ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27004— 2011

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Менеджмент информационной безопасности. Измерения

ISO/IEC 27004:2009
Information technology — Security techniques — Information security management — Measurement
(IDT)

Издание официальное

Москва
Стандартинформ
2012

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл»), Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России») и «Газпромбанк» (Открытое акционерное общество) (ГПБ (ОАО) на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 681-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27004:2009 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения» (ISO/IEC 27004:2009 «Information technology — Security techniques — Information security management — Measurement»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5, пункт 3.5.

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2012

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 1
4 Структура . . . 3
5 Общий обзор измерений, связанных с информационной безопасностью . . . 3
5.1 Цели измерений, связанных с информационной безопасностью . . . 3
5.2 Программа измерений . . . 5
5.3 Факторы успеха . . . 5
5.4 Модель измерений . . . 6
6 Обязанности руководства . . . 11
6.1 Общие положения . . . 11
6.2 Менеджмент ресурсов . . . 12
6.3 Обучение, осведомленность и компетентность, связанные с измерениями . . . 12
7 Разработка измерений и мер измерений . . . 12
7.1 Общие положения . . . 12
7.2 Определение области применения измерений . . . 12
7.3 Выявление информационной потребности . . . 13
7.4 Выбор объекта и атрибута . . . 13
7.5 Разработка конструктивных элементов измерений . . . 14
7.6 Конструктивные элементы измерений . . . 16
7.7 Сбор, анализ и распространение данных . . . 17
7.8 Реализация и документирование измерений . . . 17
8 Процесс измерений . . . 17
8.1 Общие положения . . . 17
8.2 Интеграция процедур . . . 18
8.3 Сбор, хранение и верификация данных . . . 18
9 Анализ данных и отчетность по результатам измерений . . . 18
9.1 Общие положения . . . 18
9.2 Анализ данных и изложение результатов измерений . . . 18
9.3 Распространение результатов измерений . . . 19
10 Оценивание и совершенствование программы измерений . . . 19
10.1 Общие положения . . . 19
10.2 Определение критериев оценивания программы измерений . . . 20
10.3 Мониторинг, проверка и оценивание программы измерений . . . 20
10.4 Реализация совершенствований . . . 21
Приложение А (справочное) Типовая форма конструктивных элементов измерений, связанных с информационной безопасностью . . . 22
Приложение В (справочное) Примеры конструктивных элементов измерений . . . 24
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 53
Библиография . . . 54

0 Введение

0.1 Общие положения

Настоящий стандарт содержит рекомендации по разработке и использованию измерений и мер измерения для проведения оценки эффективности реализованной системы менеджмента информационной безопасности (СМИБ), а также мер и средств контроля и управления или их групп по ИСО/МЭК 27001.

Процесс измерений затрагивает политику, менеджмент риска информационной безопасности, меры и средства контроля и управления и цели их применения, процессы и процедуры, а также поддерживает процесс проверки СМИБ, помогая определить, требуется ли изменять или совершенствовать какие-либо из процессов или мер и средств контроля и управления СМИБ. Следует помнить, что никакие измерения мер и средств контроля и управления не могут обеспечить полной безопасности.

Процесс измерений реализуется в виде программы измерений, связанных с информационной безопасностью (далее — программа измерений). Программа измерений предназначена для оказания помощи руководству организации в выявлении и оценивании несоответствующих требованиям и неэффективных процессов, мер, средств контроля и управления СМИБ, а также в определении приоритетов действий, направленных на усовершенствование или изменение этих процессов и (или) мер и средств контроля и управления. Программа измерений также может помочь организации в демонстрации соответствия СМИБ требованиям ИСО/МЭК 27001 и создании дополнительного основания для проведения руководством организации проверки процессов менеджмента риска информационной безопасности.

В данном стандарте предполагается, что отправной точкой для разработки мер измерения и измерений является доскональное понимание рисков информационной безопасности, с которыми сталкивается организация, и корректное выполнение (на основе ИСО/МЭК 27005) действий организации по оценке риска в соответствии с требованиями ИСО/МЭК 27001. Программа измерений поможет организации в предоставлении соответствующим заинтересованным сторонам достоверной информации, касающейся рисков информационной безопасности и состояния реализованной СМИБ для управления этими рисками.

Эффективно реализованная программа измерений позволит укрепить доверие заинтересованных сторон к результатам измерений, а также даст возможность заинтересованным сторонам применять меры измерений для непрерывного улучшения информационной безопасности и СМИБ.

Накопленные результаты измерений позволят следить за прогрессом в достижении целей информационной безопасности за некоторый период времени в интересах реализации процесса непрерывного совершенствования СМИБ организации.

0.2 Краткая справка для должностных лиц

ИСО/МЭК 27001 содержит требования к организации «проводить регулярные проверки эффективности СМИБ, принимая в расчет результаты измерений эффективности» и «измерять эффективность мер и средств контроля и управления с тем, чтобы подтвердить удовлетворение требований безопасности». ИСО/МЭК 27001 также содержит требования к организации «определять, каким образом проводить измерение эффективности выбранных мер и средств контроля и управления и их групп, и устанавливать, каким образом должны использоваться меры измерений для оценки эффективности мер и средств контроля и управления с тем, чтобы получать воспроизводимые и сопоставимые результаты».

Подход, принятый организацией для выполнения требований к измерениям, определенных в ИСО/МЭК 27001, будет варьироваться в зависимости от ряда существенных факторов, включающих в себя риски информационной безопасности, с которыми сталкивается организация, размер организации, имеющихся ресурсов и применимых правовых, нормативных и договорных требований. Тщательный выбор и обоснование метода, используемого для выполнения требований к измерениям, важны для того, чтобы для этой деятельности СМИБ не выделялись чрезмерные ресурсы в ущерб другой необходимой деятельности. В идеальном случае текущая деятельность, связанная с постоянными измерениями, должна быть интегрирована в обычную деятельность организации с привлечением минимальных дополнительных ресурсов.

Настоящий стандарт предлагает рекомендации, касающиеся следующей деятельности, являющейся основой для выполнения организацией требований к измерениям, установленных в ИСО/МЭК 27001:

a) разработка мер измерений (например, основные меры измерений, производные меры измерений и показатели);

b) разработка и выполнение программы измерений;

c) сбор и анализ данных;

d) обработка результатов измерений;

e) сообщение обработанных результатов измерений заинтересованным сторонам;

f) использование результатов измерений для принятия решений, относящихся к СМИБ;

g) использование результатов измерений для выявления потребностей в совершенствовании реализованной СМИБ, включая ее область действия, политики, цели, меры и средства контроля и управления, процессы и процедуры;

h) содействие постоянному совершенствованию программы измерений.

Одним из факторов, влияющих на способность организации проводить измерения, является ее размер. В целом, масштабы и сложность основной деятельности организации в сочетании с важностью информационной безопасности влияют на объем требуемых измерений как с точки зрения числа выбираемых мер измерений, так и с точки зрения частоты сбора и анализа данных. В то время как для малых и средних организаций менее детализированная программа измерений будет достаточной, крупные организации будут внедрять и использовать многочисленные программы измерений.

Единственная программа измерений может быть достаточной для малых организаций, тогда как для крупных организаций может возникнуть потребность в многочисленных программах измерений.

Рекомендации, содержащиеся в настоящем стандарте, позволят подготовить документацию, помогающую подтвердить, что эффективность мер и средств контроля и управления измеряется и оценивается.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Менеджмент информационной безопасности. Измерения

Information technology. Security techniques. Information security management. Measurement

Дата введения — 2012—01—01

1 Область применения

Настоящий стандарт устанавливает рекомендации по разработке и использованию измерений и мер измерений для оценки эффективности реализованной системы менеджмента информационной безопасности, мер и средств контроля и управления и их групп в соответствии с ИСО/МЭК 27001.

Настоящий стандарт предназначен для организаций всех видов.

Примечание — В настоящем стандарте используются глагольные формы для формулировки положений (например, «должен», «не должен»; «следует», «не следует»; «может быть», «нет необходимости»; «может», «не может»), которые определены в документе ИСО/МЭК Директивы, часть 2, 2004, приложение Н. См. также ИСО/МЭК 27000.2009, приложение А.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие ссылочные документальные источники. Для датированных стандартов применимо только указанное издание. Для недатированных стандартов применяют последнее издание стандарта, включая опубликованные изменения.

ИСО/МЭК 27000:2009 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология (ISO/IEC 27000:2009, Information technology — Security techniques — Information security management systems — Overview and vocabulary)

ИСО/МЭК 27001:2005 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements)

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000, а также следующие термины с соответствующими определениями:

3.1 **аналитическая модель измерений** (analytical model): Алгоритм или вычисление, объединяющие одну или более основных и /или производных мер измерения с соответствующими критериями принятия решений.

[ИСО/МЭК 15939:2007]

3.2 **атрибут** (attribute): Свойство или характеристика объекта, которые могут быть определены количественно или качественно вручную или автоматическими средствами.

[ИСО/МЭК 15939:2007]

Издание официальное

3.3 **основная мера [измерения]**[1] (base measure): Мера измерения, определенная через атрибут и метод его количественной оценки.

[ИСО/МЭК 15939:2007]

Примечание — Основная мера функционально независима от других мер.

3.4 **данные** (data): Совокупность значений, присвоенных для основных мер измерений, производных мер измерений и (или) показателей.

[ИСО/МЭК 15939:2007]

3.5 **критерии принятия решения** (decision criteria): Пороговые величины, целевые значения или образцы, используемые для определения необходимости действия или дальнейшего исследования или для описания уровня уверенности в данном результате.

[ИСО/МЭК 15939:2007]

3.6 **производная мера [измерения]**[1] (derived measure): Мера измерения, которая определяется как функция двух или более значений основных мер измерений.

[ИСО/МЭК 15939:2007]

3.7 **показатель** (indicator): Мера измерения, дающая качественную или количественную оценку определенных атрибутов, выведенную на основе аналитической модели, разработанной для определенных информационных потребностей.

3.8 **информационная потребность** (information need): Знание (сведения), необходимое(ые) для управления целями, задачами, рисками и проблемами.

[ИСО/МЭК 15939:2007]

3.9 **мера [измерения]**[2] (measure): Переменная, которой присваивается некоторое значение, полученное в результате измерения.

[ИСО/МЭК 15939:2007]

Примечание — Термин «меры измерений» (measures) используется для обозначения совокупности основных мер измерений, производных мер измерений и показателей.

Пример — Сравнение измеренной интенсивности отказов с расчетной интенсивностью отказов вместе с оценкой того, указывает ли различие интенсивностей на наличие проблемы или нет.

3.10 **измерение** (measurement): Процесс получения информации об эффективности СМИБ, а также мер и средств контроля и управления с использованием метода измерения, функции измерения, аналитической модели и критериев принятия решения.

3.11 **функция измерения** (measurement function): Алгоритм или вычисление, выполняемое для комбинирования двух или более основных мер измерения.

[ИСО/МЭК 15939:2007]

3.12 **метод измерения** (measurement method): Описанная в общем виде логическая последовательность операций, которая используется для количественного измерения атрибута относительно определенной шкалы.

[ИСО/МЭК 15939:2007]

Примечание — Вид метода измерения зависит от характера операций, используемых, для количественного измерения атрибута. Можно выделить следующие два вида метода измерения.

- субъективный: количественная оценка с использованием суждения человека;
- объективный: количественная оценка, основанная на числовых правилах.

3.13 **результаты измерения** (measurement results): Один или более показателей и их соответствующая интерпретация, предназначенные для информационной потребности.

3.14 **объект** (object): Элемент, который может быть охарактеризован посредством измерения его атрибутов.

3.15 **шкала** (scale): Упорядоченная совокупность значений, непрерывная или дискретная, или совокупность категорий, на которые отображается атрибут.

[ИСО/МЭК 15939:2007]

Примечание — Вид шкалы зависит от характера взаимосвязи между значениями на шкале. Обычно различают четыре вида шкал:

- номинальная: значением измерения является категория;

---

[1] См. 3.9.

[2] В контексте настоящего стандарта термин «measure» следует понимать как «мера измерения».

- порядковая (ранговая): значениями измерений являются ранги;

- интервальная: значения измерений отстоят одно от другого на равные расстояния, соответствующие одинаковым значениям атрибута,

- шкала отношений: значения измерений имеют равные расстояния, соответствующие одинаковым значениям атрибута, где нулевое значение соответствует отсутствию данного атрибута.

Представлены только примеры видов шкалы.

3.16 **единица измерения** (unit of measurement): Конкретная величина, определенная и принятая по соглашению, с которой сравниваются другие величины того же вида, чтобы выразить их значение относительно данной величины.

[ИСО/МЭК 15939:2007]

3.17 **валидация** (validation): Подтверждение посредством представления объективных свидетельств того, что требования в отношении конкретного использования или применения были выполнены.

3.18 **верификация** (verification): Подтверждение посредством предоставления объективных свидетельств того, что установленные требования были выполнены.

[ИСО 9000:2005]

Примечание — В качестве синонима может использоваться термин «проверка соответствия».

4 Структура

В настоящем стандарте представлены меры измерений и виды деятельности, связанные с измерениями, необходимыми для оценки эффективности реализации требований СМИБ к менеджменту необходимых и достаточных мер и средств контроля и управления безопасностью в соответствии с 4.2 ИСО/МЭК 27001:2005.

Настоящий стандарт имеет следующую структуру:

- общий обзор программы измерений и модели измерений, связанных с информационной безопасностью[1)] (см. раздел 5);

- обязанности руководства в отношении измерений, связанных с информационной безопасностью (см. раздел 6);

- конструктивные элементы и процессы измерений (такие, как планирование и разработка, реализация и функционирование, а также совершенствование измерений: распространение результатов измерений), подлежащие реализации в рамках программы измерений (см. разделы 7—10).

Кроме того, в приложении А представлена типовая форма конструктивных элементов измерения, составными частями которой являются элементы модели измерений (см. раздел 7). В приложении В представлены примеры конструктивных элементов измерения для конкретных мер и средств контроля и управления, а также процессов СМИБ с использованием типовой формы, представленной в приложении А.

Данные примеры предназначены для содействия организациям в проведении измерений, связанных с информационной безопасностью, а также документировании процессов измерений и их результатов.

5 Общий обзор измерений, связанных с информационной безопасностью

5.1 Цели измерений, связанных с информационной безопасностью

Цели измерений, связанных с информационной безопасностью, в контексте СМИБ включают в себя:

a) оценивание эффективности реализованных мер и средств контроля и управления или их групп [см. 4.2.2, перечисление d), рисунок 1];

b) оценивание эффективности реализованной СМИБ [см. 4.2.3, перечисление b), рисунок 1];

c) верификацию степени, до которой были удовлетворены установленные требования безопасности [см. 4.2.3, перечисление c), рисунок 1];

d) содействие повышению результативности информационной безопасности с точки зрения общих рисков основной деятельности организации;

[1)] Далее — модель измерений.

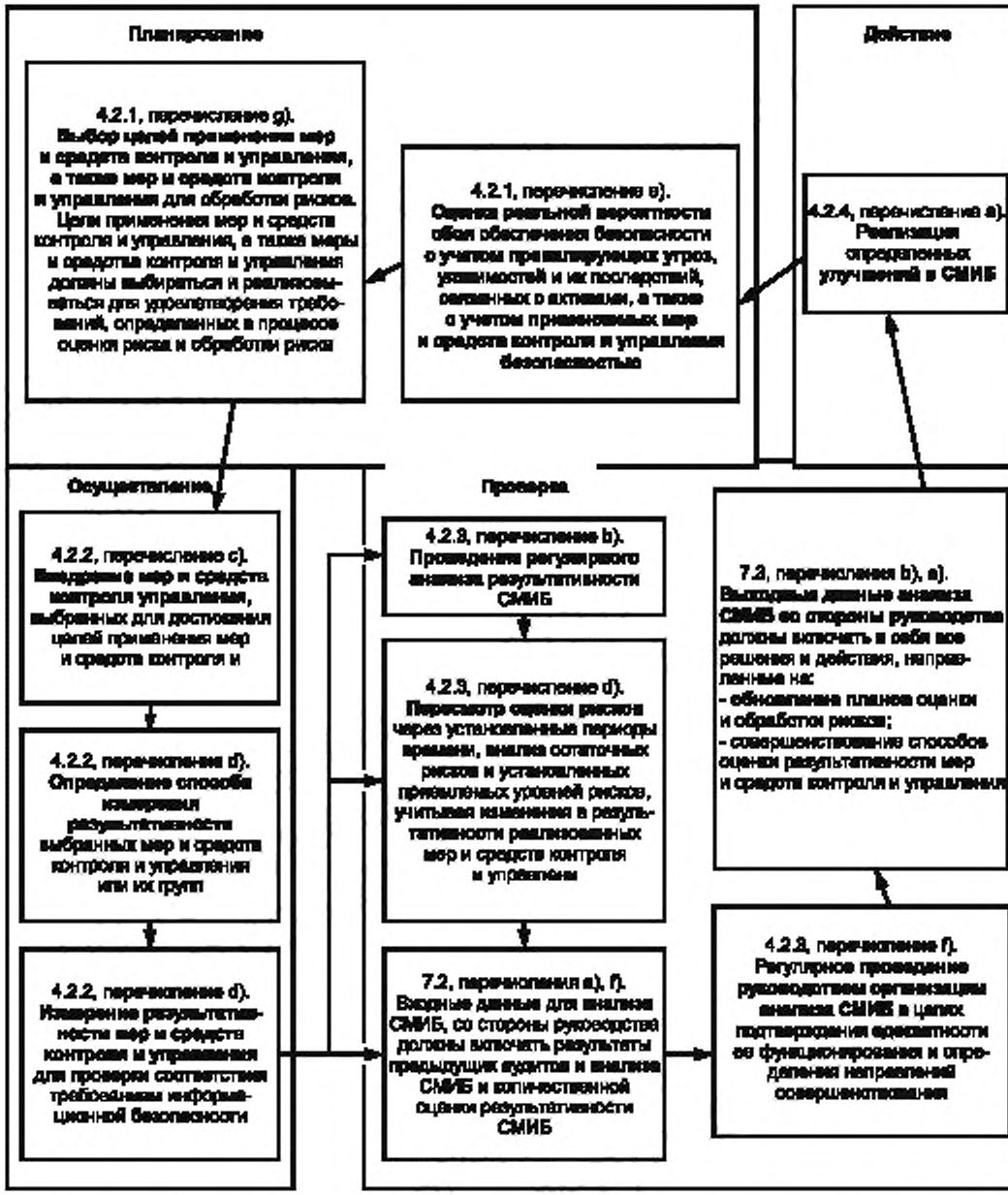


Рисунок 1 — Взаимосвязь видов деятельности, связанных с измерениями («входы-выходы»), в цикле «планирование — осуществление — проверка — действие»

e) предоставление сведений для проверки, проводимой руководством с целью содействия принятию решений, касающихся СМИБ, и обоснования необходимых улучшений в реализованной СМИБ.

Циклическая взаимосвязь видов деятельности, связанных с измерениями (их «входов-выходов»), по отношению к циклу «планирование — осуществление — проверка — действие» (PDCA — Plan—Do—Check—Act), определенному в ИСО/МЭК 27001, показана на рисунке 1. Цифры перед текстом в каждой фигуре обозначают номера подпунктов ИСО/МЭК 27001:2005.

Конкретной организации следует устанавливать цели измерений на основе ряда факторов, включающих в себя:

a) роль информационной безопасности в поддержке различных видов основной деятельности организации и рисков, с которыми она сталкивается;

b) соответствующие правовые, нормативные и договорные требования;

c) структуру организации;

d) расходы и выгоды от реализации мер, связанных с обеспечением информационной безопасности;

e) критерии принятия риска для организации;

f) необходимость сравнения нескольких СМИБ, имеющихся в одной и той же организации.

5.2 Программа измерений

Организации следует создать программу измерений и управлять ею для достижения установленных целей измерений и внедрения модели «планирование — осуществление — проверка — действие» в масштабах всей измерительной деятельности организации. Организации следует также разрабатывать и реализовывать конструктивные элементы измерений для получения воспроизводимых, объективных и пригодных результатов измерений, основанных на модели измерений (см. 5.4).

Программа измерений и разработанные конструктивные элементы измерений должны обеспечивать эффективное налаживание организацией объективных и повторяемых процессов измерения, а также предоставление результатов измерений соответствующим заинтересованным сторонам для определения потребностей в усовершенствовании реализованной СМИБ, включая область ее применения, политики, цели, меры и средства контроля и управления, а также процессы и процедуры.

Программа измерений должна включать в себя следующие процессы:

a) разработка измерений и мер измерений (см. раздел 7);

b) проведение измерений (см. раздел 8);

c) анализ данных и распространение результатов измерений (см. раздел 9);

d) оценивание и совершенствование программы измерений, связанных с информационной безопасностью (см. раздел 10).

Организационную и эксплуатационную структуру программы измерений следует определять, учитывая масштабы и сложность СМИБ, частью которой эта программа является. Во всех случаях роли и обязанности, касающиеся программы измерений, должны быть явным образом назначены компетентному персоналу (см. 7.5.8).

Меры, выбранные и реализованные в рамках программы измерений, следует непосредственно связывать с функционированием СМИБ, другими мерами измерений, а также процессами основной деятельности организации. Измерения могут быть интегрированы в обычные процессы функционирования или могут выполняться через постоянные интервалы времени, определенные руководством СМИБ.

5.3 Факторы успеха

Ниже перечислены некоторые факторы, способствующие успеху программы измерений в содействии непрерывному совершенствованию СМИБ:

a) поддержка со стороны руководства, подкрепляемая соответствующими ресурсами;

b) наличие процессов и процедур СМИБ;

c) воспроизводимый процесс, способный фиксировать и сообщать значимые данные для выведения важных тенденций за некий период времени;

d) меры безопасности, основанные на целях СМИБ, эффективность которых может быть оценена количественно;

e) легко получаемые данные, которые могут быть использованы для измерений;

f) оценивание эффективности программы измерений и реализация намеченных улучшений;

g) последовательный периодический сбор, анализ и четкое представление результатов измерений;

h) использование результатов измерений соответствующими заинтересованными сторонами для выявления потребностей в совершенствовании реализованной СМИБ, включая сферу ее применения, политики, цели, меры и средства контроля и управления, а также процессы и процедуры;

i) получение ответной реакции на результаты измерений от соответствующих заинтересованных сторон;

j) оценивание полезности результатов измерений и реализация намеченных усовершенствований.

После успешной реализации программа измерений может:

1) продемонстрировать выполнение организацией применимых правовых или нормативных требований и договорных обязательств;

2) способствовать выявлению ранее необнаруженных или неизвестных проблем информационной безопасности;

3) содействовать удовлетворению потребностей руководства в отчетности, когда определены меры измерений завершенных и текущих видов деятельности;

4) использоваться в качестве источника данных для процесса менеджмента риска информационной безопасности, внутренних аудитов СМИБ и проводимых руководством проверок.

5.4 Модель измерений

Примечание — Понятия «модель измерений» и «конструктивные элементы измерений», принятые в настоящем стандарте, основаны на понятиях, установленных в ИСО/МЭК 15939. Термин «информационный продукт» («information product»), используемый в ИСО/МЭК 15939, является синонимом термина «результаты измерений» («measurement results») настоящего стандарта, а термин «процесс измерений» («measurement process»), используемый в ИСО/МЭК 15939, является синонимом термина «программа измерений» («measurement programme») настоящего стандарта.

5.4.1 Общие положения

Модель измерений представляет собой структуру, связывающую информационную потребность с соответствующими объектами измерений и их атрибутами. В число объектов могут входить планируемые и реализованные процессы, процедуры, проекты и ресурсы.

Модель измерений описывает, как соответствующие атрибуты количественно оцениваются и преобразуются в показатели, служащие основой для принятия решений. Модель измерений показана на рисунке 2.



Рисунок 2 — Модель измерений

Примечание — Подробная информация об отдельных элементах модели измерений приведена в разделе 7.

В дальнейших подпунктах описываются отдельные элементы модели. Также в них приводятся примеры использования этих отдельных элементов.

Информационные потребности или цель измерений, используемые в примерах, содержащихся в таблицах 1—4, заключаются в оценке состояния осведомленности соответствующего персонала о соответствии политике безопасности организации (см. А.8.2 «Цель применения мер и средств контроля и управления» приложения А, а также А.8.2.1 и А.8.2.2 «Меры и средства контроля и управления» приложения А ИСО/МЭК 27001:2005).

5.4.2 Основная мера измерения и метод измерений

Основная мера измерения является самой простой мерой, которая может быть получена. Основная мера измерения является результатом применения метода измерений к выбранным атрибутам объекта измерений. У объекта измерения может быть множество атрибутов, но лишь некоторые из них могут предоставлять полезные значения, которые могут быть присвоены основной мере измерения. Один и тот же атрибут может использоваться для нескольких различных основных мер измерений.

Метод измерений — это логическая последовательность операций, используемых для количественной оценки атрибута по отношению к заданной шкале. Операция может включать в себя такие действия, как подсчет событий или наблюдение за ходом времени.

Метод измерений должен основываться на атрибутах объекта измерений. Примерами объектов измерений наряду с прочим могут служить:

- результативность мер и средств контроля и управления, реализованных в СМИБ;
- состояние информационных активов, защищенных мерами и средствами контроля и управления;
- результативность процессов, реализованных в СМИБ;
- поведение персонала, ответственного за реализацию СМИБ;
- деятельность подразделений организации, ответственных за информационную безопасность;
- степень удовлетворенности заинтересованных сторон.

Метод измерений может использовать объекты измерений и атрибуты из разнообразных источников, таких как:

- результаты анализа риска и оценки риска;
- анкеты и личные беседы;
- отчеты о внутренних и (или) внешних аудитах;
- документированную информацию о событиях, например, протоколы, статистические данные отчетов и журналы регистрации;
- сообщения об инцидентах, особенно о тех, вследствие которых был причинен ущерб;
- результаты тестирования, например, полученные в результате тестирования на проникновение, использования социальной инженерии, инструментальных средств обеспечения соответствия, а также инструментальных средств аудита безопасности;
- документированную информацию, полученную из процедур и программ организации, связанных с обеспечением информационной безопасности, например, результаты программ обучения, направленных на повышение осведомленности об информационной безопасности.

В таблицах 1—4 показано применение модели информационной безопасности для следующих мер и средств контроля и управления:

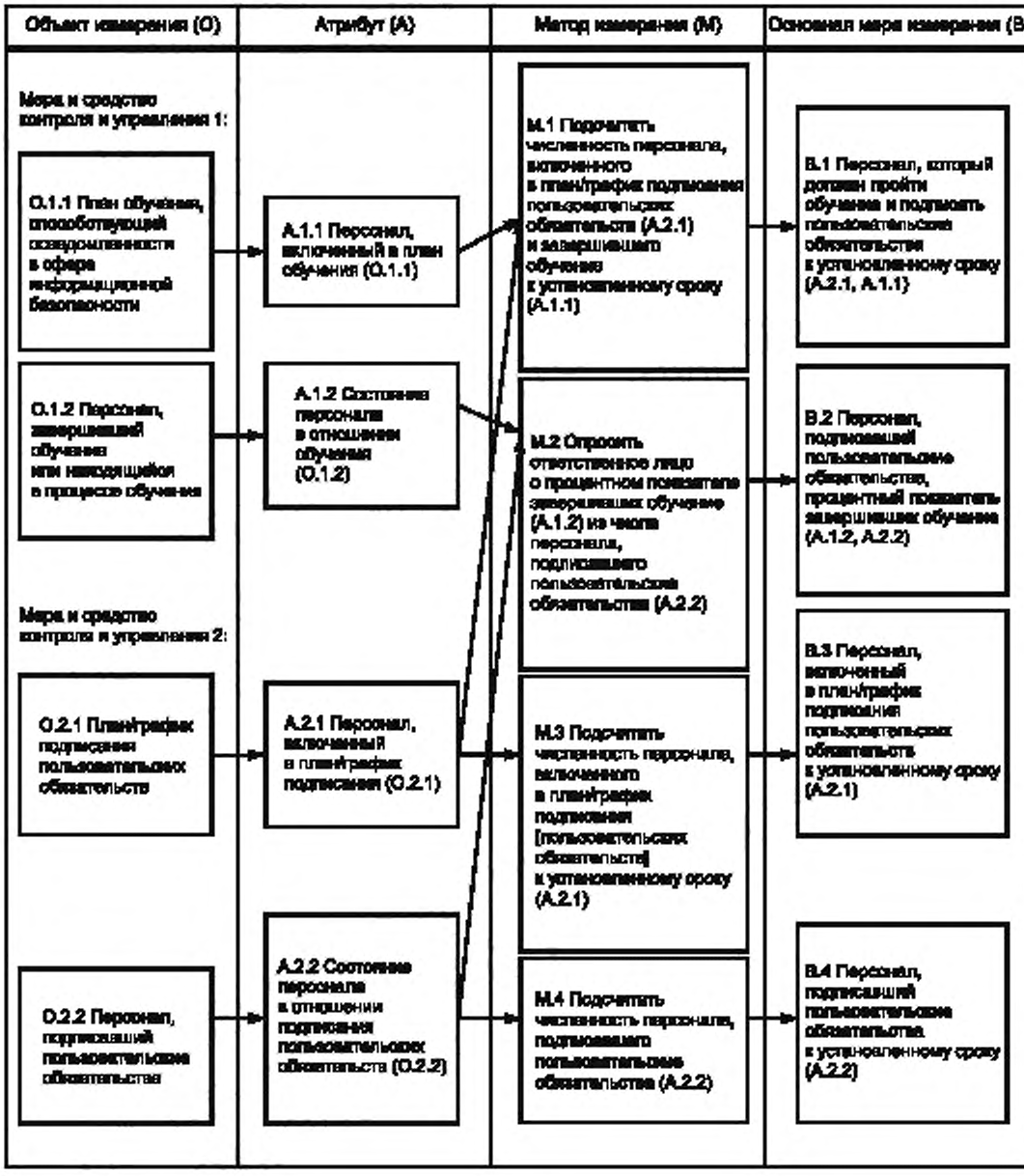
- «мера и средство контроля и управления 2» — ссылается на меру и средство контроля и управления по А.8.2.1 «Обязанности руководства», приложение А ИСО/МЭК 27001:2005 («Руководство организации должно требовать, чтобы сотрудники, подрядчики и пользователи сторонней организации были ознакомлены с правилами и процедурами обеспечения мер безопасности в соответствии с установленными требованиями»). «Мера и средство контроля и управления 2» реализуется следующим образом: «Весь персонал, имеющий отношение к СМИБ, должен быть ознакомлен с соответствующими обязательствами пользователей до получения доступа к информационной системе»;
- «мера и средство контроля и управления 1» — ссылается на меру и средство контроля и управления по А.8.2.2 «Осведомленность, обучение и переподготовка в области информационной безопасности», приложение А ИСО/МЭК 27001:2005 («Все сотрудники организации и, при необходимости, подрядчики и пользователи сторонних организаций должны проходить соответствующее обучение и переподготовку в целях регулярного получения информации о новых требованиях правил и процедур организации безопасности, необходимых для выполнения ими должностных функций»). «Мера и средство контроля и управления 1» реализуется следующим образом: «Весь персонал, имеющий отношение к СМИБ, до получения доступа к информационной системе должен пройти обучение, направленное на повышение осведомленности в сфере информационной безопасности».

Соответствующие конструктивные элементы измерений содержатся в В.1 (приложение В).

Примечание — Таблицы 1—4 состоят из столбцов (таблица 1 — из четырех столбцов, таблицы 2—4 — из трех), обозначенных буквенным идентификатором. Каждый блок, находящийся в пределах отдельных столбцов, обозначен числовым идентификатором. Комбинации из буквы и числового идентификатора используются в последующих блоках для ссылки на предыдущие блоки. Стрелками обозначены потоки данных между отдельными элементами модели измерений в рамках конкретного примера.

Пример взаимосвязей между объектом измерений, атрибутом, методом измерений и основной мерой измерения при измерении объектов, установленных для реализованных мер и средств контроля и управления, описанных выше, представлен в таблице 1.

Таблица 1 — Пример основной меры измерения и метода измерения



5.4.3 Производная мера измерения и функция измерения

Производная мера измерения является комбинацией двух или более основных мер измерений. Данная основная мера измерения может служить в качестве входных данных для нескольких производных мер измерения.

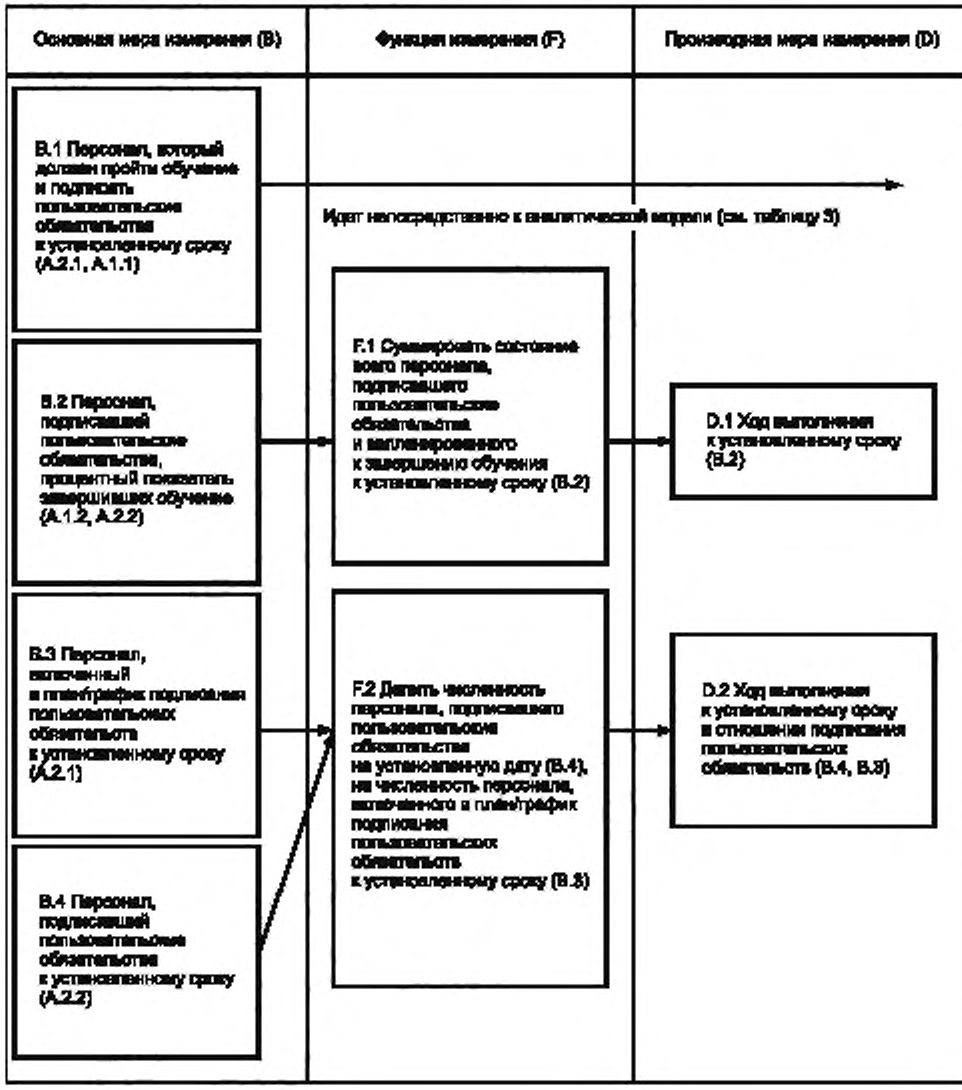
Функцией измерения является вычисление, используемое для комбинирования основных мер измерения, с целью получения производной меры измерения.

Шкала и единица измерения производной меры измерения зависят от шкал и единиц измерения основных мер измерения, на основе которых она получена, а также от того, как они комбинировались функцией измерения.

Функция измерения может использовать разнообразные методы, такие как вычисление среднего значения основных мер измерений, применение весовых коэффициентов к основным мерам измерений или присвоение основным мерам измерений качественных значений. Функция измерения может объединять основные меры измерений, используя разные значения шкалы, например, процентные соотношения и результаты качественных оценок.

Пример взаимосвязи других элементов при использовании модели измерений, т. е. основная мера измерения, функция измерения и производная мера измерения, приведен в таблице 2.

Таблица 2 — Пример производной меры измерения и метода измерения

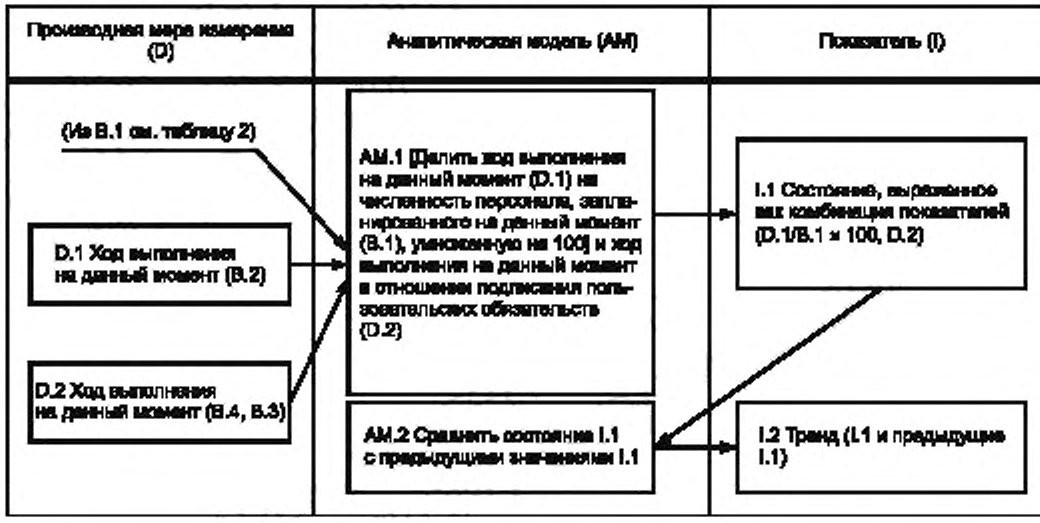


5.4.4 Показатели и аналитическая модель

Показатель является мерой, дающей качественную или количественную оценку определенных атрибутов, полученную на основе аналитической модели в отношении определенной информационной потребности. Показатели получают путем применения аналитической модели к основной и (или) производной мере измерений и комбинирования их с использованием критериев принятия решений. Шкала и метод измерения влияют на выбор аналитических методов, используемых для получения показателей.

Пример взаимосвязи между производными мерами измерений, аналитической моделью и показателями для применения модели измерений приведен в таблице 3.

Таблица 3 — Пример показателя и аналитической модели



Примечание — Если показатель представлен в графической форме, то должна быть предусмотрена возможность его использования лицами с ограничениями по зрению, а также в случае изготовления монохромных копий. С этой целью описание показателя должно охватывать использование цвета, штриховки и полутонов, шрифты и другие способы визуального представления.

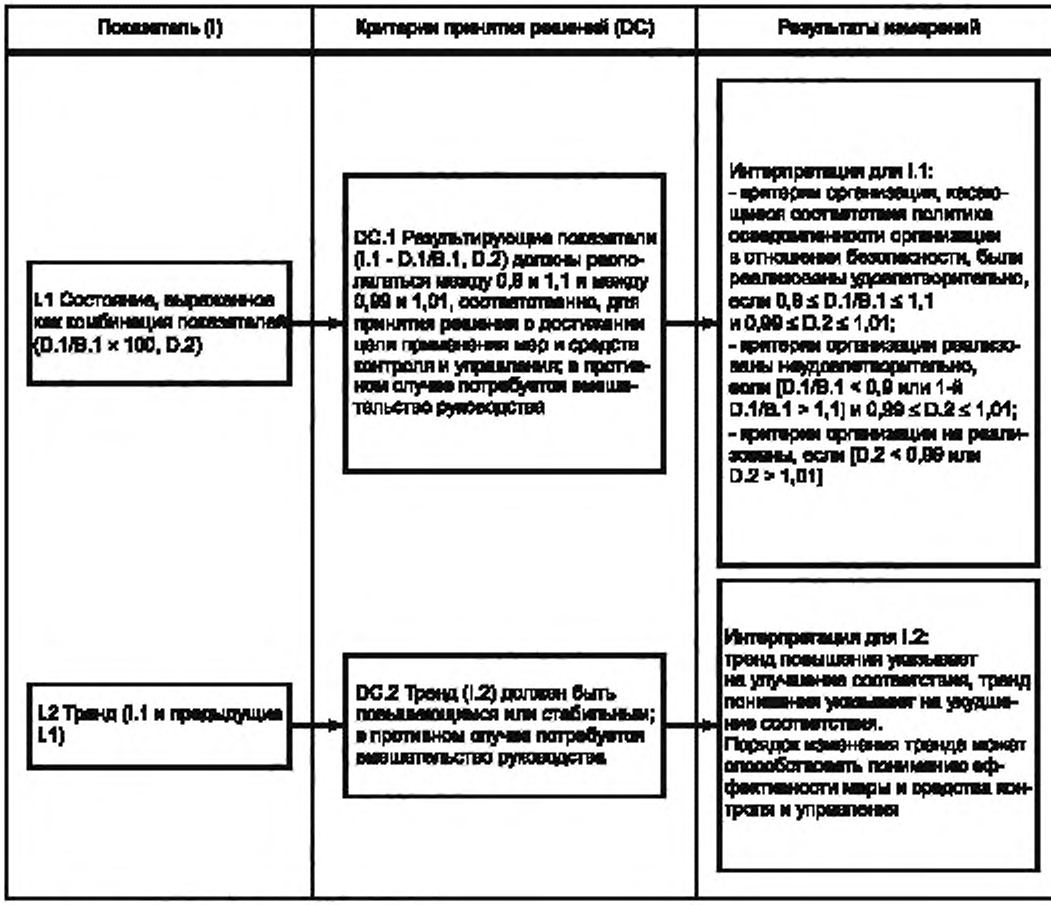
5.4.5 Результаты измерений и критерии принятия решений

Результаты измерений формируются путем интерпретации применимых показателей на основе определенных критериев принятия решений и должны рассматриваться в контексте общих целей измерения эффективности СМИБ. Критерии принятия решений используются для того, чтобы определить необходимость действия или дальнейшего исследования и характеризовать степень уверенности в результатах измерения. Критерии принятия решений могут применяться для ряда показателей, например, для проведения анализа трендов на основе показателей, полученных в разные моменты времени.

Целевые значения задают детализированные требования результативности, применимые к организации или ее частям, выведенные из целей информационной безопасности, таких как цели СМИБ и цели применения мер и средств контроля и управления, которые должны быть установлены и выполнены для достижения этих целей.

Пример взаимосвязей конечных элементов применения модели измерений (т. е. показателя, критериев принятия решений и результатов измерений) приведен в таблице 4.

Таблица 4 — Пример взаимосвязей конечных элементов применения модели измерений



6 Обязанности руководства

6.1 Общие положения

В обязанности руководства входит установление программы измерений с привлечением соответствующих заинтересованных сторон (см. 7.5.8) к видам деятельности по измерению с использованием результатов измерений в качестве входных данных для осуществляемой руководством проверки и с использованием результатов измерений в видах деятельности по улучшению в рамках СМИБ.

Для достижения этого руководству следует:

a) установить цели программы измерений;

b) установить политику программы измерений;

c) установить роли и обязанности в отношении программы измерений;

d) обеспечить адекватные ресурсы для проведения измерений, включая персонал, финансирование, инструментальные средства и инфраструктуру;

e) обеспечить достижение целей программы измерений;

f) обеспечить поддержание инструментальных средств и оборудования, используемых для сбора данных, в надлежащем состоянии;

g) установить цель измерения для каждого конструктивного элемента измерений;

h) обеспечить, чтобы измерения предоставляли заинтересованным сторонам достаточное количество информации, касающейся эффективности СМИБ и потребностей в усовершенствовании реали-

зованной СМИБ, включая сферу ее применения, политики, цели, меры и средства контроля и управления, а также процессы и процедуры;

i) обеспечить, чтобы измерения предоставляли достаточное количество информации заинтересованным сторонам относительно эффективности мер и средств контроля и управления и их групп, а также потребности в совершенствовании реализованных мер и средств контроля и управления.

Посредством соответствующего распределения связанных с измерениями ролей и обязанностей руководство должно обеспечить, чтобы на результаты измерений не оказывали влияния владельцы информации (см. 7.5.8). Этого можно достичь разделением обязанностей или, если это невозможно, использованием подробной документации, делающей возможными независимые проверки.

6.2 Менеджмент ресурсов

Руководству следует выделить и предоставить ресурсы для поддержки ключевых видов деятельности, связанных с такими измерениями, как сбор, анализ, хранение, регистрация и распространение данных. При распределении ресурсов следует установить:

a) лиц, ответственных за все аспекты программы измерений;

b) соответствующую финансовую поддержку;

c) соответствующую инфраструктурную поддержку, например, физическую инфраструктуру и инструментальные средства, используемые для осуществления процесса измерений.

Примечание — В 5.2.1 ИСО/МЭК 27001:2005 установлено требование обеспечения ресурсов для реализации и функционирования СМИБ.

6.3 Обучение, осведомленность и компетентность, связанные с измерениями

Руководство организации должно обеспечить:

a) обучение должным образом заинтересованных сторон (см. 7.5.8) для успешного выполнения их ролей и обязанностей и соответствующую квалификацию;

b) понимание заинтересованных сторон того, что в их обязанности входит внесение предложений по совершенствованию реализованной программы измерений.

7 Разработка измерений и мер измерений

7.1 Общие положения

Настоящий раздел представляет собой руководство по разработке измерений и мер измерений с целью оценки эффективности реализованной СМИБ и мер и средств контроля и управления и их групп, а также формирования характерных для организации совокупностей конструктивных элементов измерений. Виды деятельности, необходимые для разработки измерений и мер измерений, следует устанавливать и документировать, используя:

a) определение области применения измерений (см. 7.2);

b) выявление информационной потребности (см. 7.3);

c) выбор объекта измерений и его атрибутов (см. 7.4);

d) разработку конструктивных элементов измерений (см. 7.5);

e) применение конструктивных элементов измерений (см. 7.6);

f) установление процессов и инструментальных средств сбора и анализа данных (см. 7.7);

g) определение подхода к реализации измерений и документации (см. 7.8).

При установлении этих видов деятельности организации следует учитывать финансовые, кадровые и инфраструктурные (физические и связанные с инструментальными средствами) ресурсы.

7.2 Определение области применения измерений

В зависимости от возможностей и ресурсов организации первоначальная область деятельности организации в части измерений, связанных с информационной безопасностью, может быть ограничена такими элементами, как специфические меры и средства контроля и управления, информационные активы, защищенные специфическими мерами и средствами контроля и управления, специфические виды деятельности, направленные на обеспечение информационной безопасности, которым руководство присваивает наивысший приоритет. С течением времени область применения видов деятельности, связанных с измерениями, будет расширяться для того, чтобы рассматривать дополнительные компоненты реализованной СМИБ, а также меры и средства контроля и управления и их группы, учитывая приоритеты заинтересованных сторон.

Необходимо, чтобы были определены соответствующие заинтересованные стороны, которым следует принимать участие в определении области применения измерений. Соответствующие заинтересованные стороны могут быть внутренними или внешними по отношению к подразделениям организации, например, руководителями проектов, администраторами информационных систем или лицами, принимающими решения по обеспечению информационной безопасности. Специфические результаты измерений эффективности отдельных мер и средств контроля и управления и их групп следует определять и доводить до сведения соответствующих заинтересованных сторон.

Организация может рассмотреть ограничение числа результатов измерений, о которых должно быть сообщено лицам, принимающим решения в течение конкретного периода времени, с тем чтобы обеспечить им возможность влиять на совершенствование СМИБ, основанное на сообщенных результатах измерений. Чрезмерное число сообщенных результатов измерений будет влиять на возможность лица, принимающего решения, фокусировать усилия и назначать приоритеты для будущих видов деятельности по совершенствованию. Приоритеты рассмотрения результатов измерений следует основывать на важности соответствующих информационных потребностей и связанных с ними целей СМИБ.

Примечание — Область применения измерений относится к сфере применения СМИБ, установленной в соответствии с перечислением а) 4.2.1 ИСО/МЭК 27001:2005.

7.3 Выявление информационной потребности

Каждому конструктивному элементу измерений должна соответствовать, по меньшей мере, определенная информационная потребность. Пример информационной потребности, описываемой в начальной точке как цель измерения и завершающейся получением критериев, необходимых для принятия решения, представлен в приложении А.

Для выявления значительных информационных потребностей следует выполнить следующие действия:

a) исследовать СМИБ и ее процессы, такие как:

1) политика и цели СМИБ, цели применения мер и средств контроля и управления, а также меры и средства контроля и управления,

2) правовые, нормативные, договорные и организационные требования обеспечения информационной безопасности,

3) результаты процесса менеджмента риска информационной безопасности по ИСО/МЭК 27001;

b) назначать приоритеты выявленным информационным потребностям на основе критериев, таких как:

1) приоритеты обработки риска,

2) возможности и ресурсы организации,

3) интересы заинтересованных сторон,

4) политика информационной безопасности,

5) информация, необходимая для удовлетворения правовых, нормативных и договорных требований,

6) ценность информации, касающейся стоимости измерений;

c) выбирать подмножество информации, подлежащей рассмотрению в видах деятельности, связанных с измерениями, из списка приоритетов;

d) документировать информационные потребности и сообщать о них всем соответствующим заинтересованным сторонам.

Все необходимые меры измерения, применяемые для реализованной СМИБ, для мер и средств контроля и управления и их групп следует реализовывать в соответствии с установленными информационными потребностями.

7.4 Выбор объекта и атрибута

Объект измерений и его атрибуты следует определять в общем контексте и сфере применения СМИБ. Следует заметить, что объект измерений может иметь несколько применимых атрибутов.

Объект и его атрибуты, которые применяются при измерении, следует выбирать на основе приоритетов соответствующих информационных потребностей.

Значения, которые должны присваиваться соответствующей основной мере измерения, получают путем применения надлежащего метода измерения к выбранным атрибутам. Этот выбор должен также обеспечивать, чтобы:

- соответствующая основная мера измерения и надлежащий метод измерения могли быть определены;
- значимые результаты измерений могли быть выведены на основе полученных значений и разработанных мер измерений.

По характеристикам выбранных атрибутов определяют, какой вид метода измерений необходимо использовать для получения значений, которые придаются основным мерам измерений (например, качественные или количественные).

Выбранный объект и атрибуты следует документировать наряду с логическим обоснованием выбора.

Данные, характеризующие объект измерения и соответствующие атрибуты, следует использовать в качестве значений, которые присваиваются основным мерам измерений. Примерами объектов измерений могут служить:

- продукты и услуги;
- процессы;
- используемые активы, такие как оборудование, прикладные программы и информационные системы в соответствии с ИСО/МЭК 27001:2005 (см. А.7.1.1 «Инвентаризация активов» приложения А);
- основные подразделения организации;
- географическое местоположение;
- услуги сторонней организации.

Атрибуты следует анализировать для обеспечения того, чтобы:

a) были выбраны соответствующие атрибуты для измерений;

b) был определен сбор данных, обеспечивающий представление достаточного числа атрибутов, с тем чтобы сделать возможным эффективное измерение.

Следует выбирать только те атрибуты, которые являются подходящими для соответствующей основной меры измерения. Хотя при выборе атрибутов необходимо учитывать степень сложности получения атрибутов для измерения, измерение не должно проводиться только на легко получаемых данных или легко измеряемых атрибутах.

7.5 Разработка конструктивных элементов измерений

7.5.1 Краткий обзор

В подразделе 7.5 рассматривается разработка конструктивных элементов измерений (см. 7.5.2 «Выбор меры» — 7.5.8 «Заинтересованные стороны»).

7.5.2 Выбор меры измерения

Необходимо определить меры измерений, которые могли бы удовлетворять потребность в выбранной информации. Определяемые меры измерений должны быть сформулированы достаточно подробно для того, чтобы сделать возможным выбор мер измерений, подлежащих реализации. Вновь определяемые меры измерений могут включать в себя адаптацию существующей меры измерений.

Примечание — Определение основных мер измерений тесно связано с определением объектов измерения и их атрибутов.

Необходимо выбирать определяемые меры измерений, которые имели бы возможность удовлетворять потребность в выбранной информации. Следует также учитывать информацию контекста, необходимую для интерпретации или нормализации мер измерений.

Примечание — Для рассмотрения специфической информационной потребности могут быть выбраны многие различные комбинации мер измерений (т. е. основные меры измерений, производные меры измерений и показатели).

Выбранные меры измерений должны отражать приоритет информационных потребностей. Ниже перечислены критерии, которые могут быть использованы при выборе мер измерений:

- простота сбора данных;
- доступность кадровых ресурсов для сбора и управления данными,
- доступность соответствующих инструментальных средств,
- число потенциально подходящих показателей, поддерживаемых основной мерой измерения;
- простота интерпретации;
- число пользователей разработанных результатов измерений;
- доказательство адекватности меры измерения для цели или информационной потребности;
- расходы на сбор, управление и анализ данных.

7.5.3 Метод измерения

Для каждой отдельной основной меры измерения должен быть определен метод измерения. Метод измерения используется для того, чтобы количественно определять объект измерения путем придания атрибутам значения, которое придается основной мере измерения.

Метод измерения может быть субъективным или объективным. Субъективные методы основаны на количественной оценке с использованием суждения человека, тогда как объективные методы используют количественную оценку, основанную на математических правилах, таких как подсчет, который может быть реализован вручную или машинным способом.

Метод измерения количественно определяет атрибуты как значения посредством применения соответствующей шкалы. Для каждой шкалы используются свои единицы измерения. Только величины, выраженные в одних и тех же единицах измерения, являются напрямую сравнимыми.

Для каждого метода измерений следует устанавливать и документировать процесс верификации. Верификация должна обеспечивать уровень доверия значению, которое достигается применением метода измерений к атрибуту объекта измерения и назначается для основной меры измерения. Если необходимо установить достоверное значение, инструментальные средства, используемые для получения атрибутов, должны быть стандартизированы и проверены в установленные промежутки времени.

Следует принимать во внимание точность метода измерения и фиксировать связанное с ним отклонение или несоответствие.

Метод измерения должен оставаться единообразным в течение времени, с тем чтобы значения, приданные основной мере измерения, полученные в разное время, были сопоставимыми и были также сопоставимыми значения, приданные производной мере измерения и показателю.

7.5.4 Функция измерения

Для каждой отдельной производной меры измерения следует определять функцию измерения, которая применяется к двум или более значениям, приданным основным мерам измерения. Эта функция измерения используется для преобразования значений, приданных двум или более основным мерам измерения, в значение, которое должно быть придано производной мере измерения. В некоторых случаях основная мера измерения может обеспечивать входные данные непосредственно для аналитической модели в дополнение к производной мере измерения.

Функция измерения (например, вычисление) может включать в себя разнообразные приемы, такие как усреднение, присвоение качественных значений или применение весовых коэффициентов для значений, придаваемых основным мерам измерений, перед их объединением в значение, которое должно придаваться производной мере измерения. Функция измерения может комбинировать значения, придаваемые основным мерам измерений, используя различные шкалы, такие, например, как процентные отношения и результаты качественной оценки.

7.5.5 Аналитическая модель

Для каждого показателя следует определять аналитическую модель с целью преобразования одного или более значений, придаваемых основной и (или) производной мере измерения в значение, придаваемое показателю.

Аналитическая модель комбинирует соответствующие меры измерений таким способом, который дает результат, являющийся значимым для заинтересованных сторон.

При определении аналитической модели также следует рассматривать критерии принятия решений, применяемые к показателю.

Иногда аналитическая модель может быть настолько простой, что может заключаться в преобразовании единственного значения, приданного производной мере измерения, в значение, которое должно быть придано показателю.

7.5.6 Показатели

Значения, которые должны быть приданы показателям, определяются объединением значений, приданных производной мере измерения, и интерпретацией этих значений на основе критериев принятия решения. Для каждого показателя, о котором будет проинформирован заказчик измерения, следует определять формат представления показателя как часть форматов отчетности (см. 7.7).

Форматы представления показателя наглядно изображают меры измерений и дают словесное толкование показателям. Форматы представления показателя должны быть адаптированы так, чтобы удовлетворять потребности заказчика в информации.

7.5.7 Критерии принятия решений

Критерии принятия решений, соответствующие каждому показателю, следует определять и документировать на основе целей информационной безопасности для предоставления рекомендаций, обладающих исковой силой, для заинтересованных сторон. В этих рекомендациях следует рассматри-

вать ожидаемые результаты прогресса и пороговые значения первоначальных улучшающих действий, основанных на показателях.

Критерии принятия решений устанавливают цель, в соответствии с которой определяется успех (см. 5.3) и даются рекомендации по интерпретации показателя относительно приближения к цели.

Необходимо, чтобы цели были определены для каждого элемента, касающегося выполнения процессов СМИБ и мер и средств контроля и управления, выполнения задач и для эффективности СМИБ, подлежащей оцениванию.

Руководство организации может принять решение не устанавливать цели для показателей, пока не будут собраны начальные данные. После того как будут определены корректирующие действия, основанные на начальных данных, могут быть определены соответствующие критерии принятия решений и этапы реализации, реальные для конкретной СМИБ. Если в тот момент критерии принятия решений не могут быть установлены, руководство должно оценить, обеспечат ли объекты измерения и соответствующие меры измерений ожидаемое значение для организации.

Установление критериев принятия решений может быть облегчено, если данные за прошлый период, относящиеся к созданию или выбору мер измерений, являются доступными. Тенденции, наблюдаемые в прошлом, дадут представление о существовавших ранее диапазонах функционирования и рекомендации по созданию реалистичных критериев принятия решений. Критерии принятия решений могут быть вычислены или основаны на концептуальном понимании ожидаемого поведения. Критерии принятия решений могут быть получены из данных за прошлый период, планов и эвристик или вычислены как пределы статистического контроля или пределы статистической достоверности.

7.5.8 Заинтересованные стороны

Для каждой основной и (или) производной меры измерения должны быть определены и документированы соответствующие заинтересованные стороны. В число заинтересованных сторон могут входить:

a) заказчики измерений: руководство или другие заинтересованные стороны, которые запрашивают или требуют информацию об эффективности СМИБ, мер и средств контроля и управления и их групп;

b) контролер измерения: лицо или подразделение организации, которое подтверждает, что разработанные конструктивные элементы измерений являются соответствующими для оценки эффективности СМИБ, мер и средств контроля и управления и их групп;

c) владелец информации: лицо или подразделение организации, которое владеет информацией об объектах измерения и атрибутах и является ответственным за измерения;

d) сборщик информации: лицо или подразделение организации, отвечающее за сбор, фиксирование и хранение данных;

e) субъект, отвечающий за передачу информации: лицо или подразделение организации, отвечающее за проведение анализа данных и сообщение о результатах измерения.

7.6 Конструктивные элементы измерений

Конструктивные элементы измерения должны включать в себя, как минимум, следующую информацию:

a) назначение измерения;

b) цель применения меры и средства контроля и управления, которой следует достичь с помощью мер и средств контроля и управления, а также специфических мер и средств контроля и управления, их групп, и процесса СМИБ, подлежащего измерению;

c) объект измерения;

d) данные, подлежащие сбору и использованию;

e) процессы сбора и анализа данных;

f) процесс, касающийся отчетности о результатах измерений и включающий в себя форматы отчетности;

g) роли и обязанности соответствующих заинтересованных сторон;

h) цикл проверки измерения для того, чтобы удостовериться в его полезности относительно информационной потребности.

Типовая форма конструктивных элементов измерений, включающая в себя информацию по перечислениям a) — h), приведена в приложении А. Примеры конструктивных элементов измерений, применяемых для измерения процессов и мер и средств контроля и управления СМИБ, приведены в приложении В.

7.7 Сбор, анализ и распространение данных

Необходимо устанавливать процедуры сбора и анализа данных, а также процессы распространения результатов разработанных измерений. При необходимости также следует устанавливать поддерживающие инструментальные средства, оборудование и технологию измерений. Эти процедуры, инструментальные средства, оборудование и технология измерений предназначены для следующих видов деятельности:

a) сбор данных, включая хранение и верификацию данных (см. 8.3). Процедуры должны определять то, каким образом должны собираться данные при использовании метода измерений, функции измерений и аналитической модели, а также, как и где они будут храниться вместе с какой-либо контекстной информацией, необходимой для понимания и верификации данных. Верификация данных может осуществляться посредством проверки данных относительно контрольного перечня, который создается для подтверждения того, что объем недостающих данных является минимальным, а значение, которое должно придаваться каждой мере измерения, — действительным.

Примечание — Верификация значений, которые должны придаваться основным мерам измерения, тесно связана с верификацией метода измерений (см. 7.5.3);

b) анализ данных и распространение результатов разработанных измерений. Процедуры должны точно определять способы анализа данных (см. 9.2), частоту, формат и методы сообщения результатов измерений. Должен быть определен диапазон инструментальных средств, которые могут потребоваться для выполнения анализа данных.

Примеры форматов сообщения включают в себя:

- протоколы результатов для предоставления стратегической информации путем интеграции высокоуровневых показателей;
- исполнительные и операционные инструментальные панели, менее сосредоточенные на стратегических целях и более связанные с эффективностью определенных мер и средств контроля и управления, а также процессов;
- отчеты, от простых и статических по характеру, таких как список мер измерений за данный период времени, до более сложных отчетов с перекрестными ссылками, имеющих вложенные группировки, скользящие таблицы итогов, динамическое углубление в данные или связывание. Отчеты лучше всего использовать, если пользователю нужно просматривать исходные данные в удобном для чтения формате;
- показатели для представления динамических значений данных, включая предупреждения, дополнительные графические элементы и маркировку конечных точек.

7.8 Реализация и документирование измерений

Общий подход к измерениям следует отразить в плане реализации. В план реализации следует включать, как минимум, следующую информацию:

a) реализация программы измерений для организации;
b) спецификация измерений, включая:
   1) общие конструктивные элементы измерений организации,
   2) специфические конструктивные элементы измерений организации,
   3) определение диапазона и процедур для сбора и анализа данных;
c) календарный план выполнения видов деятельности, связанных с измерениями;
d) регистрационные данные, формируемые во время выполнения видов деятельности, связанных с измерениями, включая регистрационные данные о собранных сведениях и их анализ;
e) форматы сообщения о результатах измерений, подлежащих сообщению руководству / заинтересованным сторонам (см. раздел 7 «Анализ со стороны руководства» ИСО/МЭК 27001:2005).

8 Процесс измерений

8.1 Общие положения

Процесс измерений, связанных с информационной безопасностью, включает в себя виды деятельности, являющиеся важными для предоставления в результатах разработанных измерений точной информации, касающейся эффективности реализованной СМИБ, мер и средств контроля и управления и их групп, а также необходимости соответствующих действий по совершенствованию.

Эта стадия включает в себя:

a) интеграцию процедур измерений в общий процесс СМИБ;
b) сбор, хранение и верификацию данных.

8.2 Интеграция процедур

Программа измерений должна быть полностью интегрирована в СМИБ и использована ею. Процедуры измерения должны быть скоординированы с видами деятельности в рамках СМИБ, включая:

a) определение и документирование ролей, полномочий и обязанностей, относящихся к разработке, реализации и поддержке измерений, связанных с информационной безопасностью;

b) сбор данных, а при необходимости, изменение текущего процесса СМИБ для согласования видов деятельности по генерации и сбору данных;

c) сообщение об изменениях в деятельностях по сбору данных соответствующим заинтересованным сторонам;

d) поддержку компетентности сборщиков информации и понимания ими необходимых видов данных, инструментальных средств сбора данных и процедур сбора данных;

e) разработку политик и процедур, определяющих использование измерений в рамках организации, распространение связанной с измерениями информации, аудит и проверку программы измерений;

f) интеграцию анализа и сообщения данных в соответствующие процессы для обеспечения регулярного функционирования этих процессов;

g) мониторинг, анализ и оценивание результатов измерений;

h) создание процесса постепенной замены существующих мер измерений новыми в целях обеспечения их актуальности для организации;

i) установление процесса определения и поддержки сроков хранения архивных данных, необходимых для анализа трендов и динамки изменений.

8.3 Сбор, хранение и верификация данных

Деятельности, связанные со сбором, хранением и верификацией данных, включают в себя:

a) сбор необходимых данных через постоянные интервалы времени с использованием назначенного метода измерения;

b) документирование сбора данных, которое должно содержать:

1) дату, время и место сбора данных,
2) сборщика информации,
3) владельца информации,
4) любые вопросы, возникающие во время сбора данных, которые могут быть полезными,
5) информацию для верификации данных и валидации измерений;

c) верификацию собранных данных с использованием критериев выбора мер измерения и критериев валидации из конструктивных элементов измерений.

Собранные данные и любая необходимая контекстная информация должны быть сгруппированы и сохранены в форме, подходящей для анализа данных.

9 Анализ данных и отчетность по результатам измерений

9.1 Общие положения

Собранные данные следует анализировать для изложения результатов измерений, а информацию об изложенных результатах измерений необходимо распространять.

Эта деятельность включает в себя:

a) анализ данных и изложение результатов измерений;

b) сообщение о результатах измерений соответствующим заинтересованным сторонам.

9.2 Анализ данных и изложение результатов измерений

Собранные данные следует анализировать и интерпретировать с точки зрения критериев принятия решений. До проведения анализа данные могут быть агрегированы, трансформированы или перекодированы. Во время выполнения этой задачи обрабатываемые данные должны сформировать значения соответствующих показателей. Может быть применено несколько методов анализа. Глубина анализа должна определяться характером данных и информационной потребностью.

Примечание — Руководство по проведению статистического анализа можно найти в ИСО/ТО 10017 (Руководство по статистическим методам ИСО 9001).

Результаты анализа данных необходимо интерпретировать. Лицо, анализирующее результаты (субъект, ответственный за передачу информации), должно быть достаточно компетентным для того, чтобы делать некоторые первоначальные выводы на основе этих результатов. Однако, поскольку

субъект(ы), ответственный(е) за передачу информации, может(гут) быть не напрямую вовлечен(ы) в технические и управленческие процессы, то такие выводы должны проверять и другие заинтересованные стороны. Все интерпретации должны учитывать контекст мер измерения.

Анализ данных должен определять расхождения между ожидаемыми и фактическими результатами измерения реализованной СМИБ, мер и средств контроля и управления и их групп. Выявленные расхождения будут указывать на необходимость совершенствования реализованной СМИБ, включая сферу ее применения, политики, цели, меры и средства контроля и управления, а также процессы и процедуры.

Следует определять показатели, демонстрирующие несоответствие или недостаточную эффективность, которые могут быть классифицированы следующим образом:

a) несостоятельность плана по обработке риска в отношении реализации или достаточной реализации, эксплуатации и менеджмента мер и средств контроля и управления или процессов СМИБ (например, угрозы могут обходить меры и средства контроля и управления и процессы СМИБ);

b) несостоятельность оценки риска:

1) меры и средства контроля и управления или процессы СМИБ являются неэффективными, поскольку они недостаточны как для противостояния оцененным угрозам (например, по причине недооценки правдоподобия угроз), так и для противостояния новым угрозам,

2) меры и средства контроля и управления или процессы СМИБ не реализованы по причине незамеченных угроз.

Отчеты, которые используются для сообщения информации о результатах измерений соответствующим заинтересованным сторонам, следует подготавливать, используя соответствующие форматы сообщения (см. 7.7), в соответствии с планом реализации программы измерений.

Заключения по результатам анализа должны проверяться соответствующими заинтересованными сторонами для обеспечения надлежащей интерпретации данных. Результаты анализа данных следует документировать для сообщения заинтересованным сторонам.

9.3 Распространение результатов измерений

Лицу или подразделению организации, передающему информацию, следует решить, каким образом результаты измерений, связанных с информационной безопасностью, распространять, в т. ч. определять:

- о каких результатах измерений необходимо сообщать внутри организации и вне ее пределов;
- перечень мер измерений, соответствующих отдельным лицам и заинтересованным сторонам;
- результаты специфических измерений, которые должны быть предоставлены, и вид представления, приспособленные к потребностям каждой группы;
- способ получения обратной связи от заинтересованных сторон, который следует использовать для оценивания полезности результатов измерений и эффективности программы измерений.

Информацию о результатах измерений следует сообщать ряду внутренних заинтересованных сторон, помимо прочих включая в нее:

- заказчиков измерений (см. 7.5.8);
- владельцев информации (см. 7.5.8);
- персонал, в обязанности которого входит менеджмент риска информационной безопасности, особенно там, где выявлены ошибки в оценке риска;
- персонал, который несет ответственность за выявленные области, требующие совершенствования.

В некоторых случаях может потребоваться, чтобы организация распространяла отчеты с результатами измерений среди внешних сторон, включая регулирующие органы, акционеров, заказчиков измерений и поставщиков. Рекомендуется, чтобы отчеты с результатами измерений, подлежащие внешнему распространению, содержали только предназначенные для внешнего использования данные и утверждались руководством и соответствующими заинтересованными сторонами перед их выпуском.

10 Оценивание и совершенствование программы измерений

10.1 Общие положения

Организация через запланированные интервалы времени должна оценивать:

a) эффективность реализованной программы измерений для обеспечения уверенности в том, что она:

1) представляет результаты измерений эффективным образом,

2) выполняется, как было запланировано,

3) рассматривает изменения в реализованной СМИБ и (или) мерах и средствах контроля и управления,

4) рассматривает изменения в среде (например, требований, законов или технологии);

b) полезность изложенных результатов измерений для обеспечения уверенности в том, что они удовлетворяют соответствующие потребности в информации.

Руководство должно точно определить частоту повторений таких оцениваний, периодических проверок плана и устанавливать механизмы для возможности выполнения таких проверок (см. 7.2 ИСО/МЭК 27001:2005).

Соответствующими видами деятельности, являются:

1) определение критериев оценивания для программы измерений (см. 10.2);

2) мониторинг, проверка и оценивание измерений (см. 10.3);

3) реализация совершенствований (см. 10.4).

10.2 Определение критериев оценивания программы измерений

Организации следует определять критерии оценивания эффективности программы измерений, а также пригодности результатов измерений. Критерии следует определять в начале реализации программы измерений, принимая в расчет контекст технических целей и целей основной деятельности организации.

Если организации следует оценивать и совершенствовать программу измерений, то наиболее применимыми критериями являются:

- изменение целей основной деятельности организации;
- изменения законодательных или нормативных требований и договорных обязательств, связанных с информационной безопасностью;
- изменения требований организации, связанных с информационной безопасностью;
- изменения, связанные с рисками информационной безопасности организации;
- повышение доступности более детализированных или подходящих данных и/или методов сбора данных для целей проведения измерений;
- изменение объекта измерений и (или) его атрибутов.

Для оценивания изложенных результатов измерений могут применяться следующие критерии:

a) результаты измерений являются:

1) легкими для понимания,

2) распространенными своевременно,

3) объективными, сравнимыми и повторяемыми;

b) установленные процессы для изложения результатов измерений являются:

1) правильно определенными,

2) легко выполняемыми,

3) надлежащим образом соблюдаемыми;

c) результаты измерений являются полезными для повышения информационной безопасности;

d) результаты измерений адресованы соответствующим информационным потребностям.

10.3 Мониторинг, проверка и оценивание программы измерений

Организации следует осуществлять мониторинг, проверку и оценивание своей программы измерений по отношению к установленным критериям (см. 10.2).

Организации следует выявлять возможную потребность в совершенствовании программы измерений, включая:

a) обновление или отмену применяемых конструктивных элементов измерений, ставших неактуальными;

b) перераспределение ресурсов для поддержки программы измерений.

Организации следует также выявлять возможную потребность в совершенствовании реализованной СМИБ, включая область ее применения, политики, цели, меры и средства контроля и управления, а также процессы и процедуры, и документировать решения руководства, чтобы сделать возможным сравнение и анализ тенденций во время последующих проверок.

О результатах такого оценивания и выявленной возможной потребности в совершенствовании следует информировать соответствующие заинтересованные стороны для принятия решений, касающихся необходимых усовершенствований.

Организации следует обеспечивать, чтобы заинтересованные стороны стремились к установлению обратной связи по результатам такого оценивания и выявленной возможной потребности в усовершенствовании. Организации следует понимать, что обратная связь является одним из аспектов, способствующих эффективности программы измерений.

10.4 Реализация совершенствований

Организации следует обеспечить, чтобы важные заинтересованные стороны установили необходимые совершенствования программы измерений [см. 7.3, перечисление е) ИСО/МЭК 27001:2005]. Установленные совершенствования должны быть одобрены руководством. Одобренные планы совершенствования следует документировать и информировать о них соответствующие заинтересованные стороны.

Организации следует обеспечивать реализацию утвержденных усовершенствований программы измерений, как было запланировано.

Для выполнения этих усовершенствований организация может применять методы управления проектом.

Приложение А
(справочное)

Типовая форма конструктивных элементов измерений, связанных с информационной безопасностью

В настоящем приложении представлена типовая форма конструктивных элементов измерений, связанных с информационной безопасностью, которая включает в себя все компоненты, указанные в 5.4 и определенные в 7.5. Организации могут видоизменять эту типовую форму в соответствии с собственными требованиями.

Определение конструктивных элементов измерения	
Наименование конструктивного элемента измерения	Наименование измерения
Числовой идентификатор	Уникальный, специфический для организации числовой идентификатор
Назначение конструктивного элемента измерения	Описание причины для введения измерений
Цель меры и средства контроля и управления/цель процесса	Цель меры и средства контроля и управления/цель процесса при измерении (запланированная или реализованная)
Мера и средство контроля и управления (1)/процесс (1)	Мера и средство контроля и управления/процесс при измерении
Мера и средство контроля и управления (2)/процесс (2)	Дополнительно: если применимо, другие меры и средства контроля и управления/процессы в пределах группы, включенной в ту же самую меру измерения (запланированную или реализованную)
Объект измерения и атрибуты	
Объект измерения	Объект (сущность) характеризуется посредством измерения его атрибутов. Объект может включать в себя процессы, планы, проекты, ресурсы и системы или компоненты систем
Атрибут	Свойство или характеристика объекта измерения, которая может быть определена количественно или качественно вручную или автоматическими средствами
Спецификация основной меры измерения (для каждой основной меры измерения [1...*n*])	
Основная мера измерения	Основная мера измерения определяется с точки зрения атрибута и специфицированного метода измерения для его количественного определения (например, число обученного персонала, площадок, совокупные расходы на данный момент). Когда данные собраны, то для основной меры измерения устанавливается значение
Метод измерения	Логическая последовательность операций, используемых для измерения атрибута относительно определенной шкалы
Вид метода измерения	В зависимости от характера операций, используемых для количественной оценки атрибута, можно выделить следующие два вида метода: - субъективный: количественная оценка с использованием суждения человека; - объективный: количественная оценка, основанная на математических правилах, таких, например, как подсчет
Шкала	Упорядоченная совокупность значений или категорий, на которые отображается атрибут основной меры измерения
Вид шкалы	В зависимости от характера отношений между значениями на шкале обычно различают четыре вида шкалы: номинальную, порядковую, интервальную и шкалу отношений
Единица измерения	Особая величина, определенная и принятая по соглашению, с которой может сравниваться любая другая величина того же типа, для выражения показателя двух величин как некоего числа

Окончание

Спецификация производной меры измерения	
Производная мера измерения	Мера измерения, которая выведена как функция двух или более основных мер измерения
Функция измерения	Алгоритм или вычисление, выполняемое для объединения двух или более основных мер измерения. Шкала и единица производной меры измерения зависят от шкал и единиц основных мер измерения, из которых они состоят, а также от того, как они объединены функцией
Спецификация показателя	
Показатель	Мера измерения, дающая количественную оценку или обеспечивающая оценивание особых атрибутов, выведенных из аналитической модели относительно определенной информационной потребности. Показатели являются основой для анализа и принятия решений
Аналитическая модель	Алгоритм или вычисление, объединяющий(ее) одну или более основных и (или) производных мер измерения со связанными с ними критериями принятия решений. Он основан на понимании или предположении ожидаемого отношения между основной и (или) производной мерой измерения и (или) их поведения по прошествии времени. Аналитическая модель представляет количественные оценки или оценивания, соответствующие определенной информационной потребности
Спецификация критериев принятия решений	
Критерии принятия решений	Пороговые значения, задачи или образцы, используемые для определения потребности в действии или дальнейшем исследовании, или для описания уровня уверенности в данном результате. Критерии принятия решений помогают интерпретировать результаты измерений
Результаты измерений	
Интерпретация показателя	Описание того, каким образом следует интерпретировать примерный показатель (см. примерное представление в описании показателя)
Форматы отчетности	Следует определять и документировать форматы отчетности. В них описываются наблюдения, которые организация или владелец информации могут пожелать зафиксировать. Форматы отчетности наглядно отображают меры измерения и предоставляют словесное объяснение показателей. Форматы отчетности должны быть адаптированы к требованиям заказчика информации
Заинтересованные стороны	
Заказчик измерения	Руководство или другие заинтересованные стороны, запрашивающие или требующие информацию об эффективности СМИБ, мер и средств контроля и управления и их групп
Контролер измерения	Лицо или подразделение организации, которое подтверждает, что разработанные конструктивные элементы измерений являются соответствующими для оценки эффективности СМИБ, мер и средств контроля и управления и их групп
Владелец информации	Лицо или подразделение организации, которое владеет информацией об объектах измерения и атрибутах и отвечает за измерения
Сборщик информации	Лицо или подразделение организации, отвечающее за сбор, фиксирование и хранение данных
Субъект, ответственный за передачу информации	Лицо или подразделение организации, отвечающее за анализ данных и сообщение результатов измерений
Частота/период	
Частота сбора данных	Частота осуществления сбора данных
Частота анализа данных	Частота осуществления анализа данных
Частота сообщения о результатах измерений	Частота сообщения о результатах измерений (это допустимо осуществлять менее часто, чем сбор данных)
Пересмотр измерений	Дата пересмотра измерений (истечение срока или обновление действенности измерения)
Период измерений	Определяет измеряемый период

Приложение В
(справочное)

Примеры конструктивных элементов измерений

В приведенных ниже пунктах представлены примеры конструктивных элементов измерений, предназначенные для того, чтобы наглядно показать, каким образом применять настоящий стандарт, используя типовую форму, представленную в приложении А.

Содержание

В.1 Обучение, связанное со СМИБ
В.1.1 Персонал, получивший обучение, связанное со СМИБ
В.1.2 Обучение обеспечению информационной безопасности
В.1.3 Соответствие политике осведомленности в отношении информационной безопасности
В.2 Политики паролей
В.2.1 Качество паролей, генерируемых вручную
В.2.2 Качество паролей, генерируемых автоматизированным способом
В.3 Процесс проверки СМИБ
В.4 Непрерывное улучшение СМИБ
В.4.1 Эффективность менеджмента инцидентов информационной безопасности
В.4.2 Реализация корректирующих действий
В.5 Обязательства руководства
В.6 Защита от вредоносных программ
В.7 Меры и средства контроля и управления физическим доступом
В.8 Анализ журналов регистрации
В.9 Менеджмент периодического технического обслуживания
В.10 Вопросы безопасности в соглашениях со сторонними организациями

Взаимосвязанные процессы и меры и средства контроля и управления (пункт или номер меры и средства контроля и управления в приложении А ИСО/МЭК 27001)	**Примеры взаимосвязанных конструктивных элементов измерений** (ссылка в настоящем приложении)	**Названия примеров конструктивных элементов измерений**
Пункт 4.2.2, перечисление h)	В.4.1	Эффективность менеджмента инцидентов информационной безопасности
Пункт 5.2.2, перечисление d)	В.1.1	Персонал, получивший обучение, связанное со СМИБ
Пункт 8.2	В.4.2	Реализация корректирующих действий
Мера и средство контроля и управления по А.6.1.8 приложения А	В.3	Процесс проверки СМИБ
Мера и средство контроля и управления по А.6.1.1 и А.6.1.2 приложения А	В.5	Обязательства руководства
Мера и средство контроля и управления по А.6.2.3 приложения А	В.10	Вопросы безопасности в соглашениях со сторонними организациями
Мера и средство контроля и управления по А.8.2 и А.8.2.2 приложения А	В.1.2	Обучение обеспечению информационной безопасности
Мера и средство контроля и управления по А.9.1.2 приложения А	В.7	Меры и средства контроля и управления физическим доступом
Мера и средство контроля и управления по А.9.2.4 приложения А	В.9	Менеджмент периодического технического обслуживания
Мера и средство контроля и управления по А.10.4.1 приложения А	В.6	Защита от вредоносных программ
Мера и средство контроля и управления по А.10.10.1 и А.10.10.2 приложения А	В.8	Анализ журналов регистрации

Окончание

Взаимосвязанные процессы и меры и средства контроля и управления (пункт или номер меры и средства контроля и управления в приложении А ИСО/МЭК 27001)	**Примеры взаимосвязанных конструктивных элементов измерений** (ссылка в настоящем приложении)	**Названия примеров конструктивных элементов измерений**
Мера и средство контроля и управления по А.11.3.1 приложения А	В.2.1	Качество паролей, генерируемых вручную
Мера и средство контроля и управления по А.11.3.1 приложения А	В.2.2	Качество паролей, генерируемых автоматизированным способом

В.1 Обучение, связанное со СМИБ

В.1.1 Персонал, получивший обучение, связанное со СМИБ

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Персонал, получивший обучение, связанное со СМИБ
Числовой идентификатор	Характерный для организации
Назначение конструктивного элемента измерений	Для установления соответствия меры и средства контроля и управления политике информационной безопасности организации
Цель применения процесса / меры и средства контроля и управления	Пункт 5.2.2 [ИСО/МЭК 27001:2005]. Подготовка, осведомленность и квалификация персонала
Мера и средство контроля и управления (1) / процесс (1)	Пункт 5.2.2, перечисление d) [ИСО/МЭК 27001:2005]. Подготовка, осведомленность и квалификация персонала. Организация должна обеспечить необходимую квалификацию персонала, на который возложены обязанности выполнения задач в рамках СМИБ путем: d) ведение записей об образовании, подготовке, навыках, опыте и квалификации сотрудников
Мера и средство контроля и управления (2)/процесс (2)	Дополнительно: другие меры и средства контроля и управления в пределах группы, включенной в ту же меру измерения, если это применимо (запланированную или реализованную)
Объект измерения и атрибуты	
Объект измерения	База данных сотрудников
Атрибут	Записи, касающиеся обучения
Спецификация основной меры измерения (1)	
Основная мера измерения	Число сотрудников, получивших обучение, связанное со СМИБ, в соответствии с ежегодным планом обучения, связанного со СМИБ. Число сотрудников, которые должны получить обучение, связанное со СМИБ
Метод измерения	Подсчет в журналах регистрации/реестрах сведений о сфере обучения/последовательности обучения, связанной со СМИБ, с пометкой «Получено»
Вид метода измерения	Объективный
Шкала	Числовая
Вид шкалы	Шкала отношений
Единица измерения	Сотрудник
Спецификация производной меры измерения	
Производная мера измерения	Выраженная в процентах численность персонала, получившего обучение, связанное со СМИБ
Функция измерения	Разделить число сотрудников, получивших обучение, связанное со СМИБ, на число сотрудников, которые должны получить обучение, связанное со СМИБ, и умножить на 100

Окончание

Спецификация показателя	
Показатель	Использование цветовой кодировки с цветовыми идентификаторами. Гистограмма, изображающая соответствие за несколько отчетных периодов относительно пороговых значений (красный, желтый, зеленый), определяемых аналитической моделью. Число отчетных периодов, которые будут использоваться в диаграмме, должно определяться организацией
Аналитическая модель	0 %—60 % — красный цвет; 60 %—90 % — желтый, 90 %—100 % — зеленый. В отношении желтого цвета (если не достигается), по крайней мере, увеличение значения на 10 % за квартал, оценка автоматически становится красной
Спецификация критериев принятия решений	
Критерии принятия решения	Красный цвет — требуется вмешательство: должен быть проведен анализ для определения причин несоответствия и плохого функционирования. Желтый цвет — за показателем следует внимательно наблюдать на предмет возможного «сползания» к красному цвету. Зеленый цвет — никаких действий не требуется
Результаты измерений	
Интерпретация показателя	Характерная для организации
Форматы отчетности	Гистограмма с цветовой кодировкой столбцов на основе критериев принятия решения. К гистограмме должно прилагаться краткое изложение того, что означает мера измерения, и возможных действий руководства
Заинтересованные стороны	
Заказчик измерения	Руководители, отвечающие за СМИБ
Контролер измерения	Руководители, отвечающие за СМИБ
Владелец информации	Руководитель, отвечающий за обучение, — штат сотрудников
Сборщик информации	Менеджмент обучения — отдел кадров
Субъект, ответственный за передачу информации	Руководители, отвечающие за СМИБ
Частота/период	
Частота сбора данных	Ежемесячно/первый рабочий день месяца
Частота анализа данных	Ежеквартально
Частота сообщения результатов измерений	Ежеквартально
Пересмотр измерений	Ежегодно проводить проверку
Период измерений	Ежегодно

В.1.2 Обучение обеспечению информационной безопасности

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Обучение обеспечению информационной безопасности
Числовой идентификатор	Характерный для организации
Назначение конструктивного элемента измерения	Для оценивания соответствия необходимости ежегодного обучения, направленного на повышение осведомленности в отношении информационной безопасности

Продолжение

Цель применения меры и средства контроля и управления / процесса	А.8.2 приложения А [ИСО/МЭК 27001:2005] Работа по трудовому договору. Цель: обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации осведомлены об угрозах и проблемах информационной безопасности, их ответственности и обязательствах, ознакомлены с правилами и обучены процедурам для поддержания мер безопасности организации при выполнении ими своих служебных обязанностей и снижения риска человеческого фактора для информационной безопасности
Мера и средство контроля и управления (1)/процесс (1)	А.8.2.2 приложения А [ИСО/МЭК 27001:2005] Осведомленность, обучение и переподготовка в области информационной безопасности. Все сотрудники организации и, при необходимости, подрядчики и пользователи сторонних организаций должны проходить соответствующее обучение и переподготовку в целях регулярного получения информации о новых требованиях правил и процедур организации безопасности, необходимых для выполнения ими должностных функций
Объект измерения и атрибуты	
Объект измерения	База данных сотрудников
Атрибуты	Записи, касающиеся обучения
Спецификация основной меры измерения (1)	
Основная мера измерения	Число сотрудников, получивших ежегодное обучение, направленное на повышение осведомленности в отношении информационной безопасности. Число сотрудников, которые должны получить ежегодное обучение, направленное на повышение осведомленности в отношении информационной безопасности
Метод измерения	Подсчет в журналах регистрации/реестрах сведений, относящихся к ежегодному обучению сотрудников, направленному на повышение осведомленности в отношении информационной безопасности, с пометкой «получено»
Вид метода измерения	Объективный
Шкала	Числовая
Вид шкалы	Шкала отношений
Единица измерения	Сотрудник
Спецификация производной меры измерения	
Производная мера измерения	Выраженная в процентах численность персонала, получившего ежегодное обучение, направленное на обеспечение осведомленности в отношении информационной безопасности
Функция измерения	Разделить число сотрудников, получивших ежегодное обучение, направленное на повышение осведомленности в отношении информационной безопасности, на число сотрудников, которые должны получить ежегодное обучение, направленное на повышение осведомленности в отношении информационной безопасности, и умножить на 100
Спецификация показателя	
Показатель	Гистограмма, отображающая соответствие пороговым значениям (красный, желтый, зеленый, с цветовыми идентификаторами), за несколько отчетных периодов, определяемых аналитической моделью. Число отчетных периодов, которые будут использоваться в диаграмме, должно определяться организацией
Аналитическая модель	0 %—60 % — красный цвет; 60 %—90 % — желтый цвет; 90 %—100 % — зеленый цвет. В отношении желтого цвета, если не достигается увеличение значения, по крайней мере, на 10 % за квартал, то оценка автоматически становится красной
Спецификация критериев принятия решений	
Критерии принятия решений	Красный цвет — требуется вмешательство: должен быть проведен анализ для определения причин несоответствия и плохого функционирования. Желтый цвет — за показателем следует внимательно наблюдать на предмет возможного «сползания» к красному цвету. Зеленый цвет — никаких действий не требуется

Окончание

Результаты измерений	
Интерпретация показателя	Характерная для организации
Форматы отчетности	Гистограмма с цветовой кодировкой столбцов на основе критериев принятия решений. К этой столбчатой диаграмме должно прилагаться краткое изложение того, что означает мера измерения, и возможных действий руководства
Заинтересованные стороны	
Заказчик измерения	Руководители, отвечающие за СМИБ. Менеджмент безопасности. Менеджмент обучения
Контролер измерения	Руководитель, отвечающий за безопасность
Владелец информации	Лицо, ответственное за информационную безопасность, и руководитель, отвечающий за обучение
Сборщик информации	Менеджмент обучения — отдел кадров
Субъект, ответственный за передачу информации	Руководители, отвечающие за СМИБ
Частота/период	
Частота сбора данных	Ежемесячно, в первый рабочий день месяца
Частота анализа данных	Ежеквартально
Частота сообщения результатов измерений	Ежеквартально
Пересмотр измерений	Ежегодно проводить проверку
Период измерений	Ежегодно

B.1.3 Соответствие политике осведомленности в отношении информационной безопасности

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Соответствие политике осведомленности в отношении информационной безопасности
Числовой идентификатор	Характерный для организации
Назначение конструктивного элемента измерения	Для оценки состояния соответствия политике осведомленности в отношении информационной безопасности среди соответствующего персонала
Цель применения меры и средства контроля и управления/процесса	A.8.2 приложения A [ИСО/МЭК 27001:2005] Работа по трудовому договору. Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации осведомлены об угрозах и проблемах информационной безопасности, об их ответственности и обязательствах, ознакомлены с правилами и обучены процедурам для поддержки мер безопасности организации при выполнении ими своих служебных обязанностей и для снижения риска человеческого фактора для информационной безопасности
Мера и средство контроля и управления (1)/процесс (1)	A.8.2.2 приложения A [ИСО/МЭК 27001:2005] Все сотрудники организации и, при необходимости, подрядчики и пользователи сторонних организаций должны проходить соответствующее обучение и переподготовку в целях регулярного получения информации о новых требованиях правил и процедур организации безопасности, необходимых для выполнения ими должностных функций. Реализация: весь персонал, имеющий отношение к СМИБ, должен получать обучение, направленное на повышение осведомленности об информационной безопасности, до получения доступа к информационной системе. Обучение включает в себя ...
Мера и средство контроля и управления (2)/процесс (2)	A.8.2.1 приложения A [ИСО/МЭК 27001:2005] Руководство организации должно требовать, чтобы сотрудники, подрядчики и пользователи сторонней организации были ознакомлены с правилами и процедурами обеспечения мер безопасности в соответствии с установленными требованиями. Реализация: весь персонал, имеющий отношение к СМИБ, должен подписывать пользовательские обязательства до получения доступа к информационной системе

Продолжение

Объект измерения и атрибуты	
Объект измерения	1.1 План/график обучения, способствующий осведомленности в сфере информационной безопасности. 1.2 Персонал, завершивший обучение или находящийся в процессе обучения. 2.1 План/график подписания пользовательских обязательств. 2.2 Персонал, подписавший пользовательские обязательства
Атрибуты	1.1 Персонал, включенный в план обучения. 1.2 Состояние персонала в отношении обучения. 2.1 Персонал, включенный в план/график подписания. 2.2 Состояние персонала в отношении подписания пользовательских обязательств
Спецификация основной меры измерения	
Основная мера измерения	1.1 Численность персонала, который должен пройти обучение и подписать пользовательские обязательства к установленному сроку. 1.2 Численность персонала, подписавшего пользовательские обязательства. 2.1 Численность персонала, включенного в план/график подписания пользовательских обязательств к установленному сроку. 2.2 Численность персонала, подписавшего пользовательские обязательства к установленному сроку
Метод измерения	1.1 Подсчет численности персонала, включенного в план/график подписания пользовательских обязательств и завершившего обучение к установленному сроку. 1.2 Опрос ответственного лица о процентном показателе завершивших обучение из числа персонала, подписавшего пользовательские обязательства. 2.1 Подсчет численности персонала, включенного в план/график подписания пользовательских обязательств к установленному сроку. 2.2 Подсчет численности персонала, подписавшего пользовательские обязательства
Вид метода измерения	1.1 Объективный. 1.2 Субъективный. 2.1 Объективный. 2.2 Объективный
Шкала	1.1 Целые числа от нуля до бесконечности. 1.2 Целые числа от нуля до ста. 2.1 Целые числа от нуля до бесконечности. 2.2 Целые числа от нуля до бесконечности
Вид шкалы	1.1 Порядковая. 1.2 Шкала отношений. 2.1 Порядковая. 2.2 Порядковая
Единица измерения	1.1 Персонал. 1.2 Значение в процентах. 2.1 Персонал. 2.2 Персонал
Спецификация производной меры измерения	
Производная мера измерения	1 Ход выполнения на данный момент. 2 Ход выполнения подписания пользовательских обязательств к установленному сроку
Функция измерения	1 Суммировать состояние всего персонала, подписавшего пользовательские обязательства и запланированного к завершению обучения к установленному сроку. 2 Разделить значение [численность персонала, подписавшего пользовательские обязательства на данный момент] на значение [численность персонала, включенного в план/график подписания пользовательских обязательств к установленному сроку]
Спецификация показателя	
Показатель	a) состояние, выраженное как комбинация показателей; b) тренд

Продолжение

Аналитическая модель	a) разделить [достигнутый к установленному сроку прогресс] на [численность персонала, запланированного к установленному сроку, умноженную на 100] и достигнутый к установленному сроку прогресс в отношении подписания пользовательских обязательств; b) сравнить состояние с предыдущими значениями
Спецификация критериев принятия решений	
Критерии принятия решений	a) итоговые показатели должны располагаться между 0,9 и 1,1 и между 0,99 и 1,01 для принятия решения о достижении цели применения мер и средств контроля и управления соответственно; вмешательство руководства не требуется, b) тренд должен быть восходящим или стабильным
Результаты измерений	
Интерпретация показателя	Интерпретация показателя по перечислению a) должна быть следующей: - критерии организации на соответствие политике осведомленности о безопасности организации были реализованы удовлетворительно, если 0,9 ≤ первый показатель ≤ 1,1 и 0,99 ≤ второй показатель ≤ 1,01 (набраны прямым шрифтом); - критерии организации были реализованы неудовлетворительно, если первый показатель < 0,9 или первый показатель > 1,1 и 0,99 ≤ второй показатель ≤ 1,01 (набраны курсивом); - критерии организации не были реализованы, если второй показатель < 0,99 или второй показатель > 1,01 (набраны полужирным шрифтом). Интерпретация показателя по перечислению b) должна быть следующей: - тренд повышения указывает на улучшенное соответствие, тренд понижения указывает на ухудшенное соответствие. Порядок изменения тренда может способствовать пониманию эффективности реализации мер и средств контроля и управления. Резкие изменения в любом направлении показывают, что реализация мер и средств контроля и управления требует пристального изучения, чтобы установить их причину. Негативные тренды могут потребовать вмешательства руководства. Позитивные тренды следует изучать с целью определения возможных наилучших практик
Форматы отчетности	Прямой шрифт — критерии были реализованы удовлетворительно. Курсив — критерии были реализованы неудовлетворительно. Полужирный шрифт — критерии не были реализованы
Заинтересованные стороны	
Заказчик измерения	Руководители, отвечающие за СМИБ. Менеджмент безопасности. Менеджмент обучения
Контролер измерения	Руководитель, отвечающий за безопасность
Владелец информации	Лицо, ответственное за информационную безопасность, и руководитель, отвечающий за обучение
Сборщик информации	Менеджмент обучения — отдел кадров
Субъект, ответственный за передачу информации	Руководители, отвечающие за СМИБ
Частота/период	
Частота сбора данных	Ежемесячно, в первый рабочий день месяца
Частота проведения исследования данных	Ежеквартально
Частота сообщения результатов измерений	Ежеквартально
Пересмотр измерений	Ежегодно проводить проверку
Период измерений	Ежегодно

В.2 Политики паролей

В.2.1 Качество паролей, генерируемых вручную

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Качество паролей
Числовой идентификатор	Характерный для организации
Назначение конструктивного элемента измерения	Для оценки качества паролей, применяемых пользователями для доступа к системам ИТ организации
Цель применения меры и средства контроля и управления/процесса	Предотвратить выбор пользователями небезопасных паролей
Мера и средство контроля и управления (1)/процесс (1)	А.11.3.1 приложения А [ИСО/МЭК 27001:2005] Пользователи должны соблюдать правила безопасности при выборе и использовании паролей. Реализация: все пользователи должны выбирать надежные пароли для каждой системы: 1) длиной более восьми знаков; 2) не основанные на том, что можно легко отгадать или получить при использовании информации, связанной с личностью, например, на именах, телефонных номерах, датах рождения и т. п.; 3) не состоящие из слов, включенных в словари; 4) не содержащих следующих один за другим идентичных, полностью цифровых или полностью буквенных знаков. Все имена учетных записей и пароли пользователей для систем ИТ организации должны контролироваться системой обеспечения/контроля деятельности сотрудников
Объект измерения и атрибуты	
Объект измерения	База данных паролей пользователей
Атрибуты	Личные пароли
Спецификация основной меры измерения	
Основная мера измерения	1 Число зарегистрированных паролей. 2 Число паролей, которые соответствуют политике качества паролей организации для каждого пользователя
Метод измерения	1 Подсчет числа паролей в базе данных паролей пользователей. 2 Опрос каждого пользователя о том, какое число паролей соответствует политике паролей организации
Вид метода измерения	1 Объективный. 2 Субъективный
Шкала	1 Целые числа от нуля до бесконечности. 2 Целые числа от нуля до бесконечности
Вид шкалы	1 Порядковая. 2 Порядковая
Единица измерения	1 Пароли. 2 Пароли
Спецификация производной меры измерения	
Производная мера измерения	Общее число паролей, соответствующее политике качества паролей организации
Функция измерения	Сумма числа паролей каждого пользователя, соответствующая политике качества паролей организации
Спецификация показателя	
Показатель	a) Показатель для паролей, которые реализованы в соответствии с политикой качества паролей организации; b) тренд состояния соответствия относительно политики качества паролей

Окончание

Аналитическая модель	a) Разделить общее число паролей, соответствующих политике качества паролей организации, на число зарегистрированных паролей; b) сравнить показатель с предыдущим показателем
Спецификация критериев принятия решений	
Критерии принятия решений	Цель применения мер и средств контроля и управления достигнута, и никакое действие не требуется, если результирующий показатель превышает 0,9. Если результирующий показатель находится в диапазоне между 0,8 и 0,9, то цель применения мер и средств контроля и управления не достигнута, однако позитивный тренд указывает на улучшение. Если результирующий показатель меньше 0,8, то следует принять немедленные меры
Результаты измерений	
Интерпретация показателя	Интерпретация показателя по перечислению a) должна быть следующей. - критерии организации на соответствие политике паролей организации реализованы удовлетворительно при показателе > 0,9; - критерии организации на соответствие политике паролей организации реализованы неудовлетворительно при [0,8 ≤ показатель ≤ 0,9]; - критерии организации на соответствие политике паролей организации не реализованы при показателе < 0,8. Интерпретация показателя по перечислению b) должна быть следующей: - восходящий тренд показывает улучшенное соответствие; нисходящий тренд показывает ухудшенное соответствие; - порядок изменения тренда может способствовать пониманию эффективности реализованных мер и средств контроля и управления; - негативный тренд может потребовать дополнительных мер и средств контроля и управления, таких как осведомленность, или технических средств для того, чтобы заставлять выбирать надежные пароли или периодически менять пароли; - позитивные тренды следует изучать для того, чтобы оценивать необходимые сроки реализации политики паролей, начиная с текущего результирующего показателя. Влияние/воздействие нереализованных критериев приводит к повышающемуся риску конфиденциальности. К возможным причинам отклонения относятся: недостаточная осведомленность о безопасности, технические недостатки реализации и нехватка времени для реализации на всех системах ИТ
Форматы отчетности	Линия тренда, которая отображает число паролей, соответствующих политике качества паролей организации, наложенная на линии тренда, полученные в течение предыдущих периодов отчетности
Заинтересованные стороны	
Заказчик измерения	Руководители, отвечающие за СМИБ. Руководитель, отвечающий за безопасность
Контролер измерения	Менеджмент безопасности
Владелец информации	Системный администратор
Сборщик информации	Персонал, отвечающий за безопасность
Субъект, ответственный за передачу информации	Персонал, отвечающий за безопасность
Частота/период	
Частота сбора данных	Ежегодно
Частота проведения исследования данных	Ежегодно
Частота сообщения результатов измерений	Ежегодно
Пересмотр измерений	Проверка и обновление каждый год
Период измерений	Один раз в год

B.2.2 Качество паролей, генерируемых автоматизированным способом

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Качество паролей
Числовой идентификатор	Характерный для организации
Назначение конструктивного элемента измерения	Для оценки качества паролей, применяемых пользователями для доступа к системам ИТ организации
Цель применения меры и средства контроля и управления/процесса	Предотвратить выбор пользователями небезопасных паролей
Мера и средство контроля и управления (1)/процесс (1)	A.11.3.1 приложения А [ИСО/МЭК 27001:2005] Пользователи должны соблюдать правила безопасности при выборе и использовании паролей. Реализация: все пользователи должны выбирать надежные пароли для каждой системы: 1) длина которых более восьми знаков; 2) не основанные на том, что можно легко отгадать или получить при использовании информации, связанной с личностью, например, на именах, телефонных номерах, датах рождения и т. п.; 3) не состоящие из слов, включенных в словари; 4) не содержащих следующих один за другим идентичных, полностью цифровых или полностью буквенных знаков. Все имена учетных записей и пароли пользователей для систем ИТ организации должны контролироваться системой обеспечения/контроля деятельности сотрудников. Надежность паролей должна проверяться с использованием программного обеспечения по тестированию качества паролей
Объект измерения и атрибуты	
Объект измерения	База данных, содержащая имена учетных записей сотрудников
Атрибуты	Личные пароли, хранящиеся в системных учетных записях сотрудников
Спецификация основной меры измерения	
Основная мера измерения	1 Общее число паролей. 2 Общее число качественных паролей
Метод измерения	1 Запуск запроса об учетных записях сотрудников. 2 Запуск инструмента тестирования качества паролей к системным учетным записям сотрудников, использующего гибридную атаку
Вид метода измерения	1 Объективный. 2 Субъективный
Шкала	1 Целые числа от нуля до бесконечности. 2 Целые числа от нуля до бесконечности
Вид шкалы	1 Порядковая. 2 Порядковая
Единица измерения	1 Пароли. 2 Пароли
Спецификация производной меры измерения	
Производная мера измерения	Отсутствует
Функция измерения	Отсутствует
Спецификация показателя	
Показатель	1 Показатель паролей, взломанных в течение 4 ч. 2 Тренд отношения 1
Аналитическая модель	a) разделить [число качественных паролей] на [общее число паролей]; b) сравнить показатель с предыдущим показателем

Окончание

Спецификация критериев принятия решений	
Критерии принятия решений	Цель применения мер и средств контроля и управления достигнута, и никакое действие не требуется, если результирующий показатель превышает 0,9. Если результирующий показатель находится в диапазоне между 0,8 и 0,9, то цель применения мер и средств контроля и управления не достигнута, однако позитивный тренд указывает на улучшение. Если результирующий показатель меньше 0,8, то следует принять немедленные меры
Результаты измерений	
Интерпретация показателя	Интерпретация показателя по перечислению a) должна быть следующей: - критерии организации на соответствие политике паролей организации реализованы удовлетворительно при показателе > 0,9; - критерии организации на соответствие политике паролей организации реализованы неудовлетворительно при [0,8 ≤ показатель ≤ 0,9]; - критерии организации на соответствие политике паролей организации не реализованы при показателе < 0,8. Интерпретация показателя по перечислению b) должна быть следующей: - восходящий тренд указывает на улучшенное соответствие; нисходящий тренд указывает на ухудшенное соответствие; - порядок изменения тренда может способствовать пониманию эффективности реализованных мер и средств контроля и управления; - позитивные тренды следует изучать для того, чтобы оценивать необходимые сроки реализации политики паролей, начиная с текущего результирующего показателя. Влияние/воздействие нереализованных критериев приводит к повышающемуся риску компрометации паролей, что может привести к несанкционированному доступу к системе. К возможным причинам отклонения относятся недостаточная осведомленность о безопасности, технические недостатки реализации и нехватка времени для реализации на всех системах ИТ
Форматы отчетности	Линия тренда, которая отображает возможность взлома паролей для всех протестированных записей, наложенная на линии трендов, полученных в течение предыдущих тестов
Заинтересованные стороны	
Заказчик измерения	Руководители, отвечающие за СМИБ. Руководитель, отвечающий за безопасность
Контролер измерения	Менеджмент безопасности
Владелец информации	Системный администратор
Сборщик информации	Персонал, отвечающий за безопасность
Субъект, ответственный за передачу информации	Персонал, отвечающий за безопасность
Частота/период	
Частота сбора данных	Еженедельно
Частота проведения исследования данных	Еженедельно
Частота сообщения результатов измерений	Еженедельно
Пересмотр измерений	Проверка и обновление каждый год
Период измерений	Один раз в три года

B.3 Процесс проверки СМИБ

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Процесс проверки СМИБ

Продолжение

Числовой идентификатор	Характерный для организации
Назначение конструктивного элемента измерения	Для оценки уровня выполнения независимого анализа информационной безопасности
Цель применения меры и средства контроля и управления/процесса	Менеджмент информационной безопасности в пределах организации
Мера и средство контроля и управления (1)/процесс (1)	А.6.1.8 приложения А [ИСО/МЭК 27001:2005] Порядок организации и управления информационной безопасностью и ее реализация (например, изменение целей и мер управления, политики, процессов и процедур обеспечения информационной безопасности) должны быть подвергнуты независимой проверке (аудиту) через определенные промежутки времени или при появлении существенных изменений в способах реализации мер безопасности. Реализация: подход организации к менеджменту информационной безопасности и его реализации проверяется консультантом по безопасности сторонней организации ежеквартально
Объект измерения и атрибуты	
Объект измерения	1 Отчеты о проверках, проводимых сторонней организацией. 2 Планы проверок, проводимых сторонней организацией
Атрибуты	1 Представленный отчет о проверках, проводимых сторонней организацией. 2 Запланированные проверки, проводимые сторонней организацией
Спецификация основной меры измерения	
Основная мера измерения	1 Число проверок, проведенных сторонней организацией. 2 Общее число проверок, запланированных к проведению сторонней организацией
Метод измерения	1 Подсчет числа отчетов о регулярных проверках, проведенных сторонней организацией. 2 Подсчет общего числа проверок, запланированных к проведению сторонней организацией
Вид метода измерения	1 Объективный. 2 Объективный
Шкала	1 Целые числа от нуля до бесконечности. 2 Целые числа от нуля до бесконечности
Вид шкалы	1 Порядковая. 2 Порядковая
Единица измерения	1 Анализ. 2 Анализ
Спецификация производной меры измерения	
Производная мера измерения	Отсутствует
Функция измерения	Отсутствует
Спецификация показателя	
Показатель	Показатель хода завершенных независимых проверок
Аналитическая модель	Разделить [число проведенных сторонней организацией проверок] на [общее число проверок, запланированных к проведению сторонней организацией]
Спецификация критериев принятия решений	
Критерии принятия решений	Результирующее значение показателя должно находиться, в основном, между 0,8 и 1,1 для достижения цели применения мер и средств контроля и управления и чтобы не потребовалось принимать никаких мер. Оно должно превышать 0,6, если не выполняется основное условие

Окончание

Результаты измерений	
Интерпретация показателя	Интерпретация показателя должна быть следующей: - критерии организации, касающиеся менеджмента информационной безопасности в рамках организации в течение анализа, проводившегося сторонней организацией, были реализованы удовлетворительно при 0,8 ≤ показатель ≤ 1,1; - критерии организации были реализованы неудовлетворительно при [0,6 ≤ показатель < 0,8 или при показателе > 1,1]. Для того чтобы убедиться в том, что соответствующее продвижение сделано, требуется проведение мониторинга; - критерии организации не реализованы при [0 ≤ показатель < 0,6]. Для того чтобы убедиться в том, что соответствующий прогресс осуществляется, требуется проведение мониторинга. Если в конце второго квартала показатель по перечислению а) является неудовлетворительным, необходимо принять корректирующие меры и проинформировать руководство, отвечающее за СМИБ. Если в конце года показатель по перечислению а) является неудовлетворительным, следует проинформировать высшее руководство и попросить его поддержки Влиянием/воздействием нереализованных критериев является неэффективный процесс проверки, осуществляемый руководством. К возможным причинам отклонения относятся: недостаточный бюджет, ненадлежащее планирование и невыполнение критических обязательств персоналом/руководством
Форматы отчетности	Гистограмма, отражающая соответствие пороговым значениям в течение нескольких отчетных периодов, определенных критериями принятия решений
Заинтересованные стороны	
Заказчик измерения	Руководители, отвечающие за СМИБ. Руководитель системы качества
Контролер измерения	Руководители, отвечающие за СМИБ
Владелец информации	Руководители, отвечающие за СМИБ
Сборщик информации	Внутренний аудитор. Руководитель по качеству
Субъект, ответственный за передачу информации	Внутренний аудитор. Руководители системы качества, отвечающие за СМИБ
Частота/период	
Частота сбора данных	Ежеквартально
Частота проведения исследования данных	Ежеквартально
Частота сообщения результатов измерений	Ежеквартально
Пересмотр измерений	Проверка и обновление каждые два года
Период измерений	Один раз в два года

B.4 Непрерывное улучшение СМИБ

B.4.1 Эффективность менеджмента инцидентов информационной безопасности

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Эффективность менеджмента инцидентов информационной безопасности
Числовой идентификатор	Характерный для организации
Назначение конструктивного элемента измерения	Для оценки эффективности менеджмента инцидентов информационной безопасности
Цель применения меры и средства контроля и управления/процесса	Создание возможности быстрого обнаружения событий, связанных с безопасностью, и реагирование на инциденты безопасности

Продолжение

Мера и средство контроля и управления (1)/процесс (1)	Пункт 4.2.2, перечисление h) [ИСО/МЭК 27001:2005]
Объект измерения и атрибуты	
Объект измерения	СМИБ
Атрибуты	Отдельный инцидент
Спецификация основной меры измерения	
Основная мера измерения	Предварительно определенное пороговое значение
Метод измерения	Подсчет числа случаев возникновения инцидентов информационной безопасности, о которых сообщено к установленному сроку
Вид метода измерения	Объективный
Шкала	Цифровая
Вид шкалы	Порядковая
Единица измерения	Инцидент
Спецификация производной меры измерения	
Производная мера измерения	Инциденты, выходящие за пределы порогового значения
Функция измерения	Сравнение общего числа инцидентов с пороговым значением
Спецификация показателя	
Показатель	Линейный график, отображающий непрерывную горизонтальную линию (линии), иллюстрирующую(ие) пороговое(ые) значение(я), и общее число инцидентов за несколько отчетных периодов
Аналитическая модель	Красный цвет используется, если общее число инцидентов превышает пороговое значение (выходит за линию); желтый — если общее число инцидентов находится в пределах 10 % порогового значения; зеленый — если общее число инцидентов находится ниже порогового значения на 10 % или более
Спецификация критериев принятия решений	
Критерии принятия решений	Красный цвет — требуется немедленное исследование причин увеличения числа инцидентов. Желтый цвет — число инцидентов необходимо подвергнуть тщательной проверке и, если оно не изменяется в лучшую сторону, следует начать исследование. Зеленый цвет — никакого действия не требуется
Результаты измерений	
Интерпретация показателя	Если красный цвет наблюдается в двух отчетных циклах, требуется проверка процедур менеджмента инцидентов для исправления существующих процедур или определения дополнительных процедур. Если характер изменения тренда в течение двух последующих отчетных периодов не меняется на противоположный, то требуются корректирующие меры, например, внесение предложения о расширении сферы применения СМИБ
Форматы отчетности	Линейный график
Заинтересованные стороны	
Заказчик измерения	Комитет по управлению СМИБ. Руководители, отвечающие за СМИБ. Менеджмент безопасности. Менеджмент инцидентов
Контролер измерения	Руководители, отвечающие за СМИБ
Владелец информации	Руководители, отвечающие за СМИБ
Сборщик информации	Руководитель, отвечающий за менеджмент инцидентов

Окончание

Субъект, ответственный за передачу информации	Комитет по управлению СМИБ
Частота/период	
Частота сбора данных	Ежемесячно
Частота проведения исследования данных	Ежемесячно
Частота сообщения результатов измерений	Ежемесячно
Пересмотр измерений	Каждые шесть месяцев
Период измерений	Ежемесячно

В.4.2 Реализация корректирующих действий

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Реализация корректирующих действий
Числовой идентификатор	Идентификатор, характерный для организации
Назначение конструктивного элемента измерения	Оценка эффективности реализации корректирующего действия
Цель применения меры и средства контроля и управления/процесса	Пункт 8.2 [ИСО/МЭК 27001:2005] «Корректирующие действия» Организация должна проводить мероприятия по устранению причин несоответствий требованиям СМИБ с целью предупреждения их повторного возникновения
Мера и средство контроля и управления (1)/процесс (1)	Документированная процедура корректирующего действия должна определять требования к: a) выявлению несоответствий; b) установлению причин несоответствий; c) оцениванию потребности в действиях для обеспечения того, чтобы несоответствия не возникали снова; d) определению и реализации необходимого корректирующего действия; e) регистрации результатов предпринятого действия (см. 4.3.3 ИСО/МЭК 27001:2005); f) проведению проверки предпринятого корректирующего действия. (Реализовано) Организация определяет требуемые корректирующие действия и выпускает отчет о корректирующем действии, документируя информацию, касающуюся несоответствия, его причины и срока выполнения предпринятого корректирующего действия. Требуется, чтобы после получения отчета руководитель, отвечающий за сферу, где было обнаружено несоответствие, обеспечил, чтобы действия по устранению обнаруженных несоответствий и их причин предпринимались без чрезмерной задержки. Если корректирующее действие не реализовано как требовалось, необходимо определить причину невыполнения, а также альтернативы первоначальному корректирующему действию, которое было установлено как соответствующее. Предпринятые действия следует документировать с соответствующей датой и результатами. Если корректирующее действие не реализовано как планировалось, то необходимо зафиксировать как причину этого, так и альтернативное действие. Отчет следует предоставлять руководителю, отвечающему за информационную безопасность
Объект измерения и атрибуты	
Объект измерения	Отчеты о корректирующих действиях
Атрибуты	Срок выполнения корректирующего действия в отчете. Дата выполнения корректирующего действия в записи отчета. Причина задержки и невыполнения действия

Продолжение

Спецификация основной меры измерения	
Основная мера измерения	1 Число корректирующих действий, запланированных на данный момент. 2 Число корректирующих действий, реализованных как планировалось, на данный момент. 3 Число корректирующих действий, не реализованных на данный момент по какой-либо причине
Метод измерения	1 Подсчет корректирующих действий, реализация которых запланирована на данный момент. 2 Подсчет корректирующих действий, зафиксированных как реализованные, с датой срока исполнения. 3 Подсчет корректирующих действий, зафиксированных как запланированные действия, но не выполненных по какой-либо причине
Вид метода измерения	1—3 Объективный
Шкала	1—3 Целые числа от нуля до бесконечности
Вид шкалы	1—3 Порядковая
Единица измерения	1—3 Корректирующее действие
Спецификация производной меры измерения	
Производная мера измерения	a) Корректирующее действие, не реализованное к установленной дате; b) корректирующее действие, не реализованное без серьезной причины
Функция измерения	a) Вычесть [число корректирующих действий, выполненных как планировалось к установленному сроку] из [числа корректирующих действий, запланированных к установленному сроку]; b) вычесть [число корректирующих действий, не реализованных к установленному сроку] из [числа корректирующих действий, не выполненных как планировалось по какой-либо причине к установленному сроку]
Спецификация показателя	
Показатель	a) Состояние, выраженное как показатель корректирующего действия, которое не реализовано; b) состояние, выраженное как показатель корректирующего действия, которое не реализовано без какой-либо причины; c) тренд состояний
Аналитическая модель	a) Разделить [число корректирующих действий, не реализованных к установленному сроку] на [количество корректирующих действий, запланированных к установленному сроку]; b) разделить [число корректирующих действий, не реализованных без какой-либо причины] на [число корректирующих действий, запланированных к установленному сроку]; c) сравнить состояние с предыдущими состояниями
Спецификация критериев принятия решений	
Критерии принятия решений	Для того, чтобы сделать вывод о достижении цели и о том, что никакого действия не требуется, значения показателя по перечислению a) и показателя по перечислению b) должны находиться между 0,4 и 0,0 и между 0,2 и 0,0, соответственно, и тренд показателя по перечислению c) должен быть снижен в течение двух отчетных периодов. Показатель по перечислению c) должен быть представлен в сравнении с предыдущими показателями, с тем чтобы можно было изучать тренд в реализации корректирующего действия
Результаты измерений	
Интерпретация показателя	Интерпретация показателя по перечислению a) и показателя по перечислению b) должна быть следующей: - запланированные корректирующие действия должны быть реализованы, если только не произошло изменения в приоритетах организации, что привело бы к необходимости реализации других корректирующих действий или перенаправления ресурсов, выделенных для реализации корректирующих действий. Если более 40 % корректирующих действий не реализовано (независимо от причины), требуется вмешательство руководства. Если более 20 % коррек-

Окончание

	тирующих действий не реализовано (без уважительной причины), требуется вмешательство руководства. Корректирующие действия, которые не были реализованы, следует изучать, с тем чтобы установить причину нереализации. В зависимости от общего процентного показателя нереализованных корректирующих действий и причин нереализации, может потребоваться дополнительное действие. Интерпретация показателя по перечислению c) должна быть следующей: - тенденцию в реализации корректирующих действий следует изучать на предмет выявления какого-либо общего ухудшения результативности или значительного ухудшения результативности; - если процентный показатель реализованных корректирующих действий устойчиво снижался за два последних отчетных периода, требуется вмешательство руководства, несмотря на отсутствие причин несоответствия. Влиянием/воздействием нереализованных критериев является возможное отсутствие непрерывного улучшения СМИБ. К возможным причинам могут относиться: нехватка ресурсов, ненадлежащее планирование, а также невыполнение критических обязательств персоналом и руководством
Форматы отчетности	Многоярусная гистограмма с кратким изложением результатов измерений, включая основные положения выводов и возможных действий руководства, отражающая общее число корректирующих действий, разделенных на реализованные, не реализованные при отсутствии серьезной причины и не реализованные по серьезной причине
Заинтересованные стороны	
Заказчик измерения	Руководители, отвечающие за СМИБ. Руководитель по обеспечению информационной безопасности
Контролер измерения	Руководители, отвечающие за СМИБ
Владелец информации	Руководители, отвечающие за СМИБ
Сборщик информации	Руководители, отвечающие за СМИБ
Субъект, ответственный за передачу информации	Руководители, отвечающие за СМИБ
Частота/период	
Частота сбора данных	Ежеквартально
Частота проведения исследования данных	Ежеквартально
Частота сообщения результатов измерений	Ежеквартально
Пересмотр измерений	Ежегодная проверка
Период измерений	Один год

B.5 Обязательства руководства

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Частота проверок, проводимых руководством
Числовой идентификатор	Характерный для организации
Назначение конструктивного элемента измерения	Оценка обязательств руководства и действий по проверке информационной безопасности относительно действий по проводимой руководством проверке
Цель применения меры и средства контроля и управления/процесса	A.6.1 приложения A [ИСО/МЭК 27001:2005] Обеспечение управления информационной безопасностью в организации. (Запланировано) Осуществлять менеджмент информационной безопасности в пределах организации посредством регулярно проводимых руководством проверок

Продолжение

Мера и средство контроля и управления (1)/процесс (1)	А.6.1.1 приложения А [ИСО/МЭК 27001:2005] Обязанности руководства по обеспечению информационной безопасности. Руководство организации должно постоянно поддерживать заданный уровень информационной безопасности путем внедрения системы менеджмента, а также распределения обязанностей и ответственности персонала за ее обеспечение. (Реализовано) В организации должны ежемесячно проводиться заседания, касающиеся проводимых руководством проверок, для поддержки безопасности в пределах организации посредством четкого управления, демонстрируемых обязательств, точных поручений и подтверждения информационной безопасности. Проверку СМИБ, осуществляемую руководством, следует объединять с проверкой системы менеджмента качества , осуществляемой руководством
Мера и средство контроля и управления (2)/процесс (2)	А.6.1.2 приложения А [ИСО/МЭК 27001:2005] Координация вопросов обеспечения информационной безопасности. Действия по обеспечению информационной безопасности должны координироваться представителями различных подразделений организации, имеющими соответствующие функции и должностные обязанности. (Реализовано) Представителям различных подразделений, наделенным соответствующими ролями и обязанностями, следует координировать проводимые руководством проверки и участвовать в них
Объект измерения и атрибуты	
Объект измерения	1 План/график проверки информационной безопасности, проводимой руководством. 2 Записи протоколов совещаний, посвященных проводимым руководством проверкам
Атрибуты	1.1 Даты совещаний, касающихся проводимых руководством проверок, зафиксированные в плане. 1.2 Руководители, присутствие которых запланировано на совещаниях, касающихся проводимых руководством проверок. 2.1 Даты совещаний, касающихся проводимых руководством проверок, зафиксированные в протоколах совещаний. 2.2 Руководители, присутствие которых на совещаниях, касающихся проводимых руководством проверок, зафиксировано
Спецификация основной меры измерения	
Основная мера измерения	1.1 Число совещаний, касающихся проводимых руководством проверок, запланированных к установленному сроку. 1.2 Число руководителей, присутствие которых на совещаниях, касающихся проводимым руководством проверок, запланировано. 2.1.1 Число запланированных совещаний, касающихся проводимых руководством проверок, проведенных к установленному сроку. 2.1.2 Число незапланированных совещаний, касающихся проводимых руководством проверок, проведенных к установленному сроку. 2.1.3 Число повторно запланированных совещаний, касающихся проводимых руководством проверок, проведенных к установленному сроку. 2.2 Число руководителей, присутствовавших на совещаниях, касающихся проводимых руководством проверок, к установленному сроку
Метод измерения	1.1 Подсчет совещаний, касающихся проводимых руководством проверок, запланированных на данный момент. 1.2 Из расчета совещаний, касающихся проводимых руководством проверок, на данный момент, подсчитать количество руководителей, присутствие которых было запланировано, и добавить новые данные со значением по умолчанию для незапланированных чрезвычайных совещаний. 2.1.1 Подсчет числа запланированных совещаний, касающихся проводимых руководством проверок, проведенных к установленному сроку. 2.1.2 Подсчет числа незапланированных совещаний, касающихся проводимых руководством проверок, проведенных к установленному сроку. 2.1.3 Подсчет числа повторно запланированных совещаний, касающихся проводимых руководством проверок, проведенных к установленному сроку. 2.2 Для всех проведенных совещаний, касающихся проводимых руководством проверок, подсчитать число руководителей, принимавших в них участие

Продолжение

Вид метода измерения	1.1 Объективный. 1.2 Объективный или субъективный. 2.1.1 Объективный. 2.1.2 Объективный. 2.1.3 Объективный. 2.2 Объективный
Шкала	1.1 Целые числа от нуля до бесконечности. 1.2 Целые числа от нуля до бесконечности. 2.1.1 Целые числа от нуля до бесконечности. 2.1.2 Целые числа от нуля до бесконечности. 2.1.3 Целые числа от нуля до бесконечности. 2.2 Целые числа от нуля до бесконечности
Вид шкалы	1.1 Порядковая. 1.2 Порядковая. 2.1.1 Порядковая. 2.1.2 Порядковая. 2.1.3 Порядковая. 2.2 Порядковая
Единица измерения	1.1 Совещание. 1.2 Персонал. 2.1.1 Совещание. 2.1.2 Совещание. 2.1.3 Совещание. 2.2 Персонал
Спецификация производной меры измерения	
Производная мера измерения	a) Число совещаний, касающихся проводимых руководством проверок, проведенных к установленному сроку; b) коэффициент участия в совещаниях, касающихся проводимых руководством проверок, проведенных к установленному сроку
Функция измерения	a) Сложить [число запланированных совещаний, касающихся проводимых руководством проверок, проведенных к установленному сроку], [число незапланированных совещаний, касающихся проводимых руководством проверок, проведенных к установленному сроку] и [число повторно запланированных совещаний, касающихся проводимых руководством проверок, проведенных к установленному сроку]; b) для каждого совещания, касающегося проводимых руководством проверок, разделить [число руководителей, присутствовавших на совещаниях, касающихся проводимых руководством проверок] на [число руководителей, присутствие которых на совещаниях, касающихся проводимых руководством проверок, было запланировано]
Спецификация показателя	
Показатель	a) Совещания, касающиеся проводимых руководством проверок, завершенных к установленному сроку; b) показатели общего участия в совещаниях, касающихся проводимых руководством проверок, к установленному сроку
Аналитическая модель	a) Разделить [число проведенных совещаний, касающихся проведенных руководством проверок] на [число запланированных совещаний, касающихся проведенных руководством проверок]; b) вычислить среднее и стандартное отклонение от всех показателей участия для совещаний, касающихся проводимых руководством проверок
Спецификация критериев принятия решений	
Критерии принятия решений	Результирующее значение показателя по перечислению a) должно находиться в диапазоне между 0,7 и 1,1 для того, чтобы сделать вывод о достижении цели применения мер и средств контроля и управления и не требовалось никакого действия. Даже если это условие не выполняется, значение все же должно превышать 0,5, чтобы сделать вывод о минимальном достижении цели. Что касается показателя по перечислению b), то вычисленные границы доверительного интервала, основанные на стандартном отклонении, показывают вероятность того, что будет

Продолжение

	достигнут фактический результат, близкий к коэффициенту общего участия. Очень широкие границы доверительного интервала наводят на мысль о наибольшем отклонении и необходимости планирования чрезвычайных обстоятельств с тем, чтобы оперировать этим результатом
Результаты измерений	
Интерпретация показателя	Интерпретация для показателя по перечислению a) должна быть следующей: - критерии организации относительно менеджмента информационной безопасности в пределах организации в течение проводимой руководством проверки были реализованы удовлетворительно при 0,7 ≤ показатель ≤ 1,1; - критерии организации были реализованы неудовлетворительно при [0,5 ≤ показатель < 0,7 или при показателе > 1,1]. Этот результат может указывать на отсутствие обязательств руководства и потребовать корректирующего действия. Последующие результаты измерений следует подвергать мониторингу и оцениванию на предмет их улучшения; - критерии организации не реализованы при [0 ≤ показатель < 0,5]. Этот результат указывает на отсутствие обязательств руководства и требует незамедлительного вмешательства для реализации соответствующего корректирующего действия. О результате необходимо сообщать высшему руководству. Показатель, близкий к нулю, может указывать на отсутствие обязательств высшего руководства. Если руководители СМИБ не рассматривают проверки СМИБ, проводимые руководством в качестве приоритетных, то на них может воздействовать высшее руководство; - результатом влияния/воздействия нереализованных критериев является возможное отсутствие непрерывного и эффективного процесса проводимой руководством проверки. К возможным причинам отклонения в показателе по перечислению b) могут относиться ненадлежащее планирование, недостаточные обязательства руководителей, отвечающих за СМИБ, несовместимые приоритеты и (или) чрезмерная загруженность работой, влияющая на руководителей СМИБ
Форматы отчетности	Линейная диаграмма, отражающая показатель вместе с критериями за несколько периодов сбора данных и отчетных периодов с изложением результатов измерений. Число периодов сбора данных и отчетных периодов определяется организацией
Заинтересованные стороны	
Заказчик измерения	Руководители, отвечающие за СМИБ. Руководитель системы качества
Контролер измерения	Специалист по программе внутреннего аудита СМИБ
Владелец информации	Руководитель системы качества. Предполагаемая объединенная система менеджмента качества и СМИБ
Сборщик информации	Менеджер по качеству. Менеджер, отвечающий за информационную безопасность
Субъект, ответственный за передачу информации	Менеджер, отвечающий за информационную безопасность. Менеджер по качеству
Частота/период	
Частота сбора данных	Ежемесячно
Частота проведения исследования данных	Ежеквартально
Частота сообщения результатов измерений	Ежеквартально
Пересмотр измерений	Проверка и обновление каждые два года
Период измерений	Два года

B.6 Защита от вредоносных программ

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Защита от вредоносного программного средства

Продолжение

Числовой идентификатор	Характерный для организации
Назначение конструктивного элемента измерения	Оценка эффективности системы защиты от атак вредоносного программного средства
Цель применения меры и средства контроля и управления/процесса	Цель применения меры и средства контроля и управления А.10.4 [ИСО/МЭК 27001:2005]. Защищать целостность программного обеспечения и массивов информации. (Запланировано). Защита целостности программного обеспечения и информации от вредоносного программного средства
Мера и средство контроля и управления (1)/процесс (1)	Мера и средство контроля и управления А.10.4.1 приложения А [ИСО/МЭК 27001:2005]. Меры и средства контроля и управления, предназначенные для защиты от вредоносных программ. Должны быть реализованы меры и средства контроля и управления по обнаружению, предотвращению проникновения и восстановлению после проникновения вредоносной программы, а также должны быть установлены процедуры обеспечения соответствующего оповещения пользователей
Объект измерения и атрибуты	
Объект измерения	1 Отчеты об инцидентах. 2 Журналы регистрации программного обеспечения контрмер, направленных на вредоносное программное средство
Атрибуты	Инциденты, вызванные вредоносным программным средством
Спецификация основной меры измерения	
Основная мера измерения	1 Число инцидентов безопасности, вызванных вредоносным программным средством. 2 Общее число блокированных атак, вызванных вредоносным программным средством
Метод измерения	1 Подсчет числа инцидентов безопасности, вызванных вредоносным программным средством, в отчетах об инцидентах. 2 Подсчет числа записей о блокированных атаках
Вид метода измерения	1 Объективный. 2 Объективный
Шкала	1 Целые числа от нуля до бесконечности. 2 Целые числа от нуля до бесконечности
Вид шкалы	1 Порядковая. 2 Порядковая
Единица измерения	1 Инцидент безопасности. 2 Записи
Спецификация производной меры измерения	
Производная мера измерения	Стойкость защиты от вредоносного программного средства
Функция измерения	Число инцидентов безопасности, вызванных вредоносным программным средством / число обнаруженных и блокированных атак, вызванных вредоносным программным средством
Спецификация показателя	
Показатель	Тренд числа обнаруженных атак, которые не были блокированы в течение многих отчетных периодов
Аналитическая модель	Сравнить показатель с предыдущим процентным показателем
Спецификация критериев принятия решений	
Критерии принятия решений	Линии, определяющие тренд, должны находиться в соответствии с определенным числом. Результирующий тренд должен быть нисходящим или постоянным

Окончание

Результаты измерений	
Интерпретация показателя	Восходящий тренд показывает ухудшающееся соответствие, нисходящий тренд показывает улучшающееся соответствие. При сильном возрастании тренда потребуются исследование причины и возможность для внедрения дополнительной контрмеры
Форматы отчетности	Линия тренда отображает показатель обнаружения и предотвращения вредоносного программного средства по отношению к линиям, полученным в течение последних отчетных периодов
Заинтересованные стороны	
Заказчик измерения	Менеджмент безопасности
Контролер измерения	Менеджмент безопасности
Владелец информации	Системный администратор
Сборщик информации	Менеджмент безопасности. Системный администратор. Руководитель, ответственный за функционирование сети
Субъект, ответственный за передачу информации	Служба согласования
Частота/период	
Частота сбора данных	Ежедневно
Частота проведения исследования данных	Ежемесячно
Частота сообщения результатов измерений	Ежемесячно
Дата пересмотра	Проверка один раз в год
Период измерений	Один год

B.7 Меры и средства контроля и управления физическим доступом

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Меры и средства контроля и управления физическим доступом с использованием карт доступа
Числовой идентификатор	Характерный для организации
Назначение конструктивного элемента измерения	Демонстрация наличия, границ и качества системы, используемой для управления доступом
Цель применения меры и средства контроля и управления/процесса	Цель меры и средства контроля и управления по А.9.1 приложения А [ИСО/МЭК 27001:2005]. Предотвращать несанкционированные физический доступ, повреждение и воздействия на помещения и информацию организации
Мера и средство контроля и управления (1)/процесс (1)	Мера и средство контроля и управления по А.9.1.2 приложения А [ИСО/МЭК 27001:2005]. Контроль доступа в охраняемую зону. Охраняемая зона должна быть защищена соответствующими средствами контроля входа, предполагающими обеспечить уверенность в том, что только авторизованный персонал может получить доступ в зону
Объект измерения и атрибуты	
Объект измерения	Безопасные зоны
Атрибуты	Записи, касающиеся управления идентификационными данными
Спецификация основной меры измерения	
Основная мера измерения	Меры и средства контроля и управления физическим доступом с использованием карт доступа

Продолжение

Метод измерения	Относительный метод измерения, где каждый уровень подмножества является частью приведенного выше уровня. Проверяется вид системы мер и средств контроля и управления входом и рассматриваются следующие аспекты. - наличие системы карт управления доступом; - использование PIN-кода; - функциональные возможности журнала регистрации; - биометрическая аутентификация
Вид метода измерения	Субъективный
Шкала	0—5 **0 — не существует никакой системы управления доступом**. **1** — существует система доступа там, где для контроля входа используется **PIN-код** (однофакторная система). **2** — существует система **карт** управления доступом там, где для контроля входа используется карта прохода (однофакторная система). **3** — существует система карт доступа, где для контроля входа используется **карта прохода и PIN-код**. **4** — предыдущее + активированные **функциональные возможности журнала регистрации.** **5** — предыдущее + PIN-код заменен на **биометрическую аутентификацию** (отпечатки пальцев, распознавание голоса, сканирование сетчатки глаза и т. д.)
Вид шкалы	Порядковая
Единица измерения	Не применяется
Спецификация производной меры измерения	
Производная мера измерения	Отсутствует
Функция измерения	Отсутствует
Спецификация показателя	
Показатель	Индикатор выполнения. Красный — до 0,8. Зеленый — от 0,8 до 1
Аналитическая модель	Анализ мер измерения
Спецификация критериев принятия решений	
Критерии принятия решений	Значение 3 — удовлетворительно
Результаты измерений	
Интерпретация показателя	Ниже значения 3 — неудовлетворительно (3 — фактический уровень, эквивалентный недостатку обеспечения безопасности), где должны быть приняты меры в зависимости от степени недостатка обеспечения безопасности. Выше значения 3 — чаще всего удовлетворительно, где уровень может указывать на избыточные инвестиции в отношении измеряемого объекта
Форматы отчетности	Графическое представление
Заинтересованные стороны	
Заказчик измерения	Комитет по управлению
Контролер измерения	Внутренний аудитор/внешний аудитор
Владелец информации	Руководитель, отвечающий за оборудование
Сборщик информации	Внутренний аудитор/внешний аудитор
Субъект, ответственный за передачу информации	Внутренний аудитор и менеджер безопасности
Частота/период	
Частота сбора данных	Ежегодно
Частота проведения исследования данных	Ежегодно

Окончание

Частота сообщения результатов измерений	Ежегодно
Дата пересмотра	12 месяцев
Период измерений	12 месяцев

В.8 Анализ журналов регистрации

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Анализ журналов регистрации
Числовой идентификатор	Уникальный характерный для организации числовой идентификатор
Назначение конструктивного элемента измерения	Оценка состояния соответствия регулярной проверки журналов регистрации критических систем
Цель применения меры и средства контроля и управления/процесса	Цель применения меры и средства контроля и управления по А.10.10 приложения А [ИСО/МЭК 27001.2005]. Обнаруживать несанкционированные действия, связанные с обработкой информации. (Запланировано). Обнаружение несанкционированных деятельностей, связанных с обработкой информации из системного журнала регистрации критических систем
Мера и средство контроля и управления (1)	Мера и средство контроля и управления по А.10.10.2 приложения А [ИСО/МЭК 27001.2005]. Должны быть установлены процедуры, позволяющие вести мониторинг и регулярный анализ результатов мониторинга использования средств обработки информации
Объект измерения и атрибуты	
Объект измерения	Система
Атрибуты	Отдельные журналы регистрации
Спецификация основной меры измерения (1)	
Основная мера измерения	Число журналов регистрации
Метод измерения	Подсчет общего числа журналов регистрации, перечисленных в списке проверяемых журналов регистрации
Вид метода измерения	Объективный
Шкала	Целые числа от нуля до бесконечности
Вид шкалы	Порядковая
Единица измерения	Журнал регистрации
Спецификация основной меры измерения (2)	
Основная мера измерения	Число проверенных журналов регистрации
Метод измерения	Подсчет общего числа журналов регистрации по всем системам, находящимся в рамках сферы применения СМИБ
Вид метода измерения	Объективный
Шкала	Числовая
Вид шкалы	Шкала отношений
Единица измерения	Журнал регистрации
Спецификация основной меры измерения (3)	
Основная мера измерения	Число систем, находящихся в рамках сферы применения СМИБ
Метод измерения	Определение числа проверенных журналов регистрации
Вид метода измерения	Объективный
Шкала	Числовая

Окончание

Вид шкалы	Шкала отношений
Единица измерения	Журнал регистрации
Спецификация производной меры измерения	
Производная мера измерения	Процентное отношение проверенных (при необходимости) журналов регистрации (аудита) за определенный временной период
Функция измерения	Разделить (число проверенных журналов регистрации в течение определенного временного периода) на (общее число журналов регистрации) и умножить на 100
Спецификация показателя	
Показатель	Линейный график тренда частоты проверки журналов регистрации (аудита) за период времени
Аналитическая модель	Желателен восходящий тренд, стремящийся к 100 %
Спецификация критериев принятия решений	
Критерии принятия решений	Результат ниже 20 % должен быть изучен на предмет выявления причин результативности ниже установленной нормы
Результаты измерений	
Интерпретация показателя	Значения, ниже определенного организацией значения, являются неудовлетворительными, где определенное организацией значение — фактическое значение, эквивалентное недостатку безопасности. Требуется действие руководства в зависимости от степени недостатка безопасности. Значения, которые выше значения, определенного организацией, могут указывать на чрезмерное инвестирование, если эти механизмы управления доступом не требуются согласно оценке риска
Форматы отчетности	Линейный график, отражающий тренд суммарных результатов и какие-либо рекомендуемые действия руководства
Заинтересованные стороны	
Заказчик измерения	Руководители, отвечающие за СМИБ. Руководитель, отвечающий за обеспечение безопасности
Контролер измерения	Руководитель, отвечающий за обеспечение безопасности
Владелец информации	Руководитель, отвечающий за обеспечение безопасности
Сборщик информации	Персонал, отвечающий за обеспечение безопасности
Субъект, ответственный за передачу информации	Персонал, отвечающий за обеспечение безопасности
Частота/период	
Частота сбора данных	Ежемесячно
Частота проведения исследования данных	Ежемесячно
Частота сообщения результатов измерений	Ежеквартально
Дата пересмотра	Проверка и обновление каждые два года
Период измерений	Два года

B.9 Менеджмент периодического технического обслуживания

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Менеджмент периодического технического обслуживания
Числовой идентификатор	Характерный для организации
Назначение конструктивного элемента измерения	Оценка своевременности деятельностей, связанных с техническим обслуживанием, по отношению к расписанию

Продолжение

Цель применения меры и средства контроля и управления/процесса	Цель меры и средства контроля и управления по А.9.2 приложения А [ИСО/МЭК 27001:2005]. Предотвращать потерю, повреждение, хищение или компрометацию активов и прекращение деятельности организации. (Запланировано). Предотвращение потери, ущерба, кражи или компрометации активов и прерывания деятельностей организации с помощью периодического технического обслуживания системы
Мера и средство контроля и управления (1)/процесс (1)	Мера и средство контроля и управления по А.9.2.4 приложения А [ИСО/МЭК 27001:2005]. Должно проводиться надлежащее регулярное техническое обслуживание оборудования для обеспечения его непрерывной работоспособности и сохранности
Объект измерения и атрибуты	
Объект измерения	1 План/график технических обслуживаний системы. 2 Записи о технических обслуживаниях системы
Атрибуты	1 Даты, на которые запланировано/предусмотрено графиком техническое обслуживание системы. 2 Даты проведенного технического обслуживания системы
Спецификация основной меры измерения (1—4)	
Основная мера измерения	1 Даты запланированного технического обслуживания. 2 Даты проведенного технического обслуживания. 3 Общее число запланированных мероприятий по техническому обслуживанию. 4 Общее число проведенных мероприятий по техническому обслуживанию
Метод измерения	1 Выписать запланированные даты из плана технического обслуживания системы. 2 Выписать даты проведения из записей о техническом обслуживании системы. 3 Подсчитать число запланированных мероприятий по техническому обслуживанию в плане технического обслуживания системы. 4 Подсчитать записи о выполнении технического обслуживания
Вид метода измерения	Объективный
Шкала	1 Временна́я. 2 Временна́я. 3 Целые числа от нуля до бесконечности. 4 Целые числа от нуля до бесконечности
Вид шкалы	1 Упорядоченная. 2 Упорядоченная. 3 Порядковая. 4 Порядковая
Единица измерения	1 Интервал. 2 Интервал. 3 Мероприятия по техническому обслуживанию. 4 Мероприятия по техническому обслуживанию
Спецификация производной меры измерения	
Производная мера измерения	Задержка технического обслуживания на проведенное мероприятие по техническому обслуживанию
Функция измерения	Для каждого проведенного мероприятия найти разницу между [датой фактического технического обслуживания] и [датой запланированного технического обслуживания]
Спецификация показателя	
Показатель	1 Среднее значение задержки технического обслуживания. 2 Показатель проведенных мероприятий по техническому обслуживанию. 3 Тренд среднего значения задержки технического обслуживания. 4 Тренд показателя проведенных мероприятий по техническому обслуживанию

Окончание

Аналитическая модель	1 Разделить суммарное значение [задержки технического обслуживания] на [число проведенных мероприятий по техническому обслуживанию]. 2 Разделить [число проведенных мероприятий по техническому обслуживанию] на [число запланированных мероприятий по техническому обслуживанию]. 3 Сравнить показатель по перечислению 1 за несколько временных периодов. 4 Сравнить показатель по перечислению 2 за несколько временных периодов
Спецификация критериев принятия решений	
Критерии принятия решений	1 Характерные для организации, например, если средняя величина задержки последовательно оказывается более трех дней, необходимо изучить ее причины. 2 Показатель проведенных мероприятий по техническому обслуживанию должен превышать 0,9. 3 Тренд должен быть стабильным или близким к нулю. 4 Тренд должен быть стабильным или восходящим
Результаты измерений	
Интерпретация показателя	Показатель помогает оценить качество процесса технического обслуживания оборудования
Форматы отчетности	Линейный график, который отражает среднюю величину отклонения задержки технического обслуживания, совмещаемый с линиями, получаемыми в течение предыдущих отчетных периодов и количествами систем, входящих в сферу применения. Пояснение результатов и рекомендация возможных действий руководства
Заинтересованные стороны	
Заказчик измерения	Руководители, отвечающие за СМИБ. Руководитель, отвечающий за обеспечение безопасности
Контролер измерения	Руководитель, отвечающий за обеспечение безопасности
Владелец информации	Системный администратор
Сборщик информации	Персонал, отвечающий за обеспечение безопасности
Субъект, ответственный за передачу информации	Персонал, отвечающий за обеспечение безопасности
Частота/период	
Частота сбора данных	Ежегодно
Частота проведения исследования данных	Ежегодно
Частота сообщения результатов измерений	Ежегодно
Дата пересмотра	Ежегодно
Период измерений	Ежегодно

B.10 Вопросы безопасности в соглашениях со сторонними организациями

Определение конструктивных элементов измерения	
Название конструктивного элемента измерения	Вопросы безопасности в соглашениях со сторонними организациями
Числовой идентификатор	Характерный для организации
Назначение конструктивного элемента измерения	Оценивание уровня, на котором рассматриваются вопросы безопасности в соглашениях со сторонней организацией, касающиеся обработки личной информации
Цель применения меры и средства контроля и управления/процесса	Цель меры и средства контроля и управления А.6.2 приложения А [ИСО/МЭК 27001:2005]. Поддерживать безопасность информации и средств обработки информации организации при наличии доступа к ним сторонних организаций в процессах обработки и передачи этой информации

Продолжение

Мера и средство контроля и управления (1)/процесс (1)	Мера и средство контроля и управления А.6.2.3 приложения А [ИСО/МЭК 27001:2005]. Соглашения со сторонними организациями должны содержать все требования безопасности, включающие в себя правила доступа к процессам обработки, передачи информации или к управлению информацией или средствами обработки информации организации, а также в случае приобретения дополнительных программных продуктов или организации сервисного обслуживания средств обработки информации
Объект измерения и атрибуты	
Объект измерения	Соглашения со сторонними организациями
Атрибуты	Положения или требования безопасности в каждом соглашении со сторонней организацией
Спецификация основной меры измерения (1)	
Основная мера измерения	Число соглашений со сторонними организациями
Метод измерения	Проверка соглашений со сторонними организациями, подсчет числа соглашений
Вид метода измерения	Объективный
Шкала	Целые числа от нуля до бесконечности
Вид шкалы	Порядковая
Единица измерения	Соглашение со сторонними организациями
Спецификация основной меры измерения (2)	
Основная мера измерения	Число стандартных требований безопасности, необходимых для соглашений со сторонними организациями
Метод измерения	Определение числа требований безопасности, подлежащих рассмотрению в каждом соглашении согласно политике
Вид метода измерения	Объективный
Шкала	Целые числа от нуля до бесконечности
Вид шкалы	Порядковая
Единица измерения	Требование
Спецификация основной меры измерения (3)	
Основная мера измерения	Число требований безопасности, рассмотренных в каждом соглашении со сторонними организациями
Метод измерения	Проверка соглашений со сторонними организациями, подсчет числа требований безопасности, рассмотренных в каждом соглашении
Вид метода измерения	Объективный
Шкала	Целые числа от нуля до бесконечности
Вид шкалы	Порядковая
Единица измерения	Требование
Спецификация производной меры измерения	
Производная мера измерения	Среднее процентное отношение значимых требований безопасности, рассмотренных в соглашениях со сторонними организациями
Функция измерения	Отношение суммы разностей между числом необходимых требований и количеством рассмотренных требований для каждого соглашения к числу соглашений
Спецификация показателя	
Показатель	1 Средний показатель отличия стандартных требований от рассмотренных требований. 2 Тренд этого показателя

Окончание

Аналитическая модель	1 Отношение суммы разностей между общим числом рассмотренных требований безопасности и общим числом стандартных требований безопасности для каждого соглашения к числу соглашений со сторонними организациями. 2 Сравнить с предыдущим показателем по перечислению 1
Спецификация критериев принятия решений	
Критерии принятия решений	1 Показатель по перечислению 1 должен превышать 0,9. 2 Показатель по перечислению 2 должен быть стабильным или восходящим
Результаты измерений	
Интерпретация показателя	Этот показатель обеспечивает понимание способности функции аутсорсинга рассматривать требования безопасности
Форматы отчетности	Линейный график, отражающий тренд за несколько отчетных периодов. Краткое изложение результатов и возможных действий руководства
Заинтересованные стороны	
Заказчик измерения	Руководители, отвечающие за СМИБ. Руководитель, отвечающий за обеспечение безопасности
Контролер измерения	Руководитель, отвечающий за обеспечение безопасности
Владелец информации	Учреждение, указанное в контракте
Сборщик информации	Персонал, отвечающий за обеспечение безопасности
Субъект, ответственный за передачу информации	Персонал, отвечающий за обеспечение безопасности
Частота/период	
Частота сбора данных	Ежемесячно
Частота проведения исследования данных	Ежеквартально
Частота сообщения результатов измерений	Ежеквартально
Дата пересмотра	Два года
Период измерений	Два года

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименования соответствующего национального стандарта
ИСО/МЭК 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
ИСО/МЭК 27000:2009	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

IDT — идентичные стандарты.

Библиография

[1] ISO 9000:2005*, Quality management systems — Fundamentals and vocabulary

[2] ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management

[3] ISO/IEC 15504-3:2004 Information technology — Process assessment — Part 3: Guidance on performing an assessment

[4] ISO/IEC 15939:2007 Systems and software engineering — Measurement process

[5] ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management

[6] ISO/TR 10017:2003* Guidance on statistical techniques for ISO 9001:2000

[7] ISO Guide 99:2007* International vocabulary of metrology — Basic and general concepts and associated terms (VIM)

[8] NIST Special Publication 800-55, Revision 1, Performance Measurement Guide for Information Security, July 2008.

[9] ISO/IEC TR 18044:2004* Information technology — Security techniques — Information security incident management

* Официальный перевод данного стандарта находится в Федеральном информационном фонде.

УДК 351.864.1:006.354 ОКС 35.040

Ключевые слова: менеджмент информационной безопасности, измерение, программа измерений, модель измерений, объект измерений, конструктивные элементы измерений, мера измерения, метод измерения, процесс измерения, показатель измерения, критерий оценивания программы измерений

Редактор *В.Н. Копысов*
Технический редактор *Н.С. Гришанова*
Корректор *М.С. Кабашова*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 06.02.2012. Подписано в печать 27.02.2012. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 6,98. Уч.-изд. л. 6,60. Тираж 131 экз. Зак. 196.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru