ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27004— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание

(ISO/IEC 27004:2016, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН) и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 мая 2021 г. № 388-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27004:2016 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание» (ISO/IEC 27004:2016 «Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation», IDT).

ИСО/МЭК 27004 разработан подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК)

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 27004—2011

6 Некоторые положения международного документа, указанного в пункте 4, могут являться объектом патентных прав. ИСО и МЭК не несут ответственности за идентификацию подобных патентных прав

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «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 (www.gost.ru)

Содержание

Введение

Настоящий стандарт предназначен для оказания помощи организациям в оценке деятельности по обеспечению информационной безопасности (ИБ)[1] и результативности системы менеджмента информационной безопасности (СМИБ) в целях выполнения требований, изложенных в подразделе 9.1 ИСО/МЭК 27001[2].

Результаты мониторинга и оценки защищенности системы менеджмента информационной безопасности могут способствовать принятию решений, касающихся управления, менеджмента, операционной эффективности и постоянного совершенствования СМИБ.

Для условий каждой конкретной организации настоящий стандарт, как и другие стандарты серии 27000, необходимо проанализировать, интерпретировать и адаптировать. Изложенные концепции и подходы предназначены для широкого применения, но меры, необходимые для отдельной конкретной организации, зависят от присущих организации факторов, таких как размер организации, отраслевая принадлежность, зрелость, риски ИБ, обязательства соответствия и стиль управления, которые на практике могут сильно различаться.

Настоящий стандарт может быть рекомендован организациям, внедряющим СМИБ, которая отвечает требованиям ИСО/МЭК 27001. С другой стороны, он не устанавливает каких-либо новых требований и не налагает на организации какие-либо обязательства соблюдать представленные в нем руководящие принципы для СМИБ, которые соответствуют ИСО/МЭК 27001.

[1] Положения настоящего стандарта должны рассматриваться с учетом требований национальных нормативных правовых актов и стандартов Российской Федерации в области защиты информации.

[2] Здесь и далее подразумевается стандарт ИСО/МЭК 27001:2013 (примечание переводчика).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание

Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт представляет руководящие принципы, предназначенные для оказания помощи организациям в оценке деятельности по обеспечению информационной безопасности (ИБ) и результативности системы менеджмента информационной безопасности (СМИБ) в целях выполнения требований, изложенных в подразделе 9.1 ИСО/МЭК 27001.

Настоящий стандарт охватывает:

- мониторинг и оценку деятельности по обеспечению ИБ;
- мониторинг и оценку результативности системы менеджмента информационной безопасности (СМИБ), включая ее процессы и средства контроля и управления;
- анализ и оценку результатов мониторинга и оценки защищенности.

Настоящий стандарт применим для всех организаций, независимо от типа или размера.

2 Нормативные ссылки

Настоящий стандарт не содержит нормативных ссылок.

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000.

С целью использования в своих стандартах международные организации ИСО и МЭК поддерживают терминологические базы данных:

- платформа ИСО для онлайн-просмотра: доступна по адресу http://www.iso.org/obp;
- платформа МЭК Электропедия (IEC Electropedia): доступна по адресу http://www.electropedia.org/.

4 Структура и обзор стандарта

Настоящий стандарт содержит следующие разделы:

- основные принципы — раздел 5;
- характеристики — раздел 6;
- типы показателей — раздел 7;
- процессы — раздел 8.

Порядок следования разделов обеспечивает простое сопоставление с требованиями, изложенными в подразделе 9.1 ИСО/МЭК 27001, как это показано на рисунке 1.

Издание официальное

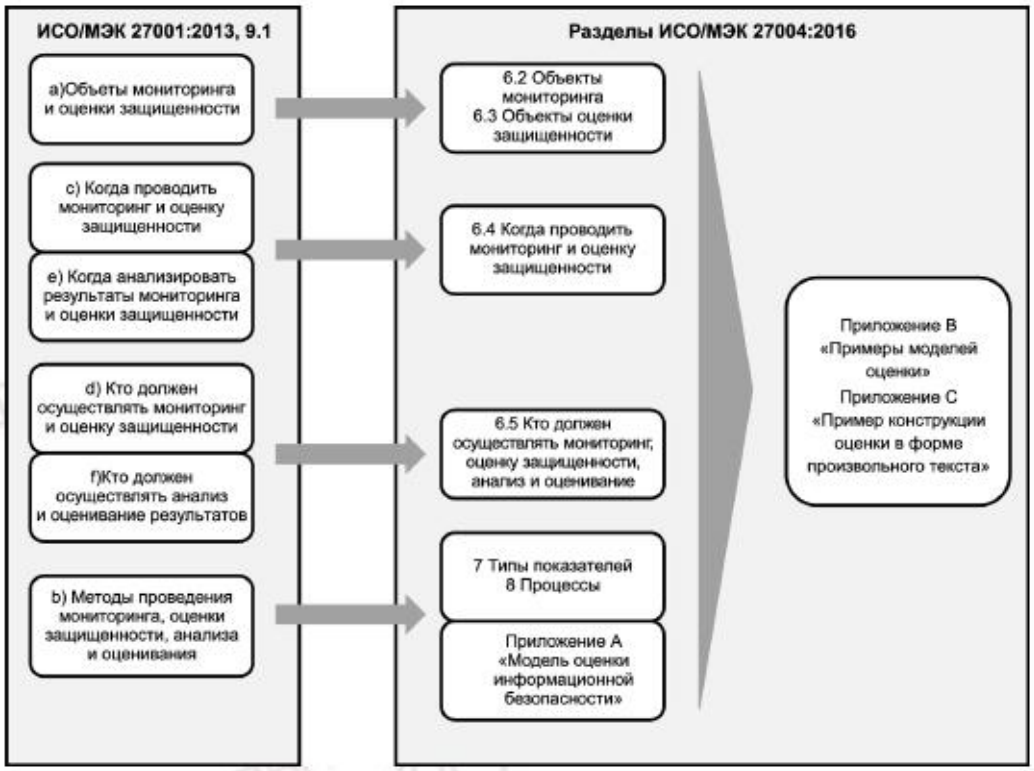

Рисунок 1 — Взаимосвязь положений настоящего стандарта и требований подраздела 9.1 ИСО/МЭК 27001

Для удовлетворения потребностей в информации организация определяет соответствующие средства, которые будут использоваться для их удовлетворения, после чего производится их мониторинг, оценка и анализ. По результатам анализа оценивается удовлетворение информационных потребностей организации.

В приложении А приведена как модель оценки защищенности, так и взаимосвязь компонентов модели оценки защищенности и требований подраздела 9.1 ИСО/МЭК 27001.

В приложении В представлен широкий спектр примеров спецификаций конструкций для оценки защищенности. Эти примеры обеспечивают организациям практическое руководство по осуществлению мониторинга, оценки защищенности, анализа и оценивания выбранных ими процессов СМИБ и области эффективности ИБ. В этих примерах используются шаблон, приведенный в таблице 1.

В приложении С представлен еще один пример спецификации конструкции для оценки эффективности с использованием альтернативного текстового формата свободной формы.

5 Основные принципы

5.1 Необходимость оценки защищенности

Основной целью СМИБ является обеспечение конфиденциальности, целостности и доступности информации в области ее применения. Существуют мероприятия СМИБ, которые касаются планирования того, как достигнуть этой цели, и реализации этих планов. Однако сами по себе эти действия не могут гарантировать, что реализация планов обеспечит достижение целей ИБ. Для проверки того, обеспечивают ли планы и действия по достижению целей ИБ выполнение требований к СМИБ, определенных в ИСО/МЭК 27001, и необходима оценка защищенности.

5.2 Выполнение требований ИСО/МЭК 27001

В подразделе 9.1 ИСО/МЭК 27001 от организации требуется оценка деятельности по обеспечению ИБ и результативности СМИБ. Показатели, способствующие выполнению этих требований, приводятся в разделе 7 настоящего стандарта.

В подразделе 9.1 ИСО/МЭК 27001 содержится требование к организации определять следующее:

- объекты мониторинга и оценки защищенности, включая процессы ИБ и средства контроля и управления;
- методы мониторинга, оценки защищенности, анализа и оценивания, обеспечивающие уверенность в достоверности результатов;
- когда проводить мониторинг и оценку защищенности;
- кто должен осуществлять мониторинг и оценку защищенности;
- когда анализировать и оценить результаты мониторинга и оценки защищенности;
- кто должен осуществлять анализ и оценивание этих результатов.

Связь этих требований с разделами настоящего стандарта показана на рисунке 1.

Также в подразделе 9.1 ИСО/МЭК 27001 содержится требование к организации хранить соответствующую документированную информацию в качестве свидетельства результатов мониторинга и оценки защищенности (см. 8.9).

Кроме того, в подраздел 9.1 ИСО/МЭК 27001 указано, что для того, чтобы результаты можно было считать достоверными, выбранные методы должны обеспечивать сопоставимые и воспроизводимые результаты, (см. 6.4).

5.3 Достоверность результатов

В целях обеспечения достоверности результатов (см. подраздел 9.1 перечисление b) ИСО/МЭК 27001) требуется, чтобы организация осуществила подбор методов оценки защищенности, мониторинга, анализа и оценивания. В вышеуказанном подразделе отмечено, что для обеспечения достоверности результаты должны быть сопоставимыми и воспроизводимыми. Для достижения этого организации должны собирать данные по показателям, анализировать их и составлять отчеты, принимая во внимание следующие моменты:

- для получения сопоставимых результатов показателей, полученных при мониторинге в различные моменты времени, важно гарантировать, что область действия и условия функционирования СМИБ неизменны;
- изменения в методах или технике, используемых для оценки защищенности и мониторинга, обычно приводят к несопоставимости результатов. Для проверки сохранения сопоставимости может потребоваться параллельное выполнение оценки с использованием оригинальных и модифицированных методов;
- если в состав методов или техники, используемых для оценки защищенности и мониторинга входят субъективные элементы, то для получения воспроизводимых результатов могут потребоваться дополнительные специфические действия. Например, результаты анкетирования должны оцениваться по определенным критериям;
- в некоторых ситуациях воспроизводимость может быть достигнута только при определенных обстоятельствах. Например, имеют место ситуации, когда результаты не воспроизводимы, однако они становятся достоверными при агрегировании.

5.4 Преимущества

Выполнение мероприятий и использование средств контроля и управления СМИБ, поддержание деятельности по обеспечению ИБ обеспечивают ряд организационных и финансовых преимуществ. При этом, мониторинг, оценка защищенности, анализ и оценивание могут обеспечить следующие основные преимущества:

- повышение прослеживаемости: повысить прослеживаемость ИБ: помогая идентифицировать ее определенные процессы или меры обеспечения ИБ, реализованные неправильно, не реализованные или неэффективные;
- повышение эффективности ИБ и процессов СМИБ: позволяют организациям количественно оценить улучшения защиты информации в рамках своей СМИБ и продемонстрировать количественный прогресс в достижении цели ИБ организации;

- доказательства соответствия требованиям: предоставляют документальное подтверждение выполнения требований ИСО/МЭК 27001 и других стандартов, а также требований применимых законов, правил и положений;

- поддержка принятия решений: поддерживают принятие решений, основанных на оценке риска, путем предоставления в процесс управления рисками количественной информации. Такая информация позволяет организациям оценивать успехи и неудачи прошлых и текущих инвестиций в информационную безопасность и предоставляет количественные данные, которые могут помочь при распределении ресурсов для будущих инвестиций.

6 Показатели

6.1 Общие положения

Мониторинг и оценка защищенности являются первыми шагами в процессе оценки деятельности по обеспечению ИБ и результативности СМИБ.

Учитывая то, что с ИБ связано большое количество объектов, каждый из которых, в свою очередь, характеризуется многообразием атрибутов, не всегда очевидно, по каким из атрибутов следует производить оценку. Проблема выбора атрибутов для оценки имеет решающее значение, поскольку оценка защищенности с использованием слишком большого количества атрибутов практически невозможна, а оценка по неправильно выбранным атрибутам приводит к неоправданным затратам и не продуктивна. При большем количестве атрибутов помимо очевидных затрат на оценку защищенности, анализ и отчетность, существует явная вероятность того, что ключевые проблемы могут затеряться в большом объеме информации или могут быть пропущены из-за отсутствия результатов по нужным показателям.

Для того, чтобы определить, мониторинг и оценку каких показателей следует производить, организация в первую очередь должна определить цель, которой она хочет достичь путем оценки деятельности по обеспечению ИБ и результативности СМИБ. Это позволяет организации определить свои информационные потребности.

Затем организация должна решить, какие оценки защищенности необходимо сделать для каждой конкретной информационной потребности и какие данные требуются для проведения необходимых оценок защищенности. Таким образом, оценки защищенности всегда должны соответствовать информационным потребностям организации.

6.2 Объекты мониторинга

Мониторинг позволяет определить результаты состояния защищенности системы, процесса, действия для обоснования управленческих решений по обеспечению их информационной безопасности.

Перечень систем, процессов и действий, которые могут подвергаться мониторингу, включает в себя, но не ограничивается следующим:

a) реализация процессов СМИБ;
b) менеджмент инцидентов;
c) менеджмент уязвимостей;
d) менеджмент конфигураций;
e) осведомленность о безопасности и обучение;
f) регистрация событий контроля доступа, брандмауэра и прочих;
g) аудит;
h) процесс оценки степени риска;
i) процесс обработки риска;
j) сторонний менеджмент рисков;
k) управление непрерывностью бизнеса;
l) управление физической и экологической безопасностью;
m) мониторинг системы.

Реализация мониторинга позволяет получать данные (журналы событий, пользовательские интервью, статистику обучения, информацию об инцидентах и т. д.), которые могут быть использованы для поддержки других мер обеспечения ИБ. Для получения вспомогательной информации в процессе определения атрибутов, подлежащих оценке защищенности, может потребоваться дополнительный мониторинг.

Следует обратить внимание на то, что мониторинг может позволить организации определить, имеет ли место тот или иной риск, и тем самым указать, какие действия можно предпринять для исключения такого риска. Кроме того, необходимо отметить, что определенные меры обеспечения ИБ могут быть ориентированы непосредственно на поддержку мониторинга. При использовании результатов оценки таких мер обеспечения ИБ для поддержки мониторинга организация должна гарантировать, что в процессе оценки учитывалось, когда были получены результаты: до или после того, как было предпринято какое-либо корректирующее действие.

6.3 Объекты оценки защищенности

В контексте ИБ оценка защищенности является действием, предпринятым для определения значения, состояния или тенденции в результативности или эффективности деятельности по обеспечению ИБ целью помочь идентифицировать потенциальные потребности в улучшениях. Любые процессы, действия, средства контроля и управления и группы средств контроля и управления СМИБ могут быть оценены.

В качестве примера, можно рассмотреть пункт c) подраздела 7.2 ИСО/МЭК 27001, который требует от организации возможных действий для приобретения необходимой компетентности. Организация может определить, все ли лица, которым требуется обучение, прошли его, и было ли обучение проведено в соответствии с планом. Результатом оценки защищенности может быть количество или процент обученных людей. Организация также может определить, действительно ли обученные лица приобрели и обладают необходимой компетентностью. Это может быть оценено путем анкетирования после обучения.

Что касается процессов СМИБ, то для организаций в ИСО/МЭК 27001 имеется ряд положений, которые непосредственно требуют определения эффективности конкретных видов действий. Например, в пункте d) подраздела 10.1 ИСО/МЭК 27001, содержится требование, чтобы организации «проверяли эффективность любых предпринятых корректирующих действий». Для подобного анализа эффективность корректирующих действий должна быть определена в первую очередь с помощью некоторого конкретного типа показателя. Для этого организация должна сначала определить соответствующую информационную потребность и показатель или показатели ее удовлетворения. Соответствующий процесс рассматривается в разделе 8.

Потенциальными кандидатами для оценки защищенности являются следующие процессы и действия СМИБ[1)]:

- планирование;
- руководство;
- менеджмент рисков;
- управление политикой;
- управление ресурсами;
- обмен информацией;
- анализ управления;
- документирование;
- мониторинг.

Что касается показателей ИБ, то наиболее очевидными кандидатами являются меры обеспечения ИБ организации или группы таких мер (или даже весь план обработки рисков). Такие меры обеспечения ИБ определяются в процессе обработки рисков и определены в ИСО/МЭК 27001 в качестве необходимых мер обеспечения ИБ. Ими могут быть как меры обеспечения ИБ, описанные в приложении А ИСО/МЭК 27001, так и специфичные для сектора меры обеспечения ИБ (например, как определено в других стандартах, таких как ИСО/МЭК 27010), меры обеспечения ИБ, определенные иными стандартами или меры обеспечения ИБ, разработанные организацией. Поскольку целью мер обеспечения ИБ является изменение степени риска, существует множество атрибутов, которые можно оценить, например:

j) степень снижения мерой обеспечения ИБ вероятности возникновения события безопасности;

k) степень уменьшения мерой обеспечения ИБ последствия события безопасности;

[1)] Дополнительными видами оценки защищенности, предусмотренными нормативными правовыми актами (НПА) Российской Федерации, являются: аттестация по требованиям ИБ и приемо-сдаточные испытания (Постановление правительства Российской Федерации № 330 от 15.05.2010 г., приказа ФСТЭК России № 239 от 25.12.2017 п. 12.7 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»).

l) частота событий безопасности, с которыми может справиться система управления до отказа;

m) сколько времени после возникновения события безопасности требуется, чтобы мера обеспечения ИБ обнаружила, что событие произошло.

6.4 Когда осуществлять мониторинг, оценку защищенности, анализ и оценивание

Организации должны определить конкретные временные рамки для мониторинга, оценки защищенности, анализа и оценивания на основе индивидуальных информационных потребностей, требуемых оценок защищенности и жизненного цикла данных для отдельных оценок защищенности. Оценки обеспечения информацией могут производиться чаще, чем анализ и представление результатов таких оценок защищенности заинтересованным сторонам. Например, несмотря на то, что данные об инцидентах безопасности могут собираться непрерывно, представление таких данных внешним заинтересованным сторонам должно основываться на конкретных требованиях, таких как серьезность (например, сообщение о нарушении требует немедленного уведомления) или суммирование значений (в случае обнаруженных и заблокированных нарушений).

До того, как приступить к анализу и оценке, организация должна иметь в виду, что для того, чтобы обеспечить содержательную основу для оценки и сравнения (например, для проведения статистического анализа) удовлетворения определенных информационных потребностей, необходимо собрать соответствующий объем данных. Кроме того, прежде чем результаты оценки защищенности могут быть представлены организации, процессы мониторинга, оценки защищенности, анализа и оценивания могут потребовать тестирования и тонкой настройки. Поэтому перед тем, как приступить к реальной задаче-оценке СМИБ, организация должна до начала анализа и оценки определить ограничение продолжительности любой точной настройки и продолжительность мониторинга и сбора данных.

По мере обновления деятельности по оценкам с учетом определенных изменений условий, перечисленных в 8.2, организация может корректировать время выполнения оценки защищенности. Например, если организация переходит от ручного сбора данных к автоматизированному, то может потребоваться изменение частоты сбора. Кроме того, для сравнения двух оценок защищенности, произведенных в разные моменты времени и, возможно, разными методами, но с целью удовлетворения одной и той же информационной потребности необходимо определить базовую линию.

Организация может решить объединить все свои действия по мониторингу, оценке защищенности, анализу и оцениванию в одну программу оценки. Однако следует отметить, что ИСО/МЭК 27001 не требует от организаций наличие такой программы.

6.5 Кто должен осуществлять мониторинг, оценку защищенности, анализ и оценивание

Организация (с учетом требований подразделов 9.1 и 5.3 ИСО/МЭК 27001) должна определить, кто осуществляет мониторинг, оценку защищенности анализ и оценивание с указанием конкретных лиц и ролей. Мониторинг, оценка защищенности, анализ и оценивание могут выполняться вручную или с помощью средств автоматизации. Независимо от того, выполняется ли оценка защищенности вручную или автоматизировано, организации могут определить следующие роли и обязанности, связанные с оценкой защищенности:

a) потребитель оценки защищенности — руководство или другие заинтересованные стороны, запрашивающее или затребовавшее информацию об результативности СМИБ, эффективности меры обеспечения ИБ или группы мер обеспечения ИБ;

b) планировщик оценки защищенности — лицо или организационная единица, определяющее структуру оценки защищенности, которое связывает оцениваемые атрибуты с конкретной информационной потребностью;

c) рецензент оценки — лицо или организационная единица, которое подтверждает, что разработанные структуры оценки защищенности подходят для оценки деятельности по обеспечению ИБ и результативности СМИБ, эффективности меры обеспечения ИБ или группы мер обеспечения ИБ;

d) владелец информации — лицо или организационная единица, которой принадлежит информация, используемая в качестве входной для оценки. Этот человек отвечает за предоставление данных, а также часто (но не всегда) отвечает за проведение оценки защищенности;

e) сборщик информации — лицо или организационная единица, ответственное за сбор, запись и хранение данных;

f) информационный аналитик — лицо или организационная единица, ответственное за анализ данных;

g) информационный коммуникатор — лицо или организационная единица, ответственное за распространение результатов анализа.

Организации могут объединять некоторые или, возможно, все эти роли.

Лицам, выполняющим разные роли и обязанности на протяжении всего процесса, потребуются различные навыки и соответствующие знания, а также может потребоваться обучение.

7 Типы показателей

7.1 Общие положения

Настоящее руководство выделяет два типа показателей выполнения запланированных действий и эффективности результатов, которые могут быть оценены:

a) показатели результативности — показатели, которые выражают запланированные результаты в терминах характеристик планируемой деятельности, таких как численность сотрудников, достижение этапа или степень, в которой были реализованы меры обеспечения ИБ;

b) показатели эффективности — показатели, отражающие влияние реализации запланированных мероприятий на цели ИБ организации.

Эти показатели могут быть специфическими для организации, поскольку каждая организация имеет свои конкретные цели, политики и требования в области ИБ.

Необходимо отметить, что термины «показатели результативности» и «показатели эффективности» не следует путать с требованием 9.1 ИСО/МЭК 27001 для оценки деятельности по обеспечению ИБ и результативности СМИБ.

7.2 Показатели деятельности по обеспечению ИБ

Показатели деятельности по обеспечению ИБ могут использоваться для демонстрации прогресса в реализации процессов СМИБ, связанных с ними процедур и конкретных мер обеспечения безопасности. Принимая во внимание, что результативность касается степени, в которой запланированные действия были реализованы и ожидаемые результаты достигнуты, показатели деятельности по обеспечению ИБ должны отражать степень, в которой были реализованы процессы и меры обеспечения ИБ. Эти показатели помогают определить, были ли процессы СМИБ и меры обеспечения ИБ реализованы в соответствии с планом.

Для оценки деятельности по обеспечению ИБ используются данные, которые можно получить из протоколов, журналов регистрации, планов проектов, инструментов автоматического сканирования и других широко используемых средств документирования, записи и мониторинга действий СМИБ.

Сбор, анализ и представление отчетов о показателях должны быть по возможности автоматизированы, чтобы снизить их стоимость, трудозатраты, а также вероятность человеческой ошибки.

Примеры:

1 При оценке в процентах степени реализации конкретного средства защиты информации, такого как шифрование жесткого диска ноутбуков результат оценки в начале, вероятно, будет менее 100 %. При достижении и сохранении результата на уровне 100 %, можно сделать вывод, что информационные системы полностью внедрили меры обеспечения ИБ, относящиеся к этому показателю, и оценки можно переориентировать на другие средства контроля и управления, требующие улучшения.

2 При внедрении новой СМИБ организация прежде всего должна стремиться к тому, чтобы высшее руководство присутствовало при проверке и на других возможных совещаниях. Запланированный (или предполагаемый) результат в этом случае — полное посещение всех собраний, за исключением болезней и разрешенного отсутствия по ранее взятым обязательствам. Показатель — это простое отношение количества присутствующих к количеству тех, кто должен присутствовать с возможной поправкой на отсутствовавших по уважительной причине. Сначала результат такой оценки может указывать на недостаточное посещение. Однако со временем результат должен достичь и оставаться близким к запланированной цели. На этом этапе организация должна начать концентрировать свои усилия по оценке показателей эффективности (см. 7.3).

После того, как большинство показателей деятельности по обеспечению ИБ достигнуты и остаются на уровне 100 %, организация должна начать сосредоточивать свои усилия на оценках показателей эффективности. Организации никогда не должны полностью отказываться от показателей деятельности по обеспечению ИБ, поскольку они могут быть полезны при определении конкретных мер обеспе-

чения ИБ, которые нуждаются в улучшении; однако со временем акцент и ресурсы, относящиеся к оценкам, должны сместиться с этих показателей на показатели эффективности (см. 7.3).

В соответствии с подразделом 9.1 ИСО/МЭК 27001 важно также оценивать результативность системы менеджмента (см. далее). Чтобы использовать СМИБ надлежащим образом, организации должны оценивать деятельность по обеспечению ИБ[1)] и результативность СМИБ через определенные планом промежутки времени.

7.3 Показатели эффективности

Показатели эффективности следует использовать для описания эффективности и влияния реализации плана обработки рисков СМИБ, процессов и средств контроля и управления СМИБ на цели ИБ организации. Эти показатели нужно использовать для определения того, работают ли процессы СМИБ и меры обеспечения ИБ так, как задумано, и достигают ли они желаемых результатов. В зависимости от целей для количественной оценки могут использоваться показатели эффективности, такие, как:

a) экономия средств, связанная с использованием СМИБ или за счет сокращения затрат на устранение последствий инцидентов ИБ;

b) повышение степени доверия клиентов из-за использования СМИБ;

c) достижение других целей ИБ.

Показатели эффективности могут быть сформированы путем объединения данных, полученных из инструментов автоматического мониторинга и оценки, с данными о функционировании СМИБ, полученными вручную. Это может потребовать мониторинга различных показателей по всей организации таким способом, который может быть напрямую связан с функционированием СМИБ и событиями безопасности. Чтобы достичь этого, организация должна обладать следующими возможностями:

d) с помощью показателей эффективности оценивать степень, в которой процессы, средства контроля и управления или группы средств управления СМИБ были реализованы;

e) получать данные из инструментов автоматического мониторинга и оценки;

f) вручную собирать данные о функционировании СМИБ;

g) нормализовать и анализировать данные, поступающие из множества автоматизированных и не автоматизированных источников;

h) интерпретировать эти данные и докладывать лицам, принимающим решения.

Такие показатели эффективности объединяют информацию о реализации плана обработки рисков с разнообразной информацией о ресурсах и могут обеспечить исходные данные для процесса менеджмента рисков. Они также могут предоставить непосредственное представление о ценности ИБ для организации и должны представлять наибольший интерес для высшего руководства.

Примеры:

3 Не секрет, что большая часть инцидентов ИБ происходит из-за использования известных уязвимостей. Чем больше число известных уязвимостей и чем дольше они не устранены, тем выше вероятность их использования соответствующими источниками угроз и тем больше подверженность риску. Показатель эффективности может помочь организации определить подверженность рискам, связанным с такими уязвимостями.

4 Учебный курс может иметь конкретные цели обучения для каждого отдельного элемента курса. Показатель эффективности может помочь организации определить, насколько каждый обучаемый понимает каждый урок и насколько он способен применить свои новые знания и навыки. Такие показатели обычно требуют нескольких совокупностей данных, таких как результаты тестов после обучения; изучение данных об инцидентах, связанных с темами обучения; или анализ обращений в службу поддержки, связанных с темами обучения.

8 Процессы

8.1 Общие положения

Мониторинг, оценка защищенности, анализ и оценивание, показанные на рисунке 2 состоят из следующих процессов:

а) выявление информационных потребностей;

б) спецификация и поддержка показателей;

[1)] В Российской Федерации деятельность по обеспечению ИБ является лицензируемой (см. пп. 1, 4, 5 ч. 1 ст. 12 от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»).

в) установка процедур;

г) мониторинг и оценка защищенности;

д) анализ результатов;

f) оценка деятельности по обеспечению ИБ и результативности СМИБ.

Кроме того, существует процесс управления СМИБ, который охватывает анализ и улучшение вышеуказанных процессов (см. 8.8).

Рисунок 2 — Процессы мониторинга, оценки защищенности, анализа и оценивания

8.2 Выявление информационных потребностей

Спецификацию показателей нужно начинать с определения информационных потребностей, которые в свою очередь могут помочь выяснить эксплуатационные характеристики и/или характеристики эффективности таких аспектов СМИБ, как:

a) потребности заинтересованных сторон;

b) стратегическое направление организации;

c) политика и цели информационной безопасности;

d) план обработки рисков.

Для определения соответствующих информационных потребностей необходимо выполнить следующие действия:

e) изучить СМИБ, ее процессы и такие элементы, как:

1) политика и цели информационной безопасности, меры обеспечения ИБ и их цели;

2) нормативно-правовые, договорные и организационные требования к информационной безопасности;

3) результаты процесса менеджмента рисков информационной безопасности.

f) определить приоритетность выявленных информационных потребностей на основе таких критериев, как:

1) приоритеты обработки рисков;

2) возможности и ресурсы организации;

3) потребности заинтересованных сторон;

4) политика и цели информационной безопасности, а также цели контроля;

5) информация, необходимая для выполнения организационных, правовых, нормативных и договорных обязательств;

6) ценность информации, которая должна быть получена относительно стоимости оценки защищенности;

g) выбрать из списка приоритетов те информационные потребности, которые должны быть охвачены оценками;

h) документировать и передать список выбранных информационных потребностей всем заинтересованным сторонам.

8.3 Спецификация и поддержка показателей

8.3.1 Общие положения

Организации должны специфицировать показатели один раз, а затем пересматривать и систематически обновлять эти показатели с запланированной периодичностью или в случаях, когда среда СМИБ претерпевает существенные изменения. Такие изменения могут включать, среди прочего:

a) изменение области применения СМИБ;

b) изменение организационной структуры;

c) изменения заинтересованных сторон, включая изменения ролей, обязанностей и полномочий заинтересованных сторон;

d) изменения бизнес-целей и требований;

e) изменения нормативно-правовых требований;

f) достижение желаемых и стабильных результатов в течение нескольких последовательных циклов;

g) внедрение или размещение технологий и систем обработки информации.

Спецификация или обновление таких показателей может включать, среди прочего, следующие шаги:

h) определить текущие практики безопасности, которые могут удовлетворить информационные потребности;

i) разработать или обновить показатели;

j) документировать показатели и определить приоритет реализации;

k) информировать и вовлекать в процесс руководство.

Ожидается, что обновление показателей потребует меньше времени и усилий, чем первоначальная спецификация.

8.3.2 Идентификация текущих методов безопасности, которые могут удовлетворить информационные потребности

Как только потребность организации в информации определена, необходимо в качестве потенциального компонента оценки защищенности рассмотреть существующие методы оценки защищенности и обеспечения безопасности. Существующие методы оценки защищенности и обеспечения и безопасности могут включать в себя оценки, связанные с:

a) менеджментом рисков;

b) управлением проектами;

c) отчетностью о соответствии;

d) политикой безопасности.

8.3.3 Спецификация или обновление показателей

Показатели должны отвечать информационным потребностям. Они могут базироваться на текущих методиках или требовать новых. Вновь определенные показатели могут также представлять собой адаптацию существующих показателей или процессов оценки защищенности. В любом случае, чтобы быть реализованными, новые показатели должны быть специфицированы достаточно подробно.

Примеры данных, которые могут быть собраны для формирования показателей безопасности:

a) выход различных логов и сканов;

b) статистические данные о подготовке кадров и других людских ресурсах;

c) соответствующие опросы и анкеты;

d) статистика инцидентов;

e) результаты внутренних аудитов;

f) результаты мероприятий по обеспечению непрерывности бизнеса/аварийному восстановлению.

g) отчеты о проверках со стороны руководства.

Эти и другие потенциальные источники данных, которые могут иметь как внутреннее, так и внешнее происхождение, должны быть изучены, а типы доступных данных должны быть определены.

Выбранные показатели должны соответствовать приоритетам информационных потребностей и могут учитывать:

h) простоту сбора данных;

i) доступность человеческих ресурсов для сбора и управления данными;

j) наличие соответствующих инструментов;

k) количество потенциально важных индикаторов эффективности, обеспечиваемых показателем;

l) простоту интерпретации;

m) количество потребителей полученных результатов оценки защищенности;

n) доказательства, подтверждающие соответствие показателей целям или информационным потребностям;

o) затраты на сбор, управление и анализ данных.

Организация должна документировать каждый показатель в форме, которая связывает показатель с соответствующей информационной потребностью (или потребностями) и предоставляет достаточную информацию о характеристиках, описывающих показатель, а также о том, как собирать, анализировать и отчитываться. Предлагаемые информационные показатели приведены в таблице 1.

Примеры в приложении В сформированы на основе шаблона, представленного в таблице 1. Два примера имеют дополнительную информационную строку, обозначенную как «действие», которое необходимо предпринять в случае, если цель не достигнута. Организации могут включать эту информационную строку, если они считают это полезным. Однако не существует универсального способа спецификации таких конструкций оценки, и в приложении С показан альтернативный подход в виде спецификации в свободной форме.

Следует отметить, что для удовлетворения потребностей разных клиентов оценки защищенности могут потребоваться разные показатели (см. таблицу 1), которые могут быть внутренними или внешними. Например, показатели удовлетворения потребностей в информации топ-менеджмента могут отличаться от подобных показателей для системного администратора. Каждая заинтересованная сторона может иметь свой конкретный диапазон, фокус, или степень детализации.

Каждый показатель должен соответствовать, по крайней мере, одной информационной потребности, но в тоже время одна информационная потребность может потребовать нескольких показателей.

Таблица 1 — Пример спецификации показателя безопасности

Информационный показатель	Значение или цель
Идентификатор показателя	Конкретный идентификатор
Информационная потребность	Доминирующая потребность в отношении данного показателя
Показатель оценки	Как описывается результат оценки защищенности, как правило, с использованием таких слов, как «процент», «число», «частота» и «среднее»
Формула/выигрыш	Как должен оцениваться показатель — формула или выигрыш
Цель	Желаемый результат оценки защищенности, например, этап или статистический показатель или набор пороговых значений. Обратите внимание, что для обеспечения непрерывного достижения цели может потребоваться постоянный мониторинг
Доказательство реализации	Доказательство, подтверждающее, что оценка защищенности выполнено, помогает определить возможные причины плохих результатов и обеспечивает входные данные для процесса. Данные для ввода в формулу
Частота	Как часто данные должны собираться и передаваться. В отдельных случаях может быть несколько частот
Ответственные стороны	Лицо, ответственное за сбор и обработку данных для показателя. По крайней мере, необходимо определить владельца информации, сборщика информации и потребителя оценки защищенности

Окончание таблицы 1

Информационный показатель	Значение или цель
Источник данных	Потенциальными источниками данных могут быть базы данных, инструменты мониторинга, другие подразделения организации, внешние организации или специфические конкретные должностные функции
Формат представления в отчете	Как показатель должен суммироваться и быть представлен в отчете, например, в виде текста, чисел, графически (круговая диаграмма, линейная диаграмма, гистограмма и т. д.), как часть «панели инструментов» или в другой форме представления

Очень важно определить показатели таким образом, чтобы единожды собранные данные могли быть использованы для различных целей. В идеале одни и те же данные должны использоваться для оценки различных мер обеспечения ИБ, отвечающих разным информационным потребностям различных заинтересованных сторон. Кроме того, следует отметить, что не всегда показатель, который легче всего оценить, будет наиболее значимым или наиболее актуальным.

Цели должны указывать желаемые конечные значения конкретных показателей для процессов и средств контроля и управления СМИБ, для достижения целей ИБ и результативности оцениваемой СМИБ.

Определение целей может оказаться проще, если имеются накопленные данные, относящиеся к специфицированным или выбранным показателям. Тенденции, наблюдаемые в прошлом, могут в некоторых случаях дать представление о результатах предыдущих оценок и могут подсказать направления для создания реалистичных целей. Тем не менее, организации должны иметь в виду, что определение целей без должного рассмотрения на основе того, что было достигнуто ранее или предыдущих результатов, может также вызвать «замораживание» текущего положения или даже препятствовать постоянному улучшению.

8.3.4 Документирование показателей и расстановка приоритетов для реализации

После определения требуемых показателей их спецификация должна быть документирована, а сами показатели должны быть расставлены по приоритетам для реализации оценки защищенности на основе приоритета каждой потребности в информации и возможности получения данных. Оценки деятельности по обеспечению ИБ должны быть реализованы в первую очередь, чтобы гарантировать, что процессы и средства контроля и управления СМИБ были введены в действие. Как только значения показателей деятельности по обеспечению ИБ достигают целевых значений, можно производить оценки показателей эффективности. О том, когда выполнять мониторинг и связанные с ним действия описано в 6.4.

8.3.5 Информирование и привлечение руководства

Для того, чтобы показатели отражали потребности руководства, к работам по спецификации показателей и реализации оценки защищенности необходимо привлечь управленческий персонал разного организационного уровня. Кроме того, руководство должно получать в удобном формате регулярные обновления для обеспечения гарантии того, что оно в должной степени информировано о деятельности по оценке безопасности в течение всего процесса разработки, реализации и использования показателей.

8.4 Последовательность действий

Для реализации определенных приоритетных оценок защищенности необходимы следующие последовательные действия:

a) заинтересованные стороны, участвующие в процессе оценки защищенности, должны быть информированы о действиях по оценке и об обоснованиях таких действий;

b) должны быть идентифицированы инструменты сбора и анализа данных и, при необходимости, модифицированы для эффективного и действенного сбора данных.

Организация должна установить процедуры сбора данных, анализа и отчетности по показателям, например:

c) сбор данных, включая безопасное хранение и проверку данных. Процедуры должны определять, как данные собираются, хранятся, проверяются и какая контекстная информация необходима для дальнейшей обработки. Проверка данных может быть выполнена с применением таких методов, как:

1) проверка нахождения значения в диапазоне возможных значений;

2) сверка со списком возможных значений;

3) сбор контекстной информации, такой, например, как время сбора данных.

d) анализ данных и подготовка отчетов по анализу мероприятий. Процедуры должны указывать методы анализа данных и периодичность предоставления отчетов о полученных значениях показателей;

e) подготовка отчетов, которые могут включать:

1) системы показателей для предоставления стратегической информации путем интеграции показателей деятельности по обеспечению ИБ высокого уровня;

Примечание — Их можно назвать «ключевыми показателями деятельности по обеспечению ИБ» (см. «Модель оценки ИБ» в приложении А).

2) исполнительные и операционные сводные графики, ориентированные на стратегические цели, а не на конкретные меры обеспечения ИБ и процессы;

3) различные форматы отчетов, начиная от простых, таких как список показателей за определенный период времени, и заканчивая более сложными отчетами с перекрестными ссылками, вложенными группировками, скользящими итогами и динамическими детализацией или связыванием. Отчеты могут быть более полезными в случае, если заинтересованным сторонам необходимо представить необработанные данные в удобном для чтения формате;

4) шаблоны для представления динамических значений, включая предупреждения, дополнительные графические элементы и маркировку конечных точек.

8.5 Мониторинг и оценка защищенности

Для мониторинга и оценки защищенности, а также для хранения и проверки данных должны быть определены процедуры, выполняемые либо вручную, либо автоматизировано. Проверка данных может быть выполнена путем сопоставления собранных данных с контрольными списками, чтобы убедиться, что влияние на анализ отсутствующих данных минимально и что значения либо верны, либо находятся в границах установленного диапазона. Чтобы обеспечить достоверность результатов анализа, необходимо собрать достаточное для анализа количество данных.

Организация должна собирать, анализировать, оценивать значения показателей и сообщать о них соответствующим заинтересованным сторонам с установленной периодичностью. При возникновении любого из условий, указанных в 8.3.1, организация должна рассмотреть возможность обновления процессов мониторинга, оценки защищенности, анализа и оценивания.

Прежде чем публиковать информацию в отчетах, информационных панелях и т. д., организация должна определить, каким образом и с кем она может делиться собранными данными и результатами, поскольку некоторые данные, связанные с ИБ, могут не подлежать разглашению по причине конфиденциальности.

Кроме того, для подтверждения того, что значения показателей собираются правильно, таким образом, чтобы они были повторяемыми, точными и непротиворечивыми, полезно иметь процесс проверки и оценки процесса сбора данных.

8.6 Анализ результатов

Собранные данные необходимо проанализировать относительно цели для каждого отдельного показателя. Руководство по проведению статистического анализа можно найти в ISO/TR 10017.

Результаты анализа данных должны быть интерпретированы. На основе результатов, анализирующий результаты (информационный аналитик), должен иметь возможность сделать некоторые первоначальные выводы. Однако, поскольку информационный аналитик может не принимать непосредственного участия в технических и управленческих процессах, то выводы должны быть рассмотрены другими заинтересованными сторонами. При интерпретации необходимо учитывать контекст показателей.

Анализ данных должен выявлять отличие ожидаемых результатов оценки защищенности от фактических результатов оценки внедренной СМИБ, средств контроля и управления или групп средств контроля и управления. Выявленные различия могут указывать на необходимость улучшения внедренной СМИБ, включая ее область применения, политику, цели, средства контроля и управления, процессы и процедуры.

8.7 Оценка деятельности по обеспечению информационной безопасности и результативности СМИБ

В соответствии с 5.2 организация должна:

а) определить свои информационные потребности с точки зрения вопросов, касающихся деятельности по обеспечению ИБ и результативности СМИБ организации;

б) с точки зрения этих информационных потребностей определить свои показатели.

Следовательно, анализ результатов мониторинга и оценки защищенности предоставляет данные, которые можно использовать для удовлетворения информационных потребностей (см. приложение А). Оценивание — это процесс интерпретации этих данных для ответа на вопросы о деятельности по обеспечению ИБ организации и результативности ее СМИБ.

8.8 Анализ и улучшения процессов мониторинга, оценки защищенности, анализа и оценивания

Процессы мониторинга, оценки защищенности, анализа и оценивания должны постоянно улучшаться с учетом потребностей СМИБ. Среди прочего действия по постоянному улучшению могут включать:

a) получение отзывов от заинтересованных сторон;

b) пересмотр методов сбора и анализа на основе извлеченных уроков и других отзывов;

c) пересмотр процедур реализации; а также

d) сравнительный анализ ИБ.

8.9 Хранение и передача документированной информации

Для выполнения требований подраздела 9.1 ИСО/МЭК 27001, в качестве доказательства мониторинга и оценки защищенности организация должна хранить документированную информацию. Организации могут самостоятельно решать, что хранить. Например, организация может документировать процессы и методы, используемые для анализа и оценки результатов.

Отчеты, которые используются при передаче результатов оценки защищенности соответствующим заинтересованным сторонам, должны быть подготовлены в должных форматах отчетности. Для обеспечения правильной интерпретации данных заключения анализа должны быть рассмотрены соответствующими заинтересованными сторонами. Для передачи заинтересованным сторонам результаты анализа данных также должны быть документированы.

Для передачи результатов оценок ИБ информационный коммуникатор должен определить:

а) какие результаты оценки защищенности следует передавать только внутри организации, а какие можно отправить наружу;

b) списки показателей, соответствующих отдельным заинтересованным сторонам и списки заинтересованных сторон;

c) конкретные результаты оценки защищенности, которые должны быть предоставлены, и тип представления, адаптированный к потребностям каждой группы;

d) средства получения обратной связи от заинтересованных сторон, которая будет использоваться для оценки полезности результатов оценки защищенности и эффективности оценки ИБ.

Приложение А
(справочное)

Модель оценки защищенности информационной безопасности

Информационная модель оценки защищенности, показанная на рисунке А.1, представлена и разъясняется в ИСО/МЭК 15939 и может применяться к СМИБ. Настоящий стандарт описывает, как атрибуты соответствующих объектов могут быть определены количественно и преобразованы в индикаторы, которые обеспечивают основу для принятия решений. Модель представляет собой структуру, которая отражает связи информационных потребностей с соответствующими объектами и представляющими интерес атрибутами.

Информационная потребность может определяться, например, степенью информированности сотрудников о политике информационной безопасности. Объекты включают в себя процессы, элементы контроля и управления, документированную информацию, системы, устройства, персонал и ресурсы. Примерами соответствующих объектов в СМИБ являются: процесс управления рисками, процесс аудита, классификация информации, управление правами доступа, политика информационной безопасности, политика мобильных устройств, оконечный компьютер, администратор и сотрудник.

Информационная модель оценки защищенности помогает понять, что планировщик оценки защищенности должен определить во время мониторинга, оценки защищенности, анализа и оценивания.

В подразделе 9.1 ИСО/МЭК 27001 содержится требование к организации оценивать деятельность по обеспечению ИБ и результативность СМИБ. Зачастую такая оценка включает в себя определение перечня показателей, из которого, в зависимости от значимости и важности показателей для целей организации, можно выделить ключевые показатели эффективности (KPI, иногда называемые также «ключевыми показателями успеха»).

Для определения таких показателей организация может определить базовые показатели и, используя функцию оценки защищенности, которая объединяет два или более базовых показателей, получить из них ключевой показатель.

Модель оценки защищенности в этом приложении (с использованием базового показателя, производного показателя, индикатора эффективности и результата оценки защищенности) является примером подхода к выполнению требований СМИБ к оценке защищенности. Есть и другие точки зрения на процессы оценки защищенности, анализа и оценивания.

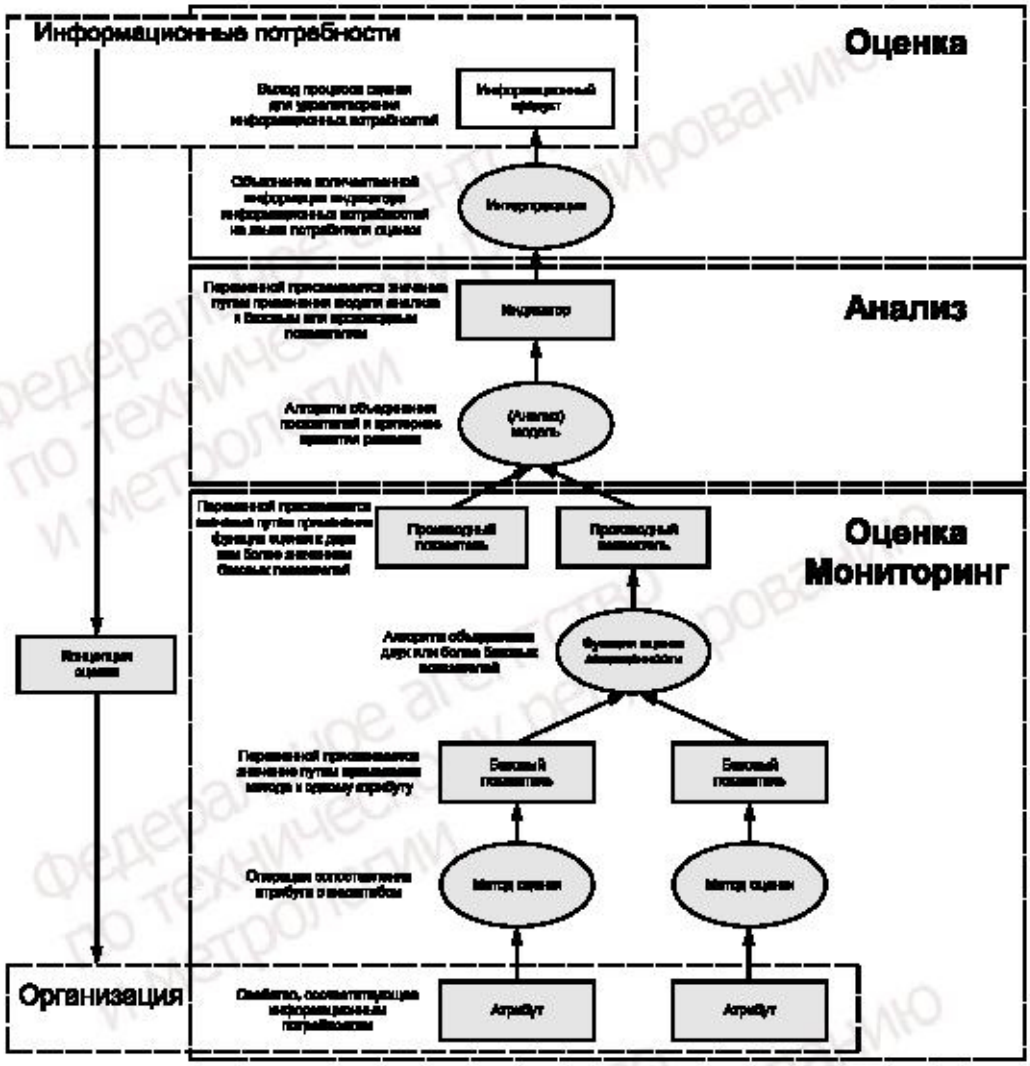

Рисунок А.1 — Ключевые отношения в информационной модели оценки

Приложение В
(справочное)

Примеры спецификаций конструкций оценки защищенности

В.1 Общие положения

Примеры в приложении В соответствуют принципам, изложенным в настоящем стандарте. В приведенной ниже таблице примерам спецификаций конструкций оценки защищенности сопоставлены конкретные пункты ИСО/МЭК 27001 или номера мер обеспечения информационной безопасности, приведенные в его приложении А.

Связанные процессы СМИБ и меры обеспечения ИБ (номер раздела или номер меры обеспечения ИБ в ИСО/МЭК 27001)	Название конструкции оценки защищенности
5.1, 7.1	В.2 Распределение ресурсов
7.5.2, А.5.1.2	В.3 Пересмотр политик
5.1, 9.3	В.4 Обязательства руководства
8.2, 8.3	В.5 Подверженность рискам
9.2, А.18.2.1	В.6 Программа аудита
10	В.7 Действия по улучшению
10	В.8 Стоимость инцидентов безопасности
10, А.16.1.6	В.9 Анализ инцидентов информационной безопасности
10.1	В.10 Реализация корректирующих действий
А.7.2	В.11 Обучение СМИБ или ознакомление с СМИБ
А.7.2.2	В.12 Обучение информационной безопасности
А.7.2.1, А.7.2.2	В.13 Согласие с политикой информационной безопасности
А.7.2.2	В.14 Эффективность информационно-просветительских кампаний СМИБ
А.7.2.2, А.9.3.1, А.16.1	В.15 Подготовленность к социальной инженерии
А.9.3.1	В.16 Качество паролей, задаваемых вручную
А.9.3.1	В.17 Качество паролей, задаваемых автоматизировано
А.9.2.5	В.18 Пересмотр прав доступа пользователя
А.11.1.2	В.19 Оценка системы контроля физического доступа
А.11.1.2	В.20 Эффективность контроля физического доступа
А.11.2.4	В.21 Управление периодическим техническим обслуживанием
А.12.1.2	В.22 Управление изменениями
А.12.2.1	В.23 Защита от вредоносного кода
А.12.2.1	В.24 Антивирус
А.12.2.1, А.17.2.1	В.25 Общая доступность
А.12.2.1, А.13.1.3	В.26 Правила брандмауэра
А.12.4.1	В.27 Анализ файлов журналов
А.12.6.1	В.28 Конфигурация устройств
А.12.6.1, А.18.2.3	В.29 Тестирования на проникновение и оценка уязвимости

Окончание

Связанные процессы СМИБ и меры обеспечения ИБ (номер раздела или номер меры обеспечения ИБ в ИСО/МЭК 27001)	Название конструкции оценки защищенности
A.12.6.1	B.30 Уровень уязвимости организации
A.15.1.2	B.31.1/B.31.2 Безопасность в сторонних соглашениях
A.16	B.32 Эффективность менеджмента инцидентов информационной безопасности
A.16.1	B.33 Тенденция инцидентов безопасности
A 16.1.3	B.34 Регистрация событий безопасности
A.18.2.1	B.35 Процесс анализа СМИБ
A.18.2.3	B.36 Устранение уязвимостей

Для каждого примера приводится ссылка на соответствующий раздел или номер цели контроля и управления в ИСО/МЭК 27001. Кроме того, для двух примеров (B.20 и B.28) приводится дополнительный пункт, обозначенный как «действие». Он определяет действие, которое необходимо предпринять в случае, если цель не достигнута. Организации могут включать этот информационный пункт по желанию, если считают его полезным. Однако, не существует единого способа определения спецификаций таких конструкции, и приложение С демонстрирует альтернативное определение в произвольной форме.

B.2 Распределение ресурсов

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Количественная оценка ресурсов, выделяемых на информационную безопасность, по сравнению с первоначальным бюджетом
Показатель оценки	Распределение ресурсов, выделяемых на информационную безопасность (внутренний персонал, персонал по контракту, оборудование, программное обеспечение, услуги) в рамках годового бюджета
Формула/выигрыш	Выделенные ресурсы/использованные ресурсы в течение запланированного периода времени
Цель	1
Доказательство реализации	Мониторинг ресурсов информационной безопасности
Частота	Ежегодно
Ответственные стороны	Владелец информации: менеджер по информационной безопасности Сборщик информации: менеджер по информационной безопасности Заказчик информации: совет директоров
Источник данных	Бюджет информационной безопасности Эффективные расходы на информационную безопасность Отчеты об использовании ресурсов информационной безопасности
Формат представления в отчете	Лепестковая диаграмма с категорией ресурса на каждой оси и двойной индикацией выделенных и используемых ресурсов

См.: ИСО/МЭК 27001:2013, 5.1: Обязанности высшего руководства
ИСО/МЭК 27001:2013, 7.1: Ресурсы

B.3 Пересмотр политик

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Чтобы оценить, пересматриваются ли через запланированные промежутки времени политики информационной безопасности или производятся значительные изменения
Показатель оценки	Процентная доля пересмотренной политики
Формула/выигрыш	(Количество политик информационной безопасности, которые были рассмотрены в предыдущем году)/(Количество действующих политик информационной безопасности) × 100
Цель	Зеленый уровень: > 80 %, Оранжевый > = 40 %, Красный < 40 %
Доказательство реализации	История редакции документа с указанием пересмотра документа или списка документов с указанием даты последнего пересмотра
Частота	Сбор данных: в соответствии с запланированным интервалом пересмотра (например, ежегодно или после значительных изменений) Отчет: после каждого сбора данных
Ответственные стороны	Владелец информации: владелец политики, который утвердил ответственность руководства за разработку, проверку и оценку политики Сборщик информации: внутренний аудитор Потребитель оценки защищенности: главный специалист по информационной безопасности
Источник данных	Обзор плана политик, история политики безопасности, список документов
Формат представления в отчете	Круговая диаграмма для текущей ситуации и линейная диаграмма для представления эволюции соответствия

См.: ИСО/МЭК 27001:2013, A.5.1.2: Пересмотр политик информационной безопасности
ИСО/МЭК 27001:2013, 7.5.2: Создание и обновление документированной информации

B.4 Обязательства руководства

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить обязательства и действия руководства по анализу информационной безопасности в отношении действий проверки со стороны руководства
Показатель оценки	Проведенные на сегодняшний день совещания руководства по анализу; средний уровень участия руководства в совещаниях по анализу на сегодняшний день
Формула/выигрыш	Разделите [проведенные совещания по рассмотрению руководством] на [запланированные совещания по рассмотрению руководством]; Рассчитайте среднее значение и стандартное отклонение всех показателей участия в совещаниях руководства
Цель	Показатель a): для вывода о достижении цели значение показателя должно быть от 0,7 до 1,1. В этом случае никаких действий не требуется. Даже если он снижается, для констатации успеха он должен быть больше 0,5; Показатель b): вычисленные доверительные интервалы, основанные на стандартном отклонении, указывают на вероятность достижения фактического результата, близкого к среднему уровню участия. Очень большой доверительный интервал предполагает потенциально большие усилия и необходимость планирования на случай непредвиденных обстоятельств для решения проблемы

Окончание

Информационный показатель	Значение или цель
Доказательство реализации	Для встреч по анализу управления необходимо: 1.1 Подсчитать количество встреч, запланированных на сегодняшний день; 1.2 Для каждой встречи по состоянию на сегодняшний день подсчитать количество менеджеров, планировавших участвовать и добавить новую строчку со значением по умолчанию для незапланированных спонтанных собраний; 2.1.1 Подсчитать запланированные встречи на сегодняшний день; 2.1.2 Подсчитать не запланированные встречи, проведенные до настоящего времени; 2.1.3 Подсчитать перенесенные собрания, проведенные до настоящего времени; 2.2 Для всех проведенных собраний подсчитать количество принимавших участие менеджеров
Частота	Сбор данных: ежемесячно; анализ: Ежеквартально; отчет: ежеквартально; пересмотр оценки защищенности: пересматривать и обновлять каждые 2 года; период оценки защищенности: применимо 2 года
Ответственные стороны	Владелец информации: менеджер системы качества (при условии объединенной системы управления СМК и СМИБ); сборщик информации: менеджер по качеству; менеджер по информационной безопасности; потребитель оценки защищенности: руководители, отвечающие за СМИБ; менеджер системы качества
Источник данных	План/график анализа управления информационной безопасностью; обзоры и протоколы встреч менеджмента по анализу управления
Формат представления в отчете	Линейная диаграмма, отображающая индикатор с критериями для нескольких периодов сбора данных и отчетности с отчетом о результатах оценки защищенности. Количество периодов сбора данных и отчетных периодов должно быть определено организацией

См.: ИСО/МЭК 27001:2013, 9.3: Проверка со стороны руководства
ИСО/МЭК 27001:2013, 5.1: Обязанности высшего руководства

B.5 Подверженность рискам

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценка подверженности организации рискам информационной безопасности
Показатель оценки	Высокие и средние риски за пределами допустимого порога; своевременный анализ высоких и средних рисков
Формула/выигрыш	Должен быть определен порог для высоких и средних рисков, а в случае превышения порога ответственные стороны должны уведомляться; количество рисков без обновления статуса
Цель	1
Доказательство реализации	Обновленный реестр рисков
Частота	Сбор данных: минимум ежеквартально; отчет: каждый квартал

Окончание

Информационный показатель	Значение или цель
Ответственные стороны	Владелец информации: сотрудники службы безопасности; сборщик информации: сотрудники службы безопасности
Источник данных	Реестр информационных рисков
Формат представления в отчете	Тенденция высоких рисков; тенденция принятых высоких и средних рисков

См.: ИСО/МЭК 27001:2013, 8.2: Оценка рисков информационной безопасности
ИСО/МЭК 27001:2013, 8.3: Обработка рисков информационной безопасности

В.6 Программа аудита

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Полнота программы аудита
Показатель оценки	Общее количество выполненных проверок по сравнению с общим количеством запланированных проверок
Формула/выигрыш	(Общее количество выполненных проверок)/(Общее количество запланированных проверок) × 100
Цель	> 95 %
Доказательство реализации	Мониторинг программы аудита и связанных с ней отчетов
Частота	Ежегодно
Ответственные стороны	Владелец информации: Менеджер по аудиту; сборщик информации: Менеджер по аудиту; потребитель оценки защищенности: Высшее руководство
Источник данных	Программа аудита и аудиторские отчеты
Формат представления в отчете	Диаграмма тенденций, связывающая соотношение выполненных и запланированных аудитов для каждого года выборки

См.: ИСО/МЭК 27001:2013, 9.2: Внутренний аудит
ИСО/МЭК 27001:2013, А.18.2.1: Независимая проверка информационной безопасности

В.7 Действия по улучшению

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Проверить состояние мероприятий по улучшению и управление ими в соответствии с планами
Показатель оценки	Процент действий по расписанию, затратам и качеству (то есть по требованиям) по отношению ко всем запланированным действиям; На начало периода действия должны быть запланированными (то есть быть готовыми к выполнению и выполняемыми)

Окончание

Информационный показатель	Значение или цель
Формула/выигрыш	[(Действия по расписанию, затраты и качество)/(Количество действий)] × 100
Цель	90 %
Доказательство реализации	Мониторинг состояния каждого действия
Частота	Ежеквартально
Ответственные стороны	Владелец информации: отдел управления проектами; сборщик информации: отдел управления проектами; потребитель оценки защищенности: менеджер по информационной безопасности
Источник данных	Соответствующие планы проекта
Формат представления в отчете	Список всех соответствующих действий и их статус (фактическое время, затраты и прогноз качества по сравнению с запланированными) с процентным соотношением действий по расписанию, затрат и качества к соответствующему количеству действий в заданный период времени

См.: ИСО/МЭК 27001:2013, раздел 10: Усовершенствование

Примечание — Обратите внимание, что показатель может быть улучшен путем присвоения каждому действию весового коэффициента с учетом их критичности (например, действий, направленных на высокие риски).

Список всех соответствующих действий должен быть дополнен синтезированным результатом так, чтобы большое количество некритических действий не скрывало сравнительно малое количество критических действий.

B.8 Стоимость инцидента безопасности

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Соображения о затратах, связанных с недостатками информационной безопасности
Показатель оценки	Сумма затрат на каждый инцидент информационной безопасности, произошедший в период выборки
Формула/выигрыш	Сумма (затраты на каждый инцидент информационной безопасности)
Цель	Менее приемлемого порога, определенного организацией
Доказательство реализации	Систематический сбор сведений о затратах на каждый инцидент информационной безопасности
Частота	Ежеквартально
Ответственные стороны	Владелец информации: группа реагирования на инциденты компьютерной безопасности; сборщик информации: менеджер по информационной безопасности; потребитель оценки защищенности: высшее руководство
Источник данных	Сообщения об инциденте
Формат представления в отчете	Столбчатая диаграмма, показывающая стоимость инцидентов информационной безопасности для этого и предыдущих периодов выборки. Она может сопровождаться следующими деталями: - средняя стоимость каждого инцидента информационной безопасности; - средняя стоимость каждого инцидента информационной безопасности для каждой категории инцидентов информационной безопасности (категории должны быть предварительно определены)

См.: ИСО/МЭК 27001:2013, A.10: Усовершенствование

B.9 Анализ инцидентов информационной безопасности

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Убедиться, что инциденты безопасности вызывают действия для улучшения текущей ситуации безопасности
Показатель оценки	Количество инцидентов безопасности, которые инициируют действия по улучшению информационной безопасности
Формула/выигрыш	(Количество инцидентов безопасности, которые вызвали действия)/(Количество инцидентов безопасности)
Цель	Значение должно быть выше порога, определенного организацией
Доказательство реализации	План действий со ссылкой на инциденты безопасности
Частота	Сбор данных: ежеквартально; отчет: каждое полугодие
Ответственные стороны	Владелец информации: группа реагирования на инциденты компьютерной безопасности; сборщик информации: менеджер по информационной безопасности; потребитель оценки защищенности: менеджер по информационной безопасности
Источник данных	Сообщения о происшествии
Формат представления в отчете	Столбчатая диаграмма, показывающая стоимость инцидентов информационной безопасности для этого и предыдущих периодов выборки. Она может сопровождаться следующими деталями: - средняя стоимость каждого инцидента информационной безопасности; - средняя стоимость каждого инцидента информационной безопасности для каждой категории инцидентов информационной безопасности (категории должны быть предварительно определены)

См.: ИСО/МЭК 27001:2013,10: Усовершенствование
ИСО/МЭК 27001:2013, A.16.1.6: Анализ инцидентов информационной безопасности

B.10 Реализация корректирующих действий

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить эффективность реализации корректирующего действия
Показатель оценки	a) статус в виде доли не выполненных корректирующих действий; b) статус в виде доли корректирующих действий, не реализованных без причины; c) тенденция статуса
Формула/выигрыш	Разделить [Число корректирующих действий, не реализованных до настоящего времени] на [Число корректирующих действий, запланированных до настоящего времени]; разделить [Число корректирующих действий, не реализованных без причины] на [Число корректирующих действий, запланированных до настоящего времени]; сравнить состояния с предыдущими состояниями

Окончание

Информационный показатель	Значение или цель
Цель	Чтобы сделать вывод о достижении цели и отсутствии необходимых действий, значения индикатора a) и b) должны иметь значения между 0,4 и 0,0 и между 0,2 и 0,0 соответственно, а тенденция (индикатор c)) должна снижаться для последних 2 отчетных периодов. Показатель c) должен быть представлен в сравнении с предыдущими показателями для того, чтобы была понятна тенденция реализации корректирующих действий
Доказательство реализации	1. Подсчет корректирующих действий, запланированных к настоящему времени 2. Подсчет корректирующих действий, отмеченных как выполненные в срок 3. Подсчет запланированных корректирующих действий, отмеченных как не выполненные с указанием причины
Частота	Сбор данных: ежеквартально Анализ: ежеквартально Отчет: ежеквартально Пересмотр оценки защищенности: ежегодный анализ Периодичность оценки защищенности: применимо 1 год
Ответственные стороны	Владелец информации: менеджеры, ответственные за СМИБ Сборщик информации: менеджеры, ответственные за СМИБ Потребитель оценки защищенности: менеджеры, ответственные за СМИБ; менеджер по информационной безопасности
Источник данных	Отчеты по корректирующим действиям
Формат представления в отчете	Гистограмма с накоплением отчетов о результатах оценки защищенности, включая краткое изложение выводов и возможных действий руководства, которая отображает общее количество корректирующих действий, с разделением на выполненные, не выполненные без уважительной причины и не выполненные по уважительной причине

См.: ИСО/МЭК 27001:2013, подраздел 10.1: Выявление несоответствий и корректирующие действия

B.11 Обучение СМИБ или осведомленность о СМИБ

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить, сколько сотрудников прошли тренинги по повышению осведомленности о СМИБ и установить контроль соответствия политике информационной безопасности организации
Показатель оценки	Процент сотрудников, принявших участие в тренинге по повышению осведомленности о СМИБ
Формула/выигрыш	I1 = [(Количество сотрудников, прошедших обучение по СМИБ)/(количество сотрудников, которые должны пройти обучение по СМИБ)] × 100; I2 = [(Количество сотрудников, которые возобновили обучение в СМИБ в прошлом году)/(количество сотрудников в области)] × 100
Цель	Зеленый уровень: если I1 > 90 и I2 > 50 % Желтый уровень: если I1 > 60% и I2 > 30 % Красный уровень: в остальных случаях Красный уровень — требуется вмешательство, необходимо провести анализ причин, чтобы определить причины несоответствия и слабых показателей Желтый уровень — следует внимательно следить за индикаторами на предмет возможного сползания к красному уровню Зеленый уровень — никаких действий не требуется

Окончание

Информационный показатель	Значение или цель
Доказательство реализации	Списки участия всего обучения осведомленности; количество журналов/реестров с заполнителем поля/строки обучения СМИБ как «Полученный»
Частота	Сбор данных: ежемесячно, в первый рабочий день месяца Анализ: ежеквартально Отчет: ежеквартально Пересмотр оценки защищенности: ежегодный анализ Периодичность оценки защищенности: ежегодно
Ответственные стороны	Владелец информации: Менеджер по обучению — Управление персоналом Сборщик информации: Менеджер по обучению — Отдел кадров Потребитель оценки защищенности: руководители, отвечающие за СМИБ, главный специалист по информационной безопасности
Источник данных	База данных сотрудников, учебные записи, список участников тренингов по повышению квалификации
Формат представления в отчете	Гистограмма с цветовой кодировкой столбцов в зависимости от цели. Краткое описание того, что означает показатель, и возможные меры управления должны прилагаться к гистограмме; Круговая диаграмма текущей ситуации и линейная диаграмма для представления эволюции соответствия

См.: ИСО/МЭК 27001:2013, 7.2: Квалификация.

B.12 Обучение информационной безопасности

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить соответствие требованиям ежегодного обучения информационной безопасности
Показатель оценки	Процент персонала, прошедшего ежегодное обучение информационной безопасности
Формула/выигрыш	[(Число сотрудников, прошедших ежегодную подготовку по повышению осведомленности в области информационной безопасности)/(Число сотрудников, которым необходимо пройти ежегодную подготовку по повышению осведомленности в области информационной безопасности)] × 100
Цель	0—60 % — Красный уровень; 60—90 % — Желтый уровень; 90—100 %-ный Зеленый уровень В случае желтого уровня, если за квартал прирост не превышает по крайней мере 10 %, уровень является автоматически красным. Красный уровень — требуется вмешательство, необходимо провести анализ причин, чтобы определить причины несоответствия и слабых показателей Желтый уровень — следует внимательно следить за индикатором на предмет возможного сползания к красному уровню Зеленый уровень — никаких действий не требуется
Доказательство реализации	Подсчет строк «Получено» в журналах/реестрах ежегодного обучения по повышению осведомленности в области информационной безопасности

Окончание

Информационный показатель	Значение или цель
Частота	Сбор данных: ежемесячно, в первый рабочий день месяца Анализ: ежеквартально Отчет: ежеквартально Пересмотр оценки защищенности: ежегодный анализ Период оценки защищенности: ежегодно
Ответственные стороны	Владелец информации: Директор по информационной безопасности и Менеджер по обучению Сборщик информации: Менеджер по обучению — Отдел кадров Потребитель оценки защищенности: руководители, отвечающие за СМИБ, главный специалист по информационной безопасности, учебное управление
Источник данных	База данных сотрудников, учебные записи
Формат представления в отчете	Гистограмма с цветовой кодировкой столбцов в зависимости от цели. Краткое описание того, что означает показатель, и возможные меры управления должны прилагаться к гистограмме

См.: ИСО/МЭК 27001:2013, А.7.2.2: Осведомленность, обучение и практическая подготовка (тренинги) в области информационной безопасности

B.13 Согласие с политикой информационной безопасности

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оцените состояние согласия соответствующего персонала с организационной политикой безопасности
Показатель оценки	Прогресс до настоящего времени; прогресс до настоящего времени с подписанием
Формула/выигрыш	Получить «прогресс на сегодняшний день», добавив всех подписавших сотрудников к запланированным подписать к сегодняшнему дню; получить «прогресс на сегодняшний день с подписанием» делением числа, подписавших на сегодняшний день, на число, запланированных подписать к сегодняшнему дню а) Вычислить [(прогресс на сегодняшний день)/(количество сотрудников запланированных подписать на сегодняшний день × 100)]/(прогресс на сегодняшний день с подписанием) б) Сравнить статус с предыдущими статусами
Цель	Для достижения цели управления полученные значения должны лежать для а) между 0,9 и 1.1, а для b) между 0,99 и 1.01. В таком случае не требуется каких-либо действий; тенденция должна быть восходящей или стабильной
Доказательство реализации	1.1. План/график обучения по информационной безопасности: персонал, указанный в плане 1.2. Персонал, который завершил или находится в процессе обучения: статус персонала в отношении обучения 2.1. План/график подписания соглашений: персонал, указанный в плане подписания 2.2. Персонал, подписавший соглашения: статус персонала в отношении подписания соглашений

Окончание

Информационный показатель	Значение или цель
Частота	Сбор данных: Ежемесячно, первый рабочий день месяца Анализ: ежеквартально Отчет: ежеквартально Пересмотр оценки защищенности: ежегодный анализ Период оценки защищенности: ежегодный
Ответственные стороны	Владелец информации: сотрудник по информационной безопасности и менеджер по обучению Сборщик информации: менеджер по обучению; отдел кадров Потребитель оценки защищенности: руководители, отвечающие за СМИБ; управление безопасности, управление обучением
Источник данных	1.1. План/график обучения по информационной безопасности: персонал, указанный в плане 1.2. Персонал, который завершил или находится в процессе обучения: статус персонала в отношении обучения 2.1. План/график подписания соглашений: персонал, указанный в плане подписания 2.2. Персонал, подписавший соглашения: статус персонала в отношении подписания соглашений
Формат представления в отчете	Стандартный шрифт = Критерии выполнены удовлетворительно Курсив Шрифт = Критерии выполнены неудовлетворительно Жирный шрифт = Критерии не выполнены

См.: ИСО/МЭК 27001:2013, А.7.2.2: Осведомленность, обучение и практическая подготовка (тренинги) в области информационной безопасности

ИСО/МЭК 27001:2013, А.7.2.1: Обязанности руководства

В.14 Эффективность информационно-просветительских кампаний СМИБ

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить, насколько сотрудники усвоили содержание информационно-просветительской кампании
Показатель оценки	Процент сотрудников, проходящих тест знаний до и после информационно-просветительской кампании СМИБ
Формула/выигрыш	Выберите определенное количество сотрудников, на которых была рассчитана кампания по повышению уровня осведомленности, и дайте им возможность пройти короткий тест на знания по темам этой кампании. Процент людей, прошедших тест
Цель	Зеленый уровень: 90—100 % людей прошли тест; Оранжевый уровень: 60—90 % людей прошли тест; Красный уровень: < 60 % людей прошли тест
Доказательство реализации	Документы/информация информационной кампании обеспечили для сотрудников; список сотрудников, следовавших за информационной кампанией; тесты знаний
Частота	Сбор данных: через один месяц после информационной кампании Отчет: для каждой кампании
Ответственные стороны	Владелец информации: Отдел кадров; сборщик информации: Отдел кадров; потребитель оценки защищенности: менеджер по информационной безопасности

Окончание

Информационный показатель	Значение или цель
Источник данных	База данных персонала, информация об просветительской кампании, результаты испытаний знаний
Формат представления в отчете	Круговая диаграмма для представления процента сотрудников, прошедших тестирование, и линейная диаграмма для представления эволюции, если для конкретной темы было организовано дополнительное обучение

См.: ИСО/МЭК 27001:2013, A.7.2.2: Осведомленность, обучение и практическая подготовка (тренинги) в области информационной безопасности

B.15 Подготовленность к социальной инженерии

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить, подготовлен ли штат для правильной реакции на некоторые случаи атак социальной инженерии
Показатель оценки	Процент персонала, который правильно отреагировал на тест, например, кто не нажимал на ссылку в тесте, состоящем в отправке фишингового электронного письма отобранным сотрудникам
Формула/выигрыш	a = (Количество сотрудников, кликнувших по ссылке)/(количество сотрудников, участвующих в тесте); b = 1 – (Количество сотрудников, сообщивших об опасном электронном письме по соответствующим каналам); c = (Количество сотрудников, которые следовали инструкциям, полученным при нажатии на ссылку, т. е. начали вводить пароль)/(количество сотрудников, участвующих в тесте); d = соответствующая взвешенная сумма вышеперечисленных величин в зависимости от характера теста
Цель	d: 0—60: Красный уровень; 60—80: Желтый уровень; 90—100: Зеленый уровень
Доказательство реализации	Подсчет активности на имитируемой команде и элементе управления, указанных по ссылке. Позаботьтесь о соблюдении аспектов конфиденциальности персонала и анонимности данных, чтобы участники теста не боялись негативных последствий этого теста
Частота	Сбор данных: ежемесячно — ежегодно, в зависимости от критичности атак социальной инженерии; отчет: для каждого набора персонала
Ответственные стороны	Владелец информации: главный специалист по информационной безопасности; сборщик информации: офицер ИТ-безопасности, обученный уважению аспектов конфиденциальности; потребитель оценки защищенности: владелец риска
Источник данных	Список сотрудников или пользователей данной услуги; информационная поддержка, общение (электронная почта или интранет)
Формат представления в отчете	Отчет об тестировании с указанием деталей тестирования, оценки защищенности, анализ результатов и рекомендации, на основе цели и согласованного исправления

См.: ИСО/МЭК 27001:2013, A.16.1: Менеджмент инцидентов информационной безопасности и улучшений;

ИСО/МЭК 27001:2013, A.9.3.1: Использование секретной аутентификационной информации;

ИСО/МЭК 27001:2013, A.7.2.2 Осведомленность, обучение и практическая подготовка (тренинги) в области информационной безопасности

B.16 Качество паролей, созданных вручную

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить качество паролей, используемых пользователями для доступа к ИТ-системам организации
Показатель оценки	Общее количество паролей, которые соответствуют политике качества паролей организации a) доля паролей, которые соответствуют политике качества паролей организации; b) тенденции соответствия политике качества паролей
Формула/выигрыш	Подсчитать количество паролей в базе паролей пользователей; определить количество паролей, которые соответствуют политике паролей организации для каждого пользователя; a) доля паролей, которые соответствуют политике качества паролей организации; b) тенденции соответствия политик качества паролей; c) разделить [Общее количество паролей, соответствующих политике качества паролей организации] на [Количество зарегистрированных паролей]; d) сравнить соотношение с предыдущим соотношением
Цель	Цель управления достигнута, и никаких действий не требуется, если полученное соотношение выше 0,9; если полученное соотношение между 0,8 и 0,9, то цель управления не достигнута, но есть положительная тенденция к улучшению; если полученное соотношение ниже 0,8, то необходимо незамедлительное принятие мер
Доказательство реализации	1 Подсчет количества паролей в базе паролей пользователей; 2 Подсчет количества паролей, которые соответствуют политике паролей организации; файл конфигурации, настройки паролей или инструмент настройки
Частота	Сбор данных: В зависимости от критичности, но минимум ежегодно Анализ: после каждого сбора данных Отчет: после каждого анализа Пересмотр оценки защищенности: ежегодно Периодичность оценки защищенности: ежегодно
Ответственные стороны	Владелец информации: системный администратор; сборщик информации: служба безопасности; потребитель оценки защищенности: менеджеры, ответственные за СМИБ, менеджеры безопасности
Источник данных	База данных паролей пользователей; отдельные пароли
Формат представления в отчете	Линия тенденции, отображающая количество паролей, соответствующих политике качества паролей организации, с наложением линий тенденции, созданных в предыдущие отчетные периоды

См.: ИСО/МЭК 27001:2013, A.9.3.1: Использование секретной аутентификационной информации

B.17 Качество паролей, созданных автоматизировано

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить качество паролей, используемых пользователями для доступа к ИТ-системам организации
Показатель оценки	1 Общее количество паролей 2 Общее количество не взламываемых паролей

Окончание

Информационный показатель	Значение или цель
Формула/выигрыш	1 Доля паролей, которые можно взломать в течение 4 часов 2 Тенденция величины 1 а) Разделить [Количество паролей, которые нельзя взломать] на [Общее количество паролей] б) Сравнить соотношение с предыдущим соотношением
Цель	Цель контроля и управления достигнута, и никаких действий не требуется, если полученное соотношение превышает 0,9. Если полученное соотношение находится между 0,8 и 0,9, цель не достигнута, но положительная тенденция указывает на улучшение. Если полученный коэффициент ниж 0,8, необходимо принять немедленные меры
Доказательство реализации	1 Запрос учетных записи сотрудника; 2 Запуск программы взлома паролей с помощью гибридной компьютерной атаки для системной учетной записи сотрудника
Частота	Сбор данных: еженедельно; анализ: еженедельно; отчет: еженедельно; пересмотр оценки защищенности: пересматривать и обновлять каждый год; период оценки защищенности: применимо 3 года
Ответственные стороны	Владелец информации: Системный администратор; сборщик информации: Служба безопасности; потребитель оценки защищенности: менеджеры, ответственные за СМИБ, менеджеры безопасности
Источник данных	База данных системной учетной записи сотрудников
Формат представления в отчете	Линия тенденции, отображающая возможность взлома пароля для всех протестированных записей, наложенная на линии, созданные в ходе предыдущих тестов

См.: ИСО/МЭК 27001:2013, А.9.3.1: Использование секретной аутентификационной информации

В.18 Пересмотр прав доступа пользователей

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценка количества проведенных систематических проверок прав доступа пользователей в критических системах
Показатель оценки	Процент критических систем, где права доступа пользователей периодически пересматриваются
Формула/выигрыш	[Количество информационных систем, классифицированных как критические, где проводятся периодические проверки прав доступа]/[Общее количество информационных систем, классифицированных как критические] × 100
Цель	Зеленый уровень: 90—100 %, Оранжевый уровень: 70—90 %, Красных уровень: < 70 %
Доказательство реализации	Доказательства отзывов прав (например, электронное письмо, отметка в системе отслеживания, завершение проверки формального подтверждения)
Частота	Сбор данных: после любых изменений, таких как продвижение, понижение в должности или увольнение; отчет: каждое полугодие

Окончание

Информационный показатель	Значение или цель
Ответственные стороны	Владелец информации: владелец риска; сборщик информации: директор по ИТ-безопасности; потребитель оценки защищенности: менеджер по информационной безопасности
Источник данных	Реестр активов, система, используемая для отслеживания выполнения проверок, например, система тикетов
Формат представления в отчете	Круговая диаграмма для текущей ситуации и линейная диаграмма для представления эволюции соответствия

См.: ИСО/МЭК 27001:2013, А.9.2.5: Пересмотр прав доступа пользователей

В.19 Оценка системы контроля физического доступа

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Показать существование, степень и качество системы, используемой для управления физическим доступом
Показатель оценки	Совершенство системы контроля физического доступа
Формула/выигрыш	Оценивается по шкале от 0 до 5: 0 нет системы контроля доступа; 1 существует система доступа, в которой для контроля доступа используется PIN-код (однофакторная система); 2 существует система с картами доступа, в которой для контроля доступа используется пропускная система (однофакторная система); 3 существует система с картами доступа, в которой для контроля доступа используется карта доступа и PIN-код; 4 система из предыдущего пункта + активирована функция ведения журнала; 5 система из предыдущего пункта, в которой PIN-код заменяется биометрической аутентификацией (отпечаток пальца, распознавание голоса, сканирование сетчатки глаза и т. д.)
Цель	Оценка 3 соответствует удовлетворительному уровню
Доказательство реализации	Качественная оценка, где каждый элемент оценки является частью оценки выше; проверка типа системы контроля входа и осмотр следующих аспектов: - наличие системы контроля доступа; - использование PIN-кода; - функциональность журнала; - биометрическая аутентификация
Частота	Сбор данных: ежегодно; анализ: ежегодно; отчет: ежегодно; пересмотр оценки: 12 месяцев; Период оценки: применимо 12 месяцев
Ответственные стороны	Владелец информации: менеджер объекта; сборщик информации: внутренний аудитор/внешний аудитор; потребитель оценки: управляющий комитет
Источник данных	Записи управления идентификацией
Формат представления в отчете	Графики

См.: ИСО/МЭК 27001:2013, А.11.1.2: Меры и средства контроля и управления физическим доступом

B.20 Эффективность контроля физического доступа

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	1 Обеспечить среду всеобъемлющей безопасности и подотчетности для персонала, объектов и продуктов; 2 Интегрировать механизмы защиты физической и информационной безопасности для обеспечения надлежащей защиты информационных ресурсов организации
Показатель оценки	Количество несанкционированных случаев входа в объекты, содержащие информационные системы (подмножество инцидентов физической безопасности)
Формула/выигрыш	Текущее количество инцидентов физической безопасности, позволяющих несанкционированные случаи входа в объекты, содержащие информационные системы/предыдущее значение; (Обратите внимание, что этот показатель должен учитывать специфический для организации контекст, такой как общее количество инцидентов физической безопасности)
Цель	Ниже 1.0
Доказательство реализации	Систематический анализ отчетов об инцидентах физической безопасности и журналов контроля доступа
Частота	Ежеквартально для сбора данных и создания отчетов
Ответственные стороны	Владелец информации: сотрудник охраны; сбор данных: группа реагирования на инциденты компьютерной безопасности; потребитель оценки: директор по ИТ, директор по ИТ-безопасности
Источник данных	Отчеты об инцидентах физической безопасности; журналы контроля физического доступа
Формат представления в отчете	График, показывающий тенденцию несанкционированного проникновения на объекты, содержащие информационные системы, за последние периоды сбора данных

См.: ИСО/МЭК 27001:2013, A.11.1.2: Меры и средства контроля и управления физическим доступом

Действие — Пересмотреть и улучшить средства контроля физической безопасности, применяемые к информационным системам.

B.21 Управление периодическим техническим обслуживанием

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить своевременность операций по техническому обслуживанию относительно расписания
Показатель оценки	Задержка обслуживания на завершенное одно событие обслуживания
Формула/выигрыш	Для каждого завершенного события вычесть [Дату фактического обслуживания] из [Даты планового техобслуживания]
Цель	Для конкретной организации, например, если средняя задержка постоянно более 3 дней, необходимо изучить причины; коэффициент завершенных мероприятий по обслуживанию должен быть больше 0,9; тенденция должна быть стабильной или близкой к 0; тенденция должна быть стабильной или восходящей

Окончание

Информационный показатель	Значение или цель
Доказательство реализации	Даты планового техобслуживания; даты завершенного обслуживания; общее количество событий планового техобслуживания; общее количество завершенных событий обслуживания
Частота	Сбор данных: ежеквартально; отчет: ежегодно
Ответственные стороны	Владелец информации: Системный администратор; сборщик информации: Служба безопасности; потребитель оценки: Менеджер безопасности, менеджер по ИТ
Источник данных	1 План/расписание обслуживания системы 2 Записи обслуживания системы
Формат	Линейная диаграмма, которая отображает среднее отклонение задержки обслуживания, наложенная на диаграммы, полученные в предыдущие отчетные периоды, и число систем; объяснение результатов и рекомендации для потенциальных действий руководства

См.: ИСО/МЭК 27001:2013, А.11.2.4: Техническое обслуживание оборудования

В.22 Управление изменениями

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить, соблюдаются ли передовая практика управления изменениями, а также политика укрепления
Показатель оценки	Процент новых установленных систем, для которых были соблюдены передовые методы управления изменениями и усилена политика
Формула/выигрыш	(Количество вновь установленных приложений или систем, в которых имеются доказательства соблюдения передовых методов управления изменениями)/(количество вновь установленных приложений)
Цель	Все системы должны соответствовать рекомендациям по управлению изменениями
Доказательство реализации	Система отслеживания, электронная почта, отчеты, контрольный список, используемый для конфигурации
Частота	Сбор данных: каждые полугодие Отчет: ежегодно руководству, каждые полгода менеджеру по информационной безопасности
Ответственные стороны	Владелец информации: владелец риска Сборщик информации: владелец риска Потребитель оценки: менеджер по информационной безопасности
Источник данных	Система отслеживания, электронные письма, отчеты, контрольный список, используемый для конфигурации, отчеты инструмента анализа конфигурации
Формат представления в отчете	Круговая диаграмма для текущей ситуации и линейная диаграмма для представления эволюции соответствия

См.: ИСО/МЭК 27001:2013, А.12.1.2: Процесс управления изменениями

B.23 Защита от вредоносного кода

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить эффективность системы защиты от вредоносных компьютерных атак
Показатель оценки	Тенденция обнаруженных компьютерных атак, которые не были заблокированы в течение нескольких отчетных периодов
Формула/выигрыш	(Количество инцидентов безопасности, вызванных вредоносным программным обеспечением)/(количество обнаруженных и заблокированных компьютерных атак, вызванных вредоносным программным обеспечением)
Цель	Линия тренда должна оставаться ниже эталонной, что означает тенденцию снижения или сохранения уровня
Доказательство реализации	1 Подсчитать количество инцидентов безопасности, вызванных вредоносным программным обеспечением, в отчетах об инцидентах 2 Подсчитать количество записей заблокированных компьютерных атак
Частота	Сбор данных: ежедневно; анализ: ежемесячно; отчет: ежемесячно; пересмотр оценки: Ежегодный анализ; период оценки: применимо 1 год
Ответственные стороны	Владелец информации; сборщик информации; потребитель оценки
Источник данных	Отчеты об инцидентах; журналы программ противодействия вредоносному ПО
Формат представления в отчете	Линия тренда, которая отображает соотношение обнаружения и предотвращения вредоносных программ с линиями, созданными в предыдущие отчетные периоды

См.: ИСО/МЭК 27001:2013, A.12.2.1: Меры обеспечения информационной безопасности в отношении вредоносных программ

Примечание — Организации, использующие этот показатель, должны учитывать следующие факторы, которые могут привести к неправильным выводам относительно показателя:

- количество обнаруженных и заблокированных компьютерных атак, вызванных вредоносным программным обеспечением, может быть очень высоким, в результате чего, значение показателя окажется очень маленьким;
- если в течение определенного периода времени наблюдается рост распространения конкретного вируса, организация может столкнуться и с увеличением количества компьютерных атак и инцидентов ИБ, связанных с вредоносными программами. При этом значение показателя может оставаться неизменным несмотря на то, что увеличение числа инцидентов может вызвать обеспокоенность.

B.24 Антивирус

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Количество систем, подверженных вредоносным программам, которые не имеют обновленного антивирусного решения
Показатель оценки	Процент систем, поврежденных вредоносным ПО, подключенных к сети организации с устаревшими (например, более одной недели) сигнатурами антивирусного ПО
Формула/выигрыш	(Количество устаревших антивирусов)/(Всего рабочих станций)

Окончание

Информационный показатель	Значение или цель
Цель	0 или небольшое значение, определенное организацией
Доказательство реализации	Мониторинг антивирусной активности каждой подвергаемой угрозе вируса системе
Частота	Ежедневно
Ответственные стороны	Владелец информации: операции ИТ; сборщик информации: операции ИТ; потребитель оценки: директор по ИТ-безопасности
Источник данных	Средства мониторинга Антивирусная консоль
Формат представления в отчете	Число на класс систем (рабочих станций, серверов, ОС)

См.: ИСО/МЭК 27001:2013, A.12.2.1: Меры обеспечения информационной безопасности в отношении вредоносных программ

B.25 Общая доступность

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Доступность ИКТ-услуг для каждой услуги по сравнению с запланированным максимальным временем простоя
Показатель оценки	Для каждой ИКТ-услуги сквозная доступность сравнивается с максимальной доступностью (то есть, исключая ранее определенные окна простоя)
Формула/выигрыш	(Общая доступность)/(Максимальная доступность без учета окон простоя)
Цель	Цель доступности сервиса
Доказательство реализации	Мониторинг сквозной доступности каждой ИКТ-услуги
Частота	Ежемесячно
Ответственные стороны	Владелец информации: операции ИКТ; сборщик информации: качество ИКТ; потребитель оценки: ИТ-директор
Источник данных	Средства мониторинга
Формат представления в отчете	Для каждой услуги две строки: строка, показывающая фактическую доступность (процент) каждого периода выборки; строка (для сравнения), показывающая цель доступности

См.: ИСО/МЭК 27001:2013, A.17.2.1: Доступность средств обработки информации

B.26 Правила брандмауэра

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить текущую производительность брандмауэра

Окончание

Информационный показатель	Значение или цель
Показатель оценки	Число неиспользуемых правил на пограничных межсетевых экранах
Формула/выигрыш	Количество правил пограничного межсетевого экрана, которые использовались 0 раз за последний период выборки
Цель	0
Доказательство реализации	Записи счетчиков использования в правилах каждого брандмауэра
Частота	Один или два раза в год
Ответственные стороны	Владелец информации: администратор сети/менеджер по информационной безопасности; сборщик информации: сетевой аналитик/аналитик по вопросам безопасности; потребитель оценки: администратор сети/менеджер по информационной безопасности
Источник данных	Консоль управления брандмауэром, отчет о проверке брандмауэра
Формат представления в отчете	Подсчет или список неиспользованных правил брандмауэра, которые нужно пометить для просмотра и возможного удаления

См.: ИСО/МЭК 27001:2013, А.13.1.3: Разграничение сетевых служб

В.27 Анализ файлов журналов

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить соответствие регулярного анализа критических файлов системного журнала
Показатель оценки	Процент проверенных по необходимости файлов журнала аудита за период времени
Формула/выигрыш	[Количество файлов журнала, просмотренных за указанный период времени/общее количество файлов журнала] × 100
Цель	При результате ниже 20 % необходимо расследование причин низкой эффективности
Доказательство реализации	Суммировать общее количество файлов журнала, перечисленных в списке проверенных журналов
Частота	Сбор: ежемесячный (в зависимости от критичности, может быть изменен на ежедневный или на режим реального времени); анализ: ежемесячный (в зависимости от критичности, может быть изменен на ежедневный или на режим реального времени); отчет: Ежеквартально; пересмотр оценки защищенности: пересматривать и обновлять каждые 2 года; период оценки: применимо 2 года
Ответственные стороны	Владелец информации: менеджер по безопасности; сборщик информации: сотрудники службы безопасности; потребитель оценки: руководители, отвечающие за СМИБ, менеджер по безопасности
Источник данных	Система; отдельные файлы журнала; свидетельство анализа журнала
Формат представления в отчете	Линейная диаграмма, которая изображает тенденцию с кратким изложением результатов и любых предлагаемых действий руководства

См.: ИСО/МЭК 27001:2013, А.12.4.1: Регистрация событий

B.28 Конфигурация устройства

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Убедиться, что устройства организации всегда настраиваются в соответствии с политикой безопасности
Показатель оценки	Процент устройств (по типу), настроенных в соответствии с политикой
Формула/выигрыш	[Количество правильно настроенных устройств]/[Общее количество устройств] × 100; Общее количество устройств зависит от организации и может включать в себя любые из следующих: - устройства, зарегистрированные в базе данных управления конфигурацией; - устройства, найденные, но не зарегистрированные в базе данных управления конфигурацией; - устройств, работающие с определенной операционной системой/версией; - мобильные устройства и т. д.
Цель	100 %
Доказательство реализации	На основе автоматического сканирования: достоверного реестра устройств; достоверного реестра программного обеспечения; результатов сканирования конфигурации
Частота	Сканирование: каждые 3 дня; отчет: немедленно
Ответственные стороны	Владелец информации: управление сетью; сборщик информации: управление сетью; потребитель оценки: ИТ-директор
Источник данных	Панель управления конфигурацией; база данных инвентаризации; инструменты сканирования
Формат представления в отчете	Линейная диаграмма для тенденций с перечислением уязвимых узлов по имени
Действие	Отключить несанкционированные устройства от сети; исправить несовместимость устройств; проанализировать и при необходимости пересмотреть рекомендации по управлению конфигурацией и т. п.

См.: ИСО/МЭК 27001:2013, A.12.6.1: Процесс управления техническими уязвимостями

B.29 Тестирование на проникновение и оценка уязвимости

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить, уязвимы ли информационные системы, обрабатывающие важную информацию (конфиденциальность, целостность), от вредоносных компьютерных атак
Показатель оценки	Процент критических информационных систем, для которых были выполнены тест на проникновение или оценка уязвимости после последней основной реализации
Формула/выигрыш	[Количество информационных систем, определенных как критические, для которых были выполнены тест на проникновение или оценка уязвимости после последней основной реализации]/[Количество информационных систем, определенных как критические] × 100; Значения уровней могут быть, например, такими; Зеленый: 100 %; Оранжевый: > = 75 %; Красный: < 75 %

Окончание

Информационный показатель	Значение или цель
Цель	Оранжевый (Зеленый уровень — это практически идеально)
Доказательство реализации	Отчеты о тестах на проникновение или оценках уязвимости, выполненных в информационных системах, по сравнению с количеством информационных систем, классифицированных при инвентаризации активов как критические
Частота	Сбор данных: ежегодно; отчет: для каждого сбора данных
Ответственные стороны	Владелец информации: владелец риска; сборщик информации: эксперты, обладающие навыками для проведения тестов на проникновение или выполнения оценок уязвимости; потребитель оценки: директор по ИТ-безопасности
Источник данных	Инвентаризация активов, протоколы испытаний на проникновение
Формат представления в отчете	Круговая диаграмма для текущей ситуации и линейная диаграмма для представления эволюции соответствия

См.: ИСО/МЭК 27001:2013, А.12.6.1: Процесс управления техническими уязвимостями
ИСО/МЭК 27001:2013, А.18.2.3: Анализ технического соответствия

В.30 Уровень уязвимости организации

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить уровень уязвимости информационных систем организации
Показатель оценки	Вес открытых (не исправленных) уязвимостей
Формула/выигрыш	Значение серьезности открытой уязвимости (например, по шкале CVSS) × Количество уязвимых систем
Цель	Определяется в зависимости от подверженности организации рискам
Доказательство реализации	Анализ деятельности по оценке уязвимости
Частота	Ежемесячно или ежеквартально
Ответственные стороны	Владелец информации: аналитики информационной безопасности или сторонние организации; сборщик информации: аналитики информационной безопасности; потребитель оценки: менеджер по информационной безопасности
Источник данных	Отчеты об оценке уязвимости; инструменты оценки уязвимости
Формат представления в отчете	Сводные значения баллов для однородных или чувствительных систем (внешние/внутренние сети, системы Unix и т. д.)

См.: ИСО/МЭК 27001:2013, А.12.6.1: Процесс управления техническими уязвимостями

B.31.1 Безопасность в сторонних соглашениях — A

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить степень безопасности в сторонних соглашениях
Показатель оценки	Средний процент соответствующих требований безопасности, указанных в сторонних соглашениях
Формула/выигрыш	[Сумма (для каждого соглашения (количество обязательных требований) — (количество удовлетворенных требований))/количество соглашений] × 100
Цель	100 %
Доказательство реализации	База данных поставщиков, записи соглашений с поставщиками
Частота	Сбор данных: ежеквартально; отчет: раз в полгода
Ответственные стороны	Владелец информации: договорной отдел; сборщик информации: служба безопасности; потребитель оценки: менеджер безопасности, управляющие делами
Источник данных	База данных поставщиков, записи соглашений с поставщиками
Формат	Линейный график, отображающий тенденцию за несколько отчетных периодов; краткое изложение выводов и возможных действий руководства

См.: ИСО/МЭК 27001:2013, A.15.1.2: Рассмотрение вопросов безопасности в соглашениях с поставщиками

Примечание — Данный показатель предполагает, что все требования безопасности равнозначны, однако на практике это обычно не так. Таким образом, общая картина может скрывать значительные различия и тем самым создавать ложное представление о безопасности. Кроме того, требования, которые организация предъявляет разным поставщикам, и способность поставщиков их выполнять также, вероятно, будут различаться. Это означает, что поставщиков не нужно оценивать одинаково. В идеале для обеспечения более точной и значимой оценки база данных поставщиков должна содержать рейтинг или категорию безопасности поставщика.

B.31.2 Безопасность в сторонних соглашениях — B

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить степень защиты в сторонних соглашениях по обработке личной информации
Показатель оценки	Средний процент соответствующих требований безопасности в сторонних соглашениях
Формула/выигрыш	Определить количество требований безопасности, которые необходимо учитывать в каждом соглашении для каждой политики (доступность, соотношение, время отклика, уровень службы поддержки, уровень обслуживания и т. д.) Сумма (для каждого соглашения (количество обязательных требований) — (количество удовлетворенных требований))/количество соглашений; 1 Среднее отношение разницы числа обязательных требований к числу удовлетворяемым требованиям: Сумма (для каждого соглашения ([Общее число требований безопасности] — [Общее число стандартных требований безопасности]))/[Количество сторонних соглашений]; 2 Тенденция соотношения: Сравнить с предыдущим показателем 1

Окончание

Информационный показатель	Значение или цель
Цель	Показатель 1 должен быть больше, чем 0,9; показатель 2 должен быть стабильным или восходящим
Доказательство реализации	Определите количество требований безопасности, которые должны быть учтены в каждом соглашении для каждой политики
Частота	Сбор данных: ежемесячно; анализ: ежеквартально; отчет: ежеквартально; пересмотр оценки: 2 года; период оценки: применимо 2 года
Ответственные стороны	Владелец информации: договорной отдел; сборщик информации: служба безопасности; потребитель оценки: менеджеры, ответственные за СМИБ, менеджеры безопасности
Источник данных	Сторонние соглашения
Формат представления в отчете	Линейный график, отображающий тенденцию за несколько отчетных периодов. Краткое изложение выводов и возможных действий руководства

См.: ИСО/МЭК 27001:2013, А.15.1.2: Рассмотрение вопросов безопасности в соглашениях с поставщиками

В.32 Эффективность менеджмента инцидентов информационной безопасности

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить эффективность менеджмента инцидентов информационной безопасности
Показатель оценки	Число инцидентов, не разрешенных в установленные сроки
Формула/выигрыш	a) Определить категории инцидентов безопасности и целевые временные рамки, в которые инциденты безопасности должны быть разрешены для каждой категории инцидентов безопасности; b) определить по категориям пороговые значения показателя для инцидентов безопасности, разрешение которых превышает заданные целевые периоды времени; c) сравнить по категориям количество инцидентов, время разрешения которых превышает целевые временные рамки с пороговыми значениями показателя
Цель	Целевые временные рамки разрешения инцидентов в пределах определенного для категории зеленого порогового значения
Доказательство реализации	Ежемесячно докладываемые целевые
Частота	Сбор данных: ежемесячно; анализ: ежемесячно; отчет: ежемесячно; пересмотр оценки: шесть месяцев; период оценки: ежемесячно
Ответственные стороны	Владелец информации: менеджеры, ответственные за СМИБ; сборщик информации: менеджер по управлению инцидентами; потребитель оценки: административный комитет СМИБ; менеджеры, ответственные за СМИБ; управление безопасностью; менеджмент инцидентов

Окончание

Информационный показатель	Значение или цель
Источник данных	СМИБ; отдельный инцидент; отчеты об инцидентах; инструмент менеджмента инцидентов
Формат представления в отчете	Значения месячного целевого индикатора в формате таблицы и диаграммы тренда

См.: ИСО/МЭК 27001:2013, А.16: Менеджмент инцидентов информационной безопасности

В.33 Тенденция инцидентов безопасности

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Тенденция инцидентов информационной безопасности; тенденция категорий инцидентов информационной безопасности
Показатель оценки	Количество инцидентов информационной безопасности за определенный период времени (например, месяц); количество инцидентов информационной безопасности определенной категории за определенный период времени (например, месяц)
Формула/выигрыш	Сравнить среднее значение оценки для последних двух периодов времени со средним значением оценки за последние 6 периодов времени. Определите пороговые значения для индикаторов тренда, например: Зеленый уровень: < 1,0; Желтый уровень: 1,00—1,30; Красный уровень: > 1,3. 1 Провести анализ для всех инцидентов 2 Выполнить анализ для каждой конкретной категории
Цель	Зеленый уровень
Доказательство реализации	Ежемесячный доклад о значениях индикатора
Частота	Ежемесячно
Ответственные стороны	Владелец информации: группа реагирования на инциденты компьютерной безопасности); сборщик информации: группа реагирования на инциденты компьютерной безопасности; потребитель оценки: — ИТ директор, директор по ИТ-безопасности
Источник данных	Сообщения о событии безопасности
Формат представления в отчете	Таблица со значениями индикатора; диаграмма тренда

См.: ИСО/МЭК 27001:2013, А.16.1: Менеджмент инцидентов информационной безопасности

В.34 Регистрация событий безопасности

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Показатель того, как регистрируются события безопасности и как они формально обрабатываются
Показатель оценки	Сумма событий безопасности, сообщенных группе реагирования на инциденты компьютерной безопасности относительно размера организации

Окончание

Информационный показатель	Значение или цель
Формула/выигрыш	Сумма событий безопасности, которые были зарегистрированы и формально обработаны в группу реагирования Количество должностей безопасности, определенных организацией
Цель	По крайней мере одно событие безопасности на должность безопасности в год
Доказательство реализации	Система отслеживания и обработки заявок о событиях безопасности
Частота	Сбор данных: ежегодно; отчет: ежегодно
Ответственные стороны	Владелец информации: группа реагирования на инциденты компьютерной безопасности; сбор данных: менеджер по информационной безопасности; потребитель оценки: менеджер по информационной безопасности, высшее руководство
Источник данных	Сообщения об инцидентах
Формат представления в отчете	Линия тренда, показывающая эволюцию зарегистрированных событий безопасности за последние периоды

См.: ИСО/МЭК 27001:2013, А.16.1.3: Сообщения о недостатках информационной безопасности

В.35 Процесс анализа СМИБ

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценить степень выполнения независимой проверки информационной безопасности
Показатель оценки	Коэффициент прогресса выполненных независимых проверок
Формула/выигрыш	Разделить [Количество проведенных сторонних проверок] на [Общее количество запланированных сторонних проверок]
Цель	Чтобы сделать вывод о достижении цели контроля и отсутствия необходимости принятия мер, значение индикатора должно попадать в интервал между 0,8 и 1,1. Значение более 0,6 означает несоответствие первичному условию
Доказательство реализации	1 Число отчетов о проведенных регулярных проверках третьей стороной 2 Общее количество запланированных сторонних проверок
Частота	Сбор данных: ежеквартально; анализ: ежеквартально; отчет: ежеквартально; пересмотр оценки: анализ и обновление каждые 2 года; период оценки: применимо 2 года
Ответственные стороны	Владелец информации: менеджеры, ответственные за СМИБ Сборщик информации: внутренний аудит; менеджер по качеству Потребитель оценки: менеджеры, ответственные за СМИБ, администратор системы качества
Источник данных	Отчеты сторонних проверок; планы сторонних проверок
Формат представления в отчете	Гистограмма, изображающая соответствие за несколько отчетных периодов относительно порогов, определяемых целью

См.: ИСО/МЭК 27001:2013, А.18.2.1: Независимая проверка информационной безопасности

B.36 Устранение уязвимости

Информационный показатель	Значение или цель
Идентификатор показателя	Определяется организацией
Информационная потребность	Оценка текущего присутствия уязвимостей в системах организации
Показатель оценки	Доля систем, которые были объектом оценки тестирования на уязвимости/проникновение
Формула/выигрыш	(Число систем, для которых выполнялась оценка уязвимостей за последний квартал или тест на проникновение за последний год)/(Общее число систем)
Цель	1
Доказательство реализации	Анализ деятельности по оценке уязвимостей и тестированию на проникновение
Частота	Ежеквартально
Ответственные стороны	Владелец информации: аналитики по информационной безопасности или сторонние подрядчики; сборщик информации: аналитики по информационной безопасности; потребитель оценки: менеджер по информационной безопасности
Источник данных	Отчеты по оценке уязвимости; инструменты оценки уязвимости; отчеты испытаний на проникновение
Формат представления в отчете	Сводная круговая диаграмма и круговая диаграмма с однородными или чувствительными системами, отображающая полученные соотношения

См.: ИСО/МЭК 27001:2013, A.18.2.3: Анализ технического соответствия

Приложение С
(справочное)

Пример спецификации конструкции оценки эффективности в форме произвольного текста

С.1 «Эффективность обучения» — конструкция оценки эффективности

В этом примере с использованием «свободного текстового формата» выясняется, будет ли более эффективным для достижения целей информационной безопасности обучать персонал формализовано, чем просто сделать политику доступной в Интернете.

Предположим, что все сотрудники (S1) обязаны прочитать онлайн-версию политики информационной безопасности организации в рамках условий своего найма (контракта).

В некоторый момент времени S2 — общее количество сотрудников, которые подтвердили, что читали политику в режиме онлайн (то есть они открыли ее в режиме онлайн и, по крайней мере, пролистали до конца текста).

S3 — количество сотрудников, которые прошли специальное обучение по информационной политике безопасности. (S3 всегда будет подмножеством S2, поскольку для курса потребуется предварительное онлайн-чтение политики).

Все сотрудники, которые хотя бы ознакомились с правилами, должны пройти онлайн-тестирование, включая тех, кто прошел официальное обучение.

S4P — количество сотрудников, которые успешно прошли тестирование только после ознакомления с политикой интрасети.

S4F — количество людей, которые проходили тестирование только после ознакомления с политикой интрасети и не смогли пройти его.

S5P — количество людей, которые успешно прошли тот же тест после посещения формального обучения.

S5F — количество людей, которые проходили тот же тест после посещения тренинга и не смогли пройти его.

E1 = S1 – S2 — количество сотрудников, которые еще не знакомы с политикой информационной безопасности.

E2 = S4P/(S4P + S4F) — доля сотрудников, которые только прочитали политику и хорошо ее понимают (это определяется порогом прохождения теста).

E3 = S5P/(S5P + S5F) — доля сотрудников, которые прошли формальное обучение и хорошо понимают политику информационной безопасности.

E4 = E3/E2 — показатель эффективности формального обучения по сравнению с простым самообучением.

S1 — S2 также является полезным показателем, показывающим, сколько сотрудников еще не прочитало онлайн-политику. Этот показатель может иметь пороговое значение, которое при превышении определенной доли от общей численности персонала, может вызывать рассылку оповещений. Однако при этом также должна учитываться продолжительность чтения онлайн-политики.

Можно предположить, что со временем, по мере повышения уровня осведомленности и культуры информационной безопасности, порог может быть повышен по мере выявления тенденций, равно как и анализ вопросов, вызывающих неудачи, что может привести к более эффективному выражению политики или установлению более реалистичной цели.

Библиография

[1] ISO/TR 10017, Guidance on statistical techniques for ISO 9001:2000

[2] ISO/IEC 15939, Systems and software engineering — Measurement process

[3] ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[4] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements

[5] NIST Special Publication 800-55, Revision 1, Performance Measurement Guide for Information Security, July 2008. http://csrc.nist.gov/publications/nistpubs/800-55Rev1/SP800-55-rev1.pdf

УДК 351.864.1:006.354 ОКС 35.040

Ключевые слова: система менеджмента информационной безопасности (СМИБ), информационная безопасность (ИБ), менеджмент информационной безопасности, эффективность системы менеджмента, мониторинг и оценка результативности СМИБ

Редактор *Г.Н. Симонова*
Технический редактор *И.Е. Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 21.05.2021. Подписано в печать 08.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,58. Уч.-изд. л. 5,02.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru