпретация индикатора	Гистограмма с полосами разного цвета, основанная на критериях принятия решений.
Формат отчета	Краткое описание того, что означает каждый показатель, и возможных управленческих действий, которые должны быть приложены к гистограмме.
Заинтересованные стороны	
Клиент измерений	Администраторы, ответственные за СУИБ.
Рецензент измерений	Администраторы, ответственные за СУИБ.
Владелец информации	Администратор обучения — департамент персонала.
Сборщик информации	Руководство по обучению — департамент персонала
Информатор	Администраторы, ответственные за СУИБ.
Частота сбора данных	Ежемесячно, первый рабочий день месяца.
Частота анализа данных	Ежеквартально.
Частота отчетов по результатам измерений	Ежеквартально.
Пересмотр измерений	Ежегодно.
Период измерений	1 год.

Заключение

На основе несомненно полезного стандарта ИСО/МЭК 27004:2009 организация сможет разработать для себя документацию, которая будет свидетельствовать, что в ней ведется контроль за обеспечением ИБ и производится его всесторонняя оценка. Но, к сожалению, в стандарте не указывается, какие именно базовые и производные показатели и индикаторы могут на практике наилучшим образом повлиять на совершенствование ее СУИБ.

СПИСОК ЛИТЕРАТУРЫ:

1. ISO/IEC 27004:2009 «Information technology. Security techniques. Information security management. Measurement».
2. *Jansen W.* Directions in Security Metrics Research. NISTIR 7564. April 2009.
3. «Performance Measurement Guide for Information Security». NIST Special Publication 800-55-rev1. U.S. Government Printing Office. Washington, July 2008.
4. *Herrmann D. S.* Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI. Auerbach Publications, 2007. — 824 p.