ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27003— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Системы менеджмента информационной безопасности. Руководство по реализации

(ISO/IEC 27003:2017, Information technology — Security techniques — Information security management systems — Guidance, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Акционерным обществом «Эшелон — Северо-Запад» (АО «Эшелон-СЗ») 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. № 387-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27003:2017 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство» (ISO/IEC 27003:2017 «Information technology — Security techniques — Information security management systems — Guidance», IDT).

ИСО/МЭК 27003 разработан подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ» совместного технического комитета СТК 1 «Информационные технологии (ИТ)» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

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

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 27003—2012

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации и Международная электротехническая комиссия 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 содержит руководство по реализации требований к системе менеджмента информационной безопасности (СМИБ), приведенных в ИСО/МЭК 27001, и предоставляет рекомендации (используя вспомогательный глагол «должен»), возможности (используя вспомогательный глагол «следует») и допустимое действие (используя вспомогательный глагол «может») в отношении этих требований. Настоящий стандарт не ставит целью предоставление общего руководства по всем аспектам информационной безопасности (ИБ)[1].

Разделы 4—10 настоящего стандарта отражают структуру ИСО/МЭК 27001.

Настоящий стандарт не содержит новых требований к СМИБ и связанных с ней терминов и определений. Организации должны обращаться за новыми требованиями и определениями к ИСО/МЭК 27001 и ИСО/МЭК 27000. Организации, внедрившие СМИБ, не обязаны соблюдать указания, содержащиеся в настоящем стандарте.

В СМИБ важны следующие этапы:

- понимание потребностей организации и необходимости установления политики и целей ИБ;
- оценка рисков организации, связанных с ИБ;
- внедрение и функционирование процессов ИБ, мер по обеспечению ИБ и других мер по обработке рисков;
- мониторинг и анализ эффективности и результативности СМИБ;
- практика постоянного улучшения.

СМИБ, как и любая другая система менеджмента, включает следующие ключевые компоненты:

a) политика;

b) лица с определенными обязанностями;

c) процессы управления, связанные с:

1) установлением политики;
2) обеспечением осведомленности и компетентности;
3) планированием;
4) реализацией;
5) эксплуатацией;
6) оценкой эффективности;
7) управленческим анализом;
8) улучшением;

d) документированная информация.

СМИБ имеет дополнительные ключевые компоненты, такие как:

e) оценка рисков ИБ;

f) обработка рисков ИБ, включая определение и реализацию мер обеспечения ИБ.

Настоящий стандарт носит общий характер и предназначен для применения во всех организациях, независимо от их типа, размера или характера. Организация определяет, какая часть этого руководства применяется к ней в соответствии с конкретным контекстом организации (см. ИСО/МЭК 27001, раздел 4).

Например, некоторые рекомендации могут быть применимы для крупных организаций, в то время как для небольших организаций (например, с числом сотрудников менее 10) эти рекомендации могут быть ненужными и неуместными[2].

Описания разделов 4—10 структурированы следующим образом:

- необходимые мероприятия: представлены ключевые мероприятия, требуемые в соответствующем подразделе ИСО/МЭК 27001;
- пояснение: объяснено, что подразумевают требования ИСО/МЭК 27001;
- руководство: предоставлена более подробная или вспомогательная информация для реализации необходимых мероприятий, включая примеры реализации;
- дополнительная информация: предоставлена дополнительная информация, которую следует рассмотреть.

---

[1] Далее по тексту введено сокращение ИБ.

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

ИСО/МЭК 27003, ИСО/МЭК 27004 и ИСО/МЭК 27005 образуют набор документов, поддерживающих и обеспечивающих руководство по ИСО/МЭК 27001. Среди этих документов ИСО/МЭК 27003 является базовым и всеохватывающим документом, который содержит руководство по всем требованиям ИСО/МЭК 27001, но не содержит подробных описаний, касающихся «мониторинга, измерения, анализа и оценки» и управления рисками ИБ. ИСО/МЭК 27004 и ИСО/МЭК 27005 фокусируются на конкретном содержании и дают более подробные руководства по «мониторингу, измерению, анализу и оценке» и управлению рисками ИБ.

В ИСО/МЭК 27001 существует несколько ссылок на документированную информацию. Тем не менее организация может сохранить дополнительную документированную информацию, которую она определяет как необходимую для эффективности своей системы менеджмента в соответствии с пунктом 7.5.1, перечисление b), ИСО/МЭК 27001. В этих случаях в настоящем стандарте используется фраза «Документированная информация об этих мероприятиях и их результатах является обязательной только в той форме и в той мере, в которой организация считает это необходимым для эффективности своей системы менеджмента (см. ИСО/МЭК 27001, 7.5.1, перечисление b))».

Федеральное агентство
по техническому регулированию
и метрологии
Федеральное агентство
по техническому регулированию
и метрологии

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Системы менеджмента информационной безопасности. Руководство по реализации

Information technology. Security techniques. Information security management systems. Guidance for implementation

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт содержит разъяснения и руководство по ИСО/МЭК 27001.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных ссылок применяют только указанное издание, для недатированных — последнее издание (включая все изменения к нему).

ISO/IEC 27000:2016, Information technology — Security techniques — Information security management systems — Overview and vocabulary (Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общие положения и терминология)

ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems -- Requirements (Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности . Требования)

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000.

ИСО и МЭК ведут терминологические базы данных для их использования в стандартизации по следующим адресам:

- IEC Electropedia: доступна по адресу http://www.electropedia.org/;
- Платформа просмотра ISO Online: доступна по адресу https://www.iso.org/obp.

4 Контекст организации

4.1 Понимание организации и ее контекста

Необходимые мероприятия

Организация определяет внешние и внутренние факторы, относящиеся к ее цели и влияющие на ее способность достичь ожидаемого(ых) результата(ов) системы менеджмента информационной безопасности (СМИБ).

Издание официальное

Пояснение

Для выполнения неотъемлемой функции СМИБ организация должна постоянно подвергать анализу как себя, так и окружающий мир. Такой анализ связан с внешними и внутренними факторами, которые каким-то образом влияют на ИБ и то, как она управляется, а также на соответствующие цели организации.

Анализ этих факторов преследует три цели:

- понимание контекста для определения области действия СМИБ;
- анализ контекста для определения рисков и возможностей;
- обеспечение адаптации СМИБ к меняющимся внешним и внутренним факторам.

Внешние факторы находятся вне контроля организации. Их часто называют средой организации. Анализ среды может включать следующие аспекты:

a) социальные и культурные;
b) политические, юридические, нормативные и правовые;
c) финансовые и макроэкономические;
d) технологические;
e) природные;
f) конкурентные.

Эти аспекты среды организации постоянно преподносят факторы, которые влияют на ИБ и на то, как она управляется. Соответствующие внешние факторы зависят от конкретных приоритетов организации и ситуации.

Например, внешние факторы для конкретной организации могут включать:

g) юридические последствия использования аутсорсинговых ИТ-услуг (юридический аспект);
h) природные условия с точки зрения возможности возникновения таких бедствий, как пожар, наводнение и землетрясение (природный аспект);
i) технические достижения хакерских инструментов и использование криптографии (технологический аспект);
j) общий спрос на услуги организации (социальные, культурные или финансовые аспекты).

Внутренние факторы находятся под контролем организации. Их анализ может включать следующие аспекты:

k) культура организации;
l) политика, цели и стратегии их достижения;
m) управление, организационная структура, роли и обязанности;
n) стандарты, руководящие принципы и модели, принятые организацией;
o) договорные отношения, которые могут непосредственно влиять на процессы организации, включенные в область действия СМИБ;
p) процессы и процедуры;
q) способности, понимаемые с точки зрения ресурсов и знаний (например, капитал, время, люди, процессы, системы и технологии);
r) физическая инфраструктура и среда;
s) информационные системы, информационные потоки и процессы принятия решений (как формальные, так и неформальные);
t) предыдущие аудиты или предыдущие результаты оценки рисков.

Результаты этих мероприятий используются в 4.3 и 6.1.

Руководство

Основываясь на понимании цели организации (например, ссылаясь на ее миссию или бизнес-план), а также ожидаемого(ых) результата(ов) ее СМИБ, организация должна:

- проанализировать внешнюю среду для выявления соответствующих внешних факторов;
- провести анализ внутренних аспектов для определения соответствующих внутренних факторов.

Для выявления соответствующих факторов можно задать следующий вопрос: как определенная категория факторов (в соответствии с перечислением «Пояснение» 4.1) влияет на цели ИБ? Ниже приведены три наглядных примера внутренних факторов.

Пример 1 касается управления и организационной структуры (перечисление m): при создании СМИБ следует учитывать уже существующие управленческие и организационные структуры. Например, организация может моделировать структуру своей СМИБ на основе структуры других существующих систем менеджмента и объединить общие функции, такие как анализ и аудит управления.

Пример 2 — о политике, целях и стратегиях (пункт l): анализ существующих политик, целей и стратегий может указывать на то, чего организация намерена достичь и как цели ИБ могут быть согласованы с бизнес-целями для обеспечения успешных результатов.

Пример 3 — об информационных системах и информационных потоках (перечисление s): при определении внутренних факторов организация должна детально определить информационные потоки между ее различными информационными системами.

Поскольку внутренние и внешние факторы со временем изменяются, то факторы и их влияние на область действия, ограничения и требования СМИБ следует регулярно пересматривать.

Документированная информация об этих мероприятиях и их результатах является обязательной только в той форме и в той мере, в которой организация считает это необходимым для эффективности своей системы менеджмента (см. ИСО/МЭК 27001, 7.5, перечисление b)).

Дополнительная информация

В ИСО/МЭК 27000 определение «организация» содержит примечание, в котором говорится, что: «Понятие организации включает, но не ограничивается, индивидуального предпринимателя, компанию, корпорацию, фирму, предприятие, орган власти, товарищество, благотворительную организацию или учреждение, или их часть, или комбинацию, независимо от того, зарегистрированы они или нет, являются ли они государственными или частными». Некоторые из этих объектов являются юридическими лицами, в то время как другие — нет.

Рассмотрим четыре случая:

1) организация является юридическим или административным лицом (например, индивидуальный предприниматель, компания, корпорация, фирма, предприятие, орган власти, товарищество, благотворительная организация или учреждение, независимо от того, зарегистрированы они или нет, являются ли они государственными или частными);

2) организация является частью юридического или административного лица (например, частью компании, корпорации, предприятия);

3) организация представляет собой совокупность юридических или административных лиц (например, консорциум индивидуальных предпринимателей, крупных компаний, корпораций, фирм);

4) организация представляет собой совокупность частей юридических или административных лиц (например, клубы, торговые ассоциации).

4.2 Понимание потребностей и ожиданий заинтересованных сторон

Необходимые мероприятия

Организация определяет заинтересованные стороны, имеющие отношение к СМИБ, и их требования к ИБ.

Пояснение

Заинтересованная сторона — это определенный термин (см. ИСО/МЭК 27000, 3.37), относящийся к лицам или организациям, которые могут влиять, находиться под влиянием или ощущать, что они находятся под влиянием решений или действий организации. Заинтересованные лица могут быть снаружи и внутри организации и могут иметь конкретные потребности, ожидания и требования к ИБ организации.

Внешние заинтересованные стороны могут включать:

a) регуляторов и законодателей;

b) акционеров, включая собственников и инвесторов;

c) поставщиков, включая субподрядчиков, консультантов и сторонних партнеров;

d) отраслевые ассоциации;

e) конкурентов;

f) клиентов и потребителей;

g) группы активистов.

Внутренние заинтересованные стороны могут включать:

h) лиц, принимающих решения, включая высшее руководство;

i) владельцев процессов, систем и информации;

j) лиц, предоставляющих вспомогательные функции, такие как ИТ или отдел кадров;

k) сотрудников и пользователей;

l) специалистов по ИБ.

Результаты этих мероприятий используются в 4.3 и 6.1.

Руководство

Необходимо предпринять следующие шаги:

- определить внешние заинтересованные стороны;
- определить внутренние заинтересованные стороны;
- определить требования заинтересованных сторон.

Поскольку потребности, ожидания и требования заинтересованных сторон со временем изменяются, эти изменения и их влияние на область действия, ограничения и требования СМИБ должны регулярно пересматриваться.

Документированная информация об этих мероприятиях и их результатах является обязательной только в той форме и в той мере, в которой организация считает это необходимым для эффективности своей системы менеджмента (см. ИСО/МЭК 27000, 3.37).

Дополнительная информация

Дополнительная информация отсутствует.

4.3 Определение области действия системы менеджмента информационной безопасности

Необходимые мероприятия

Организация определяет границы и применимость СМИБ для установления области ее действия.

Пояснение

Область действия определяет, где и для чего именно применима СМИБ, а где и для чего нет. Таким образом, определение области действия является ключевым действием, задающим основу для всех других мероприятий по внедрению СМИБ. Например, оценка и обработка риска, включая определение мер обеспечения ИБ, не дадут достоверных результатов без точного понимания того, где именно применима СМИБ. Точное знание границ и применимости СМИБ, а также методов взаимодействия и зависимостей между организацией и другими организациями также имеет решающее значение. Все последующие изменения области действия могут привести к значительным дополнительным усилиям и затратам.

На определение области действия могут влиять следующие факторы:

a) внешние и внутренние факторы, описанные в 4.1;

b) заинтересованные стороны и их требования, определенные в соответствии с подразделом 4.2 ИСО/МЭК 27001;

c) готовность бизнес-процессов быть частью области СМИБ;

d) все вспомогательные функции, т. е. функции, необходимые для поддержки этих бизнес-процессов (например, управление кадрами; ИТ-услуги и программные приложения; средства управления недвижимостью, физическими зонами, основными службами и коммунальными услугами);

e) все функции, которые передаются на аутсорсинг либо другим подразделениям организации, либо независимым поставщикам.

Область действия СМИБ может сильно отличаться от одной реализации к другой. Например, область действия может включать следующее:

- один или несколько конкретных процессов;
- одну или несколько конкретных функций;
- одну или несколько конкретных услуг;
- один или несколько конкретных разделов или местоположений;
- целое юридическое лицо;
- целый административный орган и один или несколько его поставщиков.

Руководство

Для определения области действия можно использовать многоступенчатый подход:

f) определить предварительную область действия: это мероприятие должно проводиться небольшой, но уполномоченной группой представителей руководства;

g) определить уточненную область действия: функциональные подразделения в рамках и за пределами предварительной области действия должны быть проанализированы, возможно, с последующим добавлением или исключением некоторых из этих функциональных подразделений для сокращения числа взаимодействий в пределах области действия СМИБ. При уточнении предварительной области действия следует учитывать все вспомогательные функции, необходимые для поддержки бизнес-процессов;

h) определить окончательную область действия СМИБ: уточненная область действия должна быть оценена всем руководством в рамках уточненной области действия. При необходимости ее следует откорректировать, а затем в точности описать;

i) утверждение области действия: документированная информация, описывающая область действия, должна быть официально утверждена высшим руководством.

Организация должна также рассмотреть деятельность, оказывающую влияние на СМИБ, или деятельность, которая передается на аутсорсинг либо другим подразделениям организации, либо независимым поставщикам. Для таких видов деятельности следует определить методы взаимодействия (физические, технические и организационные) и их влияние на область действия СМИБ.

Документированная информация, описывающая область действия СМИБ, может включать:

j) организационную область действия, границы и методы взаимодействия;

k) область применения информационно-коммуникационных технологий, границы и методы взаимодействия;

l) физическую область действия, границы и методы взаимодействия.

Дополнительная информация

Дополнительная информация отсутствует.

4.4 Система менеджмента информационной безопасности

Необходимые мероприятия

Организация устанавливает, внедряет, поддерживает и постоянно улучшает СМИБ.

Пояснение

В подразделе 4.4 ИСО/МЭК 27001 установлены основные требования к созданию, внедрению, поддержке и постоянному улучшению СМИБ. В то время как другие части ИСО/МЭК 27001 описывают обязательные элементы СМИБ, данный подраздел предписывает организации обеспечить соблюдение всех необходимых элементов для создания, внедрения, поддержания и постоянного совершенствования СМИБ.

Руководство

Руководство отсутствует.

Дополнительная информация

Дополнительная информация отсутствует.

5 Руководство

5.1 Роль руководства и его обязательства

Необходимые мероприятия

Высшее руководство также участвует в анализе СМИБ со стороны руководства (см. 9.3) и содействует ее постоянному улучшению (см. 10.2).

Пояснение

Роль и обязательства руководства очень важны для эффективности СМИБ.

Высшее руководство определяет (см. ИСО/МЭК 27000) лицо или группу лиц, которые направляют и контролируют формирование СМИБ на самом высоком уровне, т. е. высшее руководство несет ответственность за СМИБ. Это означает, что оно управляет СМИБ, как и другими областями организации, например распределением и мониторингом бюджета. Высшее руководство может делегировать полномочия в организации и предоставлять ресурсы для фактического выполнения деятельности, связанной с ИБ и СМИБ, но оно по-прежнему будет нести полную ответственность.

Например, организация, реализующая и эксплуатирующая СМИБ, может быть частью более крупной организации. В этом случае высшее руководство — это человек или группа людей, которые руководят и контролируют эту часть.

Высшее руководство также участвует в анализе со стороны руководства (см. 9.3) и содействует постоянному улучшению (см. 10.2).

Руководство

Высшее руководство должно устанавливать свои роли и обязательства посредством следующего:

a) высшее руководство должно обеспечить установление политики ИБ и целей ИБ и их совместимость со стратегическим направлением деятельности организации;

b) высшее руководство должно обеспечивать интеграцию требований СМИБ и мер обеспечения ИБ в процессы организации. При этом интеграция должна быть адаптирована к конкретному контексту организации. Например, организация, назначившая владельцев процессов, может делегировать ответственность за выполнение применимых требований этим лицам или группам лиц. Поддержка высшего руководства также может быть необходима для преодоления организационного сопротивления изменениям в процессах и мерах обеспечения ИБ;

c) высшее руководство должно обеспечить доступность ресурсов для эффективной СМИБ. Ресурсы необходимы для создания СМИБ, ее внедрения, поддержания и улучшения, а также для осуществления мер обеспечения ИБ. Ресурсы, необходимые для СМИБ, включают:

1) финансы;
2) персонал;
3) оборудование;
4) техническую инфраструктуру.

Необходимые ресурсы зависят от контекста организации, ее размера, сложности структуры внутренних и внешних требований. Анализ со стороны руководства должен предоставлять информацию, которая указывает, являются ли ресурсы достаточными для организации;

d) высшее руководство должно сообщать о необходимости управления ИБ в собственной организации и необходимости соответствия требованиям СМИБ. Это может быть сделано путем предоставления практических примеров, иллюстрирующих фактические потребности в контексте организации, и путем информирования о требованиях ИБ;

e) высшее руководство должно обеспечить достижение СМИБ ожидаемого(ых) результата(ов) путем поддержки осуществления всех процессов управления ИБ и, в частности, путем запроса и анализа отчетов о состоянии и эффективности СМИБ (см. 5.3, перечисление b)). Такие отчеты могут быть получены на основе измерений (см. 6.2, перечисление b) и 9.1, перечисление a)), анализа со стороны руководства и отчетов об аудите. Высшее руководство также может устанавливать цели производительности для ключевых сотрудников, связанных со СМИБ;

f) высшее руководство должно направлять и поддерживать лиц в организации, непосредственно связанных с ИБ и СМИБ. Невыполнение этого требования может негативно повлиять на эффективность СМИБ. Обратная связь от высшего руководства может отражать то, как планируемая деятельность согласуется со стратегическими потребностями организации, а также определяет приоритеты различных мероприятий в СМИБ;

g) высшее руководство должно оценивать потребности в ресурсах в ходе анализа со стороны руководства и устанавливать цели для постоянного улучшения и мониторинга эффективности планируемых мероприятий;

h) высшее руководство должно оказывать поддержку лицам, которым назначены роли и обязанности, связанные с управлением ИБ, чтобы они были мотивированы и могли направлять и поддерживать деятельность по ИБ в своей области.

В тех случаях, когда организация, реализующая и эксплуатирующая СМИБ, является частью более крупной организации, роли и обязательства руководства могут быть улучшены путем взаимодействия с человеком или группой людей, которые контролируют и руководят более крупной организацией. Если они понимают, что задействовано во внедрении СМИБ, они могут оказать поддержку высшему руководству в рамках области действия СМИБ в обеспечении лидерства, а также продемонстрировать приверженность СМИБ. Например, если заинтересованные стороны, не входящие в область действия СМИБ, участвуют в принятии решений относительно целей ИБ и критериев риска и осведомлены о результатах, полученных СМИБ, их решения относительно распределения ресурсов могут быть приведены в соответствие с требованиями СМИБ.

Дополнительная информация

Дополнительная информация отсутствует.

5.2 Политика

Необходимые мероприятия

Высшее руководство устанавливает политику ИБ.

Пояснение

Политика ИБ описывает стратегическую важность СМИБ для организации и является доступной в виде документированной информации. Политика управляет деятельностью в области ИБ в организации.

Политика устанавливает, что необходимо для ИБ в реальном контексте организации.

Руководство

Политика ИБ должна содержать краткие заявления высокого уровня о намерении и направлении в отношении ИБ. Она может быть определенной под область действия СМИБ или иметь более широкий охват.

Все другие политики, процедуры, мероприятия и цели, связанные с ИБ, должны быть согласованы с политикой ИБ.

Политика ИБ должна отражать деловую ситуацию организации, корпоративную культуру, факторы и цели организации, связанные с ИБ. Масштабы политики ИБ должны соответствовать целям и культуре организации и должны обеспечивать баланс между удобством чтения и полнотой информации. Важно, чтобы пользователи политики могли отождествлять себя со стратегическими направлениями политики.

Политика ИБ может либо включать цели ИБ для организации, либо описывать порядок установки целей ИБ (т.е. кто устанавливает их и как они должны быть раскрыты в рамках СМИБ). Например, в очень крупных организациях цели высокого уровня должны быть установлены высшим руководством всей организации, а затем в соответствии с порядком, установленным в политике ИБ, цели должны быть детализированы таким образом, чтобы они задавали направление всем заинтересованным сторонам.

Политика ИБ должна содержать четкое заявление высшего руководства об их обязательствах выполнять требования, связанные с ИБ.

Политика ИБ должна содержать четкое заявление о том, что высшее руководство поддерживает постоянное совершенствование всех видов деятельности. Этот принцип важно изложить в политике, чтобы лица, входящие в область действия СМИБ, знали о нем.

Политика ИБ должна быть доведена до сведения всех лиц, входящих в область действия СМИБ. Следовательно, ее формат и язык должны быть легкими для понимания сотрудниками.

Высшее руководство должно решить, каким заинтересованным сторонам следует сообщить о политике. Политика ИБ может быть сформулирована таким образом, чтобы ее можно было донести до соответствующих внешних заинтересованных сторон за пределами организации. Примерами таких внешних заинтересованных сторон являются заказчики, поставщики, подрядчики, субподрядчики и регулирующие органы. Если политика ИБ предоставляется внешним заинтересованным сторонам, она не должна включать конфиденциальную информацию.

Политика ИБ может быть реализована либо как отдельная независимая политика, либо как часть общей политики, охватывающей несколько систем менеджмента в рамках организации (например, качество, окружающая среда и ИБ).

Политика ИБ должна быть доступна в виде документированной информации. Требования ИСО/МЭК 27001 не предполагают какой-либо конкретной формы для этой документированной информации, и поэтому организация может решить, какая форма является наиболее подходящей. Если организация имеет стандартный шаблон для политик, политика ИБ должна ему соответствовать.

Дополнительная информация

Дополнительную информацию о политиках, связанных с ИБ, можно найти в ИСО/МЭК 27002.

Дополнительную информацию о взаимосвязи политики ИБ и других политик можно найти в приложении А.

5.3 Организационные роли, обязанности и полномочия

Необходимые мероприятия

Высшее руководство должно обеспечивать распределение обязанностей и полномочий в отношении ролей, имеющих отношение к информационной безопасности, и информирование об этом всей организации.

Пояснение

Высшее руководство обеспечивает распределение и доведение ролей и обязанностей, а также необходимых полномочий, имеющих отношение к ИБ.

Цель этого требования состоит в том, чтобы возложить обязанности и полномочия для обеспечения соответствия СМИБ требованиям ИСО/МЭК 27001, а также обеспечить предоставление отчетности о производительности СМИБ высшему руководству.

Руководство

Высшее руководство должно регулярно следить за тем, чтобы обязанности и полномочия в отношении СМИБ были распределены таким образом, чтобы система менеджмента выполняла требования,

изложенные в ИСО/МЭК 27001. Высшее руководство не должно распределять все роли, обязанности и полномочия, но должно надлежащим образом делегировать полномочия на это. Высшее руководство должно утвердить основные роли, обязанности и полномочия СМИБ.

Следует распределить обязанности и полномочия, связанные с деятельностью в области ИБ. Они включают в себя:

a) координацию создания, внедрения, поддержания, отчетности о производительности и улучшении СМИБ;

b) консультирование по вопросам оценки и обработки рисков ИБ;

c) разработку процессов и систем ИБ;

d) установление стандартов, касающихся определения, настройки и функционирования мер обеспечения ИБ;

e) управление инцидентами ИБ;

f) анализ и аудит СМИБ.

Соответствующие обязанности и полномочия в области ИБ должны быть включены не только в роли, непосредственно связанные с ИБ, но и в другие роли. Например, обязанности по ИБ могут быть включены в роли:

g) владельцев информации;

h) владельцев процесса;

i) владельцев активов (например, владельцы приложений или инфраструктуры;

j) владельцев рисков;

k) координатора ИБ (эта специфическая роль обычно играет вспомогательную роль в СМИБ);

l) руководителей проектов;

m) линейных менеджеров;

n) пользователей информации.

Документированная информация об этих мероприятиях и их результатах является обязательной только в той форме и в той мере, в которой организация считает это необходимым для эффективности своей системы менеджмента (см. ИСО/МЭК 27001, 7.5, перечисление b)).

Дополнительная информация

Дополнительная информация отсутствует.

6 Планирование

6.1 Мероприятия по обработке рисков и возможностей

6.1.1 Политики информационной безопасности

Обзор

В подразделе 6.1 ИСО/МЭК 27001 говорится о планировании мероприятий по обработке всех типов рисков и возможностей, которые имеют отношение к СМИБ. Это ведет к оценке риска и планированию обработки риска.

ИСО/МЭК 27001 в процессе планирования подразделяет риски на две категории:

a) риски и возможности, относящиеся к ожидаемому(ым) результату(ам) СМИБ в целом;

b) риски ИБ, связанные с потерей конфиденциальности, целостности и доступности информации в рамках СМИБ.

Первая категория должна обрабатываться в соответствии с требованиями, определенными в ИСО/МЭК 27001, раздел 6 (общие положения). Риски, которые попадают в эту категорию, могут быть связаны с самой СМИБ, определением области действия СМИБ, обязательствами высшего руководства по обеспечению ИБ, ресурсами для эксплуатации СМИБ и т. д. Возможности, которые попадают в эту категорию, могут быть связаны с результатом(ами) СМИБ, коммерческой ценностью СМИБ, эффективностью рабочих процессов СМИБ и мерами обеспечения ИБ и т. д.

Вторая категория состоит из совокупности рисков, которые связаны с потерей конфиденциальности, целостности и доступности информации в рамках СМИБ. Эти риски должны обрабатываться в соответствии с 6.1.2 и 6.1.3.

Организации могут использовать разные методы для каждой категории.

Разделение требований по обработке рисков можно объяснить следующим образом:

- обеспечение поддержки совместимости с другими стандартами по системам менеджмента для тех организаций, в которых эти системы интегрированы для различных аспектов, таких как качество, окружающая среда и ИБ;

- требование к тому, чтобы организация определяла и применяла полные и подробные процессы для оценки и обработки рисков ИБ;

- подчеркивание, что управление рисками ИБ является ключевым элементом СМИБ.

В ИСО/МЭК 27001, пункт 6.1.1, приведены формулировки: «определить риски и возможности» и «обработать эти риски и возможности». Слово «определить» можно считать эквивалентным слову «оценивать», используемому в ИСО/МЭК 27001, пункт 6.1.2 (т. е. идентифицировать, анализировать и оценивать). Аналогично слово «обработать» можно считать эквивалентным слову «устранить», используемому в ИСО/МЭК 27001, пункт 6.1.3.

Необходимые мероприятия

При планировании СМИБ организация определяет риски и возможности, учитывая факторы, указанные в 4.1, и требования, указанные в 4.2.

Пояснение

При рассмотрении рисков и возможностей, относящихся к ожидаемому(ым) результату(ам) СМИБ, предполагается, что организация определяет их на основе внутренних и внешних факторов (см. 4.1) и требований заинтересованных сторон (см. 4.2). После чего организация осуществляет планирование своей СМИБ для того, чтобы:

a) обеспечить достижение ожидаемых результатов СМИБ, при этом риски ИБ должны быть известны владельцам рисков и обработаны до приемлемого уровня;

b) предотвратить или уменьшить нежелательные эффекты рисков, относящихся к ожидаемому(ым) результату(ам) СМИБ;

c) добиваться постоянного улучшения (см. 10.2), например, через соответствующие механизмы для выявления и исправления слабых мест в процессах управления или использования возможностей для улучшения ИБ.

Риски, относящиеся к перечислению a), могут быть связаны с непонятными процессами и обязанностями, плохой осведомленностью среди сотрудников, низкой вовлеченностью со стороны руководства и т. д. Риски, относящиеся к перечислению b), могут быть связаны с неэффективным управлением рисками или с плохой осведомленностью о них. Риски, относящиеся к перечислению c), могут быть связаны с неэффективным управлением документацией и процессами СМИБ.

Когда организация стремится использовать возможности в своей деятельности, эта деятельность затем влияет на контекст организации (см. ИСО/МЭК 27001, 4.1) или на потребности и ожидания заинтересованных сторон (см. ИСО/МЭК 27001, 4.2) и может изменить риски для организации. Примерами возможностей могут быть: сосредоточение своего бизнеса на некоторых областях продуктов или услуг, разработка маркетинговой стратегии для некоторых географических регионов или расширение деловых партнерских отношений с другими организациями.

Возможности также существуют в постоянном улучшении процессов и документации СМИБ, наряду с оценкой ожидаемых результатов, предоставляемых СМИБ. Например, рассмотрение относительно новой СМИБ часто приводит к выявлению возможностей для уточнения процессов путем уточнения интерфейсов, сокращения административных накладных расходов, устранения частей процессов, которые не являются экономически эффективными, путем уточнения документации и внедрения новых информационных технологий.

Планирование в этом разделе включает определение:

d) мероприятий по обработке рисков и возможностей;

e) способа:

1) интеграции и внедрения этих мероприятий в процессы СМИБ;

2) оценивания эффективности этих мероприятий.

Руководство

Организация должна:

f) определить риски и возможности, которые могут повлиять на достижение целей, описанных в перечислениях a), b) и c), с учетом факторов, указанных в 4.1, и требований, указанных в 4.2;

g) разработать план для осуществления определенных мероприятий и оценить эффективность этих мероприятий; мероприятия должны планироваться с учетом интеграции процессов ИБ в существующие структуры и их документирования; все эти действия связаны с целями ИБ (подраздел 6.2), в отношении которых оцениваются и обрабатываются риски ИБ (см. 6.1.2 и 6.1.3).

Общие требования к постоянному улучшению СМИБ, установленные в подразделе 10.2 ИСО/МЭК 27001, подтверждаются требованиями, заданными в 6.1.1, а также другими соответствующими требованиями подраздела 5.1 ИСО/МЭК 27001, перечисление g), подраздела 5.2, перечисление d), подразделов 9.1, 9.2 и 9.3.

Мероприятия могут быть различными для стратегического, тактического и эксплуатационного уровней, для разных сайтов или для различных сервисов или систем.

Для выполнения требований 6.1.1 может быть использовано несколько подходов, два из которых:

- рассматривают риски и возможности, связанные с планированием, внедрением и эксплуатацией СМИБ отдельно от рисков ИБ;

- учитывают все риски одновременно.

Организация, которая интегрирует СМИБ в установленную систему менеджмента, может обнаружить, что требования этого раздела соответствуют существующей методологии бизнес-планирования организации. В этом случае следует позаботиться о том, чтобы методология охватывала все требования настоящего раздела.

Документированная информация об этих мероприятиях и их результатах является обязательной только в той форме и в той мере, в которой организация считает это необходимым для эффективности своей системы менеджмента (см. ИСО/МЭК 27001, 7.5, перечисление b)).

Дополнительная информация

Дополнительную информацию об управлении рисками можно найти в ИСО 31000.

6.1.2 Оценка риска информационной безопасности

Необходимые мероприятия

Организация определяет и применяет процесс оценки рисков ИБ.

Пояснение

Организация определяет процесс оценки риска ИБ, который:

a) устанавливает и поддерживает:

1) критерии принятия риска;

2) критерии для проведения оценки риска ИБ, которые могут включать критерии для оценки последствий и вероятности, а также правила для определения уровня риска;

b) гарантирует, что повторные оценки риска ИБ приводят к согласованным, действительным и сопоставимым результатам.

Процесс оценки риска ИБ затем определяется по следующим подпроцессам:

c) идентификация рисков ИБ:

1) идентификация рисков, связанных с потерей конфиденциальности, целостности и доступности информации в рамках СМИБ;

2) идентификация владельцев рисков, связанных с этими рисками, то есть определение и назначение лиц с соответствующими полномочиями и ответственностью за управление идентифицированными рисками;

d) анализ рисков ИБ:

1) оценка потенциальных последствий в случае реализации идентифицированных рисков, например прямых воздействий на бизнес, таких как денежные потери, или косвенных воздействий на бизнес, таких как ущерб репутации; оцененные последствия могут быть выражены количественными или качественными значениями;

2) оценка реальной вероятности возникновения идентифицированных рисков в количественных (то есть вероятность или частота) или качественных значениях;

3) определение уровня идентифицированного риска в виде заранее определенной комбинации оцененных последствий и вероятностей;

e) оценка рисков ИБ:

1) сравнение результатов анализа риска с критериями принятия риска, установленными ранее;

2) определение приоритетов анализируемых рисков для обработки рисков, то есть определение срочности обработки неприемлемых рисков и последовательности их обработки в том случае, если несколько рисков нуждаются в обработке.

Затем применяется процесс оценки риска ИБ.

Все этапы процесса оценки риска ИБ (см. 6.1.2), а также результаты его применения сохраняются организацией в виде документированной информации.

Руководство

Руководство по установлению критериев риска (см. 6.1.2, перечисление а))

Критерии риска ИБ должны быть установлены с учетом контекста организации и требований заинтересованных сторон и, с одной стороны, должны быть определены в соответствии с предпочтениями и восприятием рисков высшим руководством, а с другой стороны — должны предусматривать выполнимый и соответствующий процесс управления рисками.

Критерии риска ИБ должны быть установлены в соответствии с ожидаемым(и) результатом(ами) СМИБ.

В соответствии с пунктом 6.1.2, перечисление а) ИСО/МЭК 27001 должны быть установлены критерии оценки риска ИБ, которые включают оценку вероятности и последствий. Кроме того, должны быть установлены критерии приемлемости риска.

После установления критериев оценки последствий и вероятностей возникновения рисков ИБ организация должна установить метод их объединения для определения уровня риска. Последствия и вероятности могут быть выражены качественной, количественной или приближенной оценкой.

Следует отметить, что критерии приемлемости риска относятся к оценке риска (на этапе оценки, когда организация должна определить, является ли риск приемлемым или нет) и к мероприятиям по обработке риска (когда организация должна определить, является ли предложенная обработка риска достаточной для достижения приемлемого уровня риска).

Критерии принятия риска могут быть основаны на максимально допустимом уровне рисков, экономической целесообразности или на последствиях для организации.

Критерии принятия риска должны быть утверждены ответственным руководством.

Руководство по получению согласованных, действительных и сопоставимых результатов оценки рисков (см. 6.1.2, перечисление b))

Процесс оценки рисков должен основываться на методах и средствах, разработанных с достаточной детализацией, чтобы он приводил к согласованным, действительным, сопоставимым и проверяемым результатам.

Какой бы ни был выбран метод, процесс оценки риска ИБ должен обеспечивать:

- учет всех рисков на необходимом уровне детализации;
- последовательность и воспроизводимость результатов оценки (идентификация рисков, их анализ и оценка должны быть понятны третьей стороне, и результаты должны быть одинаковы, когда разные лица оценивают риски в том же контексте);
- сопоставимость результатов повторных оценок риска (т. е. можно определить, увеличивается или уменьшается уровень риска).

Несоответствия или расхождения в результатах, когда весь процесс или часть процесса оценки риска ИБ повторяется, может указывать на то, что выбранный метод оценки риска не является адекватным.

Руководство по идентификации рисков ИБ (см.6.1.2, перечисление с))

Целью идентификации рисков является создание полного перечня рисков на основе тех событий, которые могут создавать, повышать, предупреждать, снижать, ускорять или приостанавливать достижение целей ИБ.

Идентификация риска — это процесс обнаружения, распознавания и описания рисков. Он включает в себя идентификацию источников риска, событий, их причин и потенциальных последствий.

Для идентификации рисков ИБ обычно используют два подхода:

- подход, основанный на событиях и рассматривающий источники риска в общем виде. События могли произойти в прошлом или могут ожидаться в будущем. В первом случае они могут включать ретроспективные данные, во втором случае они могут основываться на теоретическом анализе и экспертных оценках;
- подход, основанный на идентификации активов, угроз безопасности информации и уязвимостей и рассматривающий два типа источников рисков: активы с их внутренними уязвимостями и активы, подвергающиеся угрозам безопасности информации. Рассматриваемые в данном случае потенциальные события представляют собой способы использования угрозами определенной уязвимости активов для воздействия на цели организации.

Оба подхода соответствуют принципам и общим руководствам по оценке рисков в ИСО 31000.

Также могут использоваться другие подходы для идентификации рисков, если они доказали аналогичную практическую полезность и если они могут гарантировать выполнение требований 6.1.2, перечисление b).

Примечание — Подход, основанный на активах, угрозах безопасности информации и уязвимостях, соответствует подходу идентификации риска ИБ, указанному в издании ИСО/МЭК 27001 2006 года, и совместим с требованиями версии 2020 года. Это гарантирует, что предыдущий вклад в идентификацию риска не будет потерян.

Рекомендуется, чтобы идентификация риска была достаточно детализированной при первой итерации оценки риска. Наличие высокого уровня детализации и четкого представления о рисках ИБ гораздо лучше, чем отсутствие представления вообще.

Руководство по анализу рисков ИБ (см. 6.1.2, перечисление d))

Целью анализа риска является определение уровня риска.

ИСО 31000 ссылается на ИСО/МЭК 27001 как на общую модель. ИСО/МЭК 27001 рекомендует, чтобы анализ риска основывался на оценке последствий, возникающих в результате реализации идентифицированного риска, и оценке вероятности возникновения таких последствий для определения уровня риска.

Методы анализа риска, основанные на вероятности и последствиях, могут быть:

- качественными с использованием шкалы качественных признаков (например, высокий, средний, низкий);
- количественными с использованием шкалы с числовыми значениями (например, денежные затраты, частота или вероятность возникновения);
- комбинированными, использующими качественные шкалы с присвоенными значениями.

Какой бы метод анализа риска ни использовался, следует учитывать уровень его объективности.

Существует несколько методов анализа рисков. Оба упомянутых выше подхода (подход на основе событий и подход, основанный на идентификации активов, угроз информационной безопасности и уязвимостей) могут быть пригодны для анализа рисков ИБ. Процесс идентификации и анализа рисков может быть наиболее эффективным, когда он осуществляется с помощью экспертов по соответствующим обсуждаемым рискам.

Руководство по оценке рисков ИБ (см. 6.1.2, перечисление e))

Оценка анализируемых рисков включает в себя использование процессов принятия решений в организации для сравнения оцененного уровня каждого риска с заранее определенными критериями приемлемости для определения вариантов обработки риска.

На этом заключительном этапе оценки риска проверяется, могут ли риски, которые были проанализированы на предыдущих этапах, быть приняты в соответствии с критериями приемлемости, определенными в 6.1.2, перечисление a), или они нуждаются в дальнейшей обработке. В 6.1.2, перечисление d), представлена информация о величине риска, но нет непосредственной информации о срочности реализации вариантов обработки риска. В зависимости от обстоятельств, при которых возникают риски, они могут иметь разные приоритеты для обработки. Следовательно, необходим ранжированный список рисков по возрастанию приоритетов.

Полезно сохранить дополнительную информацию об этих рисках на этапе идентификации рисков и анализа рисков для поддержки решений по обработке рисков.

Дополнительная информация

ИСО/МЭК 27005 представляет руководство по проведению оценки рисков ИБ.

6.1.3 Обработка риска информационной безопасности

Необходимые мероприятия

Организация определяет и применяет процесс обработки рисков ИБ.

Пояснение

Обработка риска ИБ — это общий процесс выбора вариантов обработки риска, определения соответствующих мер обеспечения ИБ для реализации таких вариантов, формулирования плана обработки риска и получения одобрения плана обработки риска от владельца(ев) риска.

Все этапы процесса обработки риска ИБ (см. 6.1.3), а также результаты его применения сохраняются организацией в виде документированной информации.

Руководство

Руководство по вариантам обработки риска ИБ (см. 6.1.3, перечисление a))

Варианты обработки риска:

a) избежание риска путем принятия решения не начинать или не продолжать деятельность, которая порождает риск, или устранение источника риска (например, закрытие системы электронной коммерции);

b) взятие на себя дополнительных рисков или увеличение рисков для того, чтобы воспользоваться бизнес-возможностями (например, открытие системы электронной коммерции);

c) модификация риска путем изменения вероятности (например, уменьшение уязвимостей) или/и последствий (например, разнообразие активов);

d) разделение риска с другими сторонами посредством страхования, заключения субподряда или финансирования риска;

e) сохранение риска на основе критериев принятия риска или обоснованного решения (например, поддержание существующей системы электронной коммерции в исходном виде).

Каждый отдельный риск должен быть обработан в соответствии с целями ИБ одним или несколькими вариантами, чтобы соответствовать критериям приемлемости риска.

Руководство по определению необходимых мер обеспечения ИБ (см. 6.1.3, перечисление b))

Особое внимание следует уделить определению необходимых мер обеспечения ИБ. Любую меру следует определять на основе ранее оцененных рисков ИБ. Если организация имеет низкую оценку риска ИБ, то у нее ограничивается выбор мер обеспечения ИБ.

Соответствующее определение мер обеспечивает:

f) включение всех необходимых мер обеспечения ИБ и исключение ненужных мер;

g) разработку необходимых мер, удовлетворяющих требуемому объему и глубине защиты.

Вследствие плохого выбора мер обеспечения ИБ предлагаемая обработка рисков ИБ может быть:

h) нерезультативной;

i) неэффективной и, следовательно, неоправданно дорогой.

В целях обеспечения результативной и эффективной обработки рисков ИБ важно иметь возможность наглядно показывать связь между необходимыми мерами обеспечения ИБ, результатами оценки рисков и процессами обработки рисков.

Для достижения требуемого плана обработки рисков ИБ может потребоваться использование нескольких мер обеспечения ИБ. Например, если выбран вариант с изменением последствий определенного события, могут потребоваться меры для быстрого обнаружения этого события, а также меры для реагирования и восстановления после него.

При определении мер обеспечения ИБ организация должна принимать во внимание те меры, которые необходимы для услуг, предоставляемых внешними поставщиками, например приложения, процессы и функции. Как правило, эти меры устанавливаются путем включения требований ИБ в соглашения с этими поставщиками, включая способы получения информации и о том, в какой степени эти требования выполняются (например, право на аудит). Могут быть ситуации, когда организация желает определить и описать подробные меры обеспечения ИБ как часть своей собственной СМИБ, даже если они выполняются внешними поставщиками. Независимо от принятого подхода организация всегда должна учитывать меры обеспечения ИБ, требуемые для поставщиков, при определении мер для своей СМИБ.

Руководство по сравнению мер обеспечения ИБ ИСО/МЭК 27001, приложение А (см. 6.1.3, перечисление c))

В приложении А ИСО/МЭК 27001 содержится исчерпывающий перечень целей и мер обеспечения ИБ. Пользователям настоящего стандарта рекомендуется использовать приложение А ИСО/МЭК 27001 в целях получения общего представления о мерах. Это гарантирует, что все необходимые меры обеспечения ИБ не будут упущены из виду. По сравнению с приложением А ИСО/МЭК 27001 также можно идентифицировать альтернативные меры обеспечения ИБ, определенные в 6.1.3, перечисление b), которые могут быть более эффективными при изменении риска ИБ.

Цели этих мер косвенным образом включены в выбранные меры обеспечения ИБ. Перечисленные в приложении А ИСО/МЭК 27001 цели не являются исчерпывающими, при необходимости следует использовать дополнительные цели и меры обеспечения ИБ.

Не каждую меру обеспечения ИБ в рамках приложения А ИСО/МЭК 27001 необходимо включать в СМИБ. Если мера не способствует модификации риска, она должна быть исключена с соответствующим обоснованием.

Руководство по созданию Положения о применимости (см. 6.1.3, перечисление d))

Положение о применимости содержит:

- все необходимые меры обеспечения ИБ (см. 6.1.3, перечисления b) и c)) и для каждой меры:
  - обоснование ее включения;
  - информация о ее реализации (например, полностью реализована, в процессе реализации, еще не реализована);

- обоснование исключения любой из мер ИСО/МЭК 27001, приложение А.

Обоснованием для включения меры в СМИБ является ее влияние на модификацию риска ИБ. Ссылки на результаты оценки рисков ИБ и план обработки рисков должны быть достаточными наряду с предполагаемыми изменениями риска в результате реализации мер обеспечения ИБ.

Обоснование исключения мер обеспечения ИБ, содержащихся в приложении А ИСО/МЭК 27001, может включать следующее:

- было установлено, что мера не является необходимой для реализации выбранного(ых) варианта(ов) обработки риска ИБ;

- мера не применима, потому что она выходит за рамки СМИБ (например, в ИСО/МЭК 27001:2013 мера А.14.2.7 «Разработка с использованием аутсорсинга» не применима, если вся разработка систем в организации осуществляется собственными силами);

- мера нейтрализуется другой пользовательской мерой (например, в ИСО/МЭК 27001:2013 мера А.8.3.1 «Управление сменными носителями информации» может быть исключена, если пользовательская мера запрещает использование сменных носителей).

Примечание — Пользовательская мера — это мера, не включенная в приложение А ИСО/МЭК 27001.

Эффективное Положение о применимости может быть сформировано в виде таблицы, содержащей в строках все 114 мер обеспечения ИБ ИСО/МЭК 27001, приложение А, плюс строки с дополнительными мерами, которые не упомянуты в приложении А ИСО/МЭК 27001, если это необходимо. Одна графа таблицы может указывать на необходимость меры для реализации варианта(ов) обработки риска или ее исключение. Следующая графа может содержать обоснование для включения или исключения меры обеспечения ИБ. Последняя графа таблицы может показывать текущий статус реализации меры обеспечения ИБ. Можно использовать дополнительные графы, например для детализации, которые не требуются в соответствии с ИСО/МЭК 27001, но которые обычно полезны для последующих проверок; детализация может представлять собой более подробное описание того, как реализована мера обеспечения ИБ, или перекрестную ссылку на более подробное описание и документированную информацию или политику, относящуюся к реализации этой меры.

Несмотря на то, что это не является конкретным требованием ИСО/МЭК 27001, организации могут посчитать целесообразным включить ответственность за функционирование каждой меры, содержащейся в Положении о применимости.

Руководство по разработке плана обработки рисков ИБ (см. 6.1.3 , перечисление е))

ИСО/МЭК 27001 не определяет структуру или содержание плана обработки рисков ИБ. Однако план должен быть разработан на основе результатов 6.1.3, перечисления а) — с). Таким образом, для каждого обработанного риска в плане должно быть задокументировано:

- выбранный(е) вариант(ы) обработки риска;
- необходимая(ые) мера(ы) обеспечения ИБ;
- статус реализации.

Документ также может включать в себя:

- владельца(ев) рисков;
- ожидаемый остаточный риск после реализации мероприятий.

Если какое-либо мероприятие требуется выполнить в соответствии с планом обработки риска, то оно должно быть запланировано с указанием ответственности и сроков завершения (см. подраздел 6.2); план мероприятий может быть представлен в виде списка этих мероприятий.

Эффективный план обработки рисков ИБ может быть разработан в виде таблицы, в которой отсортированы риски, выявленные в ходе оценки рисков, с указанием всех определенных мер обеспечения ИБ.

Например, в этой таблице могут быть графы, в которых указаны имена лиц, ответственных за обеспечение мер ИБ. В других графах могут быть указаны дата реализации этих мер, информация о том, как мера (или процесс) должна функционировать, и целевой статус ее реализации.

В качестве примера рассмотрим кражу мобильного телефона. Последствиями этого являются потеря доступности и потенциальное нежелательное раскрытие информации. Если оценка риска показала, что его уровень является неприемлемым, организация может принять решение об изменении вероятности или последствий риска.

Чтобы изменить вероятность потери или кражи мобильного телефона, организация может определить, какие подходящие меры обеспечения ИБ обяжут сотрудников посредством политики в отно-

шении мобильных устройств следить за мобильными телефонами и периодически проверять их на предмет потерь.

Чтобы изменить последствия от потери или кражи мобильного телефона, организация может определить такие меры, как:

- процесс управления инцидентами, чтобы пользователи могли сообщать о потере;
- удаленное управление мобильными устройствами для удаления данных телефона в случае его потери;
- план резервного копирования мобильных устройств для восстановления данных телефона.

Подготавливая свое Положение о применимости (см 6.1.3, перечисление d)), организация может включать выбранные ею меры обеспечения ИБ (политика в отношении мобильных устройств и удаленного управления мобильными устройствами), основываясь на влиянии изменения вероятности и последствий от потери или кражи мобильного телефона, что приводит к снижению остаточного риска.

Сравнивая эти меры с теми, которые перечислены в ИСО/МЭК 27001, приложение А (см. 6.1.3, перечисление c)), можно увидеть, что политика в отношении мобильных устройств присутствует в ИСО/МЭК 27001, А.6.2.1, но мера «Управление мобильными устройствами» непосредственно с ней не связана и должна рассматриваться как дополнительная пользовательская мера обеспечения ИБ. Если управление мобильными устройствами и другие меры определены как необходимые меры в плане обработки рисков информационной безопасности организации, их следует включить в Положение о применимости («Руководство по созданию положения о применимости» (см. 6.1.3, перечисление b)).

Если организация нацелена на еще большее снижение риска, то она может рассмотреть политику управления доступом из ИСО/МЭК 27001, А.9.1.1, а именно определить, чего ей не хватает для управления доступом к мобильным телефонам, и изменить свою политику в отношении мобильных устройств, чтобы ввести использование ПИН-кодов на всех мобильных телефонах. Это должно стать дополнительной мерой обеспечения ИБ для изменения последствий от потерь или кражи мобильных телефонов.

При разработке плана обработки рисков ИБ (см. 6.1.3, перечисление e)) организация должна включить мероприятия по реализации политики в отношении мобильных устройств и управления мобильными устройствами, а также распределить обязанности и временные рамки.

Руководство по получению одобрения владельцев рисков (см. 6.1.3, перечисление f))

При разработке плана обработки рисков ИБ организация должна получить разрешение от владельцев риска. Такое разрешение должно основываться на определенных критериях принятия рисков или на их обоснованном принятии, если есть какие-либо отклонения от них.

С помощью процессов управления организация должна фиксировать принятие владельцем остаточных рисков и одобрение руководством плана обработки рисков.

Например, принятие владельцем риска может быть задокументировано путем внесения исправлений в план обработки риска, описанный в руководстве 6.1.3, перечисление e), в графах, указывающих на эффективность мер обеспечения ИБ, а также на остаточный риск и одобрение владельца риска.

Дополнительная информация

Дополнительную информацию об обработке рисков можно найти в ИСО/МЭК 27005 и ИСО 31000.

6.2 Цели информационной безопасности и планирование их достижения

Необходимые мероприятия

Организация устанавливает цели ИБ и планы по их достижению для соответствующих функций и уровней.

Пояснение

Цели ИБ помогают реализовать стратегические цели организации, а также политику ИБ. Таким образом, цели СМИБ — это цели ИБ для обеспечения конфиденциальности, целостности и доступности информации. Цели ИБ также помогают определять и измерять эффективность мер обеспечения ИБ, процессов ИБ в соответствии с политикой ИБ (см. 5.2).

Организация планирует, устанавливает и определяет цели ИБ для соответствующих функций и уровней.

Требования в ИСО/МЭК 27001, относящиеся к целям ИБ, применяются ко всем целям ИБ. Если политика ИБ содержит цели, то эти цели должны соответствовать критериям, изложенным в этом разделе. Если политика содержит структуру для постановки целей, то цели, создаваемые этой структурой, должны соответствовать требованиям этого подраздела.

Требования, которые необходимо принимать во внимание при определении целей, это те требования, которые определяются при понимании организации и ее контекста (см. 4.1), а также потребностей и ожиданий заинтересованных сторон (см. 4.2).

Результаты оценки и обработки риска используются в качестве входных данных для постоянного анализа целей, чтобы убедиться, что они по-прежнему соответствуют условиям организации.

Цели ИБ являются исходными данными для оценки риска: критерии принятия риска и критерии для проведения оценки риска ИБ (см. 6.1.2) учитывают цели ИБ, и, таким образом, обеспечивается соответствие уровней риска с целями.

Цели ИБ согласно ИСО/МЭК 27001:

a) соответствуют политике ИБ;

b) измеримы, если это практически возможно; это означает, что важно уметь определять, была ли достигнута цель или нет;

c) связаны с применимыми требованиями ИБ и являются результатом оценки и обработки риска;

d) доведены до сведения;

e) обновляются по возможности.

Организация хранит документированную информацию о целях ИБ.

При планировании мероприятий по достижению целей ИБ организация определяет:

f) что будет сделано;

g) какие ресурсы потребуются;

h) кто будет нести ответственность;

i) когда это будет завершено;

j) как будут оцениваться результаты.

Упомянутое выше требование относительно планирования является общим и применимо также к другому планированию, регулируемому ИСО/МЭК 27001. Планирование, которое необходимо рассмотреть для СМИБ, включает:

- планы по улучшению СМИБ, как описано в 6.1.1 и 8.1;
- планы обработки идентифицированных рисков, как описано в 6.1.3 и 8.3;
- любые другие планы, которые будут признаны необходимыми для эффективной работы (например, планы по развитию компетенции и повышению осведомленности, коммуникации, оценке эффективности, внутреннему аудиту и контролю качества).

Руководство

Политика ИБ должна устанавливать цели ИБ или обеспечивать основу для их постановки.

Цели ИБ могут быть выражены различными способами. Это выражение должно соответствовать требованию об измеримости (если это практически возможно) (ИСО/МЭК 27001:2013, 6.2 b)).

Например, цели ИБ могут быть выражены в виде:

- числовых значений с их ограничениями, например «не превышать определенный предел» и «достичь уровня 4»;
- целей для измерения эффективности ИБ;
- целей для измерения эффективности СМИБ (см. 9.1);
- соответствия требованиям ИСО/МЭК 27001;
- соответствия процедурам СМИБ;
- необходимости выполнения действий и планов;
- критериев риска, которые должны быть выполнены.

Следующее руководство применимо к основополагающим целям, представленным выше:

- политика ИБ определяет требования к ИБ в организации. Все другие специфические требования, установленные для соответствующих функций и уровней, должны им соответствовать. Если политика ИБ содержит цели ИБ, то любая другая конкретная цель ИБ должна быть связана с целями, указанными в политике. Если политика ИБ только предоставляет структуру для постановки целей, то следует придерживаться этой структуры для обеспечения того, чтобы более конкретные цели были связаны с более общими (см. перечисление a));

- не каждая цель может быть измеримой, но если сделать ее таковой, то это поспособствует улучшению ее понимания и достижению. Важно иметь возможность качественно или количественно описать степень достижения цели. Например, для определения приоритетов для дополнительных усилий в случае, если цели не были достигнуты, или для предоставления возможностей для повышения эффективности СМИБ, если цели трудно достижимы. Также должна быть возможность понять, были ли достигнуты поставленные цели или нет, каким образом определяется достижение целей, а также

можно ли определить степень достижения целей, используя количественные измерения. Описания достижения цели в количественном выражении должны включать информацию о том, как проводилось соответствующее измерение. Может оказаться невозможным количественно определить степень достижения всех целей. ИСО/МЭК 27001 рекомендует, чтобы цели были измеримы, если это практически осуществимо (см. перечисление b));

- цели ИБ должны быть согласованы с потребностями ИБ; по этой причине результаты оценки и обработки рисков[1)] следует использовать в качестве исходных данных при определении целей ИБ (см. перечисление c));

- цели ИБ должны быть доведены до соответствующих внутренних заинтересованных сторон организации. Они также могут быть доведены до внешних заинтересованных сторон, например до клиентов или иных заинтересованных сторон, в той степени, в которой они должны знать о них и в которой их затрагивают цели ИБ (см. перечисление d));

- когда потребности в ИБ меняются со временем, тогда должны обновляться и соответствующие цели ИБ. Об их обновлении следует сообщать, как требуется в перечислении d), внутренним и внешним заинтересованным сторонам по возможности (см. перечисление e)).

Организация должна планировать, как достичь своих целей ИБ. Она может использовать любую методологию или механизм, который выберет для планирования и достижения своих целей ИБ. Может существовать единый план ИБ, один или несколько планов проектов или действий, включенных в другие организационные планы. Независимо от того, какую бы форму планирование не принимало, итоговые планы должны как минимум определять (см. перечисления f), g), h), i), j)):

- мероприятия, которые необходимо выполнить;
- необходимые ресурсы, которые должны быть выделены для выполнения мероприятий;
- ответственность;
- сроки и этапы мероприятий;
- методы и измерения, позволяющие оценить, достигают ли результаты поставленных целей, включая время проведения таких оценок.

ИСО/МЭК 27001 рекомендует организациям сохранять документированную информацию о целях ИБ. Такая документированная информация может включать в себя:

- планы, мероприятия, ресурсы, ответственность, сроки и методы оценки;
- требования, задачи, ресурсы, ответственность, частоту и методы оценки.

Дополнительная информация

Дополнительная информация отсутствует.

7 Поддержка

7.1 Ресурсы

Необходимые мероприятия

Организация определяет и предоставляет ресурсы для создания, внедрения, обслуживания и постоянного улучшения СМИБ.

Пояснение

Ресурсы имеют основополагающее значение для выполнения любого вида деятельности. Категории ресурсов могут включать в себя:

a) лиц, управляющих и выполняющих мероприятия;

b) время для выполнения мероприятий и время предоставления результатов, прежде чем делать следующий шаг;

c) финансовые ресурсы для приобретения, разработки и реализации того, что необходимо;

d) информацию для поддержки решений, измерения эффективности действий и повышения осведомленности;

e) инфраструктуру и другие средства, которые могут быть приобретены или созданы: технологии, инструменты и материалы, независимо от того, являются они продуктами информационных технологий или нет.

[1)] Термин «риск» определяется как «влияние неопределенности на цели» (ИСО/МЭК 27000).

Эти ресурсы должны быть приведены в соответствие с потребностями СМИБ и при необходимости должны быть адаптированы.

Руководство

Организация должна:

f) оценивать ресурсы, необходимые для всех мероприятий, связанных со СМИБ, с точки зрения количества и качества (способностей и возможностей);

g) приобретать ресурсы по мере необходимости;

h) предоставлять ресурсы;

i) поддерживать ресурсы по всем процессам СМИБ и конкретным мероприятиям;

j) проверять предоставленные ресурсы в соответствии с потребностями СМИБ и корректировать их по мере необходимости.

Документированная информация об этих мероприятиях и их результатах является обязательной только в той форме и в той мере, в которой организация считает это необходимым для эффективности своей системы менеджмента (см. ИСО/МЭК 27001, 7.5.1, перечисление b)).

Дополнительная информация

Дополнительная информация отсутствует.

7.2 Компетентность

Необходимые мероприятия

Организация определяет компетенции лиц, занимающихся обеспечением ИБ, и обеспечивает их компетентность.

Пояснение

Компетентность — это способность применять знания и умения для достижения намеченных результатов. На нее влияют знания, опыт и образование.

Компетенции могут быть специфическими (например, в отношении технологий или конкретных областей управления, таких как управление рисками) или общими (например, навыки работы с людьми, надежность и основные технологические и управленческие навыки).

Компетенции относятся к лицам, которые работают под контролем организации. Это означает, что управление компетенциями должно осуществляться для лиц, являющихся сотрудниками организации, и для других лиц по мере необходимости.

Приобретение высокого уровня компетентности или новых компетенций может быть достигнуто как внутри организации, так и за ее пределами посредством получения опыта, обучения (например, курсов, семинаров и практикумов), наставничества, найма или заключения контрактов с внешними лицами.

Для компетенций, которые необходимы лишь временно — для специфической деятельности или на короткий период времени, например, в связи с непредвиденной временной нехваткой внутреннего персонала, — организации могут нанимать или заключать контракты с внешними лицами, компетенции которых должны быть описаны и проверены.

Руководство

Организация должна:

a) определить ожидаемые компетенции для каждой роли в рамках СМИБ и решить, должны ли они быть задокументированы (например, в должностной инструкции);

b) назначить роли в рамках СМИБ (см. 5.3) лицам с необходимыми компетенциями. При необходимости это можно сделать следующим образом:

1) выявить лиц в рамках организации, обладающих компетенциями (например, на основании их образования, опыта или наличия сертификатов);

2) планировать и осуществлять мероприятия, направленные на получение компетенций лицами в рамках организации (например, путем организации обучения, наставничества, перевода имеющихся сотрудников);

3) привлечь новых лиц, обладающих компетенциями (например, путем найма или заключения контрактов);

c) оценить эффективность мероприятий, указанных в перечислении b) выше.

Примеры

1 Рассмотреть, приобрели ли лица компетенции после обучения.

2 Проанализировать компетенции вновь нанятых сотрудников через некоторое время после их появления в организации.

3 Убедиться, что план приобретения новых лиц выполнен должным образом;

d) проверить компетентность лиц для своих ролей;

e) обеспечить развитие компетенции со временем по мере необходимости и их соответствие ожиданиям.

В качестве доказательства компетентности требуется соответствующая документированная информация. Поэтому организация должна хранить документацию о необходимых компетенциях, влияющих на показатели ИБ, и о том, как эти компетенции обеспечиваются соответствующими лицами.

Дополнительная информация

Дополнительная информация отсутствует.

7.3 Осведомленность

Необходимые мероприятия

Лица, выполняющие работу под контролем организации, должны быть осведомлены о политике ИБ, их вкладе в эффективность СМИБ, преимуществах повышения результативности ИБ и последствиях несоответствия требованиям СМИБ.

Пояснение

Осведомленность лиц, работающих под контролем организации, означает наличие необходимого понимания и мотивации относительно того, что от них ожидается в части ИБ.

Осведомленность касается лиц, которые должны знать, понимать, принимать, а также:

a) поддерживать цели, изложенные в политике ИБ;

b) соблюдать правила, чтобы соответствующим образом выполнять свои повседневные задачи, касающиеся поддержки ИБ.

Кроме того, лица, выполняющие работу под контролем организации, также должны знать, понимать и принимать последствия несоответствия требованиям СМИБ. Последствия могут быть негативными для организации или для человека.

Сотрудники организации должны знать, что существует политика ИБ и где можно найти необходимую информацию о ней. Многим сотрудникам организации не нужно знать подробное содержание политики. Вместо этого им достаточно знать, понимать, принимать и реализовывать цели и требования ИБ, определенные в политике, касающиеся их должности и/или роли. Эти требования могут быть включены в стандарты или процедуры, которым они должны следовать при выполнении своей работы.

Руководство

Организация должна:

c) подготовить программу с конкретными знаниями, ориентированными на каждую аудиторию (например, на внутренних и внешних лиц);

d) включить потребности и ожидания в области ИБ в информационные и учебные материалы по другим темам для учета этих потребностей в соответствующем контексте организации;

e) подготовить план для распространения информации через запланированные интервалы времени;

f) проверять усвоение и понимание полученных знаний как после занятия по повышению осведомленности, так и произвольно между занятиями;

g) проверять, действуют ли лица в соответствии с полученными знаниями, и использовать примеры «хорошего» и «плохого» поведения для лучшего усвоения информации.

Документированная информация об этих мероприятиях и их результатах является обязательной только в той форме и в той мере, в которой организация считает это необходимым для эффективности своей системы менеджмента (см. ИСО/МЭК 27001, 7.5.1, перечисление b)).

Дополнительная информация

Дополнительную информацию об осведомленности в области ИБ можно найти в пункте 7.2.2 ИСО/МЭК 27002.

7.4 Взаимодействие

Необходимые мероприятия

Организация определяет потребность во взаимодействии внутри организации и с внешними сторонами по вопросам, связанным со СМИБ.

Пояснение

Взаимодействие является ключевым процессом в рамках СМИБ. Необходимо адекватное взаимодействие с внутренними и внешними заинтересованными сторонами (см. 4.2).

Взаимодействие может осуществляться между внутренними заинтересованными сторонами на всех уровнях в организации или между организацией и внешними заинтересованными сторонами. Взаимодействие может быть инициировано внутри организации или внешней заинтересованной стороной.

Организации должны определить:

- какие данные необходимо передать, например политики ИБ, цели, процедуры, их изменения, знания о рисках ИБ, требования к поставщикам и обратная связь об эффективности ИБ;
- предпочтительное или оптимальное время для взаимодействия;
- кто должен участвовать в процессах взаимодействия и кто является целевой аудиторией каждого взаимодействия;
- кто должен инициировать процесс взаимодействия, например определенные данные могут потребовать, чтобы взаимодействие было инициировано конкретным человеком или организацией;
- какие процессы являются движущими или инициирующими взаимодействие и какие процессы являются целевыми или затрагивают процессы взаимодействия.

Взаимодействие может происходить регулярно или по мере необходимости. Оно может быть проактивным или реактивным.

Руководство

Взаимодействие основывается на процессах, каналах и протоколах. Они должны быть выбраны таким образом, чтобы обеспечить целостное восприятие передаваемого сообщения, его правильное понимание и, когда это уместно, принятие соответствующих мер обеспечения ИБ.

Организации должны определить, какие сведения должны быть переданы, например:

a) планы и результаты управления рисками для заинтересованных сторон, когда это необходимо и уместно, при идентификации, анализе, оценке и обработке рисков;

b) цели ИБ;

c) достигнутые цели ИБ, в том числе те, которые могут поддержать их положение на рынке (например, выданный сертификат ИСО/МЭК 27001; утверждение о соответствии законодательству по защите персональных данных);

d) инциденты или непредвиденные обстоятельства, где прозрачность часто является ключом к сохранению и повышению доверия и уверенности в способности организации управлять своей ИБ и справляться с неожиданными ситуациями;

e) роли, обязанности и полномочия;

f) информация об обмене между функциями и ролями в соответствии с требованиями процессов СМИБ;

g) изменения в СМИБ;

h) сведения, выявленные путем анализа мер обеспечения ИБ и процессов в рамках СМИБ;

i) сведения о ситуациях (например, уведомление об инцидентах или непредвиденных обстоятельствах), требующих передачи информации регулирующим органам или другим заинтересованным сторонам;

j) запросы или другие сообщения от внешних сторон, таких как потенциальные клиенты, пользователи услуг, органы власти.

Организации должны определить требования к взаимодействию по соответствующим вопросам:

k) лица, которым разрешено осуществлять внешнее и внутреннее взаимодействие (например, в особых случаях, таких как нарушение конфиденциальности данных), путем распределения конкретных ролей с соответствующими полномочиями. Например, должностные лица по связям с общественностью могут быть наделены соответствующими полномочиями. Они могут быть сотрудниками по связям с общественностью для внешнего взаимодействия и сотрудниками службы безопасности для внутреннего взаимодействия;

l) триггеры или частота взаимодействия (например, для взаимодействия по случаю события триггером является установление факта наступления события);

m) содержание сообщений для ключевых заинтересованных сторон (например, клиентов, регулирующих органов, широкой общественности, важных внутренних пользователей) на основе сценариев воздействия высокого уровня. Взаимодействие может быть более эффективным, если оно основано на сообщениях, подготовленных и предварительно утвержденных на соответствующем уровне управления в рамках плана взаимодействия, плана реагирования на инциденты или плана обеспечения непрерывности бизнеса;

n) предполагаемые получатели сообщения. В некоторых случаях следует вести список (например, для сообщения об изменениях в услугах или о непредвиденных обстоятельствах);

o) средства связи и каналы. Для взаимодействия следует использовать специальные средства и каналы, необходимые для того, чтобы взаимодействующие стороны были убеждены, что сообщение является официальным и имеет соответствующие полномочия. Каналы связи должны удовлетворять любым потребностям по защите конфиденциальности и целостности передаваемой информации;

p) разработанный процесс и метод для обеспечения того, чтобы сообщения были отправлены, правильно приняты и поняты.

Сообщения, переданные в процессе взаимодействия, должны классифицироваться и обрабатываться в соответствии с требованиями организации.

Документированная информация об этих мероприятиях и их результатах является обязательной только в той форме и в той мере, в которой организация считает это необходимым для эффективности своей системы менеджмента (см. ИСО/МЭК 27001, 7.5.1, перечисление b)).

Дополнительная информация

Дополнительная информация отсутствует.

7.5 Документированная информация

7.5.1 Общие положения

Необходимые мероприятия

Организация включает документированную информацию в СМИБ в соответствии с требованиями ИСО/МЭК 27001, а также в соответствии с определением ее необходимости для эффективности СМИБ.

Пояснение

Документированная информация необходима для определения и информирования о целях, политике, руководствах, инструкциях, мерах обеспечения ИБ, процессах, процедурах ИБ и о том, что должны делать лица или группы лиц и как они должны себя вести. Документированная информация также необходима для аудитов СМИБ и поддержания стабильной СМИБ, при смене лиц, выполняющих ключевые роли. Кроме того, документированная информация необходима для регистрации мероприятий, решений и результатов процессов СМИБ и мер обеспечения ИБ.

Документированная информация может содержать:

- информацию о целях ИБ, рисках, требованиях и стандартах;
- информацию о необходимых процессах и процедурах, которым необходимо следовать;
- записи входных данных (например, для анализа со стороны руководства) и результаты процессов (включая планы и результаты мероприятий).

Существует множество видов деятельности в рамках СМИБ, по результатам которых производят документированную информацию и которые используются в большинстве случаев в качестве входных данных для другой деятельности.

ИСО/МЭК 27001 рекомендует наличие набора обязательной документированной информации и содержит общее требование о том, что дополнительная документированная информация требуется, если это необходимо для эффективности СМИБ.

Количество необходимой документированной информации часто зависит от размера организации.

В целом достаточно обязательной и дополнительной документированной информации для того, чтобы выполнить требования по оценке эффективности, указанные в разделе 9.

Руководство

Организация должна определить, какая документированная информация необходима для обеспечения эффективности СМИБ в дополнение к обязательной документированной информации, требуемой ИСО/МЭК 27001.

Чтобы соответствовать цели, документированная информация должна быть точной и основываться на фактах.

Примерами документированной информации, которую организация может определить как необходимую для обеспечения эффективности СМИБ, являются:

- результаты установления контекста организации (см. раздел 4);
- роли, обязанности и полномочия (см. раздел 5);
- отчеты о различных этапах управления рисками (см. раздел 6);
- определенные и предоставленные ресурсы (см. 7.1);
- ожидаемая компетентность (см. 7.2);
- планы и результаты мероприятий по повышению осведомленности (см. 7.3);
- планы и результаты коммуникационных мероприятий (см. 7.4);
- документированная информация внешнего происхождения, необходимая для СМИБ (см. 7.5.3);
- процесс контроля за документированной информацией (см. 7.5.3);
- политики, правила и директивы для управления и обеспечения мероприятий по ИБ;
- процессы и процедуры, используемые для внедрения, поддержания и улучшения СМИБ и общего состояния ИБ (см. раздел 9);
- планы действий;
- подтверждение результатов процессов СМИБ (например, управления инцидентами, контроля доступа, непрерывности ИБ, обслуживания оборудования и т. д.).

Документированная информация может иметь внутреннее или внешнее происхождение.

Дополнительная информация

Желание организации управлять своей документированной информацией в системе управления документами может быть реализовано в соответствии с требованиями ИСО 30301.

7.5.2 Создание и обновление

Необходимые мероприятия

Во время создания и обновления документированной информации организация обеспечивает ее надлежащую идентификацию, описание, формат, носителя, а также проверку и утверждение.

Пояснение

Организация тщательно разрабатывает структуру документированной информации и определяет надлежащий подход к документированию.

Проверка и утверждение соответствующим руководством гарантирует, что документированная информация является правильной, подходящей для данной цели, а также имеет адекватную форму и достаточную детализацию для целевой аудитории. Регулярные проверки обеспечивают постоянную пригодность и адекватность документированной информации.

Руководство

Документированная информация может храниться в любой форме, например, в традиционной (бумажной и электронной форме), в виде веб-страниц, баз данных, компьютерных журналов, сгенерированных компьютером отчетов, в форме аудио и видео. Кроме того, документированная информация может состоять как из подробного описания намерений (например, политика ИБ), так и из записей о производительности (например, результаты аудита) или их комбинации. Руководство, представленное ниже, относится непосредственно к документам в традиционной форме и должно толковаться соответствующим образом применительно к другим формам документированной информации.

Организации должны создать структурированную документированную информационную библиотеку, связывающую различные части документированной информации посредством:

a) определения структуры документированной информационной базы;

b) определения типовой структуры документированной информации;

c) предоставления шаблонов для различных типов документированной информации;

d) определения ответственности за подготовку, утверждение, публикацию и управление документированной информацией;

e) определения и документирования процесса пересмотра и утверждения для обеспечения постоянной пригодности и адекватности.

Организации должны определить подход к документированию, который включает в себя общие атрибуты каждого документа, позволяющие четко и уникально его идентифицировать. Общие атрибуты обычно включают в себя тип документа (например, политику, директиву, правило, руководство, план, форму, процесс или процедуру), цель и область применения, заголовок, дату публикации, классификацию, ссылочный номер, номер версии и историю изменений. Должны быть указаны сведения об авторе и лице(ах), которые в настоящее время несут ответственность за документ, его применение и изменение, а также сведения об утверждающем(их) лице(ах) или утверждающем органе.

Требования к формату могут включать определение подходящих языков документа, форматов файлов, версии программного обеспечения для работы с документами и графического содержимого. Требования к носителям определяют, на каких физических и электронных носителях должна быть доступна информация.

Заявления и стиль написания должны быть адаптированы к аудитории и объему документации.

Следует избегать дублирования документированной информации и использовать перекрестные ссылки, а не копировать одну и ту же информацию в разные документы.

Выбранный подход к документированию должен обеспечивать своевременную проверку документированной информации и утверждение всех изменений в документе. Соответствующие критерии проверки могут быть связаны со временем (например, максимальные периоды времени между проверками документа) или с содержанием. Должны быть определены критерии утверждения, которые гарантируют, что документированная информация является правильной, подходящей для данной цели, а также имеет адекватную форму и достаточную детализацию для целевой аудитории.

Дополнительная информация

Дополнительная информация отсутствует.

7.5.3 Контроль документированной информации

Необходимые мероприятия

Организация управляет документированной информацией на протяжении всего ее жизненного цикла и делает ее доступной там, где и когда это необходимо.

Пояснение

После утверждения документированная информация передается целевой аудитории. Документированная информация доступна там, где и когда это необходимо, сохраняя при этом свою целостность, конфиденциальность и актуальность на протяжении всего жизненного цикла.

Следует обратить внимание, что мероприятия, описанные «по возможности» в пункте 7.5.3 ИСО/МЭК 27001, необходимо проводить, если они выполнимы и являются полезными для организации, с учетом потребностей и ожиданий организации.

Руководство

Для облегчения доступа к документированной информации можно использовать структурированную библиотеку документированной информации.

Вся документированная информация должна быть классифицирована (см. ИСО/МЭК 27001, приложение А, пункт А.8.2.1) в соответствии со схемой классификации организации. Документированная информация должна защищаться и обрабатываться в соответствии с уровнем ее классификации (см. ИСО/МЭК 27001, приложение А, пункт А.8.2.3).

Процесс управления изменениями документированной информации должен гарантировать, что только уполномоченные лица имеют право изменять и распространять ее по мере необходимости с помощью соответствующих и заранее определенных средств. Документированная информация должна быть защищена, чтобы обеспечить сохранность достоверности и подлинности.

Документированная информация должна распространяться и предоставляться уполномоченным заинтересованным сторонам. Для этого организация должна установить, кто является соответствующей заинтересованной стороной для каждого вида документированной информации (или группы документированной информации), а также средства, используемые для распространения, доступа, поиска и использования этой информации (например, веб-сайт с соответствующими механизмами контроля доступа). Распространение должно соответствовать любым требованиям, связанным с защитой и обработкой классифицированной информации.

Организация должна установить соответствующий срок хранения документированной информации в соответствии с ее предполагаемым сроком действия и другими соответствующими требованиями. Также организация должна обеспечить, чтобы информация была разборчивой в течение всего срока ее хранения (например, при использовании форматов, которые могут быть прочитаны с помощью доступного программного обеспечения, или проверка на отсутствие повреждений бумажного носителя).

Организация должна определить, что делать с документированной информацией после истечения срока ее хранения.

Организация также должна управлять документированной информацией внешнего происхождения (т. е. от клиентов, партнеров, поставщиков, регулирующих органов и т. д.).

Документированная информация об этих мероприятиях и их результатах является обязательной только в той форме и в той мере, в которой организация считает это необходимым для эффективности своей системы менеджмента (см. ИСО/МЭК 27001, 7.5.1, перечисление b)).

Дополнительная информация

Дополнительная информация отсутствует.

8 Эксплуатация

8.1 Оперативное планирование и контроль

Необходимые мероприятия

Организация планирует, внедряет и контролирует процессы в соответствии с требованиями ИБ и для достижения целей ИБ.

Организация хранит документированную информацию, необходимую для обеспечения уверенности в том, что процессы осуществляются в соответствии с планом.

Организация контролирует запланированные изменения и анализирует последствия непреднамеренных изменений, а также обеспечивает выявление, определение и контроль процессов, находящихся на аутсорсинге.

Пояснение

Процессы, которые организация использует для удовлетворения своих требований ИБ, планируются и после их внедрения контролируются, особенно когда требуются изменения.

Опираясь на планирование СМИБ (см. 6.1 и 6.2), организация выполняет необходимое оперативное планирование и мероприятия по внедрению процессов, необходимых для выполнения требований ИБ.

Процессы, отвечающие требованиям ИБ, включают в себя:

a) процессы СМИБ (например, анализ со стороны руководства, внутренний аудит);

b) процессы, необходимые для реализации плана обработки рисков ИБ.

Реализация планов приводит к управляемым и контролируемым процессам.

Организация должна нести ответственность за планирование и контроль любых процессов, переданных на аутсорсинг, для достижения целей ИБ. Таким образом, организация должна:

c) определить процессы с учетом рисков ИБ, связанных с аутсорсингом;

d) обеспечивать контроль за процессами, находящимися на аутсорсинге (т. е. планирование, мониторинг и проверки), таким образом, чтобы не возникало никаких сомнений в том, что они работают не по назначению (также с учетом целей ИБ и плана обработки рисков ИБ).

После завершения внедрения процессы управляются, подвергаются мониторингу и проверкам, чтобы гарантировать, что они продолжают выполнять требования, определенные после понимания потребностей и ожиданий заинтересованных сторон (см. 4.2).

Изменения СМИБ могут быть запланированными или непреднамеренными. Всякий раз, когда организация вносит изменения в СМИБ (намеренно или непреднамеренно), она оценивает потенциальные последствия от изменений для контроля любых неблагоприятных последствий.

Организация может получить уверенность в эффективности выполнения планов, документируя мероприятия и используя документированную информацию в качестве входных данных для процессов оценки эффективности, указанных в разделе 9. Поэтому организация устанавливает список необходимой документированной информации для хранения.

Руководство

Процессы, которые были определены в результате планирования, описанного в разделе 6, должны быть внедрены, эксплуатироваться и проверяться в рамках всей организации. Необходимо рассмотреть и осуществить:

e) процессы, специфичные для управления ИБ (такие как управление рисками, управление инцидентами, управление непрерывностью, внутренние аудиты, анализ со стороны руководства);

f) процессы, вытекающие из мер обеспечения ИБ в плане обработки рисков ИБ;

g) разработку структуры отчетности (содержание, периодичность, формат, ответственность и т. д.) в области ИБ, например отчеты об инцидентах, отчеты об измерении достижения целей ИБ, отчеты о выполненных мероприятиях и т. д.;

h) разработку структуры совещаний (частота, участники, назначение и полномочия), связанных с ИБ. Мероприятия по ИБ должны координироваться представителями различных подразделений организации с соответствующими ролями и должностными функциями для эффективного управления ИБ.

Для запланированных изменений организация должна:

i) планировать их выполнение и назначать задачи, обязанности, сроки и ресурсы;

j) вносить изменения в соответствии с планом;

k) контролировать их выполнение, чтобы подтвердить, что они выполняются в соответствии с планом;

l) собирать и хранить документированную информацию о выполнении изменений в качестве доказательства того, что они были выполнены в соответствии с планом (например, с указанием обязанностей, сроков, оценок эффективности и т. д.).

Для наблюдаемых непреднамеренных изменений организация должна:

m) проанализировать последствия от них;

n) определить, имели ли место какие-либо неблагоприятные последствия или они могут произойти в будущем;

o) планировать и осуществлять действия для смягчения любых неблагоприятных последствий по мере необходимости;

p) собирать и хранить документированную информацию о непреднамеренных изменениях и действиях, предпринятых для смягчения неблагоприятных последствий.

Если часть функций или процессов организации передается на аутсорсинг, организация должна:

q) определить все аутсорсинговые отношения;

r) установить соответствующие интерфейсы для поставщиков;

s) решать вопросы, связанные с ИБ, в соглашениях с поставщиками;

t) осуществлять мониторинг и проверку услуг поставщиков, чтобы убедиться, что они работают так, как запланировано, а связанные с этим риски ИБ соответствуют критериям приемлемости рисков организации;

u) при необходимости управлять изменениями в услугах поставщика.

Дополнительная информация

Дополнительная информация отсутствует.

8.2 Оценка риска информационной безопасности

Необходимые мероприятия

Организация проводит оценку рисков ИБ и сохраняет документированную информацию о ее результатах.

Пояснение

При проведении оценки риска ИБ организация выполняет процесс, определенный в 6.1.2. Эти оценки выполняются либо в соответствии с заранее определенным планом, либо в ответ на значительные изменения или инциденты ИБ. Результаты оценок риска ИБ сохраняются в виде документированной информации в качестве доказательства того, что процесс, определенный в 6.1.2, был выполнен в соответствии с требованиями.

Документированная информация, полученная в результате оценки рисков ИБ, важна для обработки рисков ИБ, а также важна для оценки эффективности (см. раздел 9).

Руководство

Организации должны иметь план проведения оценки рисков ИБ.

В случае каких-либо значительных изменений СМИБ (или ее контекста) или инцидентов ИБ организация должна определить:

a) какие из этих изменений или инцидентов требуют дополнительной оценки риска ИБ;

b) чем вызвано проведение этих оценок.

Уровень детализации в идентификации рисков должен постепенно уточняться в ходе дальнейших итераций оценки рисков ИБ в контексте постоянного улучшения СМИБ. Масштабная оценка рисков ИБ должна проводиться не реже одного раза в год.

Дополнительная информация

ИСО/МЭК 27005 предоставляет руководство по проведению оценки рисков ИБ.

8.3 Обработка риска информационной безопасности

Необходимые мероприятия

Организация реализует план обработки риска ИБ и хранит документированную информацию о результатах.

Пояснение

Чтобы обработать риск ИБ, организации необходимо выполнить процесс обработки риска ИБ, определенный в 6.1.3. В процессе эксплуатации СМИБ, когда оценка риска обновляется в соответствии с 8.1, организация затем обрабатывает риск в соответствии с 6.1.3 и обновляет план по его обработке. Обновленный план обработки риска выполняется снова.

Результаты обработки риска ИБ сохраняются в документированной информации в качестве доказательства того, что процесс, определенный в 6.1.3, был выполнен в соответствии с требованиями.

Руководство

Процесс обработки риска ИБ должен выполняться после каждой итерации процесса оценки ИБ, приведенного в 8.2, или при неудачной реализации плана обработки риска или его частей.

Эта деятельность должна определять и контролировать ход осуществления плана обработки рисков ИБ.

Дополнительная информация

Дополнительная информация отсутствует.

9 Оценка эффективности

9.1 Мониторинг, измерение, анализ и оценка

Необходимые мероприятия

Организация оценивает эффективность ИБ и СМИБ.

Пояснение

Цель мониторинга и измерения заключается в том, чтобы помочь организации понять, достигнуты ли ожидаемые результаты мероприятий по ИБ, включая оценку и обработку рисков в соответствии с планом.

Мониторинг определяет состояние системы, процесса или деятельности, а оценка — это процесс определения значения. Таким образом, мониторинг может быть достигнут путем выполнения аналогичных измерений в течение некоторого периода времени.

Для мониторинга и оценки организация устанавливает:

a) что подвергать мониторингу и измерять;

b) кто и когда производит мониторинг и измерения;

c) методы, которые должны использоваться для получения достоверных результатов (то есть сопоставимых и воспроизводимых).

Для анализа и оценки организация устанавливает:

d) кто и когда анализирует и оценивает результаты мониторинга и измерений;

e) методы, которые будут использоваться для получения достоверных результатов.

Существует два аспекта оценки:

f) оценка эффективности ИБ для определения, работает ли организация, как это ожидается, что включает определение, насколько хорошо процессы в рамках СМИБ соответствуют их спецификациям;

g) оценка эффективности СМИБ для определения, предпринимает ли организация верные шаги, включая определение степени достижения целей ИБ.

Примечание — Термин «по возможности» (см. подраздел 9.1, перечисление b) ИСО/МЭК 27001) означает, что если методы мониторинга, измерения, анализа и оценки могут быть определены, то их необходимо определить.

Руководство

Хорошей практикой является определение «информационной потребности» при планировании мониторинга, измерений, анализа и оценки. Информационная потребность обычно выражается в виде вопроса или заявления высокого уровня, касающихся ИБ, которые помогают организации оценить эффективность ИБ и СМИБ. Другими словами, мониторинг и измерение должны проводиться для достижения определенной информационной потребности.

Следует проявлять осторожность при определении признаков, которые будут измеряться. Сложно выполнимо, дорого и контрпродуктивно измерять слишком много признаков или неправильно выбранные признаки. Помимо затрат на измерение, анализ и оценку многочисленных признаков, существует вероятность того, что ключевые факторы могут быть скрыты или совсем пропущены.

Существует два типа измерений:

h) измерения производительности, которые выражают запланированные результаты с точки зрения характеристик планируемой деятельности, таких как подсчет количества сотрудников, достижение контрольных показателей или степени, в которой реализованы меры обеспечения ИБ;

i) оценка эффективности, которая выражает влияние реализации запланированных мероприятий на цели ИБ организации.

Может оказаться целесообразным определить и назначить особые роли тем, кто участвует в мониторинге, измерении, анализе и оценке. Этими ролями могут быть заказчик измерения, планировщик измерений, проверяющий измерения, владелец информации, сборщик информации, информационный аналитик и ответственный за передачу информации для оценки (ИСО/МЭК 27004, подраздел 6.5).

Обязанности по мониторингу и измерению, а также по анализу и оценке часто возлагаются на отдельных лиц, которым требуется различная компетентность.

Дополнительная информация

Мониторинг, измерение, анализ и оценка имеют решающее значение для эффективности СМИБ. В ИСО/МЭК 27001 имеется ряд положений, которые явно требуют определения эффективности некоторых мероприятий. Например, ИСО/МЭК 27001, 6.1.1, перечисление e), 7.2, перечисление c) или 10.1, перечисление d).

Дополнительную информацию можно найти в ИСО/МЭК 27004, который содержит руководство по выполнению требований, приведенных в подразделе 9.1 ИСО/МЭК 27001. В частности, в нем расширяются все упомянутые выше понятия, такие как роли, обязанности и формы, и приводятся многочисленные примеры.

9.2 Внутренний аудит

Необходимые мероприятия

Организация проводит внутренние аудиты для предоставления информации о соответствии СМИБ требованиям.

Пояснение

Оценка СМИБ через запланированные интервалы времени посредством проведения внутренних аудитов обеспечивает уверенность в состоянии СМИБ для высшего руководства. Аудит характеризуется рядом принципов: целостность, честное представление результатов, профессионализм сотрудников, конфиденциальность, независимость и подход, основанный на доказательствах (ИСО 19011).

Внутренние аудиты предоставляют информацию, соответствует ли СМИБ «собственным требованиям организации» к ее СМИБ, а также требованиям ИСО/МЭК 27001. Собственные требования организации могут включать:

a) требования, изложенные в политике ИБ и процедурах;

b) требования, предъявляемые структурой для установления целей ИБ, включая результаты процесса обработки рисков;

c) правовые и договорные требования;

d) требования к документированной информации.

Аудитор также оценивает, эффективно ли внедрена и поддерживается СМИБ.

Программа аудита описывает общую структуру для ряда аудитов, запланированных на конкретные сроки и направленных на конкретные цели. Она отличается от плана аудита, который описывает мероприятия и механизмы для конкретного аудита. Критерии аудита — это набор политик, процедур или требований, используемых в качестве эталона, с которым сравниваются аудиторские доказательства, т. е. критерии аудита описывают то, что аудитор ожидает получить.

Внутренний аудит может выявить несоответствия, риски и возможности. Управление несоответствиями производится на основании требований, описанных в 10.1. Управление рисками и возможность их возникновения осуществляется в соответствии с требованиями, описанными в 4.1 и 6.1.

Организация должна хранить документированную информацию о программе(ах) и результатах аудита.

Руководство

Управление программой аудита

Программа аудита определяет структуру и ответственность за планирование, проведение, отчетность и контроль за отдельными мероприятиями по аудиту. Программа аудита, как таковая, должна гарантировать, что проводимые аудиты являются уместными, имеют правильную область проверки,

минимально влияют на деятельность организации, и поддерживать необходимое качество аудитов. Программа аудита должна также обеспечивать компетентность групп по аудиту, надлежащее ведение записей аудита, а также мониторинг и анализ процессов, рисков и эффективности аудитов. Кроме того, программа аудита должна гарантировать, что СМИБ (т. е. все соответствующие процессы, функции и меры обеспечения ИБ) проверяются в течение определенного периода времени. Наконец, программа аудита должна включать документированную информацию о типах, продолжительности, местах и графике проведения аудитов.

Степень и частота проведения внутренних аудитов должны быть основаны на размере и характере организации, а также на характере, функциональности, сложности и уровне сформированности СМИБ (риск-ориентированная программа аудита).

Эффективность внедренных мер обеспечения ИБ следует рассматривать в рамках внутренних аудитов. Программа аудита должна быть разработана таким образом, чтобы покрывать все необходимые меры, и должна включать оценку эффективности отдельно выбранных мер с течением времени. Ключевые меры обеспечения ИБ (в соответствии с риск-ориентированной программой аудита на основе оценки рисков) должны быть включены в каждый аудит, в то время как остальные меры, применяемые для управления более низкими рисками, могут проверяться реже.

Программа аудита также должна учитывать, что некоторые процессы и меры обеспечения ИБ должны работать в течение некоторого времени, чтобы можно было оценить соответствующие доказательства.

Внутренние аудиты, касающиеся СМИБ, могут эффективно выполняться в сотрудничестве с другими внутренними аудитами организации. Программа аудита может включать аудиты, связанные с одним или несколькими стандартами систем менеджмента, проводимые отдельно или в комбинации.

Программа аудита должна включать документированную информацию о критериях и методах аудита, выборе групп по аудиту, процессах обеспечения конфиденциальности, ИБ, охране здоровья и других подобных вопросах.

Компетентность и оценка аудиторов

Организация должна:

e) определить требования к компетентности своих аудиторов;

f) выбрать внутренних или внешних аудиторов, обладающих соответствующей компетентностью;

g) иметь процесс мониторинга эффективности аудиторов и групп по аудиту;

h) включить в состав групп по внутреннему аудиту персонал, обладающий соответствующими отраслевыми знаниями и знаниями в области ИБ.

Аудиторы должны выбираться с учетом того, что они должны быть компетентными, независимыми и надлежащим образом подготовленными.

Выбор внутренних аудиторов может быть затруднительным для небольших компаний. Если в организации нет необходимых ресурсов и компетенций, должны быть привлечены внешние аудиторы. Когда организации привлекают внешних аудиторов, то они должны убедиться, что аудиторы имеют или получают достаточно знаний о контексте организации. Эта информация должна быть представлена внутренним персоналом.

Организации должны учитывать, что сотрудники, выступающие в качестве внутренних аудиторов, могут иметь возможность проводить детальные аудиты с учетом контекста организации, но при этом могут не обладать достаточными знаниями о проведении аудитов.

Организации должны учитывать особенности и потенциальные недостатки внутренних и внешних аудиторов и создавать подходящие группы по аудиту с необходимыми знаниями и компетенциями.

Проведение аудита

При проведении аудита руководитель группы по аудиту должен подготовить план аудита с учетом результатов предыдущих аудитов и необходимости отслеживать ранее сообщенные несоответствия и неприемлемые риски. План аудита должен быть сохранен в виде документированной информации и должен включать критерии, область и методы аудита.

Группа по аудиту должна проверить:

- адекватность и эффективность процессов и определенных мер обеспечения ИБ;
- выполнение целей ИБ;
- соответствие требованиям, определенным в ИСО/МЭК 27001, разделы 4—10;
- соответствие организации собственным требованиям ИБ;
- соответствие Положения о применимости с результатами процесса обработки рисков ИБ;

- соответствие фактического плана обработки рисков ИБ с идентифицированными, оцененными рисками и критериями принятия рисков;

- актуальность (с учетом размера и сложности организации) результатов анализа со стороны руководства;

- влияние результатов анализа со стороны руководства (включая потребности в улучшении) на организацию.

Степень и надежность имеющегося мониторинга эффективности мер обеспечения ИБ, созданного СМИБ (см. 9.1), могут помочь аудиторам при условии, что они подтвердили эффективность методов измерения.

Если результат аудита включает несоответствия, аудитор должен подготовить план действий для каждого несоответствия, который должен быть согласован с руководителем группы по аудиту. План последующих действий обычно включает в себя:

i) описание обнаруженного несоответствия;

j) описание причин(ы) несоответствия;

k) описание краткосрочных и долгосрочных корректирующих действий для устранения обнаруженного несоответствия в установленный срок;

l) лиц, ответственных за реализацию плана.

Отчеты с результатами аудита должны быть распространены среди высшего руководства.

Результаты предыдущих аудитов должны быть проверены, а программа аудита должна быть выверена с целью лучшего управления областями, которые подвергаются более высоким рискам из-за наличия несоответствия.

Дополнительная информация

Дополнительную информацию можно найти в ИСО 19011, в котором содержится общее руководство по системам управления аудитом, включая принципы проведения аудита, управление программой аудита и проведение аудита системы управления. В нем также содержится руководство по оценке компетентности лиц или групп лиц, участвующих в аудите, в том числе лиц, управляющих программой аудита, аудиторов и групп по аудиту.

Кроме того, в дополнение к руководству, содержащемуся в ИСО 19011, необходимую информацию можно найти в:

a) ИСО/МЭК 27007, в котором содержатся конкретные рекомендации по управлению программой аудита СМИБ, проведению аудитов и компетенции аудиторов СМИБ;

b) ИСО/МЭК 27008, который содержит руководство по оценке средств контроля ИБ.

9.3 Анализ со стороны руководства

Необходимые мероприятия

Анализ СМИБ со стороны высшего руководства проводится с запланированной периодичностью.

Пояснение

Целью анализа со стороны руководства является обеспечение постоянной пригодности, адекватности и эффективности СМИБ. Под пригодностью подразумевается постоянное соответствие целям организации. Адекватность и эффективность относятся к проектированию и организационному внедрению СМИБ, а также к эффективному внедрению процессов и мер обеспечения ИБ, которые управляются СМИБ.

В целом анализ со стороны руководства — это процесс, осуществляемый на различных уровнях в организации. Он может варьироваться от ежедневных, еженедельных или ежемесячных собраний подразделений организации до простых обсуждений отчетов. Высшее руководство в итоге несет ответственность за анализ со стороны руководства с участием всех уровней организации.

Руководство

Высшее руководство должно требовать и регулярно анализировать отчетность об эффективности СМИБ.

Существует множество способов, с помощью которых руководство может анализировать СМИБ, таких как получение и анализ результатов измерений и отчетов, электронная и устная связь. Ключевыми входными данными являются результаты измерений ИБ, как описано в 9.1, и результаты внутренних аудитов, описанных в 9.2, а также результаты оценки рисков и статус выполнения плана обработки рисков. При анализе результатов оценки рисков ИБ и статуса выполнения плана обработки рисков ру-

ководство должно подтвердить, что остаточные риски соответствуют критериям приемлемости рисков и что план обработки рисков учитывает все актуальные риски и возможные варианты их обработки.

В целом все аспекты СМИБ должны анализироваться руководством через запланированные промежутки времени (по крайней мере раз в год) путем составления соответствующих графиков и обсуждения повесток на совещаниях руководства. Новые или не очень развитые СМИБ должны чаще анализироваться руководством для повышения эффективности.

Повестка собрания для анализа со стороны руководства должна касаться следующих тем:

a) статус выполнения действий по результатам предыдущих анализов со стороны руководства;

b) изменения во внешних и внутренних факторах (см. 4.1), которые имеют отношение к СМИБ;

c) отзывы об эффективности ИБ, включая тенденции о:

1) несоответствиях и корректирующих действиях;

2) результатах мониторинга и измерений;

3) результатах аудита;

4) достижениях целей ИБ;

d) отзывы заинтересованных сторон, в том числе предложения по улучшению, запросы на изменения и жалобы;

e) результаты оценки рисков ИБ и статус выполнения плана обработки рисков;

f) возможности постоянного улучшения, включая повышение эффективности как СМИБ, так и мер обеспечения ИБ.

Входные данные для анализа должны иметь определенный уровень детализации в соответствии с целями, установленными для руководства, участвующего в анализе. Например, высшее руководство должно оценивать только сводные данные по всем элементам в соответствии с целями ИБ или целями высокого уровня.

Результаты процесса анализа должны включать решения, касающиеся возможностей постоянного улучшения и любых потребностей в изменениях СМИБ. Они также могут включать доказательства решений относительно:

g) изменения политики и целей ИБ, например, обусловленных изменениями во внешних и внутренних факторах и требованиях заинтересованных сторон;

h) изменения критериев принятия риска и критериев оценки риска ИБ (см. 6.1.2);

i) действий, при необходимости, после оценки эффективности ИБ;

j) изменения ресурсов или бюджета для СМИБ;

k) обновленного плана обработки рисков ИБ или Положения о применимости;

l) необходимых улучшений мероприятий по мониторингу и измерениям.

Требуется документировать информацию по анализам со стороны руководства. Ее также следует сохранять, чтобы продемонстрировать, что внимание было уделено всем областям, перечисленным в ИСО/МЭК 27001, даже если было решено, что никаких действий не требуется.

Когда на разных уровнях организации проводится несколько анализов со стороны руководства, они должны быть соответствующим образом связаны друг с другом.

Дополнительная информация

Дополнительная информация отсутствует.

10 Улучшение системы менеджмента информационной безопасности

10.1 Несоответствия и корректирующие действия

Необходимые мероприятия

Организация реагирует на несоответствия, оценивает их и принимает решения об их исправлении, а также о корректирующих действиях, если это необходимо.

Пояснение

Несоответствие — это невыполнение требований СМИБ. Требования — это потребности или ожидания, которые заявлены, подразумеваются или являются обязательными. Существует несколько типов несоответствий, таких как:

a) невыполнение требования (полностью или частично) ИСО/МЭК 27001 в СМИБ;

b) неспособность правильно выполнить или соответствовать требованию, правилу или мере, установленным СМИБ;

c) частичное или полное несоблюдение юридических, договорных или согласованных требований клиента.

Несоответствия могут касаться, например:

d) лиц, которые ведут себя не так, как ожидается в соответствии с процедурами и политиками;

e) поставщиков, не предоставляющих согласованные продукты или услуги;

f) проектов, не дающих ожидаемых результатов; и

g) мер обеспечения ИБ, функционирующих не так, как было задумано.

Несоответствия могут быть определены по:

h) недостаткам мероприятий, осуществляемых в рамках СМИБ;

i) неэффективным мерам обеспечения ИБ, которые не устраняются соответствующим образом;

j) анализу инцидентов ИБ, показывающих невыполнение требования СМИБ;

k) жалобам клиентов;

l) предупреждениям от пользователей или поставщиков;

m) результатам мониторинга и измерений, не соответствующим критериям приемлемости;

n) целям, которые не были достигнуты.

Исправления направлены на немедленное устранение несоответствия и его последствий (см. ИСО/МЭК 27001, 10.1, перечисление a)).

Корректирующие действия направлены на устранение причины несоответствия и предотвращение его повторения (см. ИСО/МЭК 27001, 10.1, перечисления b) — g)).

Следует обратить внимание, что понятие «по возможности» (ИСО/МЭК 27001, 10.1, перечисление a)) означает, что если действие по контролю и исправлению несоответствия осуществимо, то оно должно быть предпринято.

Руководство

Инциденты ИБ не обязательно означают, что существует несоответствие, но они могут быть индикаторами несоответствия. Внутренний и внешний аудиты и жалобы клиентов являются другими важными источниками, которые помогают в выявлении несоответствий.

Реакция на несоответствие должна основываться на определенном процессе обработки. Процесс должен включать в себя:

- выявление масштабов и последствий несоответствия;

- принятие решения об исправлениях для ограничения влияния несоответствия. Исправления могут включать переключение в предыдущее, отказоустойчивое или другое соответствующие состояние. Следует позаботиться о том, чтобы исправления не усугубляли ситуацию в отношении:

- общения с соответствующим персоналом для обеспечения проведения исправлений;

- проведения исправлений в соответствии с решением;

- мониторинга ситуации, чтобы убедиться, что исправления имели ожидаемый эффект и не привели к непреднамеренным побочным эффектам;

- дальнейших действий по исправлению несоответствия, если оно все еще не устранено;

- по возможности общения с другими заинтересованными сторонами.

В результате процесс обработки должен привести к ситуации, где несоответствия и связанные с ними последствия находятся под контролем. Однако одни только исправления не предотвратят повторения несоответствия.

Корректирующие действия могут проходить после или параллельно с исправлениями. Для этого необходимо предпринять следующие шаги:

- принять решение о необходимости выполнения корректирующих действий в соответствии с установленными критериями (например, влияние несоответствия, повторяемость и т. д.);

- проанализировать несоответствия, учитывая:

  - были ли зарегистрированы подобные несоответствия;

  - все последствия и побочные эффекты, вызванные несоответствием;

  - предпринятые исправления;

- выполнить углубленный анализ причин несоответствия, учитывая:

  - что пошло не так; конкретный триггер или ситуация, которая привела к несоответствию (ошибки, вызванные людьми, методами, процессами или процедурами, аппаратными или программными средствами, неправильными измерениями, средой);

  - модели и критерии, которые могут помочь идентифицировать подобные ситуации в будущем;

- выполнить анализ возможных последствий несоответствий СМИБ, учитывая:

- существуют ли подобные несоответствия в других областях, например, с помощью моделей и критериев, найденных в ходе анализа причин этих последствий;

- соответствуют ли другие области указанным моделям или критериям так, что подобное несоответствие является лишь вопросом времени;

- определить действия, необходимые для устранения причины, оценить, соразмерны ли они последствиям и влиянию несоответствия, и проверить, не имеют ли они побочных эффектов, которые могут привести к другим несоответствиям или значительным новым рискам ИБ;

- планировать корректирующие действия, отдавая, если возможно, приоритет тем областям, где существует более высокая вероятность повторения несоответствия и более существенных последствий от него. Планирование должно включать ответственное лицо за корректирующие действия и сроки для их выполнения;

- выполнить корректирующие действия в соответствии с планом;

- оценить корректирующие действия, чтобы определить, действительно ли они устранили причину несоответствия и предотвратили возникновение других связанных несоответствий. Эта оценка должна быть беспристрастной, основанной на фактических доказательствах и должна быть задокументирована. Об этом также следует сообщить соответствующим ролям и заинтересованным сторонам.

В результате исправлений и корректирующих действий, возможно, будут выявлены новые возможности для улучшения. К ним следует относиться соответствующим образом (см. 10.2).

Необходимо сохранить достаточное количество документированной информации, чтобы продемонстрировать, что организация действовала надлежащим образом в ходе устранения несоответствия и боролась с соответствующими последствиями. Все существенные этапы управления несоответствиями (начиная с обнаружения и исправления) и корректирующими действиями (анализ причин, проверка, решение о реализации действий, анализ и принятие решений об изменениях, принятых для самой СМИБ) должны быть задокументированы. В документированной информации должны быть доказательства, помогли ли предпринятые действия достичь ожидаемых результатов.

Некоторые организации ведут реестры для отслеживания несоответствий и корректирующих действий. Может быть несколько реестров (например, один для каждой функциональной области или процесса) и на разных носителях (бумага, файл, приложение и т. д.). При этом их следует создавать и контролировать как документированную информацию, и они должны позволять проводить всесторонний анализ всех несоответствий и корректирующих действий для обеспечения правильной оценки необходимости действий.

Дополнительная информация

ИСО/МЭК 27001 явно не устанавливает каких-либо требований к «превентивным действиям». Это связано с тем, что одна из ключевых целей формальной системы менеджмента — действовать в качестве превентивного инструмента. Следовательно, общий текст, используемый в стандартах ИСО по системам менеджмента, требует оценки «внешних и внутренних факторов организации, относящихся к ее цели и влияющих на ее способность достичь ожидаемого(ых) результата(ов)», приведенных в 4.1, и «определения рисков и возможностей, которые необходимо устранить: обеспечить, чтобы СМИБ смогла достичь ожидаемого(ых) результата(ов); предотвратить или уменьшить нежелательные эффекты и достичь постоянного улучшения», приведенных в 6.1. Считается, что эти два набора требований охватывают концепцию «превентивных действий», а также расширяют взгляд на риски и возможности.

10.2 Постоянное улучшение

Необходимые мероприятия

Организация постоянно улучшает пригодность, адекватность и эффективность СМИБ.

Пояснение

Организации и их контекст никогда не бывают статичными. Кроме того, риски для информационных систем и способы их компрометации быстро развиваются. Наконец, ни одна СМИБ не идеальна, всегда есть способ ее улучшить, даже если организация и ее контекст не меняются.

Примером улучшений, не связанных с несоответствиями или рисками, является оценка элемента СМИБ (с точки зрения пригодности, адекватности и эффективности), которая может показать, что элемент превышает требования СМИБ или является неэффективным. Если это так, то есть возможность улучшить СМИБ, изменив оцениваемый элемент.

Системный подход с использованием постоянного улучшения приведет к более эффективной СМИБ, которая улучшит ИБ организации. Менеджмент ИБ управляет оперативной деятельностью организации, чтобы избежать чересчур реактивного подхода, когда большая часть ресурсов не была использована для поиска проблем и решения этих проблем. СМИБ работает систематически посредством постоянного улучшения, чтобы у организации был более проактивный подход. Высшее руководство может ставить цели для постоянного улучшения, например, путем измерения эффективности, стоимости или зрелости процесса.

Как следствие, организация относится к своей СМИБ как к развивающейся, обучающейся, живой части бизнес-операций. Чтобы СМИБ не отставала от изменений, она регулярно оценивается на предмет соответствия цели, эффективности и соответствия целям организации. Ничто не должно восприниматься как должное и ничто не должно рассматриваться как «недосягаемое» только потому, что оно было достаточно хорошим во время его реализации.

Руководство

Постоянное улучшение СМИБ должно повлечь за собой оценку самой СМИБ и всех ее элементов с учетом внутренних и внешних факторов (см. 4.1), требований заинтересованных сторон (см. 4.2) и результатов оценки эффективности (см. раздел 9). Оценка должна включать анализ:

a) пригодности СМИБ, с учетом внешних и внутренних факторов, требований заинтересованных сторон, установленных целей ИБ и идентифицированных рисков ИБ посредством планирования и внедрения СМИБ и мер обеспечения ИБ;

b) адекватности СМИБ с учетом совместимости процессов и мер обеспечения ИБ с общими целями организации, мероприятиями и процессами;

c) эффективности СМИБ, учитывая при этом, достигнут(ы) ли ожидаемый(ые) результат(ы) СМИБ, соблюдены ли требования заинтересованных сторон, управляются ли риски ИБ для достижения целей ИБ, управляются ли несоответствия, а ресурсы, необходимые для создания, внедрения, поддержки и постоянного улучшения СМИБ, соответствуют ли этим результатам.

Оценка также может включать анализ эффективности СМИБ и ее элементов с учетом целесообразности использования ими ресурсов, если существует риск того, что недостаточная эффективность может привести к ее потере или к невозможности ее повышения.

Возможности улучшения также могут быть определены при управлении несоответствиями и корректирующими действиями.

После определения возможностей для улучшения в соответствии с 6.1.1 организация должна:

d) оценить их, чтобы установить, стоит ли за ними наблюдать;

e) определить изменения в СМИБ и ее элементах для достижения улучшения;

f) спланировать и провести мероприятия по использованию возможностей, обеспечивающих реализацию преимуществ и отсутствие несоответствий;

g) оценить эффективность мероприятий.

Эти мероприятия следует рассматривать как подмножество мероприятий для обработки рисков и возможностей, описанных в 6.1.1.

Дополнительная информация

Дополнительная информация отсутствует.

Приложение А
(справочное)

Структура политики

Приложение А содержит руководство по структуре документации, которая включает политику ИБ.

В целом политика — это заявление о намерениях и направлении деятельности организации, формально выраженное ее высшим руководством (ИСО/МЭК 27000).

Содержание политики является основой действий и решений, касающихся темы политики.

Организация может иметь несколько политик — по одной на каждую из важных областей деятельности, значимых для организации. Некоторые политики независимы друг от друга, в то время как другие политики могут быть иерархично связаны.

Как правило, организация имеет общую политику, например кодекс профессиональной этики, на самом высоком уровне иерархии политики. Общая политика поддерживается другими политиками, относящимися к различным темам, и может быть применима к конкретным областям или функциям организации. Политика ИБ является одной из этих политик.

Политика ИБ поддерживается рядом тематических политик, связанных с аспектами ИБ. Некоторые из них обсуждаются в ИСО/МЭК 27002, например, политика ИБ может поддерживаться политиками, касающимися контроля доступа, классификации информации (и обработки), физической и экологической безопасности, а также политиками, ориентированными на конечного пользователя. В структуру политики могут быть включены дополнительные уровни. Структура политики показана на рисунке А.1. Следует обратить внимание, что некоторые организации используют другие термины для документированных тематических политик: «стандарты», «директивы» или «правила».

Рисунок А.1 — Иерархия политик

ИСО/МЭК 27001 рекомендует, чтобы организации имели политику ИБ. Однако в нем не указывается какая-либо конкретная связь между политикой ИБ и другими политиками организации.

Содержание политик основано на контексте организации. В частности, при разработке любой политики следует учитывать:

1) цели и задачи организации;
2) стратегии для достижения этих целей;
3) структуру и процессы, принятые в организации;
4) цели и задачи, связанные с тематикой политики;
5) требования соответствующих политик более высокого уровня;
6) целевую группу, на которую направлена эта политика.

Эти данные показаны на рисунке А.2.

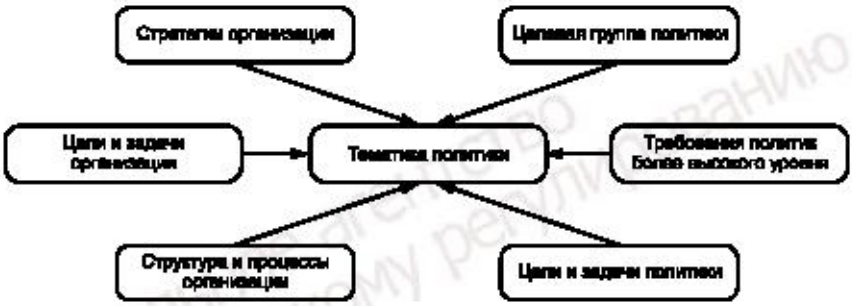

Рисунок А.2 — Исходные данные для разработки политики

Политики могут иметь структуру, состоящую из следующих разделов:

a) Административный — название политики, версия, дата публикации/срок действия, история изменений, владелец и утверждающий, классификация, предполагаемая аудитория и т. д.;

b) Краткое изложение политики — обзор из одного или двух предложений (иногда это можно объединить с введением);

c) Введение — краткое объяснение темы политики;

d) Область действия — описывает те части или виды деятельности организации, на которые влияет политика. Если уместно, в этом разделе перечисляются другие политики, которые поддерживаются этой политикой;

e) Цели — описывает цель политики;

f) Принципы — описывает правила, касающиеся действий и решений для достижения целей. В некоторых случаях может быть полезно определить ключевые процессы, связанные с темой политики, а затем правила для управления процессами;

g) Ответственность — описывает, кто несет ответственность за действия, отвечающие требованиям политики. В некоторых случаях этот раздел может включать описание организационных мероприятий, а также обязанности и полномочия лиц с назначенными ролями;

h) Ключевые результаты — описывает результаты бизнеса, если цели будут достигнуты. В некоторых случаях это может быть объединено с целями;

i) Связанные политики — описывает другие политики, относящиеся к достижению целей, обычно путем предоставления дополнительной информации по конкретным темам;

j) Требования политики — описывает подробные требования политики.

Содержание политики может быть организовано различными способами. Например, организации, которые делают упор на роли и обязанности, могут упростить описание целей и применять принципы специально для описания обязанностей.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального, межгосударственного стандарта
ISO/IEC 27000	IDT	ГОСТ Р ИСО/МЭК 27000—2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»
ISO/IEC 27001	IDT	ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

Примечания — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:
- IDT — идентичный стандарт.

Библиография

[1] ISO 19011, Guidelines for auditing management systems

[2] ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls

[3] ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance

[4] ISO/IEC 27004:2016, Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

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

[6] ISO/IEC 27007, Information technology — Security techniques — Guidelines for information security management systems auditing

[7] ISO/IEC/TR 27008, Information technology — Security techniques — Guidelines for auditors on information security controls

[8] ISO 30301, Information and documentation — Management systems for records — Requirements

[9] ISO 31000, Risk management — Principles and guidelines (Менеджмент риска. Принципы и руководство)

УДК 006.34:004.056:004.056.5:004.056.53:006.354 ОКС 35.030

Ключевые слова: система менеджмента информационной безопасности, информационная безопасность, оценка рисков, оценка эффективности

Редактор *Н.Н. Кузьмина*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *М.В. Лебедевой*

Сдано в набор 21.05.2021. Подписано в печать 02.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,61.

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

Федеральное агентство
по техническому регулированию
и метрологии
Федеральное агентство
по техническому регулированию
и метрологии