ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ГОСТ Р ИСО/МЭК 27003— 2012**

## Информационная технология

# Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности

ISO/IEC 27003:2010
Information technology — Security techniques — Information security management systems implementation guidance
(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

## Предисловие

1 ПОДГОТОВЛЕН Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации — «Фирма «Интерстандарт» (ФБУ «КВФ «Интерстандарт») совместно с Евро-Азиатской ассоциацией производителей товаров и услуг в области безопасности (Ассоциация ЕВРААС) и ООО «Научно-испытательный институт систем обеспечения комплексной безопасности» (ООО «НИИ СОКБ») на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 812-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27003:2010 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности» (ISO/IEC 27003:2010 «Information technology — Security techniques — Information security management systems implementation guidance»).

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

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). 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 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 (gost.ru)*

© Стандартинформ, 2014

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

## Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 2
4 Структура настоящего стандарта . . . 2
4.1 Общая структура разделов настоящего стандарта . . . 2
4.2 Общая структура раздела настоящего стандарта . . . 3
4.3 Схемы . . . 3
5 Получение одобрения руководства для запуска проекта СМИБ . . . 5
5.1 Описание получения одобрения руководства для запуска проекта СМИБ . . . 5
5.2 Определение приоритетов организации для разработки СМИБ . . . 5
5.3 Определение предварительной области действия СМИБ . . . 8
5.4 Разработка технического обоснования и плана проекта для получения санкции руководства . . . 9
6 Определение области действия СМИБ, границ и политики СМИБ . . . 11
6.1 Общее описание определения области действия СМИБ, границ и политики СМИБ . . . 11
6.2 Определение организационной области действия и границ . . . 11
6.3 Определение области действия и границ для информационных и коммуникационных технологий (ИКТ) . . . 13
6.4 Определение физической области действия и границ . . . 14
6.5 Объединение всех областей действия и границ для получения области действия и границ СМИБ 15
6.6 Разработка политики СМИБ и получение одобрения руководства . . . 16
7 Проведение анализа требований к информационной безопасности . . . 16
7.1 Общее описание проведения анализа требований к информационной безопасности . . . 16
7.2 Определение требований к информационной безопасности для процесса СМИБ . . . 17
7.3 Определение активов в рамках области действия СМИБ . . . 19
7.4 Проведение оценки информационной безопасности . . . 19
8 Проведение оценки риска и планирование обработки риска . . . 20
8.1 Описание проведения оценки риска и планирования обработки риска . . . 20
8.2 Проведение оценки риска . . . 21
8.3 Выбор целей и средств управления . . . 23
8.4 Получение санкции руководства на внедрение и использование СМИБ . . . 23
9 Разработка СМИБ . . . 24
9.1Описание разработки СМИБ . . . 24
9.2 Разработка информационной безопасности организации . . . 25
9.3 Разработка информационной безопасности ИКТ и физических объектов . . . 30
9.4 Создание условий для обеспечения надежного функционирования СМИБ . . . 32
9.5 Составление окончательного плана проекта СМИБ . . . 34
Приложение А (справочное) Описание контрольного перечня . . . 35
Приложение В (справочное) Роли и сферы ответственности в области информационной безопасности 40
Приложение С (справочное) Информация по внутреннему аудиту . . . 44
Приложение D (справочное) Структура политики . . . 45
Приложение Е (справочное) Мониторинг и измерения . . . 48
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 53
Библиография . . . 54

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Информационная технология**

# Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности

Information technology. Security techniques. Information security management systems. Implementation guidance of information security management system

**Дата введения — 2013—12—01**

## 1 Область применения

В настоящем стандарте рассматриваются важнейшие аспекты, необходимые для успешной разработки и внедрения системы менеджмента информационной безопасности (СМИБ) в соответствии со стандартом ISO/IEC 27001:2005. В нем описывается процесс определения и разработки СМИБ от запуска до составления планов внедрения. В нем описывается процесс получения одобрения руководством внедрения СМИБ, определяется проект внедрения СМИБ (упоминается в настоящем стандарте как проект СМИБ) и представлены рекомендации по планированию проекта СМИБ, в результате которого получается окончательный план внедрения СМИБ.

Настоящий стандарт предназначен для использования организациями, применяющими СМИБ. Он применяется ко всем типам организаций (например, коммерческим предприятиям, правительственным органам, некоммерческим организациям) любых размеров. Сложность структуры и риски каждой организации уникальны, и на внедрение СМИБ будут влиять ее особые требования. Небольшие организации могут посчитать, что действия, указанные в настоящем стандарте, применимы к ним и могут быть упрощены. Крупным организациям или организациям со сложной структурой для эффективного выполнения действий, указанных в настоящем стандарте, может потребоваться многоуровневая система организации или управления.

Однако в обоих случаях соответствующие действия можно планировать, применяя настоящий стандарт.

Настоящий стандарт содержит рекомендации и разъяснения; в нем не указано никаких требований. Настоящий стандарт предназначен для использования в сочетании с ISO/IEC 27001:2005 и ISO/IEC 27002:2005, но не предназначен для изменения или сокращения требований, указанных в ISO/IEC 27001:2005, или рекомендаций, содержащихся в ISO/IEC 27001:2005.

Предъявление требований на соответствие настоящему стандарту не применяется.

## 2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты (для недатированных ссылок следует использовать только последнее издание указанного стандарта, включая поправки).

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

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

**Издание официальное**

## 3 Термины и определения

В настоящем стандарте применены термины и определения по ISO/IEC 27000:2009, ISO/IEC 27001:2005, а также следующий термин с соответствующим определением.

3.1 **проект СМИБ** (ISMS project): Структурированные действия, предпринимаемые организацией для внедрения системы управления информационной безопасностью.

## 4 Структура настоящего стандарта

### 4.1 Общая структура раздела настоящего стандарта

Внедрение системы менеджмента информационной безопасности (СМИБ) является важным видом деятельности и обычно осуществляется в организации как проект. В настоящем стандарте объясняется внедрение СМИБ с подробным описанием запуска, планирования и определения проекта. Процесс планирования конечного внедрения СМИБ включает пять фаз, и каждая фаза представлена в отдельном пункте. Все разделы имеют одинаковую структуру, описываемую ниже. Эти пять фаз следующие:

a) получение одобрения руководства для запуска проекта СМИБ (раздел 5);

b) определения области действия и политики СМИБ (раздел 6);

c) проведение анализа организации (раздел 7);

d) проведение анализа рисков и планирование обработки рисков (раздел 8);

e) разработка СМИБ (раздел 9).

На рисунке 1 представлены пять фаз планирования проекта СМИБ с указанием стандартов ISO/IEC и основных выходных документов.

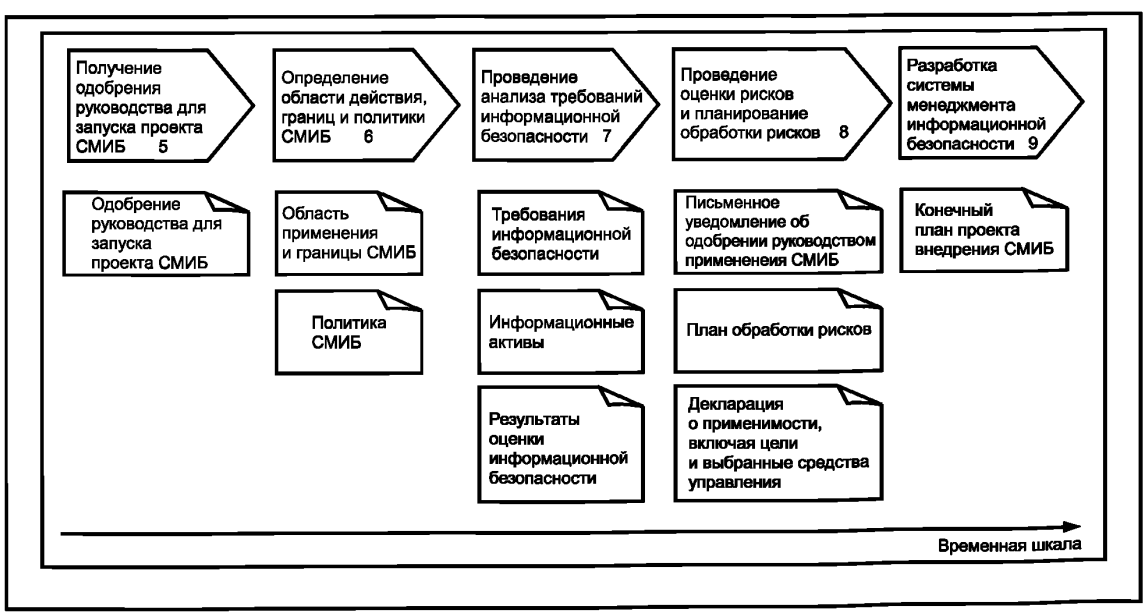



Рисунок 1 — Фазы проекта СМИБ

Дополнительная информация приведена в приложениях:

Приложение A. Описание контрольного перечня.

Приложение B. Роли и сферы ответственности в области информационной безопасности.

Приложение C. Информация по внутреннему аудиту.

Приложение D. Структура политики.

Приложение E. Мониторинг и измерения.

### 4.2 Общая структура раздела настоящего стандарта

Каждый раздел содержит:

a) цель или цели (начиная с того, чего необходимо достичь), указанные в начале каждого раздела в текстовом окне,

или

b) действие или действия, необходимые для достижения цели или целей данной фазы.

Каждое действие описывается в соответствующем пункте.

Описания действий в каждом подпункте структурированы следующим образом:

**Действие**

Действие определяет, что необходимо сделать для выполнения данного действия, чтобы достичь всех целей или части целей данной фазы.

**Исходные данные**

В исходных данных представлено описание отправной точки, например, наличие документированных решений или выходных данных других действий, описываемых в настоящем стандарте. Исходные данные могут упоминаться как полный набор исходных данных в начале соответствующего пункта или конкретная информация по какому либо действию, которая может добавляться после ссылки на соответствующий пункт.

**Рекомендации**

В рекомендациях содержится подробная информация, позволяющая выполнить данное действие. Некоторые рекомендации могут не соответствовать для применения во всех случаях, и другие способы достижения результата могут быть более оптимальными.

**Выходные данные**

В выходных данных описывается результат(ы) или документ(ы) для сдачи, получаемые после выполнения действия. Выходные данные являются одинаковыми независимо от размера организации и области действия СМИБ.

**Дополнительная информация**

В разделе дополнительной информации содержится дополнительная информация, которая может помочь в выполнении действия, например, ссылки на другие стандарты.

Примечание — Фазы и действия, описываемые в данном стандарте, включают предлагаемую последовательность выполнения действий на основе зависимостей, определяемых на основе описаний «исходных данных» и «выходных данных» для каждого действия. Однако в зависимости от множества различных факторов (например, эффективности существующей системы управления, понимания важности информационной безопасности, причин внедрения СМИБ) организация может выбирать в любом порядке любые действия, необходимые для подготовки к учреждению и внедрению СМИБ.

### 4.3 Схемы

Проект часто изображается в графическом виде или в виде схем, показывающих выполняемые действия и их результаты.

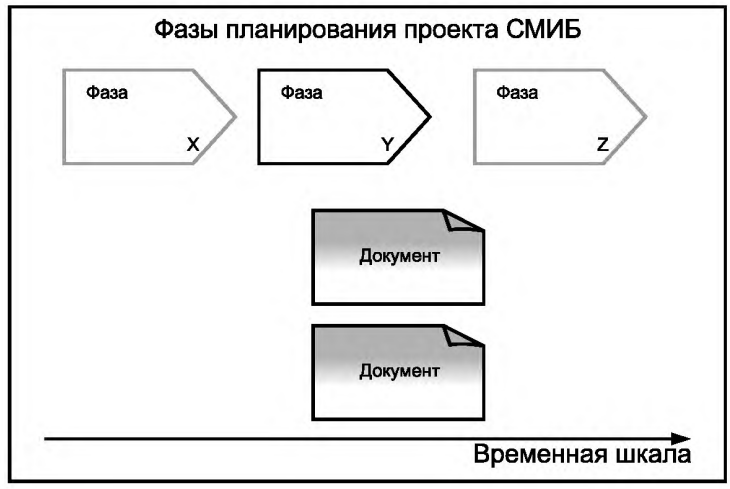
На рисунке 2 показаны условные обозначения на схемах, указываемых в пункте обзора каждой фазы. Схемы обеспечивают обзор высокого уровня действий, входящих в каждую фазу.

В верхнем прямоугольнике показаны фазы планирования проекта СМИБ. Фаза, разъясняемая в конкретном пункте, затем указывается вместе с ключевыми выходными документами.

Нижняя схема (действия в фазе) показывает ключевые действия в указанной фазе верхнего прямоугольника и основные выходные документы каждой фазы.

Временная шкала на нижней схеме основывается на временной шкале верхней схемы.

Действия A и B могут выполняться одновременно. Действие C следует начинать после завершения действий A и B.



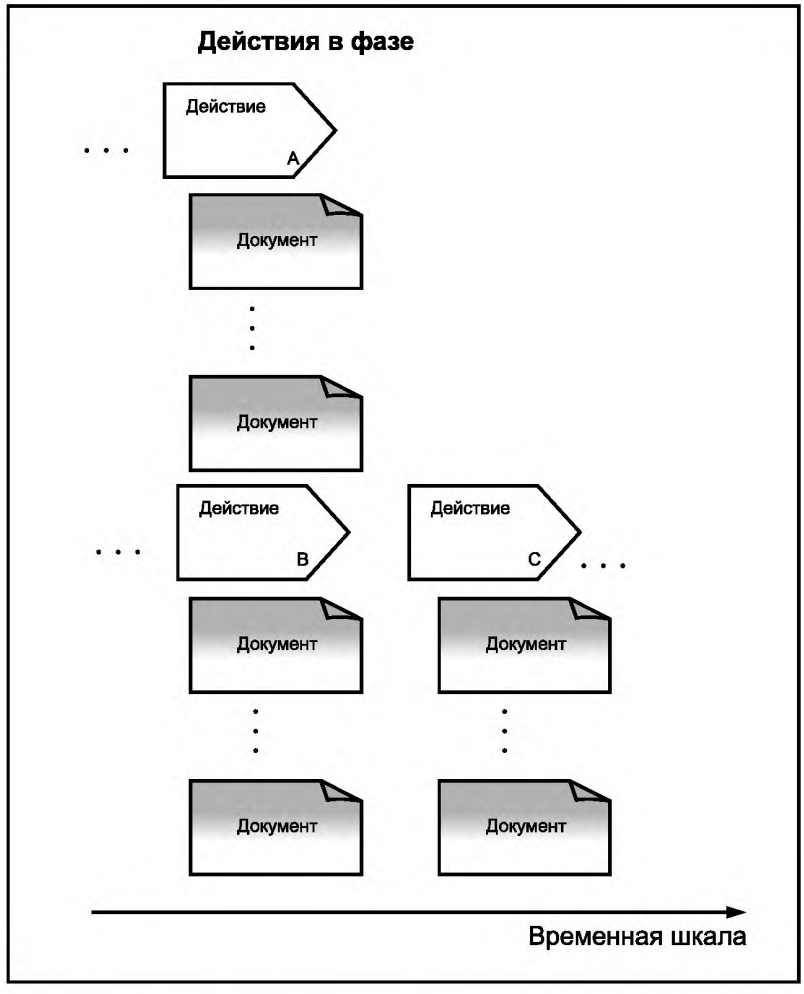




Рисунок 2 — Условные обозначения на блок-схеме

# 5 Получение одобрения руководства для запуска проекта СМИБ

## 5.1 Описание получения одобрения руководства для запуска проекта СМИБ

Существует несколько факторов, которые необходимо учитывать при принятии решения о внедрении СМИБ. Для того чтобы учесть эти факторы, руководство должно рассмотреть деловые аргументы в пользу внедрения проекта СМИБ и утвердить его. Следовательно, цель этой фазы — получить одобрение руководства для запуска проекта СМИБ посредством определения случая применения СМИБ для данного предприятия и плана проекта.

Чтобы получить одобрение руководства, организация должна составить описание случая применения СМИБ для данного предприятия, включающее приоритеты и цели внедрения СМИБ, а также структуру организации для СМИБ. Наряду с этим следует составить начальный план проекта СМИБ.

Работа, выполняемая в данной фазе, позволит организации понять важность СМИБ и определить роли и сферы ответственности в области информационной безопасности внутри организации, требуемые для проекта СМИБ.

Ожидаемым результатом этой фазы будет предварительное разрешение руководства и принятие им обязательства по внедрению СМИБ и выполнению действий, описываемых в настоящем стандарте. Выходные данные в этом пункте включают описание случая применения СМИБ для данного предприятия и предварительный план проекта СМИБ с описанием ключевых этапов.

На рисунке 3 показан процесс получения одобрения руководства для запуска проекта СМИБ.

Примечание — Выходные данные раздела 5 (документированное поручение руководства на планирование и внедрение СМИБ) и один из документов с выходными данными раздела 7 (документированное описание состояния информационной безопасности) не являются требованиями ISO/IEC 27001:2005. Однако выходные данные по этим действиям являются рекомендованными исходными данными для других действий, описываемых в данном документе.

## 5.2 Определение приоритетов организации для разработки СМИБ

**Действия**

Цели внедрения СМИБ должны учитываться при рассмотрении приоритетов и требований организации к информационной безопасности.

**Исходные данные:**

a) стратегические цели организации;

b) обзор существующих систем управления;

c) перечень правовых, нормативных и договорных требований к информационной безопасности, применяемых в организации.

**Рекомендации**

Для запуска проекта СМИБ обычно требуется одобрение руководства. Следовательно, первое действие, которое необходимо выполнить, — сбор существенной информации, показывающей значение СМИБ для организации. Организация должна определить, зачем нужна СМИБ, определить цели внедрения СМИБ и запустить проект СМИБ.

Цели внедрения СМИБ можно определить, ответив на следующие вопросы:

a) менеджмент риска — как может СМИБ улучшить управление рисками для информационной безопасности?

b) результативность — как может СМИБ улучшить управление информационной безопасностью?

c) преимущества для предприятия — как может СМИБ создать конкурентные преимущества для организации?

Чтобы ответить на приведенные выше вопросы, необходимо рассмотреть приоритеты и требования организации в области информационной безопасности на основе следующих факторов:

a) важнейшие сферы деятельности предприятия и организации:

1 Что является важнейшими сферами деятельности предприятия и организации?

2 Какие сферы деятельности организации обеспечивают ведение бизнеса и чему уделяется особое внимание?

3 Какие существуют взаимоотношения и соглашения с третьими сторонами?

4 Привлекаются ли сторонние организации для оказания каких-либо услуг?

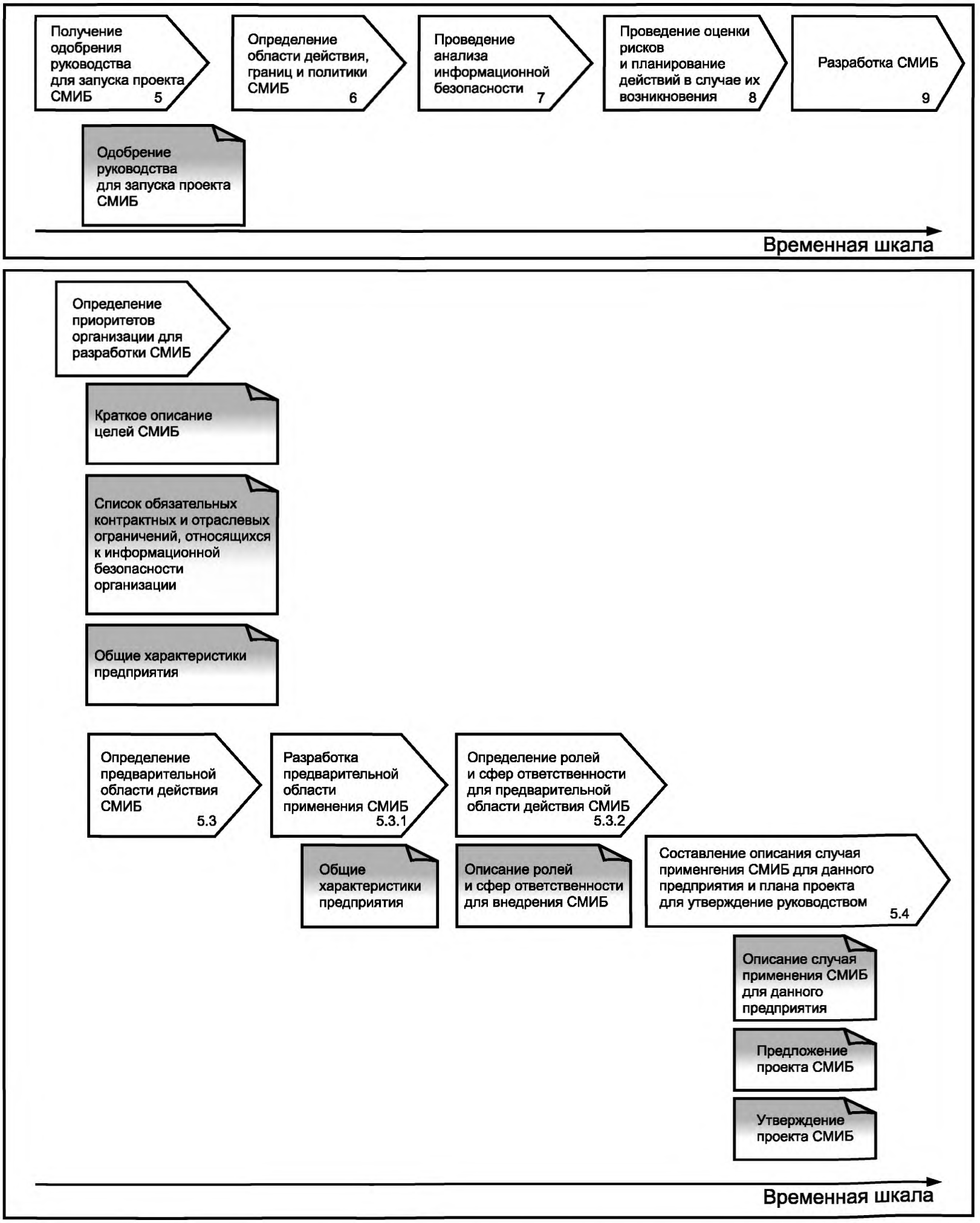



Рисунок 3 — Описание получения одобрения руководства для запуска проекта СМИБ

b) засекреченная или ценная информация:

1 Какая информация является наиболее важной для организации?

2 Какими могли бы быть возможные последствия при разглашении определенной информации неуполномоченным сторонам (например, потеря конкурентных преимуществ, ущерб по отношению к бренду или репутации, судебный иск и т. д.)?

c) законы, делающие обаятельным принятие мер информационной безопасности:

1 Какие законы, относящиеся к обработке риска или информационной безопасности, применяются в организации?

2 Является ли организация публичной глобальной организацией, для которой требуется внешняя финансовая отчетность?

d) контрактные или организационные соглашения, относящиеся к информационной безопасности:

1 Какие требования предъявляются к хранению данных (включая сроки хранения)?

2 Существуют ли контрактные требования, связанные с секретностью или качеством (например, соглашение об уровне услуг — SLA)?

e) отраслевые требования, определяющие конкретные способы управления и меры информационной безопасности:

1 Какие требования, характерные для данной отрасли, применяются к организации?

f) угрозы:

1 Какие нужны виды защиты и от каких угроз?

2 Для каких отдельных категорий информации требуется защита?

3 Каковы отдельные типы информационной деятельности, требующие защиты?

g) Конкурентные движущие факторы:

1 Какие минимальные требования к информационной безопасности существуют на рынке?

2 Какие дополнительные способы менеджмента информационной безопасности могут быть стимулированы конкурентными преимуществами организации?

h) требования непрерывности бизнес-процессов

1 Какие существуют важнейшие бизнес-процессы?

2 Как долго организация может выдерживать приостановки каждого из важнейших бизнес-процессов?

Предварительную область действия СМИБ можно определить, ответив на приведенные выше вопросы. Это также необходимо для того, чтобы определить случай применения СМИБ для данного предприятия и общий план проекта СМИБ для утверждения руководством. Подробная область действия СМИБ должна быть определена во время составления проекта СМИБ.

Требования, указанные в ISO/IEC 27001:2005, пункт 4.2.1, a), определяют область действия на основе характеристик предприятия, организации, местонахождения, активов и технологий. Определению этих факторов способствует информация, полученная на основе вышеуказанных вопросов.

Перечень некоторых тем, которые необходимо рассмотреть при принятии первоначальных решений, касающихся области действия СМИБ:

a) каковы обязательные требования к менеджменту информационной безопасности, определенные руководством организации, и обязательства, накладываемые на организацию извне?

b) несут ли ответственность за предлагаемые системы в рамках области действия СМИБ руководящие группы (например, сотрудники разных филиалов и отделов)?

c) как будут передаваться документы, связанные с СМИБ, внутри организации (например, на бумаге или через корпоративную сеть)?

d) могут ли существующие системы управления удовлетворять потребности организации? Являются ли они полнофункциональными, поддерживаются ли в работоспособном состоянии и функционируют ли, как это необходимо?

Примеры целей управления, которые могут использоваться в качестве исходных данных для определения предварительной области действия СМИБ, включают:

a) содействие непрерывности бизнес-процессов и восстановлению их в чрезвычайных ситуациях;

b) повышение устойчивости к инцидентам;

c) внимание к соответствию законам (условиям) контракта и обязательствам;

d) обеспечение возможности сертификации по другим стандартам ISO/IEC;

e) обеспечение развития и положения организации;

f) снижение затрат на управление безопасностью;

g) защита стратегически важных активов;

h) создание благоприятной и эффективной среды внутреннего управления;

i) обеспечение уверенности заинтересованных сторон в том, что информационные активы соответствующим образом защищены.

**Выходные данные**

Выходные данные после выполнения этого действия следующие:

a) документ, излагающий цели, приоритеты в области информационной безопасности и требования организации к СМИБ;

b) перечень законных, контрактных и отраслевых требований к информационной безопасности организации;

c) описание характеристик предприятия, организации, местонахождения, активов и технологий.

**Дополнительная информация**

ISO/IEC 9001:2008, ISO/IEC 14001:2004, ISO/IEC 20000-1:2005.

### 5.3 Определение предварительной области действия СМИБ

#### 5.3.1 Разработка предварительной области действия СМИБ

**Действия**

Цели, связанные с внедрением СМИБ, должны включать определение предварительной области действия СМИБ, которая необходима для проекта СМИБ.

**Исходные данные**

Выходные данные действия 5.2, определение приоритетов организации для разработки СМИБ.

**Рекомендации**

Чтобы осуществить проект внедрения СМИБ, необходимо определить структуру организации для реализации СМИБ. Предварительная область действия СМИБ должна быть определена, чтобы обеспечить для руководства рекомендации для принятия решений по внедрению системы и поддержать дальнейшие действия.

Предварительная область действия СМИБ нужна для того, чтобы определить случай применения СМИБ для данного предприятия и предложить план проекта для утверждения руководством.

Выходные данные на этом этапе должны представлять собой документ, определяющий предварительную область действия СМИБ, а именно:

a) изложение обязательных требований к менеджменту информационной безопасности, определяемых руководством организации, и обязательств, накладываемых на организацию извне;

b) описание того, как части области действия системы взаимодействуют с другими системами управления;

c) перечень целей предприятия в области менеджмента информационной безопасности (как определено в 5.2);

d) перечень важнейших бизнес-процессов, информационных активов, организационных структур и регионов, где будет использоваться СМИБ;

e) соотношение существующих систем управления, регулирования, соответствия и целей организации;

f) характеристики предприятия, организация, местонахождение, активы и технологии.

Необходимо определить общие элементы и практические различия между существующими системами управления и предлагаемой СМИБ.

**Выходные данные**

Выходные данные представляют собой документ, описывающий предварительную область действия СМИБ.

**Дополнительная информация**

Дополнительной специальной информации не требуется.

Примечание — Следует обратить особое внимание на то, что в случае сертификации должны быть выполнены особые требования к документации согласно ISO/IEC 27001:2005 в том, что касается области действия СМИБ, независимо от существующей в организации системы управления.

#### 5.3.2 Определение ролей и сфер ответственности для предварительной области действия СМИБ

**Действия**

Необходимо определить общие роли и сферы ответственности для предварительной области действия СМИБ.

**Исходные данные:**

a) выходные данные действия 5.3.1, разработка предварительной области действия СМИБ;

b) список заинтересованных сторон, которые получат выгоду в результате реализации проекта СМИБ.

**Рекомендации**

Для осуществления проекта СМИБ необходимо определить роль организации в реализации проекта. Эта роль обычно различается в разных организациях, что обусловлено количеством людей, имеющих дело с информационной безопасностью. Организационная структура и ресурсы для обеспечения информационной безопасности различаются в зависимости от размера, типа и структуры организации. Например, в небольших организациях несколько функций может выполнять один человек. Однако руководство организации должно однозначно определить его роль (обычно начальник отдела информационной безопасности, управляющий по информационной безопасности и т. п.) с полной ответственностью за менеджмент информационной безопасности, а для сотрудников должны быть определены роли и сферы ответственности на основе квалификации, требуемой для выполняемой работы. Это важно для обеспечения эффективного выполнения задач.

Наиболее важными соображениями при определении ролей в области менеджмента информационной безопасности являются следующие:

a) полная ответственность за выполнение задач остается на уровне руководства;

b) одно лицо (обычно начальник отдела информационной безопасности) назначается для содействия и координации процессов обеспечения информационной безопасности;

c) каждый работник несет равную ответственность за выполнение своей первоначальной задачи и обеспечение информационной безопасности на рабочем месте и в организации.

Должностные лица, занятые в менеджменте информационной безопасности, должны работать совместно; этому может содействовать создание форума по информационной безопасности или аналогичного органа.

Необходимо осуществлять (и документировать) взаимодействие с соответствующими специалистами предприятия на всех этапах разработки, внедрения, использования и поддержания СМИБ.

Представители подразделений, входящих в определенную область действия системы (например, менеджмент риска), являются потенциальными членами группы по внедрению СМИБ. Эта группа должна иметь минимально необходимую с практической точки зрения численность для быстрого и эффективного использования ресурсов. В эту группу могут входить не только представители подразделений, выполняющих задачи в определенной области действия системы (например, в области менеджмента риска), которые являются потенциальными членами группы по внедрению СМИБ, но также и представители других подразделений, например юридического отдела, административного отдела. Эта группа должна иметь минимально необходимую с практической точки зрения численность для быстрого и эффективного использования ресурсов.

**Выходные данные**

Выходные данные представляют собой документ или таблицу, описывающую роли и сферы ответственности с указанием имен и организацию, необходимую для успешного внедрения СМИБ.

**Дополнительная информация**

В Приложении В представлена подробная информация по ролям и сферам ответственности, необходимым в организации для успешного внедрения СМИБ.

### 5.4 Разработка технического обоснования и плана проекта для получения санкции руководства

**Действия**

Одобрение руководства и выделение ресурсов для реализации проекта внедрения СМИБ должны быть получены путем определения случая применения СМИБ для данного предприятия и предложения проекта СМИБ.

**Исходные данные:**

a) выходные данные действия 5.2, определение приоритетов организации для разработки СМИБ;

b) выходные данные действия 5.3, определение предварительной области действия СМИБ — документы предварительные.

1 Область действия СМИБ и

2 Связанные с ней роли и сферы ответственности.

**Рекомендации**

Информация по случаю применения СМИБ для данного предприятия и первоначальный план проекта СМИБ должны включать определенные временные шкалы, ресурсы и этапы, требуемые для выполнения основных действий, указанных в пунктах 6—9 настоящего стандарта.

Определение случая применения СМИБ для данного предприятия и первоначальный план проекта СМИБ служат основой проекта, но также обеспечивают выделение и утверждение руководством ресурсов, требуемых для внедрения СМИБ. То как применяемая СМИБ будет подкреплять цели предприятия, способствует эффективности организационных процессов и повышает эффективность работы предприятия.

Информация по случаю применения СМИБ для данного предприятия должна включать короткие заявления, связанные с целями организации, и охватывать следующие вопросы:

a) цели и конкретные задачи;

b) выгоды для организации;

c) предварительная область действия СМИБ, включая затрагиваемые бизнес-процессы;

d) важнейшие процессы и факторы для достижения целей СМИБ;

e) описание проекта высокого уровня;

f) первоначальный план внедрения системы;

g) определенные роли и сферы ответственности;

h) требуемые ресурсы (технологические и людские);

i) соображения, касающиеся внедрения системы, включая существующую систему информационной безопасности;

j) временная шкала с ключевыми этапами;

k) предполагаемые затраты;

l) важнейшие факторы успеха;

m) количественное определение выгод для организации.

План проекта должен включать соответствующие действия из фаз, описываемых в пунктах 6—9 настоящего стандарта.

Лица, влияющие на СМИБ или находящиеся под ее влиянием, должны быть определены; им должно быть предоставлено необходимое время для того, чтобы изучить и прокомментировать описание случая применения СМИБ для данного предприятия и предложение по проекту СМИБ. Описание случая применения СМИБ для данного предприятия и предложение по проекту СМИБ должны при необходимости обновляться по мере появления исходных данных. При получении достаточной поддержки описание случая применения СМИБ для данного предприятия и предложение по проекту СМИБ должны быть представлены руководству для утверждения.

Руководство должно утвердить описание случая применения СМИБ для данного предприятия и первоначальный план проекта, чтобы составить поручения для всей организации и начать реализацию проекта СМИБ.

Предполагаемые выгоды от поручения руководства на внедрение СМИБ следующие:

a) знание и применение соответствующих законов, норм, договорных обязательств и стандартов, касающихся информационной безопасности, которое позволит избежать ответственности и взысканий в случае несоответствия;

b) эффективное использование множества процессов обеспечения информа-ционной безопасности;

c) устойчивость и растущая уверенность в росте благодаря лучшему менеджменту риска информационной безопасности;

d) определение и защита важной для предприятия информации.

**Выходные данные**

Выходные данные этого действия следующие:

a) документированное одобрение руководством выполнения проекта СМИБ с распределенными ресурсами;

b) документированное описание случая применения СМИБ для данного предприятия;

c) начальное предложение по проекту СМИБ с основными этапами, такими как выполнение оценки риска, реализация проекта, внутренний аудит и проверки, осуществляемые руководством.

**Дополнительная информация**

ISO/IEC 27000:2009 в качестве примеров важнейших факторов успеха в подкрепление описания случая применения СМИБ для данного предприятия.

# 6 Определение области действия СМИБ, границ и политики СМИБ

## 6.1 Общее описание определения области действия СМИБ, границ и политики СМИБ

Одобрение руководства для внедрения СМИБ основывается на предварительном определении области действия СМИБ, случая применения СМИБ для данного предприятия и первоначальном плане проекта. Подробное определение области действия и границ СМИБ, определение политики СМИБ и ее принятие и поддержка руководством являются ключевыми первичными факторами для успешного внедрения СМИБ.

Следовательно, цели этой фазы следующие:

**Цели:** Детально определить область действия и границы СМИБ, разработать политику СМИБ и получить одобрение руководства.

**ISO/IEC 27001:2005, ссылки:** 4.2.1 a) и 4.2.1 b).

Чтобы достичь цели «детального определения области действия и границ СМИБ», необходимо выполнить следующие действия:

a) определить организационную область действия и границы;

b) область действия и границы информационных и коммуникационных технологий (ИКТ) и

c) физическую область действия и границы;

d) определенные характеристики в ISO/IEC 27001:2005, 4.2.1 a) и b), т. е. аспекты области действия и границ, связанные с предприятием, организацией, местонахождением, активами и технологиями, и политика формируются в процессе определения этой области действия и границ;

e) введение элементарной области действия и границ для получения области действия и границ СМИБ.

Для достижения определения политики СМИБ и получения одобрения руководства необходимо отдельное действие.

Чтобы построить эффективную систему управления для организации, необходимо детально определить область действия СМИБ с учетом важнейших информационных активов организации. Важно иметь общую терминологию и систематический подход для определения информационных активов и оценки жизнеспособных механизмов обеспечения безопасности. Это обеспечивает простоту коммуникации и способствует устойчивому пониманию всех фаз внедрения системы. Также важно обеспечить включение в область действия системы важнейших подразделений организации.

Можно определить область действия СМИБ, чтобы охватить всю организацию или ее часть, например подразделение или четко ограниченный вспомогательный элемент. Например, в случае оказания «услуг» клиентам областью действия СМИБ может быть система управления услугами или пересекающимися функциями (целое подразделение или часть подразделения). Требования ISO/IEC 27001:2005 должны быть выполнены для получения сертификации независимо от систем управления, существующих в организации.

Определение организационной области действия и границ, области действия и границ технологии передачи информации (6.3) и физической области действия и границ (6.4) не всегда должно выполняться последовательно. Однако полезно указать на уже полученные области действия и границы при определении других областей действия и границ.

## 6.2 Определение организационной области действия и границ

**Действия**

Необходимо определить организационную область действия и границы.

**Исходные данные:**

a) выходные данные действия 5.3, определение предварительной области действия СМИБ — документированная предварительная область действия СМИБ, охватывающая:

1 Соотношения существующих систем управления, регулирования, соответствия и целей организации;

2 Характеристики предприятия, организации, его или ее местонахождения, активов и технологий;

b) выходные данные действия 5.2, определение приоритетов организации для разработки СМИБ — документированное утверждение руководством внедрения СМИБ и запуск проекта с необходимыми распределенными ресурсами.

На рисунке 4 представлено общее описание определения области действия, границ и политики СМИБ.

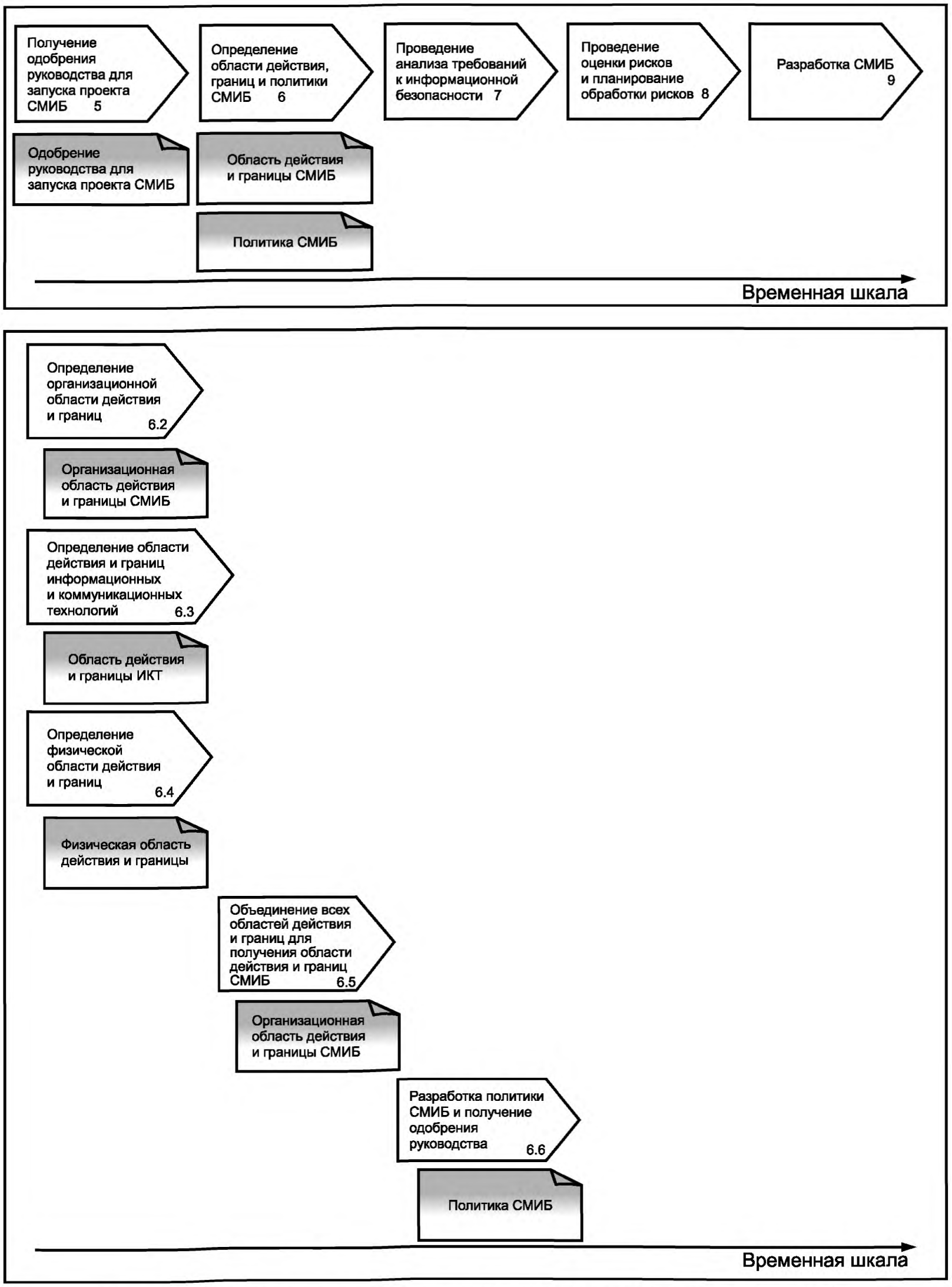



Рисунок 4 — Общее описание определения области действия, границ и политики СМИБ

**Рекомендации**

Степень усилий, требуемых для внедрения СМИБ, зависит от величины области действия, к которой эти усилия прилагаются. Этот фактор также может повлиять на все действия, связанные с поддержанием информационной безопасности элементов, входящих в область действия системы (например, процессов, материальных объектов, информационных систем и людей), включая внедрение и содержание средств управления операциями и выполнение таких задач, как определение информационных активов и оценка риска. Если руководство решает исключить некоторые части организации и области действия СМИБ, причины такого решения также должны быть документированы.

Когда определена область действия СМИБ, важно, чтобы границы были достаточно ясными, чтобы объяснить их сотрудникам, участвующим в их определении.

Некоторые меры и средства контроля и управления, касающиеся информационной безопасности, могут уже существовать в организации в результате ввода в действие других систем управления. Их следует учитывать при планировании СМИБ, но они необязательно определяют границы области действия существующей СМИБ.

Одним из методов определения организационных границ является определение сфер ответственности, не перекрывающих друг друга, чтобы облегчить назначение подотчетности в организации.

Сферы ответственности, напрямую связанные с информационными активами или производственными процессами, включаемые в область действия СМИБ, должны выбираться как часть организации, находящейся под контролем СМИБ. При определении организационных границ следует учитывать следующие факторы:

a) форум по менеджменту СМИБ должен состоять из руководящих работников, непосредственно связанных с областью действия СМИБ;

b) членом руководства, ответственным за СМИБ, должен быть сотрудник, в конечном счете отвечающий за все затронутые сферы ответственности (т. е. его роль должна диктоваться его сферой контроля и ответственности в организации);

c) в случае, если сотрудник, отвечающий за управление СМИБ, не является членом высшего руководства, необходим поручитель высшего руководства, представляющий интересы информационной безопасности и действующий в качестве защитника СМИБ на высших уровнях организации;

d) область действия и границы необходимо определить для того, чтобы быть уверенным в том, что все связанные активы принимаются в расчет при оценке риска, и охватить риски, которые могут выйти за пределы этих границ.

На основе такого подхода анализируемые организационные границы должны определять всех сотрудников, попадающих под действие СМИБ, и эти границы должны быть включены в область действия системы. Определение сотрудников может быть связано с процессами и (или) функциями в зависимости от выбранного подхода. Если некоторые процессы в организации выполняются третьими сторонами, эти зависимости должны быть четко документированы. Такие зависимости подлежат дополнительному анализу в проекте внедрения СМИБ.

**Выходные данные**

Выходные данные этого действия следующие:

a) описание организационных границ СМИБ, включая обоснования исключения каких-либо частей организации из области действия СМИБ;

b) функции и структура частей организации, находящихся в области действия СМИБ;

c) определение информации, подлежащей обмену в рамках области действия системы, и информации, обмен которой осуществляется через границы;

d) процессы в организации и сферы ответственности за информационные активы в области действия системы и за ее пределами;

e) процесс в иерархии принятия решений, а также ее структура в рамках СМИБ.

**Дополнительная информация**

Дополнительная специальная информация не требуется.

### 6.3 Определение области действия и границ для информационных и коммуникационных технологий (ИКТ)

**Действия**

Необходимо определить область действия и границы элементов информационных и коммуникационных технологий (ИКТ) и другие технологические элементы, подпадающие под действие СМИБ.

**Исходные данные:**

a) выходные данные действия 5.3, определение предварительной области действия СМИБ — документ с описанием предварительной области действия СМИБ;

b) выходные данные действия 6.2, определение организационной области действия и границ.

**Рекомендации**

Определение области действия и границ ИКТ может быть получено на основе анализа имеющихся информационных систем (вместо подхода на основе информационных технологий). Когда принимается решение руководства о включении процессов информационной системы в область действия СМИБ, необходимо также рассмотреть все связанные элементы ИКТ. Эти элементы включают все части организации, которые хранят, обрабатывают или передают важную информацию, активы или являются важными для других частей организации, входящих в область действия системы. Информационные системы могут охватывать границы организации или государства. В любом случае необходимо принять во внимание следующие факторы:

a) социально-культурная среда;

b) законные, обязательные или контрактные требования, применяемые к организациям;

c) подотчетность за ключевые сферы ответственности;

d) технические ограничения (например, доступная ширина полосы частот, наличие сервиса и т. д.).

Если принять во внимание вышесказанное, границы ИКТ, если это практически применимо, должны включать описание следующих элементов:

a) инфраструктура связи, в которой ответственность за ее управление входит в компетенцию организации, располагающей различными технологиями (например, беспроводные и проводные сети или сети передачи данных и телефонной связи);

b) программное обеспечение в рамках организационных границ, используемое и контролируемое организацией;

c) аппаратное обеспечение ИКТ, требуемое для сети или сетей, приложений или производственных систем;

d) роли и сферы ответственности, связанные с аппаратным обеспечением ИКТ, сетью и программным обеспечением.

Если один или более из вышеприведенных пунктов не контролируется организацией, необходимо документировать зависимости от третьих сторон. См. 6.2, рекомендации.

**Выходные данные**

Выходные данные этого действия следующие:

a) информация, обмен которой осуществляется в рамках области действия системы, и информация, обмен которой осуществляется через границы;

b) границы ИКТ для СМИБ с обоснованием исключения каких-либо элементов ИКТ, находящихся под управлением организации, из области действия СМИБ;

c) информация об информационных системах и телекоммуникационных сетях, описывающая, какие из них находятся в пределах области действия СМИБ вместе с ролями и сферами ответственности для этих систем. Также необходимо кратко описать системы, не входящие в область действия СМИБ.

**Дополнительная информация**

Дополнительная специальная информация не требуется.

### 6.4 Определение физической области действия и границ

**Действия**

Необходимо определить физическую область действия и границы, которые должны охватываться СМИБ.

**Исходные данные:**

a) выходные данные действия 5.3, определение предварительной области действия СМИБ — документ с описанием предварительной области действия СМИБ;

b) выходные данные действия 6.2, определение организационной области действия и границ;

c) выходные данные действия 6.3, определение области действия и границ информационных и коммуникационных технологий (ИКТ).

**Рекомендации**

Определение физической области действия и границ состоит в определении помещений, объектов и оборудования в организации, которые должны стать частью СМИБ. При этом сложнее работать с информационными системами, пересекающими физические границы, и для этого требуется:

a) периферийное оборудование;

b) средства связи с информационными системами клиентов и обслуживание, предоставляемое третьими сторонами;

c) применение соответствующих средств связи и уровней обслуживания.

Если принять во внимание вышесказанное, физические границы, если это практически применимо, должны включать описание следующих элементов:

a) описания функций или процессов с учетом их физического местонахождения и степени контроля их организацией;

b) специальное оборудование, используемое для хранения (размещения) аппаратного обеспечения ИКТ или данных, применяемых в системе СМИБ (например, на резервных пленках), на основе покрытия границ ИКТ.

Если один или более из вышеприведенных пунктов не контролируется организацией, необходимо документировать зависимости от третьих сторон (см. 6.2, Рекомендации).

**Выходные данные**

Выходные данные этого действия следующие:

a) описание физических границ СМИБ с обоснованием для исключения каких-либо физических границ, находящихся под управлением организации, из области действия СМИБ;

b) описание организации и ее географических характеристик, относящихся к области действия СМИБ.

**Дополнительная информация**

Дополнительная специальная информация не требуется.

### 6.5 Объединение всех областей действия и границ для получения области действия и границ СМИБ

**Действия**

Область действия и границы СМИБ должны быть получены путем объединения всех областей действия и границ.

**Исходные данные:**

a) выходные данные действия 5.3, определение предварительной области действия СМИБ — документ с описанием предварительной области действия СМИБ;

b) выходные данные действия 6.2, определение организационной области действия и границ;

c) выходные данные действия 6.3, определение области действия и границ информационных и коммуникационных технологий (ИКТ);

d) выходные данные действия 6.4, определение физической области действия и границ.

**Рекомендации**

Область действия СМИБ можно описать и обосновать различными способами. Например, можно выбрать физический объект — центр обработки и хранения данных или офис и перечислить важнейшие процессы, каждый из которых охватывает области за пределами центра обработки и хранения данных, вводя эти элементы, находящиеся за пределами центра обработки и хранения данных, в область действия СМИБ. Одним из таких важнейших процессов может быть, например, мобильный доступ к центральной информационной системе.

**Выходные данные**

Выходные данные этого действия представляют собой документ, описывающий область действия и границы СМИБ и содержащий следующую информацию:

a) ключевые характеристики организации (функция, структура, услуги, активы и область действия и границы ответственности для каждого актива);

b) процессы в организации, находящиеся в области действия СМИБ;

c) конфигурация оборудования и сетей, находящихся в области действия СМИБ;

d) предварительный перечень информационных активов, находящихся в области действия СМИБ;

e) перечень активов ИКТ, находящихся в области действия СМИБ (например, серверов);

f) схемы объектов, находящихся в области действия СМИБ, определяющие физические границы СМИБ;

g) описание ролей и сфер ответственности в рамках СМИБ и их связи со структурой организации;

h) подробное описание и обоснование исключений каких-либо элементов из области действия СМИБ.

**Дополнительная информация**

Дополнительная специальная информация не требуется.

### 6.6 Разработка политики СМИБ и получение одобрения руководства

**Действия**

Необходимо разработать политику СМИБ и получить одобрение руководства.

**Исходные данные:**

a) выходные данные действия 6.5, объединение всех областей действия и границ для получения области действия и границ СМИБ — документированная область действия и границы СМИБ;

b) выходные данные действия 5.2, определение приоритетов организации для разработки СМИБ — документированные цели внедрения СМИБ;

c) выходные данные действия 5.4, составление описания случая применения СМИБ для данного предприятия и проекта плана для утверждения руководством — документы:

1 Требования и приоритеты организации в области информационной безопасности;

2 Первоначальный проект плана внедрения СМИБ с основными этапами, такими как проведение оценки риска, внутренний аудит и проверка, осуществляемая руководством.

**Рекомендации**

При определении политики СМИБ следует принять во внимание следующие аспекты:

a) установить цели СМИБ на основе требований и приоритетов организации в области информационной безопасности;

b) установить общие фокусные точки и руководства к действию для достижения целей СМИБ;

c) учесть законные обязательные требования организации и договорные обязательства, связанные с информационной безопасностью;

d) ситуация с управлением рисками в организации;

e) установить критерии для оценки рисков (см. ISO/IEC 27005:2008) и определения структуры оценки риска;

f) определить сферы ответственности руководителей высшего уровня в отношении СМИБ;

g) получить одобрение руководства.

**Выходные данные**

Выходные данные представляют собой документ, описывающий и документирующий утвержденную руководством политику СМИБ. Этот документ должен быть повторно утвержден в следующей фазе проекта, поскольку зависит от результатов оценки риска.

**Дополнительная информация**

Стандарт ISO/IEC 27005:2008 содержит дополнительную информацию по критериям оценки риска.

## 7 Проведение анализа требований к информационной безопасности

### 7.1 Общее описание проведения анализа требований к информационной безопасности

Анализ текущего положения в организации важен, поскольку существуют требования и информационные активы, которые необходимо принять во внимание при внедрении СМИБ. Действия, описываемые в этой фазе, могут предприниматься в основном параллельно с действиями, описываемыми в разделе 6, из соображений эффективности и практичности.

**Цели:**

Определить соответствующие требования, которым должна соответствовать СМИБ, определить информационные активы и получить данные по текущему состоянию информационной безопасности в рамках области действия СМИБ

**ISO/IEC 27001:2005, ссылки:** 4.2.1, c),1) частично, 4.2.1, d), 4.2.1, e)

Информация, собранная в процессе анализа информационной безопасности, должна:

a) стать основной для управления (т. е. должна иметь корректные базовые данные);

b) определять и документировать условия для внедрения СМИБ;

c) обеспечивать четкое и обоснованное понимание возможностей организации;

d) учитывать определенные обстоятельства и положение в организации;

e) определять требуемый уровень защиты информации;

f) определять сбор и обработку информации, требуемые для всего предприятия или его части, находящейся в рамках предложенной области действия СМИБ.

### 7.2 Определение требований к информационной безопасности для процесса СМИБ

**Действия**

Необходимо проанализировать и определить подробные требования к информационной безопасности для процесса СМИБ.

**Исходные данные:**

a) выходные данные действия 5.2, определение приоритетов организации для разработки СМИБ — документы:

1 Краткое изложение целей, приоритетов в области информационной безопасности и требований организации к СМИБ;

2 Перечень регулирующих, контрактных и отраслевых ограничений, относящихся к информационной безопасности организации;

b) выходные данные действия 6.5, объединение всех областей действия и границ для получения области действия и границ СМИБ — область действия и границы СМИБ;

c) выходные данные действия 6.6, разработка политики СМИБ и получение одобрения руководства — политика СМИБ.

**Рекомендации**

Для первого этапа требуется собрать всю вспомогательную информацию для СМИБ. Для каждого процесса в организации и задачи для специалиста требуется принять решение в отношении того, насколько важной является информация, т. е. какой требуется уровень защиты. На информационную безопасность могут влиять множество внутренних условий, их необходимо определить. На данном этапе нет необходимости в подробном описании информационной технологии. Требуется базовое краткое описание проанализированной информации по процессам в организации и связанным приложениям и системам ИКТ.

На рисунке 5 представлено описание проведения фазы определения требований к информационной безопасности.

Анализ процессов в организации дает информацию о влияниях инцидентов информационной безопасности на деятельность организации. Во многих случаях достаточно работы с базовым описанием процессов в организации. Процессы, функции, объекты, информационные системы и коммуникационные сети необходимо определить и документировать, если они еще не были включены как часть области действия СМИБ.

Для получения подробных требований к информационной безопасности для СМИБ следует рассмотреть следующие вопросы:

a) предварительное определение важных информационных активов и текущего состояния защиты информации;

b) определение представлений организации и влияния определенных представлений на будущие требования к информационной безопасности;

c) анализ существующих форм обработки информации, системного программного обеспечения, коммуникационных сетей, определения действий и ресурсов для информационных технологий и т. д.;

d) определение всех существенных требований (например, законных и обязательных требований, договорных обязательств, требований организации, отраслевых стандартов и соглашений с клиентами, условий страхования и т. д.);

e) определение уровня информированности в области информационной безопасности и определение требований к обучению и образованию в отношении каждого функционального и административного подразделения.

**Выходные данные**

Выходные данные этого действия следующие:

a) определение основных процессов, функций, объектов, информационных систем и коммуникационных сетей;

b) информационные активы организации;

c) классификация важнейших процессов (активов);

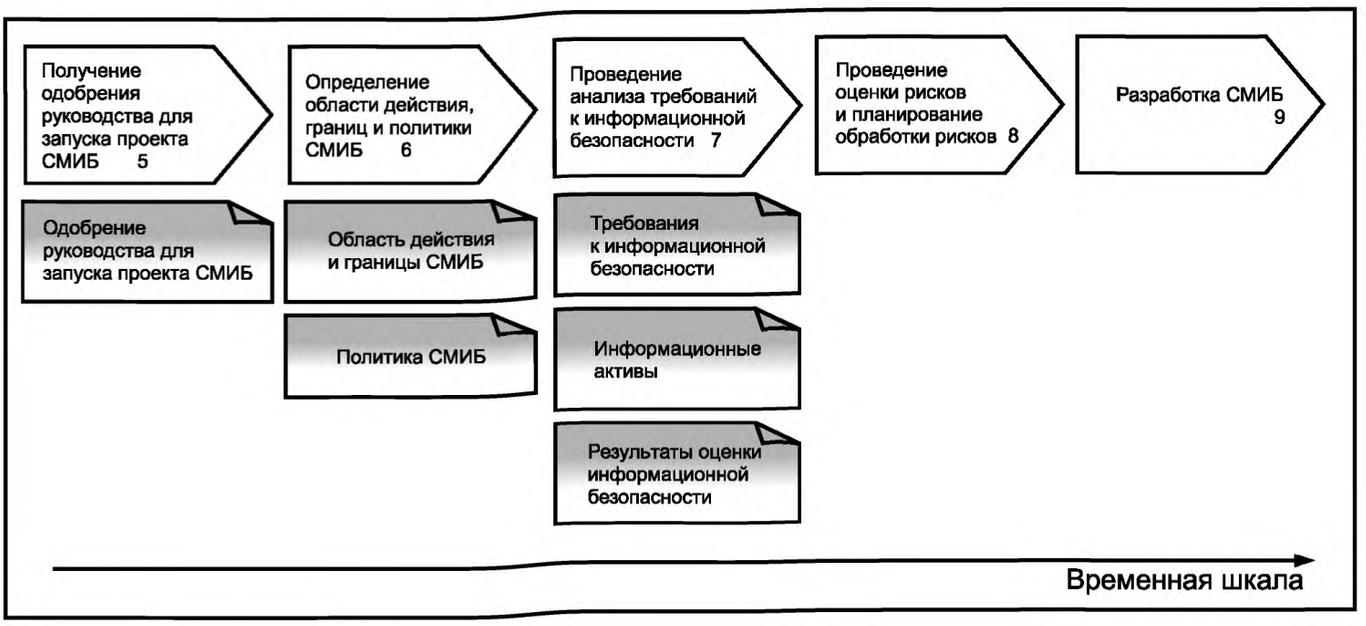
d) требования к информационной безопасности, сформулированные на основе законных, обязательных и контрактных требований;

e) перечень известных уязвимостей, которые должны быть устранены в результате выполнения требований к информационной безопасности;

f) требования к обучению и образованию в области информационной безопасности в организации.

**Дополнительная информация**

Дополнительная специальная информация не требуется.



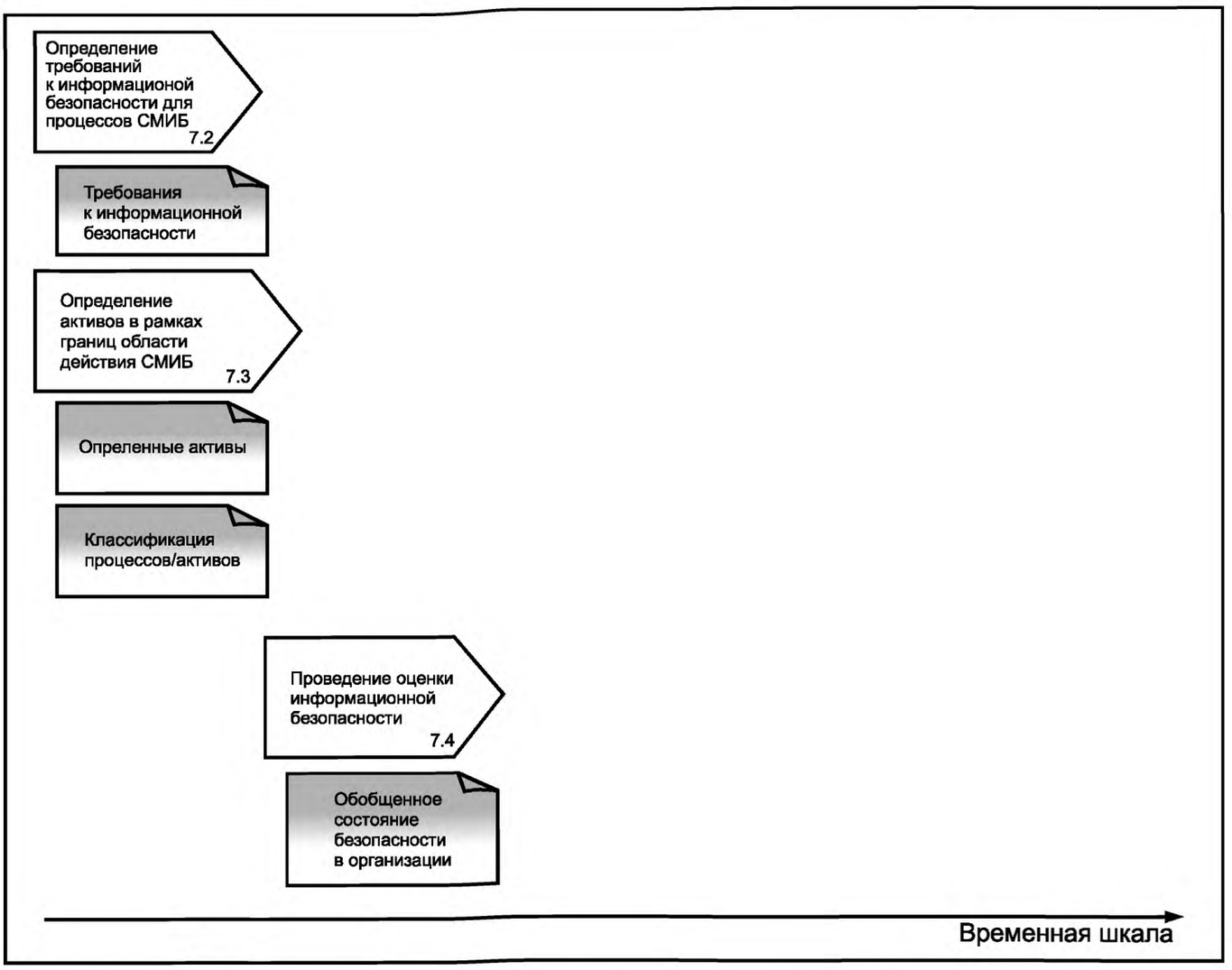




Рисунок 5 — Описание проведения фазы определения требований к информационной безопасности

### 7.3 Определение активов в рамках области действия СМИБ

**Действия**

Необходимо определить активы, которые должны поддерживаться системой СМИБ.

**Исходные данные:**

a) выходные данные действия 6.5, объединение всех областей действия и границ для получения области действия и границ СМИБ — область действия и границы СМИБ;

b) выходные данные действия 6.6, разработка политики СМИБ и получение одобрения руководства — политика СМИБ;

c) выходные данные действия 7.2, определение требований к информационной безопасности для процесса СМИБ.

**Рекомендации**

Для определения активов в рамках области действия СМИБ необходимо определить и указать следующую информацию:

a) уникальное наименование процесса;

b) описание процесса и связанные с ним действия (создание, хранение, передача, удаление);

c) важность процесса для организации (критический, важный, вспомогательный);

d) владелец процесса (подразделение организации);

e) процессы, обеспечивающие исходные и выходные данные этого процесса;

f) приложения ИТ, поддерживающие процесс;

g) классификация информации (конфиденциальность, сохранность, доступ-ность, контроль доступа, неотказуемость и (или) другие важные для организации свойства, например, как долго может храниться информация).

**Выходные данные**

Выходные данные этого действия следующие:

a) определенные информационные активы основных процессов в организации в рамках области действия СМИБ;

b) классификация важнейших процессов и информационных активов с точки зрения информационной безопасности.

**Дополнительная информация**

Дополнительная специальная информация не требуется.

### 7.4 Проведение оценки информационной безопасности

**Действия**

Необходимо провести оценку информационной безопасности путем сравнения текущего состояния информационной безопасности в организации с целями организации.

**Исходные данные:**

a) выходные данные действия 6.5, объединение всех областей действия и границ для получения области действия и границ СМИБ – область действия и границы СМИБ;

b) выходные данные действия 6.6, разработка политики СМИБ и получение одобрения руководства — политика СМИБ;

c) выходные данные действия 7.2, определение требований к информационной безопасности для процесса СМИБ;

d) выходные данные действия 7.3, определение активов в рамках области действия СМИБ.

**Рекомендации**

Оценка информационной безопасности — это действия по определению существующего уровня информационной безопасности (т. е. процедур по защите информации, применяемых в организации в настоящее время). Фундаментальной целью оценки информационной безопасности является предоставление информации, подкрепляющей описание, требуемое для системы управления, в форме политики и рекомендаций. Необходимо обеспечить, чтобы выявленные недостатки устранялись параллельно, с помощью плана приоритетных действий. Все вовлеченные стороны должны быть ознакомлены с результатами анализа организации, стандартными документами и иметь доступ к соответствующим руководящим работникам.

При оценке информационной безопасности анализируется текущая ситуация в организации путем использования следующей информации и определяется текущее состояние информационной безопасности и недостатки в документации:

a) изучение предпосылок на основе важнейших процессов;

b) классификация информационных активов;

c) требования организации к информационной безопасности.

Результаты оценки информационной безопасности вместе с целями организации часто являются важной частью стимуляции будущей работы в области информационной безопасности. Оценка информационной безопасности должна проводиться внутренним или внешним проверяющим, независимым по отношению к организации.

Участвовать в оценке информационной безопасности должны лица, хорошо знающие существующую среду, условия и ясно представляющие, что является важным в отношении информационной безопасности. Эти лица должны выбираться таким образом, чтобы представлять широкий круг работников организации. Круг таких лиц должен включать:

a) линейных руководителей (например, начальников подразделений организации);

b) владельцев процессов (т. е. представителей важных подразделений организации);

c) других лиц, хорошо знающих существующую среду, условия и то, что является важным в отношении информационной безопасности. Например, пользователи бизнес-процессов, а также сотрудники, выполняющие оперативные, административные и юридические функции.

Для успешной оценки информационной безопасности важными являются следующие действия:

a) определение и перечисление соответствующих стандартов организации (например, ISO/IEC 27002:2005);

b) определение известных требований к управлению, установленных на основе политики, законных и обязательных требований, договорных обязательств, результатов прошедших проверок или оценок рисков;

c) использование этих документов в качестве справочных для приблизительной оценки существующих требований организации, касающихся уровня информационной безопасности.

Назначение приоритетов в сочетании с анализом организации создает основу, для которой должны рассматриваться предупредительные мероприятия по безопасности и проверки (контроль).

Подход к проведению оценки информационной безопасности следующий:

a) выбрать важные бизнес-процессы в организации и этапы процессов, касающиеся требований к информационной безопасности;

b) составить подробную блок-схему, охватывающую основные процессы в организации, включая инфраструктуру (логическую и техническую), если она еще не была составления во время анализа организации;

c) обсудить и проанализировать с ключевыми сотрудниками существующую ситуацию в организации в отношении требований к информационной безопасности. Например, какие процессы являются критическими, насколько хорошо они в настоящее время работают? (Полученные результаты в дальнейшем используются при оценке риска);

d) определить недостатки в управлении путем сравнения существующих средств управления с ранее определенными требованиями к управлению;

e) определить и документировать текущее состояние организации.

**Выходные данные**

Выходные данные этого действия представляют собой документ, описывающий состояние безопасности в организации и обнаруженные уязвимости.

**Дополнительная информация**

Оценка информационной безопасности, проводимая на данном этапе, дает только предварительную информацию о состоянии информационной безопасности в организации и уязвимостях, поскольку полный набор политики и стандартов информационной безопасности разрабатывается на следующем этапе (см. раздел 9), а оценка риска еще не проведена.

## 8 Проведение оценки риска и планирование обработки риска

### 8.1 Описание проведения оценки риска и планирования обработки риска

При внедрении СМИБ необходимо учитывать связанные с этим риски для информационной безопасности. Определение, оценка и планируемые действия в случае возникновения риска, а также выбор целей и средств управления являются важными этапами внедрения СМИБ и должны быть проработаны на данном этапе.

Стандарт ISO/IEC 27005:2008 содержит специальные рекомендации по менеджменту риска для информационной безопасности и должен упоминаться в разделе 8.

Предполагается, что руководство дало поручение на внедрение СМИБ и область действия и политика СМИБ определены, а также известны информационные активы и результаты оценки информационной безопасности.

**Цель:**

Определить методологию оценки риска, определить, проанализировать и оценить риски для информационной безопасности, чтобы выбрать варианты обработки риска и цели, а также меры и средства контроля и управления.

**ISO/IEC 27001, ссылки** с 4.2.1, c) по 4.2.1, j).

### 8.2 Проведение оценки риска

**Действия**

Необходимо провести оценку риска.

**Исходные данные:**

a) выходные данные раздела 7, проведение анализа требований к информационной безопасности — информация, касающаяся:

1 Обобщенного состояния информационной безопасности;

2 Определенных информационных активов;

b) выходные данные действий раздела 6, определение области действия, границ и политики СМИБ — документы:

1 Область действия СМИБ;

2 Политика СМИБ;

c) ISO/IEC 27005:2008.

На рисунке 6 представлено описание фазы оценки риска.

**Рекомендации**

Оценка риска безопасности на предприятии для подкрепления области действия СМИБ необходима для успешного внедрения СМИБ в соответствии ISO/IEC 27001:2005. В результате оценки риска необходимо:

a) определить угрозы и их источники;

b) определить существующие и планируемые меры и средства контроля и управления;

c) определить уязвимости, которые могут в случае угрозы нанести ущерб активам или организации;

d) определить последствия потери конфиденциальности, сохранности, доступности, неотказуемости или нарушения других требований к безопасности для активов;

e) оценить влияние на предприятие, которое может возникнуть в результате предполагаемых или фактических инцидентов информационной безопасности;

f) оценить вероятность чрезвычайных сценариев;

g) оценить уровень риска;

h) сравнить уровни риска с критериями оценки и приемлемости рисков.

Участвовать в оценке риска должны лица, хорошо знающие цели организации и понимающие проблемы безопасности (например, хорошо представляющие, что в настоящее время важно с точки зрения угроз по отношению к целям организации). Эти лица должны выбираться таким образом, чтобы представлять широкий круг сотрудников организации (справочную информацию см. в приложении B).

Организация может использовать методологию оценки риска, которая является стандартной по отношению к проекту, компании или отрасли.

**Выходные данные**

Выходные данные этого действия следующие:

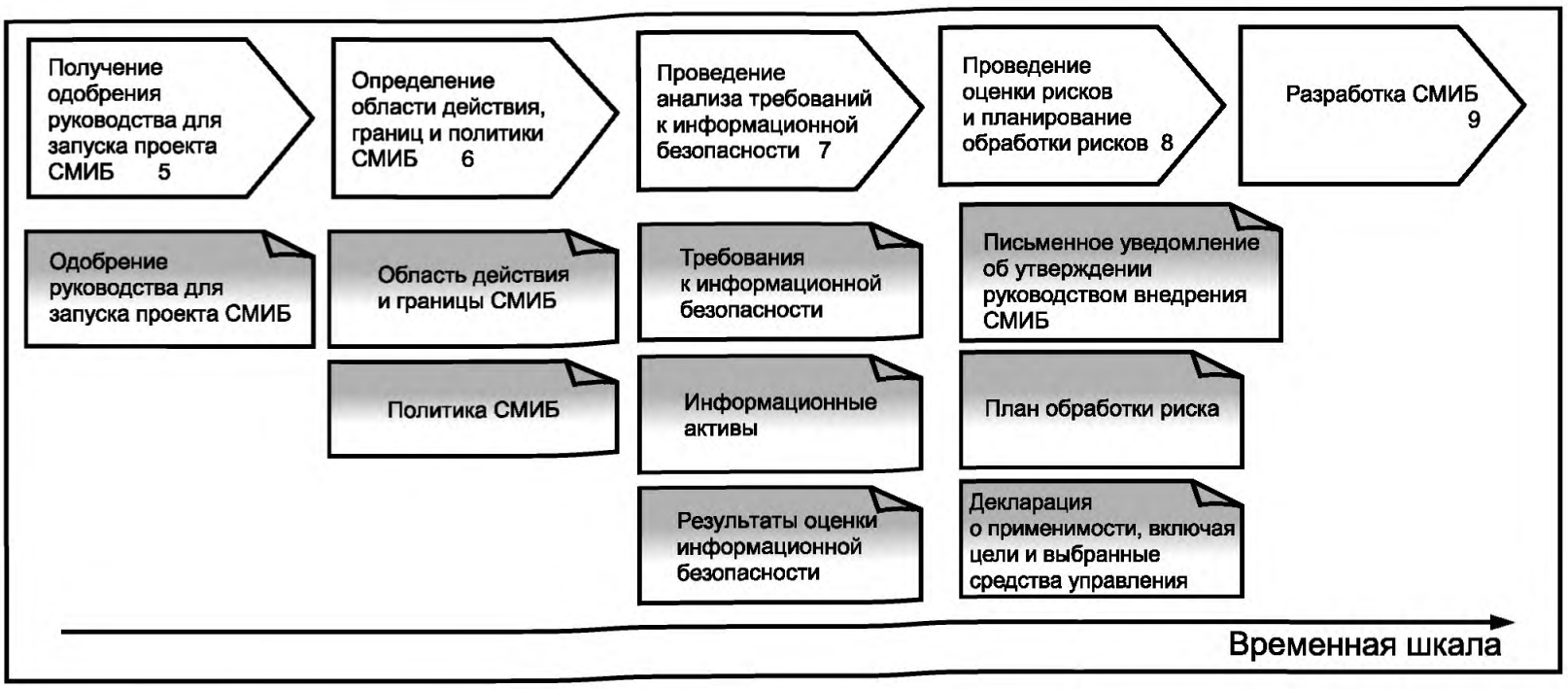
a) описание методологий оценки риска;

b) результаты оценки риска.

**Дополнительная информация**

Приложение B — информация по ролям и сферам ответственности.

Примечание — Чрезвычайный сценарий — это описание угрозы, оказывающей влияние на определенную уязвимость или несколько уязвимостей во время инцидента с информационной безопасностью. В стандарте ISO/IEC 27001 описываются чрезвычайные сценарии, такие как «нарушения безопасности» (см. ISO/IEC 27005:2008).



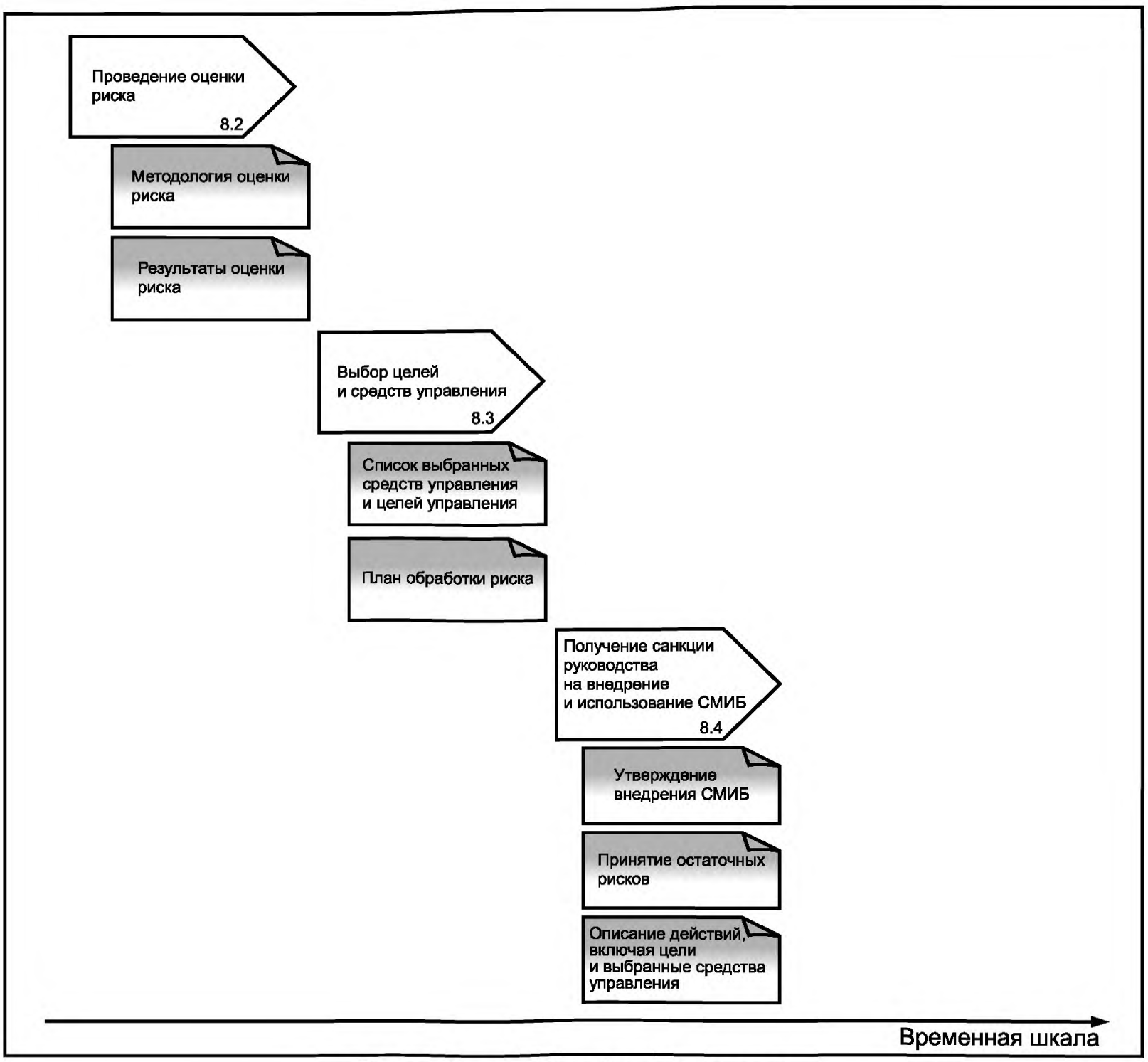




Рисунок 6 — Описание фазы оценки риска

### 8.3 Выбор целей и средств управления

**Действия**

Необходимо определить варианты действий в случае возникновения риска, а также выбор соответствующих средств управления, в соответствии с определенными вариантами действий в случае возникновения риска.

**Исходные данные:**

a) выходные данные действия 8.2, проведение оценки риска — результаты оценки риска;

b) ISO/IEC 27005:2008;

c) ISO/IEC 27002:2005.

**Рекомендации**

Важно определить соотношение меду рисками и выбранными вариантами обработки риска (например, план обработки риска), поскольку эти соотношения дают обобщение обработки риска. Возможные варианты обработки рисков перечисляются в стандарте ISO/IEC 27001:2005, 4.2.1, f).

Приложение А к стандарту ISO/IEC 27001:2005 (нормативное) «Цели и меры (средства контроля)» используется для выбора целей и средств управления действиями в случае возникновения риска. Если в Приложении А нет подходящих целей и средств управления, следует определить и использовать дополнительные цели, и меры, и средства контроля и управления. Важно продемонстрировать, как выбранные меры и средства контроля и управления могут снизить риск, что требуется в соответствии с планом обработки риска.

Данные, приведенные в стандарте ISO/IEC 27001:2005, Приложение А, не являются исчерпывающими. Для подкрепления потребностей конкретного предприятия, а также СМИБ можно определить меру и средство контроля и управления, характерные для данной отрасли.

В случае снижения риска установление соотношения между каждым риском и выбранными целями и средствами управления является полезным для разработки внедрения СМИБ. Это соотношение можно добавить в список соотношений между рисками и вариантами обработки рисков.

Для облегчения аудита организация должна составить перечень средств управления, выбранных как подходящие и применимые для СМИБ организации. Это дает дополнительные преимущества, связанные с улучшением деловых отношений, например электронный аутсорсинг, путем предоставления описания средств управления на месте.

Важно знать о том, что описание средств управления с большой вероятностью может содержать секретную информацию. Следовательно, соблюдать осторожность при предоставлении доступа к описанию средств управления как внутренним, так и внешним получателям. Фактически может возникнуть необходимость учета информации, появляющейся в результате создания СМИБ, во время определения активов.

**Выходные данные**

Выходные данные этого действия следующие:

a) перечень выбранных целей и средств управления;

b) план обработки риска, включающий:

1 Описание соотношения между рисками и выбранным вариантом обработки риска;

2 Описание соотношения между рисками и выбранными целями и средствами управления (особенно в случае снижения риска).

**Дополнительная информация**

ISO/IEC 27002:2005.

### 8.4 Получение санкции руководства на внедрение и использование СМИБ

**Действия**

Необходимо получить санкцию руководства на внедрение СМИБ, а также документировать принятие остаточных рисков.

**Исходные данные:**

a) выходные данные действий в 5.4, составление описания случая применения СМИБ для данного предприятия и плана проекта для утверждения руководством — первоначальное утверждение руководством проекта СМИБ;

b) выходные данные действий в пункте 6, определение области действия, границ и политики СМИБ — документы:

1 Политика и цели СМИБ;

2 Область действия СМИБ;

c) выходные данные действия 8.2, проведение оценки риска — документы:

1 Описание методологий оценки риска;

2 Результаты оценки риска;

d) выходные данные действия 8.3, выбор целей и средств управления — план обработки риска.

**Рекомендации**

Для получения одобрения руководства необходимо подготовить документы, описываемые как исходные данные для данного подпункта, и представить их на рассмотрение руководства для оценки и принятия решения.

Подготовка декларации о применимости (SoA) должна быть включена как часть работ по менеджменту информационной безопасности. Уровень детализации, с которым определяются меры и средства контроля и управления, должен соответствовать требованиям, подкрепляющим утверждение СМИБ руководством организации.

Необходимо получить одобрение высшего руководства для принятия решения о принятии остаточных рисков, а также санкцию на фактическое использование СМИБ. Эти решения должны основываться на оценке рисков и вероятности их возникновения в результате внедрения СМИБ, в сравнении с рисками, возникающими в случае, когда система не применяется.

**Выходные данные**

Выходные данные этого действия следующие:

a) письменное уведомление об одобрении руководством внедрения СМИБ;

b) принятие руководством остаточных рисков;

c) декларация о применимости, включая цели и выбранные меры и средства контроля и управления.

**Дополнительная информация**

Дополнительная специальная информация не требуется.

## 9 Разработка СМИБ

### 9.1 Описание разработки СМИБ

На данном этапе должны быть разработаны рабочий проект СМИБ и планируемые действия по внедрению системы. Конечный проект СМИБ должен быть уникальным в деталях для конкретной организации в зависимости от результатов предыдущих действий, а также результатов конкретных действий в фазе разработки, описываемых в данном пункте.

Результатом выполнения данного пункта является конкретный конечный план проекта СМИБ. На основе этого плана может быть запущен проект СМИБ в организации как самая первая фаза осуществления ("DO") цикла PDCA (Plan, Do, Check & Act — план, осуществление, проверка, действие), описываемого в стандарте ISO/IEC 27001:2005.

Предполагается, что руководство дало поручение на внедрение СМИБ, которое определено в области действия и политике СМИБ. Предполагается, что информационные активы, а также результаты оценки информационной безопасности доступны. Кроме того, должен быть доступен план обработки риска, описывающий риски, варианты обработки риска и определенные выбранные цели, а также меры и средства контроля и управления.

Описываемая здесь разработка СМИБ сосредоточена на внутренней структуре и требованиях СМИБ. Следует отметить, что в определенных случаях разработка СМИБ может прямо или косвенно влиять на разработку бизнес-процессов. Также следует отметить, что обычно требуется объединение компонентов СМИБ с существовавшими ранее планами управления и инфраструктурой.

**Цель**

Составить конечный план внедрения СМИБ посредством разработки системы безопасности организации на основе выбранных вариантов обработки риска, а также требований, касающихся записей и документов и разработки средств управления, объединяющих меры безопасности ИКТ, физические и организационные процессы и разработку специальных требований для СМИБ.

**ISO/IEC 27001: 2005, ссылка:** 4.2.2, a)—e),h)

При разработке СМИБ следует принять во внимание следующие вопросы:

a) безопасность организации — охватывает административные аспекты информационной безопасности, включая ответственность, возникающую при выполнении процессов в организации, за обработку риска. Эти аспекты следует оформить в группу действий, в результате которых формируется политика, цели, процессы и процедуры проработки и повышения информационной безопасности в отношении потребностей и рисков организации;

b) безопасность ИКТ — охватывает аспекты информационной безопасности, связанные с ответственностью за снижение рисков при выполнении операций с ИКТ. Эти аспекты должны обеспечивать выполнение требований, установленных организацией, и техническое внедрение средств управления для снижения рисков;

c) безопасность физических объектов — охватывает аспекты информационной безопасности, связанные, в частности, с ответственностью, возникающей при проработке физического окружения, например зданий и их инфраструктуры, за снижение риска. Эти аспекты должны обеспечивать выполнение требований, установленных организацией, и техническое внедрение средств управления для снижения рисков;

d) особые требования к СМИБ — охватывают аспекты, связанные с различными особыми требованиями к СМИБ в соответствии с ISO/IEC 27001:2005, в отличие от аспектов, охватываемых в трех других областях. Основное внимание уделяется определенным действиям, которые должны выполняться при внедрении СМИБ для получения работоспособной системы, включая:

1 Мониторинг;

2 Измерения;

3 Внутренний аудит СМИБ;

4 Обучение и информирование;

5 Управление в чрезвычайных ситуациях;

6 Проверки, осуществляемые руководством;

7 Усовершенствование СМИБ, включая корректирующие и предупреждающие действия.

При разработке проекта СМИБ и связанного с ним планируемого внедрения средств управления должны использоваться квалификация и опыт работников тех частей организации, которые находятся в области действия СМИБ или несут административную ответственность, связанную с СМИБ. Аспекты, связанные с СМИБ, требуют диалога с руководством.

Для разработки выбранных средств управления, применяемых для обработки риска, важно разработать среду безопасности ИКТ и безопасности физических объектов, а также среду безопасности организации. Безопасность ИКТ связана не только с информационными системами и сетями, но также и с техническими требованиями. Безопасность физических объектов связана со всеми аспектами контроля доступа, неотказуемости, физической защиты информационных активов и хранимой информации, а также сама является средством защиты для управления безопасностью.

Меры и средства контроля и управления, выбранные в действиях, описываемых в 8.3, должны применяться в соответствии с особым структурированным и детализированным планом внедрения, являющимся частью плана проекта СМИБ. Эта особая часть плана проекта СМИБ должна описывать действия в случае возникновения каждого вида риска для достижения целей управления. Эта особая часть плана проекта СМИБ является важной, если необходимо правильно и эффективно применить выбранные меры и средства контроля и управления. Группа управления информационной безопасностью отвечает за составление этой особой части плана внедрения СМИБ, которая затем образует конечный план проекта СМИБ.

### 9.2 Разработка информационной безопасности организации

#### 9.2.1 Разработка конечной структуры организации для информационной безопасности

**Действия**

Необходимо сопоставить функции, роли и сферы ответственности в организации, связанные с информационной безопасностью, с обработкой рисков.

**Исходные данные:**

a) выходные данные действия 5.3.2, определение ролей и сфер ответственности для предварительной области действия СМИБ — таблица ролей и сфер ответственности;

b) выходные данные действия 6.5, объединение всех областей действия и границ для получения области действия и границ СМИБ — область действия и границы СМИБ.

На рисунке 7 представлено описание фазы разработки СМИБ;

c) выходные данные действия 6.6, разработка политики СМИБ и получение одобрения руководства — политика СМИБ;

d) выходные данные действия 7.2, определение требований к информационной безопасности для процесса СМИБ;

e) выходные данные действия 7.3, определение активов в рамках области действия СМИБ;

f) выходные данные действия 7.4, проведение оценки информационной безопасности;

g) выходные данные действия 8.2, проведение оценки риска — результаты оценки риска;

h) выходные данные действия 8.3, выбор целей и средств управления;

i) ISO/IEC 27002:2005.

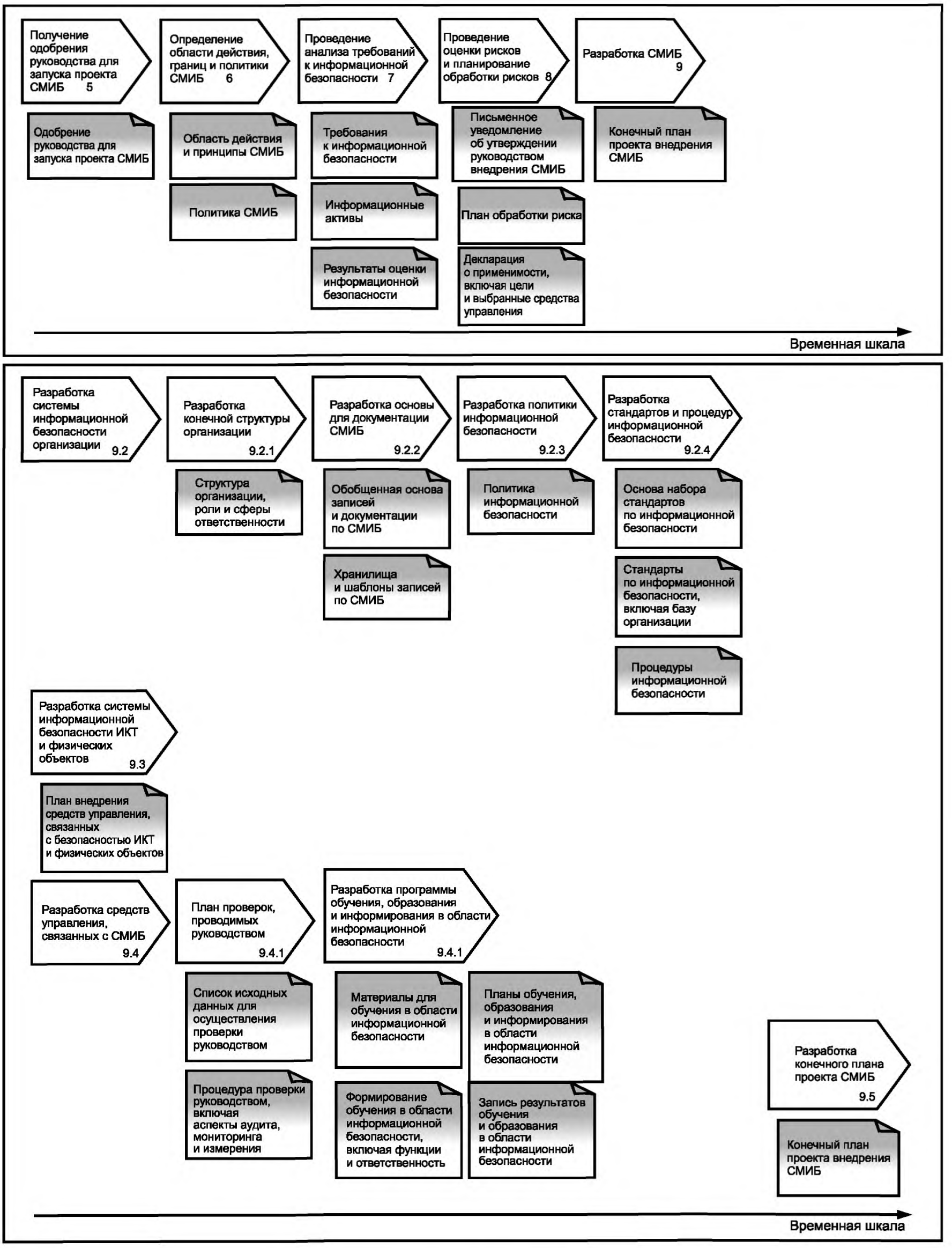



Рисунок 7 — Описание фазы разработки СМИБ

**Рекомендации**

При разработке структуры организации и процессов для внутренних операций СМИБ следует попытаться создать их и объединить с уже существующими, если это практически применимо. Точно также объединение СМИБ с более широкими ранее существовавшими системами управления (например, внутренний аудит) следует учитывать в процессе разработки СМИБ.

Структура организации, разрабатываемая для СМИБ, должна отражать действия по внедрению и использованию СМИБ, а также, например, проработку методов мониторинга и записи как часть операции СМИБ.

Соответственно структура операций СМИБ должна разрабатываться на основе планируемого применения СМИБ с учетом следующего:

a) нужна ли каждая роль по внедрению СМИБ для выполнения операций СМИБ?

b) отличаются ли определенные роли от ролей по внедрению СМИБ?

c) какие роли должны быть добавлены для внедрения СМИБ?

Например, можно добавить следующие роли для выполнения операций СМИБ:

a) лицо, ответственное за операции по информационной безопасности в каждом подразделении;

b) лицо, ответственное за измерение СМИБ в каждом подразделении.

Рассмотрение пунктов, указанных в Приложении В «Роли и сферы ответственности в области информационной безопасности», способствует принятию решения по структуре и ролям по выполнению операций СМИБ путем пересмотра структуры и ролей по внедрению СМИБ.

**Выходные данные**

Выходные данные этого действия представляют собой документ, описывающий структуру организации, роли и сферы ответственности.

**Дополнительная информация**

Приложение В — Роли и сферы ответственности в области информационной безопасности.

Приложение С — Информация по внутреннему аудиту.

### 9.2.2 Разработка основы для документирования СМИБ

**Действия**

Необходимо проконтролировать записи и документы в системе СМИБ путем определения требований и основы, позволяющей выполнить требования по текущему контролю записей и документов в системе СМИБ.

**Исходные данные:**

a) выходные данные действия 6.5, объединение всех областей действия и границ для получения области действия и границ СМИБ — область действия и границы СМИБ;

b) область действия и границ СМИБ;

c) выходные данные действия 6.6, разработка политики СМИБ и получение одобрения руководства — политика СМИБ;

d) выходные данные действия 8.4, получение санкции руководства на внедрение и использование СМИБ;

e) выходные данные действия 9.2.1, разработка конечной организационной структуры для информационной безопасности;

f) ISO/IEC 27002:2005.

**Рекомендации**

Разработка записей СМИБ включает следующие действия:

a) основа, описывающая принципы документирования СМИБ, структура процедур документирования СМИБ, связанные роли, форматы данных и каналы передачи данных для отчетности перед руководством;

b) разработка требований к документации;

c) разработка требований к записям.

Документация по СМИБ должна включать записи решений руководства, обеспечивать возможность отслеживания действий для принятия решений и разработки политики руководством и воспроизводимость записанных результатов.

Документы по СМИБ должны содержать признаки того, что меры и средства контроля и управления выбраны на основе результатов оценки риска и обработки риска и что такие процессы применяются в сочетании с политикой и целями СМИБ.

Документация важна для воспроизводимости результатов и процедур. В том, что касается выбранных средств управления, установка и документирование процедур должны содержать ссылку на лицо, ответственное за фактическую часть документации.

Документация по СМИБ должна включать документацию, указанную в ISO/IEC 27001:2005, пункт 4.3.1.

Необходимо осуществлять управление документами по СМИБ и сделать их доступными персоналу при необходимости. Эти действия включают:

a) учреждение административной процедуры управления документами по СМИБ;

b) подтверждение соответствия формата документов перед изданием;

c) обеспечение определения изменений и текущего состояния редакций документов;

d) защита и контроль документов как информационных активов организации.

Важно, чтобы соответствующие версии применяемых документов были доступны в пунктах использования, чтобы документы были удобочитаемыми, легко идентифицируемыми, передавались, хранились или, в конечном счете, отклонялись в соответствии с процедурами, применяемыми к их классификации.

Кроме того, важно обеспечить, чтобы документы из внешних источников легко идентифицировались, чтобы контролировалось распространение документов, предотвращая непредусмотренное использование устаревших документов и применяя к ним соответствующие процедуры отслеживания, если они сохраняются с какой-либо целью.

Записи должны создаваться, сохраняться и контролироваться как свидетельство того, что СМИБ организации соответствует стандарту ISO/IEC 27001:2005 и что операции эффективны.

Также требуется сохранять записи состояния внедрения системы для всей фазы PDCA, а также записи об инцидентах и событиях, связанных с информационной безопасностью, записи об образовании, обучении, навыках, опыте и квалификации, внутреннем аудите СМИБ, корректирующих и предупреждающих действиях и организационные записи.

Для контроля записей необходимо выполнить следующие задачи:

a) документировать меры и средства контроля и управления, требуемые для идентификации, хранения, защиты, поиска и удаления данных, и документировать продолжительность хранения;

b) определить, что и в какой степени должно записываться в процессах управления организацией;

c) если соответствующим законодательством определен какой-либо период хранения, он должен быть установлен в соответствии с этими законными требованиями.

**Выходные данные**

Выходные данные этого действия следующие:

a) документ, описывающий требования к записям СМИБ и контролю документации;

b) хранилища и шаблоны требуемых записей СМИБ.

**Дополнительная информация**

Дополнительная специальная информация не требуется.

**9.2.3 Разработка политики информационной безопасности**

**Действия**

Необходимо документировать стратегическую позицию руководства и администрации, связанную с целями информационной безопасности в отношении использования СМИБ.

**Исходные данные:**

a) выходные данные действия 5.2, определить приоритеты организации для разработки СМИБ — обобщенные цели и перечень требований;

b) выходные данные действия 5.4, составление описания случая применения СМИБ для данного предприятия и плана проекта для утверждения руководством — первоначальное утверждение руководством проекта СМИБ;

c) выходные данные действия 6.5, объединение всех областей действия и границ для получения области действия и границ — область действия и границы СМИБ;

d) выходные данные действия 6.6, разработка политики СМИБ и получение одобрения руководства — политика СМИБ;

e) выходные данные действия 7.2, определение требований к информационной безопасности для процесса СМИБ;

f) выходные данные действия 7.3, определение активов в рамках области действия СМИБ;

g) выходные данные действия 7.4, проведение оценки информационной безопасности;

h) выходные данные действия 8.2, проведение оценки риска — результаты оценки риска, выходные данные действия 8.3, выбор целей и средств управления;

i) выходные данные действия 9.2.1, разработка конечной структуры организации для информационной безопасности;

j) выходные данные действия 9.2.2, разработка основы для документирования СМИБ;

k) ISO/IEC 27002:2005, пункт: 5.1.1.

**Рекомендации**

Политика информационной безопасности документирует стратегическую позицию организации в отношении информационной безопасности во всей организации.

Политика строится на основе информации и знания. Моменты, признанные руководством важными во время ранее проведенного анализа, должны быть сделаны наглядными, им должно быть уделено особое внимание в политике, чтобы обеспечить стимуляцию и мотивацию в организации. Также важно отметить, что происходит, если не следовать выбранной политике, и подчеркнуть влияния законов и регулирующих положений на рассматриваемую организацию.

Примеры политики информационной безопасности можно взять из справочной литературы, сети Интернет, в сообществах по интересам и отраслевых объединениях. Формулировки и подсказки можно найти в годовых отчетах, других документах по политике или документах, сохраняемых руководством.

Относительно фактического объема документации по политике могут существовать различные интерпретации и требования. Эта документация должна быть в достаточной степени суммирована, чтобы работники организации понимали значение политики. Кроме того, она должна достаточно четко показывать, каких целей необходимо достичь, чтобы установить набор правил и целей организации.

Объем и структура политики информационной безопасности должны подкреплять документы, которые используются на следующем этапе процесса, для введения системы управления информационной безопасностью (см. также приложение D — Структура политики).

Для больших организаций со сложной структурой (например, с широким спектром различных областей деятельности) может возникнуть необходимость создания общей политики и множества политик более низкого уровня, адаптированных к конкретным областям деятельности.

Рекомендации по содержанию документов по политике информационной безопасности представлены в стандарте ISO/IEC 27002:2005, пункт 5.1.1.

Предлагаемая политика (с номером версии и датой) должна быть подвергнута перекрестной проверке и учреждена в организации оперативным руководителем. После учреждения в группе управления или аналогичном органе оперативный руководитель утверждает политику информационной безопасности. Затем она доводится до сведения каждого работника организации надлежащим способом, чтобы стать доступной и понятной для читателей.

**Выходные данные**

Выходными данными этого действия является документ по политике информационной безопасности.

**Дополнительная информация**

Приложение B — Роли и сферы ответственности.

Приложение D — Структура политики.

**9.2.4 Разработка стандартов и процедур обеспечения информационной безопасности**

**Действия**

Необходимо разработать стандарты и процедуры обеспечения информационной безопасности, касающиеся всей организации или ее отдельных частей.

**Исходные данные:**

a) выходные данные действия 6.5, объединение всех областей действия и границ для получения области действия и границ — область действия и границы СМИБ;

b) выходные данные действия 6.6, разработка политики СМИБ и получение одобрения руководства — политика СМИБ;

c) выходные данные действия 8.2, проведение оценки риска;

d) выходные данные действия 8.3, выбор целей и средств управления;

e) выходные данные действия 8.4, получение санкции руководства на внедрение и использование СМИБ – декларация о применимости, включая цели и выбранные меры и средства контроля и управления;

f) выходные данные действия 9.2.1, разработка конечной структуры организации для информационной безопасности;

g) выходные данные действия 9.2.2, разработка основы для документирования СМИБ;

h) выходные данные действия 9.2.3, разработка политики информационной безопасности;

i) ISO/IEC 27002:2005.

**Рекомендации**

Чтобы обеспечить основу для работы в области информационной безопасности в организации, стандарты по информационной безопасности, а также набор применяемых законных и обязательных требований должны быть доступны всем, кому нужно их знать.

В процессе разработки стандартов и процедур должны участвовать представители разных частей организации, попадающих в область действия СМИБ. Участники процесса должны иметь полномочия и являться представителями организации. Например, могут быть включены следующие роли:

a) менеджеры по информационной безопасности;

b) представители по вопросам безопасности физических объектов;

c) владельцы информационных систем;

d) владельцы процессов в стратегических и оперативных подразделениях.

Рекомендуется, чтобы редакторская группа была как можно меньше по численности с возможностью назначения специалистов в группу на временной основе по мере необходимости. Каждый представитель должен активно поддерживать связь со своим подразделением в организации для обеспечения непрерывной оперативной поддержки. Впоследствии это должно способствовать дальнейшему совершенствованию в виде процедур и действий на оперативном уровне.

Стандарты и процедуры по информационной безопасности должны впоследствии использоваться в качестве основы для разработки подробных технических и оперативных процедур.

Действенным способом разработки стандартов и процедур по информационной безопасности является учет каждого пункта руководства по внедрению системы менеджмента информационной безопасности в стандартах ISO/IEC 27001:2005 и ISO/IEC 27002:2005, который считается применимым (на основе результатов оценки риска), и точное описание того, как он должен применяться.

Оценка любых существующих стандартов и процедур по информационной безопасности должна рассматриваться. Например, могут ли они усовершенствоваться и развиваться, нет ли необходимости в их полной замене?

Уместная и актуальная документация должна предоставляться каждому сотруднику организации, попадающему в область действия системы. Стандарты и процедуры по информационной безопасности должны применяться ко всей организации или точно указывать, какие роли, системы и подразделения попадают под их действие. Первая версия должна быть выпущена своевременно.

Процесс редактирования и проверки должен быть определен на ранней стадии. Необходимо составить стратегию, касающуюся того, как должна распространяться информация об изменениях политики.

**Выходные данные:**

a) выходные данные этого действия представляют собой структурированный подробный план внедрения средств управления, относящихся к информационной безопасности как часть конечного плана проекта СМИБ, включая документированную основу набора стандартов по информационной безопасности;

b) стандарты по информационной безопасности, включая исходные данные организации;

c) процедуры обеспечения информационной безопасности для получения стандартов по информационной безопасности.

**Дополнительная информация**

Приложение D — Структура политики.

### 9.3 Разработка информационной безопасности ИКТ и физических объектов

**Действия**

Необходимо разработать меры и средства контроля и управления средой безопасности ИКТ и физических объектов.

**Исходные данные:**

a) выходные данные действия 6.5, объединение всех областей действия и границ для получения области действия и границ — область действия и границы СМИБ;

b) выходные данные действия 6.6, разработка политики СМИБ и получение одобрения руководства — политика СМИБ;

c) выходные данные действия 7.2, определение требований к информационной безопасности для процесса СМИБ;

d) выходные данные действия 7.3, определение активов в рамках области действия СМИБ;

e) выходные данные действия 7.4, проведение оценки информационной безопасности;

f) выходные данные действия 8.3, выбор целей и средств управления;

g) выходные данные действия 8.4, получение санкции руководства на внедрение и использование СМИБ — декларация о применимости, включая цели, выбранные меры, средства контроля и управления;

h) ISO/IEC 27002:2005.

**Рекомендации**

В этом действии, которое должно стать частью плана проекта СМИБ, необходимо документировать следующую информацию для каждых мер и средств контроля и управления:

a) имя лица, ответственного за внедрение мер и средств контроля и управления;

b) приоритет внедряемых мер и средств контроля и управления;

c) задачи или действия по внедрению;

d) установление времени, в течение которого должно быть внедрено средство управления;

e) лицо, перед которым нужно отчитываться о внедрении мер и средств контроля и управления по его завершению;

f) ресурсы для внедрения (рабочая сила, требуемое пространство, затраты).

Первоначально безопасность ИКТ и физических объектов должна быть разработана на концептуальном уровне. Необходимо учитывать, что сферы ответственности за процесс первоначального внедрения обычно включают:

a) задание целей управления с описанием предполагаемого планируемого состояния;

b) распределение ресурсов (объем работ, финансовые ресурсы);

c) реальное заданное время внедрения мер и средств контроля и управления;

d) варианты объединения с системами безопасности ИКТ, физических объектов и организации.

После разработки концепции необходимо фактически разработать, например, систему, чтобы получить и внедрить лучшие практические методы для организации. Необходимо учитывать следующее:

Сферы ответственности за процесс фактического внедрения включают:

a) разработку каждого из средств управления для области безопасности ИКТ, физических объектов и организации на оперативном уровне рабочего места;

b) конкретизацию каждой меры и каждого средства контроля и управления в соответствии с согласованным проектом;

c) предоставление процедур и информации для органов управления и учебных курсов, способствующих информированию в сфере безопасности;

d) оказание помощи и внедрение средств управления на рабочем месте.

В зависимости от средств управления (ИКТ, физические объекты или организация) проведение отчетливой границы между начальной и конечной частями процесса внедрения не всегда является уместным или необходимым.

Для внедрения средств управления часто требуется взаимодействие между сотрудниками, занимающими различные должности в организации. Таким образом, например, лица, ответственные за системы, могут быть задействованы для приобретения, установки и обслуживания технического оборудования. Других сотрудников целесообразно привлечь для разработки и документирования процедур, контролирующих использование систем.

Информационная безопасность должна быть объединена в процедуры и процессы, применяемые во всей организации. Если для части организации или третьей стороны окажется трудным внедрение этих процедур и процессов, соответствующие стороны должны сообщить об этом немедленно, чтобы согласовать решение проблемы. Решение по подобным вопросам включает изменение процедур или процессов, перераспределение должностей и сфер ответственности и адаптацию технических процедур.

Результаты внедрения средств управления СМИБ должны быть следующими:

a) план внедрения, в котором подробно описывается внедрение средств управления, например, график, структура группы по внедрению и т. д.;

b) записи и документация по результатам внедрения.

**Выходные данные**

Выходные данные этого процесса представляют собой структурированный подробный план внедрения средств управления, связанных с безопасностью ИКТ и физических объектов, как часть плана проекта СМИБ для каждой меры и средства контроля и управления:

a) подробное описание;

b) сферы ответственности за разработку и внедрение;

c) предполагаемые временные шкалы;

d) связанные задачи;

e) требуемые ресурсы;

f) собственность (линии отчетности).

**Дополнительная информация**

Дополнительная специальная информация не требуется.

### 9.4 Создание условий для обеспечения надежного функционирования СМИБ

#### 9.4.1 План проверок, проводимых руководством

**Действия**

Необходимо разработать план, обеспечивающий участие руководства и выдачу поручений на проверку работы СМИБ и проводимых усовершенствований.

**Исходные данные:**

a) выходные данные действия 6.5, объединение всех областей действия и границ для получения области действия и границ — область действия и границы СМИБ;

b) выходные данные действия 6.6, разработка политики СМИБ и получение одобрения руководства — политика СМИБ;

c) выходные данные действия 8.4, получение санкции руководства на внедрение и использование СМИБ — декларация о применимости, включая цели, выбранные меры, средства контроля и управления;

d) выходные данные действия 9.2.3, разработка политики информационной безопасности;

e) ISO/IEC 27004:2009.

**Рекомендации**

Проверка руководством действия по внедрению СМИБ должна начинаться на самых ранних стадиях задания условий для СМИБ и составления описания случая применения СМИБ для данного предприятия и продолжаться вплоть до регулярных проверок операций СМИБ. Это непосредственное участие является средством подтверждения соответствия СМИБ потребностям предприятия и поддержания связи предприятия с СМИБ.

Планирование проверок, проводимых руководством, включает установление времени и способа проведения проверок. Подробная информация, касающаяся предварительных условий для проверок, проводимых руководством, содержится в подпункте 7.2 стандарта ISO/IEC 27001:2005.

Чтобы запланировать проверку, необходимо определить, какие должностные лица должны в ней участвовать. Назначенные должностные лица должны быть утверждены руководством и проинформированы об этом как можно раньше. Рекомендуется предоставлять руководству соответствующие данные, касающиеся необходимости и цели проведения процесса проверки (более подробную информацию о ролях и сферах ответственности см. в Приложении B).

Проверки, проводимые руководством, должны основываться на результатах измерений СМИБ и другой информации, накопленной за время использования СМИБ. Эта информация используется для выполнения действий руководством СМИБ для определения готовности и эффективности СМИБ. Требуемые исходные и выходные данные для измерений СМИБ приведены в ISO/IEC 27001:2005, а дополнительная информация по измерениям СМИБ — в Приложении E и ISO/IEC 27004:2009.

Также следует отметить, что эти проверки должны включать проверки методологии и результатов оценки риска. Проверки должны проводиться с запланированным интервалом с учетом изменения среды, например, организации и технологии.

Планирование внутреннего аудита СМИБ должно выполняться для того, чтобы иметь возможность регулярно оценивать СМИБ по мере ее внедрения. Результаты внутреннего аудита СМИБ являются важными исходными данными для проверок СМИБ, проводимых руководством. Следовательно, до проведения проверки руководством необходимо запланировать внутренний аудит. Внутренний аудит СМИБ должен включать проверку того, эффективно ли внедряются и сохраняются цели, меры и средства контроля и управления, процессы и процедуры СМИБ и соответствуют ли они:

a) требованиям ISO/IEC 27001:2005;

b) действующему законодательству и правилам;

c) определенным требованиям к информационной безопасности.

(Дополнительную информацию по планированию аудита см. в Приложении C).

Предварительным условием для проведения проверок руководством является информация, собранная на основе внедренной и используемой СМИБ. Информация, предоставляемая группе руководителей, проводящих проверку, может включать следующее:

a) отчеты об инцидентах за последний период использования системы;

b) подтверждение эффективности управления и обнаруженные несоответствия;

c) результаты других регулярных проверок (более подробные, если во время проверки были обнаружены несоответствия с политикой информационной безопасности);

d) рекомендации по усовершенствованию СМИБ.

В плане мониторинга должны документироваться его результаты, которые должны записываться и сообщаться руководству (дополнительную информацию по мониторингу см. в Приложении E).

**Выходные данные**

Выходные данные этого действия представляют собой документ, содержащий план, необходимый для организации проверок, проводимых руководством:

a) исходные данные, требуемые для проверки СМИБ руководством;

b) процедуры проверок, проводимых руководством и касающихся аспектов аудита, мониторинга и измерения.

**Дополнительная информация**

Приложение B — Роли и сферы ответственности в области информационной безопасности.

Приложение C — Информация по внутреннему аудиту.

Приложение E — Мониторинг и измерения.

**9.4.2 Разработка программы информирования, обучения и образования в области информационной безопасности**

**Действия**

Необходимо разработать программу информирования, обучения и образования в области информационной безопасности.

**Исходные данные:**

a) выходные данные действия 6.5, объединение всех областей действия и границ для получения области действия и границ — область действия и границы СМИБ;

b) выходные данные действия 6.6, разработка политики СМИБ и получение одобрения руководства — политика СМИБ;

c) выходные данные действия 7.2, определение требований к информационной безопасности для процесса СМИБ;

d) выходные данные действия 8.4, получение санкции руководства на внедрение и использование СМИБ — декларация о применимости, включая цели и выбранные меры и средства контроля и управления;

e) выходные данные действия 8.3, выбор целей и средств управления — План обработки риска;

f) выходные данные действия 9.2.3, разработка политики информационной безопасности;

g) выходные данные действия 9.2.4, разработка стандартов и процедур обеспечения информационной безопасности;

h) обзор общей программы образования и обучения в организации.

**Рекомендации**

Руководство отвечает за образование и обучение, чтобы сотрудники, назначенные на определенные должности, имели необходимые знания для выполнения требуемых операций. В идеале содержание программы образования и обучения должно помогать всем сотрудникам знать и понимать значение и важность операций по обеспечению информационной безопасности, в которых они участвуют, и то, как они могут способствовать достижению целей.

На этом этапе важно обеспечить, чтобы каждый работник в рамках области действия СМИБ получил необходимое обучение и (или) образование. В больших организациях одного набора материалов по обучению, как правило, недостаточно, поскольку он должен содержать слишком много данных, относящихся только к отдельным типам работ, и, следовательно, будет большим, сложным и трудным в использовании. В таких случаях обычно рекомендуется иметь разные наборы материалов по обучению, разработанных для разных групп ролей, например, офисных работников, обслуживающих работников или руководителей в области информационных технологий, которые обеспечивают конкретные нужды этих работников.

Программа обучения и образования с целью информирования по вопросам информационной безопасности должна обеспечивать составление записей по обучению и образованию в области информационной безопасности. Эти записи должны регулярно проверяться для обеспечения получения требуемого обучения всеми сотрудниками. Необходимо назначить должностное лицо, ответственное за этот процесс.

Материалы по обучению в области информационной безопасности должны быть разработаны таким образом, чтобы они были связаны с другими обучающими материалами, используемыми в организации, особенно учебные курсы для пользователей информационных систем. Обучение по существенным аспектам информационной безопасности в идеале должно включаться в каждый учебный курс для пользователей информационных технологий.

Обучающие материалы по информационной безопасности должны включать как минимум следующие пункты в зависимости от целевой аудитории:

a) риски и угрозы, связанные с информационной безопасностью;

b) основные термины по информационной безопасности;

c) четкое определение инцидента безопасности: рекомендации по обнаружению инцидента, его устранению и отчетности;

d) политики информационной безопасности, стандарты и процедуры организации;

e) сферы ответственности и каналы отчетности, связанные с информационной безопасностью в организации;

f) рекомендации по оказанию помощи в повышении информационной безопасности;

g) рекомендации, связанные с нарушениями информационной безопасности и отчетностью;

h) где получить дополнительную информацию.

Необходимо определить группу по обучению информационной безопасности, которая может выполнять следующие задачи:

a) создание и управление записями по информационной безопасности;

b) составление и управление материалами по обучению;

c) проведение обучения.

Эти задачи могут ставиться с учетом использования существующего обучающего персонала. Но для существующего персонала может потребоваться обучение концепциям информационной безопасности, чтобы обеспечить их эффективное и точное представление.

Программа информирования, образования и обучения в области информационной безопасности должна включать процедуру, обеспечивающую регулярную проверку и обновление обучающих материалов. Для проверки и обновления обучающих материалов можно назначить специальное должностное лицо.

**Выходные данные**

Выходные данные этого действия следующие:

a) материалы по информированию, обучению и образованию в области информационной безопасности;

b) формирование программ информирования, образования и обучения в области информационной безопасности, включая роли и сферы ответственности;

c) планы информирования, образования и обучения в области информационной безопасности;

d) актуальные записи, показывающие результаты информирования, образования и обучения работников в области информационной безопасности.

**Дополнительная информация**

Дополнительная специальная информация не требуется.

### 9.5 Составление окончательного плана проекта СМИБ

**Действия**

Необходимо составить конечный план проекта СМИБ, включая действия, необходимые для внедрения выбранных средств управления.

**Исходные данные:**

a) выходные данные действия 6.5, объединение всех областей действия и границ для получения области действия и границ — область действия и границы СМИБ;

b) выходные данные действия 6.6, разработка политики СМИБ и получение одобрения руководства — политика СМИБ;

c) выходные данные действия 9.2 — разработка информационной безопасности организации;

d) выходные данные действия 9.3 — разработка информационной безопасности ИКТ и физических объектов;

e) выходные данные действия 9.4 — разработка информационной безопасности, связанной с СМИБ;

f) ISO/IEC 27002:2005.

**Рекомендации**

Действия, требуемые для внедрения выбранных средств управления и выполнения других действий, связанных с СМИБ, должны быть оформлены в виде подробного плана внедрения как части конечного проекта СМИБ. Подробный план внедрения системы также может подкрепляться описаниями предложенных инструментов и методов внедрения. Поскольку проект СМИБ включает множество различных ролей в организации, важно, чтобы действия были четко определены для ответственных сторон и план был распространен на ранних стадиях проекта во всей организации.

В отношении других проектов необходимо, чтобы лицо, ответственное за проект, обеспечило выделение достаточных ресурсов для проекта.

**Выходные данные**

Выходные данные этого действия представляют собой конечный план проекта внедрения СМИБ.

**Дополнительная информация**

Дополнительная специальная информация не требуется.

**Приложение А**
**(справочное)**

## Описание контрольного перечня

Цель:

- представить контрольную таблицу с описанием действий, требуемых для учреждения и внедрения СМИБ;
- способствовать мониторингу процесса выполнения работ по внедрению СМИБ;
- связать определенные действия по внедрению СМИБ с соответствующими требованиями ISO/IEC 27001.

Таблица А.1

| Фаза внедрения ISO/IEC 27003 | Номер этапа | Действия, ссылка на ISO/IEC 27003 | Предварительные условия для данного этапа | Документированные выходные данные | Ссылка на ISO/IEC 27001 |
|---|---|---|---|---|---|
| 5 Получение одобрения руководства для внедрения СМИБ | 1 | Собрать корпоративные цели предприятия | Нет | Список корпоративных целей предприятия | Не применяется |
| | 2 | Приобретение знаний о существующих системах управления | Нет | Описание существующих систем управления | Не применяется |
| | 3 | 5.2 Определить цели, потребности информационной безопасности и требования предприятия к СМИБ | 1, 2 | Описание целей, потребностей информационной безопасности и требований предприятия к СМИБ | Не применяется |
| | 4 | Собрать соответствующие регулятивные стандарты, стандарты соответствия и отраслевые стандарты, применяемые к корпорации | Нет | Описание регулятивных стандартов, стандартов соответствия и отраслевых стандартов, применяемых к корпорации | Не применяется |
| | 5 | 5.3 Определить предварительную область действия СМИБ | 3, 4 | Описание предварительной области действия СМИБ (5.3.1) Определение ролей и сфер ответственности в области СМИБ (5.3.2) | Не применяется |
| | 6 | 5.4 Составить описание случая применения СМИБ для данного предприятия и план проекта для утверждения руководством | 5 | Описание случая применения СМИБ для данного предприятия и план проекта | Не применяется |
| | 7 | 5.5 Получить одобрение руководства и поручение на запуск проекта внедрения СМИБ | 6 | Одобрение руководством запуска проекта внедрения СМИБ | Не применяется |

*Продолжение таблицы А.1*

| Фаза внедрения ISO/IEC 27003 | Номер этапа | Действия, ссылка на ISO/IEC 27003 | Предварительные условия для данного этапа | Документированные выходные данные | Ссылка на ISO/IEC 27001 |
|---|---|---|---|---|---|
| 6 Определение области действия и политики СМИБ | 8 | 6.2 Определить границы организации | 7 | Описание границ организации;<br>Функции и структура организации;<br>Обмен информацией через границы;<br>Производственные процессы и сферы ответственности за информационные активы в области действия СМИБ и за ее пределами | 4.2.1,a) (частично) |
| | 9 | 6.3 Определение границ технологии передачи информации | 7 | Описание границ ИКТ<br>Описание информационных систем и телекоммуникационных сетей, описывающее системы и сети внутри области действия СМИБ и за ее пределами | 4.2.1,a) (частично) |
| | 10 | 6.4 Определение физических границ | 7 | Описание физических границ СМИБ<br>Описание организации и ее географических характеристик, описывающее внутреннюю и внешнюю области действия | 4.2.1,a) (частично) |
| | 11 | 6.5 Окончательно определить границы области действия СМИБ | 8, 9, 10 | Документ, описывающий область действия и границы СМИБ | 4.2.1,a) |
| | 12 | 6.6 Разработка политики СМИБ | 11 | Утвержденная руководством политика СМИБ | 4.2.1,b) |
| 7 Проведение анализа организации | 13 | 7.2 Определение требований к информационной безопасности, подкрепляющих СМИБ | 12 | Список основных процессов, функций, объектов, информационных систем, коммуникационных сетей | Не применяется |
| | | | | Требования организации, касающиеся конфиденциальности, доступности и целостности | Не применяется |
| | | | | Требования организации, касающиеся законных, обязательных, контрактных и отраслевых требований к информационной безопасности | 4.2.1,c) 1) (частично) |
| | | | | Перечень известных уязвимостей в организации | 4.2.1,d) 3) |

*Продолжение таблицы А.1*

| Фаза внедрения ISO/IEC 27003 | Номер этапа | Действия, ссылка на ISO/IEC 27003 | Предварительные условия для данного этапа | Документированные выходные данные | Ссылка на ISO/IEC 27001 |
|---|---|---|---|---|---|
| | 14 | 7.3 Определение активов в рамках области действия СМИБ | 13 | Описание основных процессов в организации | Не применяется |
| | | | | Определение информационных активов основных процессов в организации | 4.2.1,d) 1) |
| | | | | Классификация важнейших процессов (активов) | Не применяется |
| | 15 | 7.4 Запуск оценки информационной безопасности | 14 | Документ по фактическому состоянию и оценке информационной безопасности в организации, включая существующие меры и средства контроля и управления информационной безопасностью | 4.2.1,e) 2) (частично) |
| 8 Проведение оценки риска и выбор вариантов обработки риска | 16 | 8.2 Проведение оценки риска | 15 | Область действия для оценки риска<br>Утвержденная методология оценки риска, совмещенная с контекстом стратегического менеджмента риска в организации<br>Критерии принятия риска | 4.2.1,c) 1) |
| | 17 | 8.3 Выбор целей и средств управления | 16 | Документированная оценка риска высокого уровня | 4.2.1,e) 3) (частично) |
| | | | | Определение необходимости дополнительной глубокой оценки риска | Не применяется |
| | | | | Документированная глубокая оценка риска | 4.2.1,e) 3) (частично) |
| | | | | Сгруппированные результаты оценки риска | Не применяется |
| | 18 | 8.4 Получить одобрение руководства для внедрения СМИБ | 17 | Риски и определенные для них варианты оценки риска | 4.2.1,f) |
| | | | | Выбранные цели, меры и средства контроля и управления для снижения риска | 4.2.1,g) |

*Продолжение таблицы А.1*

| Фаза внедрения ISO/IEC 27003 | Номер этапа | Действия, ссылка на ISO/IEC 27003 | Предварительные условия для данного этапа | Документированные выходные данные | Ссылка на ISO/IEC 27001 |
|---|---|---|---|---|---|
| | 19 | Утверждение руководством остаточных рисков | 18 | Документированное утверждение руководством предложенных остаточных рисков (должно входить в число выходных данных действия 8.4) | 4.2.1,h) |
| | 20 | Санкция руководства на внедрение и использование СМИБ | 19 | Документированная санкция руководства на внедрение и использование СМИБ (должно входить в число выходных данных действия 8.4) | 4.2.1,i) |
| | 21 | Подготовка декларации о применимости | 18 | Декларация о применимости | 4.2.1,j) |
| 9 Разработка СМИБ | 22 | 9.2 Разработка безопасности организации | 20 | Структура организации, связанная с ролями и сферами ответственности, связанными с информационной безопасностью | 5.1,c) |
| | | | | Определение документации, связанной со СМИБ. Шаблоны записей по СМИБ и инструкции по их использованию и хранению | 4.3 |
| | | | | Документ по политике информационной безопасности | ISO/IEC 27002; 5.1.1 |
| | | | | Основа политики и процедур обеспечения информационной безопасности (и планы разработки конкретных политики, процедур и т. д., если таковые применяются) | |
| | 23 | 9.3 Разработка информационной безопасности ИКТ и физических объектов | 20, 21 | Планы проектов внедрения для процессов внедрения выбранных средств управления безопасностью, связанных с информационной безопасностью ИКТ и физических объектов | 4.2.2,c) (частично) |

*Окончание таблицы А.1*

| Фаза внедрения ISO/IEC 27003 | Номер этапа | Действия, ссылка на ISO/IEC 27003 | Предварительные условия для данного этапа | Документированные выходные данные | Ссылка на ISO/IEC 27001 |
|---|---|---|---|---|---|
| | 24 | 9.4 Разработка информационной безопасности, связанной со СМИБ | 22, 23 | Процедуры, описывающие процессы отчетности и проверки, проводимой руководством | 7.1 |
| | 25 | | | Описания аудита, мониторинга и измерения | 4.2.3, a) (частично); 4.2.3, b) (частично); 6 |
| | 26 | | | Программа обучения и информирования | 5.2.2 |
| | 27 | 9.5 Составление окончательного плана проекта СМИБ | 25 | План проекта внедрение для процессов внедрения, утвержденный руководством | Не применяется |
| | 28 | Окончательный план проекта СМИБ | 28 | План проекта внедрения СМИБ организацией, охватывающий запланированное выполнение действий по информационной ее безопасности, ИКТ и физических объектов, а также связанные с системой СМИБ требования по ее внедрению в соответствии с результатами действий, описываемых в ISO/IEC 27003 | Не применяется |

**Приложение В**
**(справочное)**

## Роли и сферы ответственности в области информационной безопасности

Данное приложение содержит дополнительные рекомендации по ролям и сферам ответственности в организации, связанным с информационной безопасностью. Роли сначала указаны с точки зрения организации для внедрения СМИБ. В таблице В.1 изложена эта информация и представлены общие примеры ролей и сфер ответственности.

1. Роль комитета по информационной безопасности

Комитет по информационной безопасности должен играть ведущую роль в СМИБ в организации. Комитет по информационной безопасности должен отвечать за управление информационными активами организации и обладать достаточным пониманием информационной безопасности в отношении управления, мониторинга и выполнения необходимых задач.

Далее приведены примеры возможных ролей комитета по информационной безопасности:

a) управление рисками, составление плана работы с документами по СМИБ, ответственность за определение содержания этих документов и получение одобрения руководства;

b) планирование приобретения нового оборудования и (или) принятие решений о повторном использовании существующего оборудования, которым уже располагает организация;

c) решение любых проблем при их возникновении;

d) рассмотрение усовершенствований, которые могут быть достигнуты в результате дальнейшего внедрения и измерения СМИБ;

e) стратегическое управление СМИБ (при выполнении проекта внедрения и использовании системы);

f) обеспечение связи между высшим руководством, группой по внедрению проекта и работниками, занятыми в сфере информационной безопасности.

2. Роли группы по планированию информационной безопасности

Проектная группа, ответственная за СМИБ при планировании проекта, должна получать поддержку от членов, хорошо понимающих важные информационные активы в рамках области действия СМИБ и обладающих достаточными знаниями, чтобы обсуждать, как распорядиться этой информацией. Например, при определении того, как распорядиться информационными активами, могут иметь место разные мнения среди подразделений, находящихся в области действия СМИБ, поэтому может возникнуть необходимость согласовать положительные и отрицательные последствия выполнения плана. Проектная группа должна координировать противоречия, возникающие между разными подразделениями. Для этого членам группы потребуются навыки общения, накопленные по опыту работы, и возможности координации, а также высокий уровень знаний в области безопасности.

3. Специалисты и внешние консультанты

Организации необходимо выбрать сотрудников для выполнения вышеуказанных задач (желательно сотрудников с одной исключительной ролью), прежде чем учредить СМИБ. Однако этим сотрудникам потребуются обширные знания и опыт в области информационной безопасности, например «ИТ», «управленческих решений» и «понимания организации». Лица, ответственные за выполнение данных операций в организации, могут лучше знать свои специфические сферы деятельности. Многие специалисты, являющиеся экспертами в отдельных областях в своей организации, должны привлекаться к работе над СМИБ, если она имеет отношение к использованию системы в их областях деятельности. Также важен баланс их профессиональных и обширных знаний, необходимых для того, чтобы достичь целей организации. Внешние консультанты могут давать рекомендации на основе своих макроскопических точек зрения на организацию и опыта действий в подобных случаях, даже несмотря на то, что они не обязательно обладают глубокими знаниями специфики организации и знают подробности ее работы. Термины, используемые в вышеприведенных примерах, например, "комитет по информационной безопасности" и "группа по планированию информационной безопасности", не так важны. Необходимо понимать только функцию каждой структуры.

В идеальном варианте это должны быть внутренние структуры, координирующие информационную безопасность организации, поддерживающие связь и работающие в тесном сотрудничестве с каждым техническим отделом.

4. Владельцы информационных активов

Необходимо назначить сотрудника для каждого процесса в организации и области применения специальных знаний; этот сотрудник действует в качестве так называемого «владельца информационного актива» по всем вопросам информационной безопасности, связанным с обработкой данных в рамках конкретного процесса в организации. Контактное лицо или владелец процесса отвечает, например, за постановку задач и обработку информации в рамках процессов в организации, для которых они назначены.

В случае распределения риска, предотвращения риска и удержания риска должны быть приняты необходимые действия с точки зрения безопасности организации. Если было принято решение о переносе рисков, необходимо предпринять соответствующие действия с использованием контрактов, гарантий и структуры организации, например партнерства или совместных предприятий.

На рисунке В.1 показан пример структуры организации для учреждения СМИБ. Основные роли и сферы ответственности в организации, приведенные ниже, основаны на этом примере.

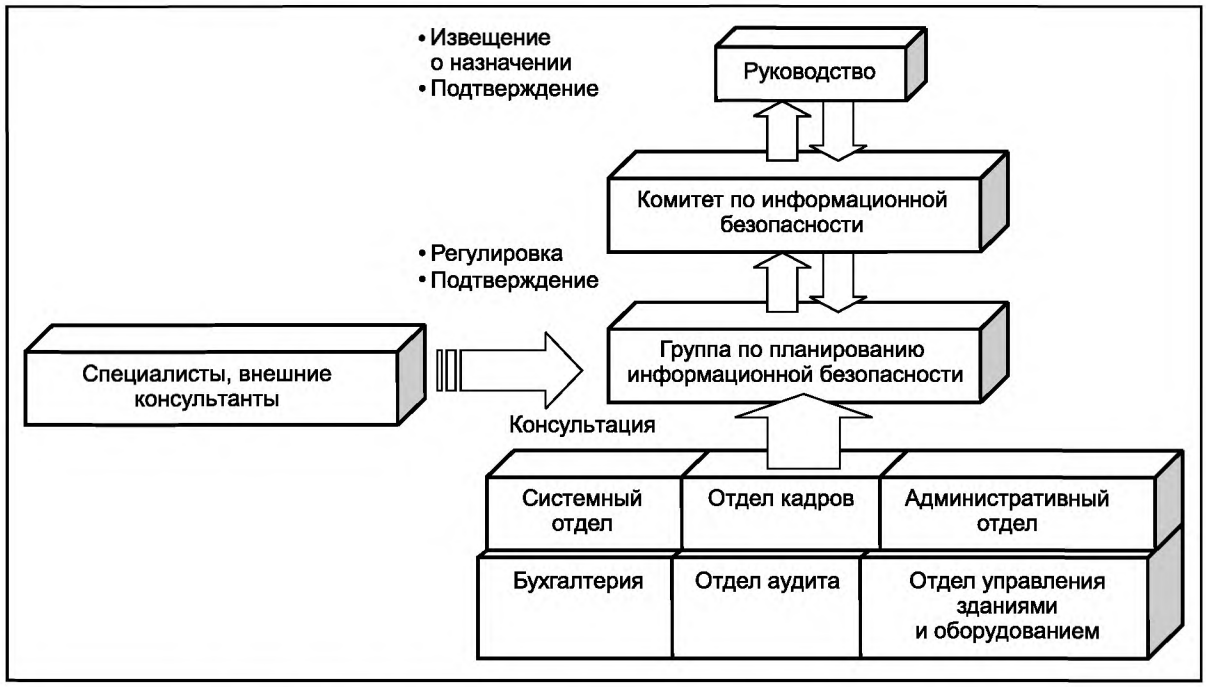



Рисунок В.1 — Пример структуры организации для учреждения СМИБ

**Взаимодействие в рамках организации**

Все вовлеченные стороны должны изучить и очень хорошо знать существующие требования по защите активов организации. Участвовать в анализе организации должны сотрудники, обладающие хорошим знанием организации и среды, в которой она функционирует. Эти сотрудники должны быть выбраны таким образом, чтобы представлять широкий круг работников организации и должны включать:

a) высшее руководство (например, главный управляющий и финансовый директор);

b) членов комитета по информационной безопасности;

c) членов группы по планированию информационной безопасности;

d) линейных руководителей (например, руководителей подразделений организации);

e) владельцев процессов (т. е. представителей важных оперативных подразделений);

f) специалистов и внешних консультантов.

Примеры общих ролей и сфер ответственности, связанных с информационной безопасностью

Информационная безопасность является обширной областью, влияющей на всю организацию. По существу четко определенные сферы ответственности в области информационной безопасности являются важными для успешного внедрения СМИБ. Поскольку роли и сферы ответственности, связанные с информационной безопасностью, могут различаться, понимание различных ролей является крайне важным для понимания некоторых действий, описываемых далее в настоящем стандарте. В таблице ниже изложены роли и сферы ответственности, связанные с безопасностью. Следует отметить, что эти роли являются общими, и для каждого отдельного случая внедрения СМИБ требуются конкретные описания.

Таблица В.1 — Перечень примерных ролей и сфер ответственности, связанных с информационной безопасностью

| Роль | Краткое описание сферы ответственности |
|---|---|
| Высшее руководство (например, главный управляющий, исполнительный директор, директор по безопасности и финансовый директор) | Отвечает за видение СМИБ, стратегические решения и координирует действия по управлению и контролю организации |
| Линейные руководители | Несут высшую ответственность за функции организации |

*Продолжение таблицы В.1*

| Роль | Краткое описание сферы ответственности |
|---|---|
| Директор по информационной безопасности | Несет полную ответственность и осуществляет руководство информационной безопасностью, обеспечивая правильное управление информационными активами |
| Комитет по информационной безопасности (члены) | Осуществляют управление информационными активами и играют ведущую роль в работе СМИБ в организации |
| Группа по планированию информационной безопасности (члены) | Работает во время операций, пока учреждается СМИБ. Группа по планированию работает со всеми подразделениями и разрешает противоречия, пока учреждается СМИБ |
| Заинтересованная сторона | В контексте описаний других ролей, связанных с информационной безопасностью, в данном документе заинтересованные стороны определяются, главным образом, как лица организации, не связанные с обычной работой организации — например, совет, собственники (организации-собственники, если организация является частью группы или правительственной организации и (или) непосредственные собственники, например, акционеры в частной организации). Другими примерами заинтересованных сторон могут служить дочерние компании, клиенты, поставщики или более публичные организации, такие как правительственные органы финансового контроля или соответствующие фондовые биржи, если указана организация |
| Системный администратор | Системный администратор отвечает за систему информационных технологий |
| Управляющие по информационным технологиям | Управляющий всеми информационными ресурсами (например, начальник отдела информационных технологий) |
| Безопасность физических объектов | Лицо, ответственное за безопасность физических объектов, например, зданий и т. д., часто называемый руководителем объекта |
| Управление рисками | Лицо (лица), ответственные за структуру управления рисками в организации, включая оценку, обработку и мониторинг риска |
| Юрисконсульт | Многие риски для информационной безопасности имеют юридические аспекты, и юрисконсульт отвечает за их учет |
| Кадры | Лицо (лица), несущее(ие) полную ответственность за эти разработки |
| Архив | Все организации имеют архивы, содержащие важную информацию, которую необходимо хранить в течение длительного времени. Информация может находиться на разных типах носителей, и необходим специальный сотрудник, отвечающий за ее хранение |
| Персональные данные | Если того требуют государственные законы, может быть назначен сотрудник, отвечающий за связь с органом контроля данных или аналогичной официальной организацией, осуществляющей контроль защиты персональных данных и прав собственности |
| Разработчик систем | Если организация разрабатывает собственные информационные системы, кто-то должен отвечать за эти разработки |

*Окончание таблицы В.1*

| Роль | Краткое описание сферы ответственности |
|---|---|
| Специалист/эксперт | Специалисты и эксперты, отвечающие за некоторые операции в организации, должны привлекаться к работам по СМИБ по мере возникновения проблем, относящихся к их компетенции |
| Внешний консультант | Внешние консультанты могут предоставлять консультации на основе их макроскопического видения организации и опыта работы в данной отрасли. Однако консультанты могут не располагать глубокими знаниями организации и ее работы |
| Работник/персонал/пользователь | Каждый работник несет равную ответственность за поддержание информационной безопасности на рабочем месте и в своем окружении |
| Аудитор | Аудитор отвечает за оценку СМИБ |
| Инструктор | Инструктор реализует программы обучения и информирования |
| Ответственный за информационные технологии или информационную безопасность на месте | В крупных организациях часто назначаются сотрудники на местах, ответственные за вопросы информационных технологий на месте, и, возможно, также за информационную безопасность |
| Независимый эксперт | Это по существу не ответственное лицо, но в крупных организациях может быть очень полезным на стадии внедрения системы. Желательно иметь людей, обладающих глубокими знаниями в области внедрения СМИБ, которые могут поддерживать понимание и доводы в пользу применения СМИБ. Они могут положительно влиять на мнение участников работ по внедрению СМИБ и часто называются «посредниками» |

**Приложение С**
**(справочное)**

## Информация по внутреннему аудиту

В данном приложении содержатся дополнительные рекомендации по планированию аудита.

Внедрение СМИБ должно оцениваться с постоянным интервалом путем внутреннего и независимого аудита. Аудит также служит для упорядочения и оценки опыта, накапливаемого в ходе повседневной практики. Для внедрения СМИБ необходимо планировать формы аудита.

При аудите СМИБ результаты аудита должны определяться на основе конкретных признаков. Следовательно, необходимо назначать подходящие периоды времени для выполнения операций, связанных со СМИБ для сбора необходимых доказательств.

Внутренний аудит СМИБ должен внедряться и осуществляться регулярно для оценки того, соответствуют ли цели и меры и средства контроля и управления, процессы и процедуры СМИБ требованиям ISO/IEC 27001 и соответствующим законам или нормам, соответствуют ли они определенным требованиям к информационной безопасности, и эффективно ли они внедряются и поддерживаются.

Однако выбор аудиторов для внутреннего аудита СМИБ может оказаться сложным для небольших компаний. Если у организации недостаточно ресурсов для проведения таких видов аудита, выполняемых опытными сотрудниками организации, следует привлекать для выполнения аудита внешних экспертов. Когда организация привлекает внешних аудиторов, следует принять во внимание следующее: внешние аудиторы хорошо знакомы с процедурой внутреннего аудита СМИБ, однако не обладают достаточными знаниями об организационной среде организации. Эта информация должна быть им предоставлена сотрудниками организации. С другой стороны, внутренние аудиторы могут иметь возможность проводить подробный аудит, принимая по внимание организационную среду организации, но могут не обладать достаточными знаниями о выполнении аудита СМИБ. Организации должны учитывать характеристики и потенциальные недостатки внутреннего аудита по сравнению с внешним при проведении внутреннего аудита СМИБ.

Эффективность и результативность применяемых средств управления (см. ISO/IEC 27004:2009) следует проверять в рамках внутреннего аудита.

Важно отметить, что аудит не проводится сотрудниками, которые были заняты в планировании и разработке целей безопасности, поскольку сложно найти свои собственные ошибки. Следовательно, в качестве аудиторов руководство должно привлекать подразделения организации или сотрудников, находящихся вне области действия внутреннего аудита СМИБ. Эти аудиторы должны планировать и проводить внутренний аудит СМИБ и составлять отчеты для получения дальнейших распоряжений руководства. В зависимости от размера организации может быть полезным отзыв внешних аудиторов, чтобы избежать ситуации, в которой сотрудники ограничены в своей работе.

При проведении внутреннего аудита СМИБ следует проверить, чтобы система эффективно работала, поддерживалась и оправдывала все ожидания. При планировании программы аудита аудиторы должны учитывать состояние и важность целей руководства, средств управления, процессов и процедур, подлежащих аудиту, а также результаты предыдущего аудита.

При проведении аудита необходимо документировать критерии, применяемую область действия, частоту проведения и метод аудита.

При выборе аудиторов необходимо обеспечить объективность и честность процесса аудита. При проведении серии процессов аудита аудиторы должны быть компетентны в следующих областях:

a) планирование и проведение аудита;

b) отчетность по результатам;

c) предложение корректирующих и предупреждающих действий и т. д.

Кроме того, организация должна определить сферы ответственности аудиторов и серию процессов аудита в процедурной документации.

Руководитель, отвечающий за процесс, подвергаемый аудиту, должен обеспечить, чтобы несоответствия и их причины должным образом устранялись без задержки. Однако это не означает, что несоответствие обязательно нужно устранить немедленно. Кроме того, выполняемые корректирующие действия должны включать проверку выполняемого действия и отчет по результатам проверки.

С точки зрения управления внутренний аудит СМИБ может проводиться эффективно, как часть других видов внутреннего аудита организации или в сочетании с ними. При проведении аудита следует обращаться к документу «Требования к организациям, проводящим аудит и сертификацию СМИБ ISO/IEC 27006:2007».

**Приложение D**
**(справочное)**

## Структура политики

В данном приложении содержатся дополнительные рекомендации по структуре политики, включая политику информационной безопасности.

Политика — это общие намерения и указания, официально выраженные руководством (см. FCD 27000 и ISO/IEC 27002). Содержание политики управляет действиями и решениями, касающимися предмета политики. Организация может иметь несколько политик, по одной для каждой сферы деятельности, важной для организации. Некоторые политики независимы одна от другой, в то время как другие политики находятся в иерархическом соотношении. В области безопасности политики, как правило, иерархически организованы. Обычно политика безопасности организации является политикой высшего уровня. Она подкрепляется более конкретными политиками, включая политику информационной безопасности и политику системы менеджмента информационной безопасности. В свою очередь, политика информационной безопасности может подкрепляться более детальными политиками по конкретным предметам, относящимся к аспектам информационной безопасности. Многие из этих политик описываются в стандарте ISO/IEC 27002, например, политика информационной безопасности подкрепляется политиками, касающимися контроля доступа, политики «чистого стола» и «чистого экрана», использования сетевых служб и криптографического контроля. В некоторых случаях возможно включение дополнительных уровней политики. Эта классификация показана на рисунке D1.

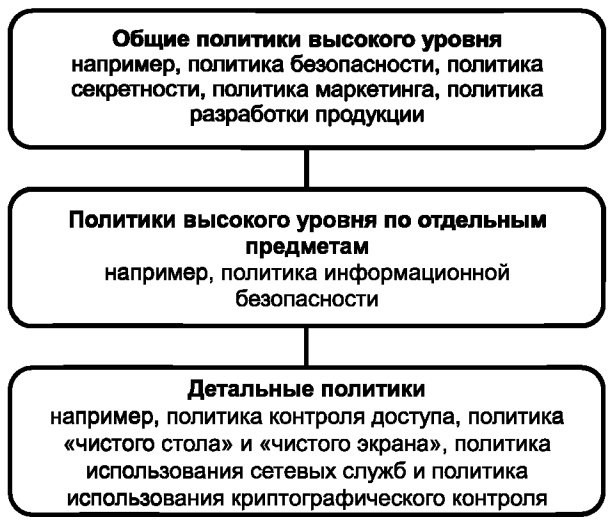



Рисунок D.1 — Иерархия политики

Согласно стандарту ISO/IEC 27001 требуется, чтобы организации имели политику СМИБ и политику информационной безопасности. Однако это не подразумевает каких-либо конкретных соотношений между этими политиками. Требования к политике СМИБ приведены в пункте 4.2.1 стандарта ISO/IEC 27001. Рекомендации по политике информационной безопасности приведены в пункте 5.1.1 стандарта ISO/IEC 27002. Эти политики могут разрабатываться как равноправные политики: политика СМИБ может подчиняться политике информационной безопасности, или, наоборот, политика информационной безопасности может подчиняться политике СМИБ.

Содержание политики основано на контексте, в котором работает организация. В частности, при разработке любой политики в рамках основ политики нужно учитывать следующее:

1) цели и задачи организации;
2) стратегии, адаптированные для достижения этих целей;
3) структуру и процессы, адаптированные организацией;
4) цели и задачи, связанные с предметом политики;
5) требования связанных политик более высокого уровня.

Этот процесс показан на рисунке D.2.

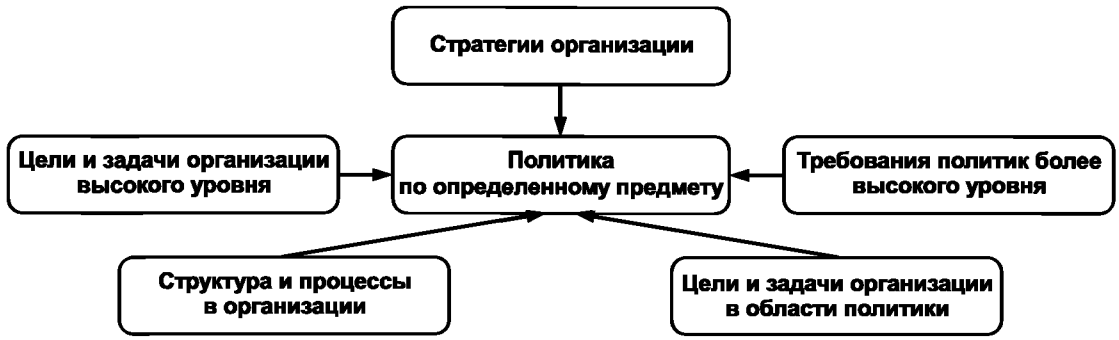



Рисунок D.2 — Исходные данные для разработки политики

Политики могут иметь следующую структуру:

1. Краткое изложение политики — общее описание из одного-двух предложений. (Иногда может объединяться с введением).

2. Введение — краткое объяснение предмета политики.

3. Область действия — описывает части или действия организации, находящиеся под влиянием политики. При необходимости в пункте «Область действия» перечисляются другие политики, подкрепляемые данной политикой.

4. Цели — описание назначения политики.

5. Принципы — описание правил, касающихся действий и решений для достижения целей. В некоторых случаях может быть полезным определить ключевые процессы, связанные с предметом политики, и затем — правила выполнения процессов.

6. Сферы ответственности — кто отвечает за действия по выполнению требований политики. В некоторых случаях этот пункт может содержать описание организационных соглашений, а также сферы ответственности лиц с определенными ролями.

7. Ключевые результаты — описание результатов, получаемых предприятием, если цели достигнуты.

8. Связанные политики — описание других политик, относящихся к достижению целей, обычно с представлением дополнительных подробностей, касающихся отдельных предметов.

Примечание — Содержание политики может быть организовано различными способами. Например, организации, которые делают акцент на ролях и сферах ответственности, могут упростить описание целей и применять принципы конкретно к ролям и сферам ответственности.

Далее приведен пример политики информационной безопасности, показывающий ее структуру и пример содержания.

**Политика информационной безопасности (пример)**

*Краткое изложение политики*

Информация всегда должна быть защищена независимо от ее формы и способа ее распространения, передачи и хранения.

Введение

Информация может существовать во многих различных формах. Она может быть напечатана или написана на бумаге, храниться в электронном виде, передаваться по почте или с использованием электронных устройств, показываться на пленках или передаваться устно в процессе общения.

Информационная безопасность — это защита информации от различных угроз, призванная обеспечить непрерывность бизнес-процессов, минимизировать риск для бизнеса и максимизировать возвращение вложений и обеспечить возможности деловой деятельности.

Область действия

Данная политика подкрепляет общую политику безопасности организации.

Данная политика применяется ко всем сотрудникам организации.

Цели информационной безопасности

1) Понимание и обработка стратегических и оперативных рисков для информационной безопасности, чтобы они были приемлемы для организации.

2) Защита конфиденциальности информации клиентов, разработок продукции и планов маркетинга.

3) Сохранение целостности материалов бухгалтерского учета.

4) Соответствие общих веб-сервисов и внутренних сетей соответствующим стандартам доступности.

Принципы информационной безопасности

1) Данная организация способствует принятию рисков и преодолевает риски, которые не могут преодолеть организации с консервативным управлением, при условии понимания, мониторинга и обработки рисков для

информации при необходимости. Подробное описание подходов, применяемых для оценки и обработки рисков, можно найти в политике СМИБ.

2) Весь персонал должен быть осведомлен и подотчетен за информационную безопасность в отношении своих должностных обязанностей.

3) Необходимо принять меры для финансирования средств управления информационной безопасностью и процессов управления проектами.

4) Возможности мошенничества и злоупотреблений в области информационных систем должны быть приняты в расчет при общем управлении информационными системами.

5) Отчеты о состоянии информационной безопасности должны быть доступны.

6) Необходимо отслеживать риски для информационной безопасности и предпринимать действия, когда изменения приводят к возникновению непредвиденных рисков.

7) Критерии классификации рисков и приемлемости рисков можно найти в политике СМИБ.

8) Ситуации, которые могут привести организацию к нарушению законов и установленных норм, не должны допускаться.

Сферы ответственности

1) Группа руководителей высшего звена отвечает за обеспечение соответствующей проработки информации во всей организации.

2) Каждый руководитель высшего звена отвечает за то, чтобы сотрудники, работающие под его руководством, осуществляли защиту информации в соответствии со стандартами организации.

3) Начальник отдела безопасности консультирует группу руководителей высшего звена, оказывает экспертную помощь сотрудникам организации и обеспечивает доступность отчетов о состоянии информационной безопасности.

4) Каждый сотрудник организации отвечает за информационную безопасность как часть выполнения своих должностных обязанностей.

Ключевые результаты

1) Инциденты информационной безопасности не должны приводить к серьезным непредвиденным затратам или серьезным срывам работы служб и деятельности предприятия.

2) Потери из-за мошенничества должны быть известны и находиться в рамках приемлемых ограничений.

3) Вопросы информационной безопасности не должны оказывать неблагоприятного влияния на прием заказчиками продукции и услуг.

Связанные политики

Следующие детальные политики содержат принципы и рекомендации по отдельным аспектам информационной безопасности:

1) Политика системы менеджмента информационной безопасности (СМИБ);
2) Политика контроля доступа;
3) Политика «чистого стола» и «чистого экрана»;
4) Политика неразрешенного программного обеспечения;
5) Политика, касающаяся получения файлов программного обеспечения из внешних сетей или через них;
6) Политика, касающаяся мобильного кода;
7) Политика резервного копирования;
8) Политика, касающаяся обмена информацией между организациями;
9) Политика, касающаяся допустимого использования электронных средств связи;
10) Политика сохранения записей;
11) Политика использования сетевых служб;
12) Политика, касающаяся мобильных вычислений и связи;
13) Политика дистанционной работы;
14) Политика использования криптографического контроля;
15) Политика соответствия;
16) Политика лицензирования программного обеспечения;
17) Политика удаления программного обеспечения;
18) Политика защиты и секретности данных.

Все эти политики подкрепляют:

- идентификацию риска путем предоставления основы средств управления, которые могут использоваться для обнаружения недостатков в проектировании и внедрении систем;

- обработку риска путем оказания помощи в определении способов обработки для определенных уязвимостей и угроз.

Идентификация риска и обработка риска — это процессы, определенные в разделе политики «Принципы». Подробности см. в политике СМИБ.

**Приложение Е**
**(справочное)**

## Мониторинг и измерения

В данном приложении представлены дополнительные рекомендации по поддержке планирования и разработки мониторинга и измерений.

Информация о назначении мониторинга и измерений

Разработка особых требований к СМИБ включает программу мониторинга и измерения безопасности для СМИБ, поддерживающую проверки, осуществляемые руководством.

Разработка мониторинга

На рисунке Е.1 представлена последовательность процесса мониторинга.

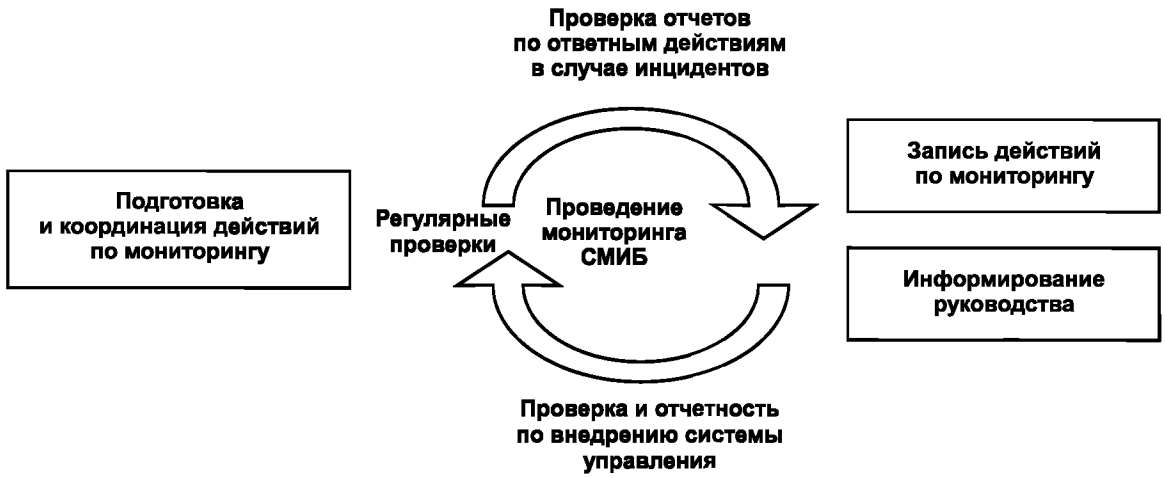



Рисунок Е.1 — Последовательность процесса мониторинга

Подготовка и координация: Определение соответствующих активов для мониторинга

Следует отметить, что мониторинг является непрерывным процессом, и при его разработке следует учитывать наладку процесса мониторинга, а также разработку фактических потребностей и действий по мониторингу. Эти действия необходимо координировать, что является частью процесса разработки.

На основе предыдущей информации, установленной на основе определенной области действия и активов, в сочетании с результатами анализа риска и выбора средств управления можно определить цели мониторинга. Эти цели должны включать:

- что нужно определить;
- когда;
- против чего.

С практической точки зрения ранее установленные действия (процессы) в организации и связанные с ними активы являются основной областью действия для мониторинга (пункт «против чего» выше). Для разработки мониторинга может потребоваться выбор, чтобы охватить активы, важные с точки зрения информационной безопасности. Также следует принять во внимание обработку риска и выбор средств управления, чтобы определить, что нужно отслеживать в активах и связанных с ними действиях (процессах) в организации. (При этом устанавливаются пункты «что нужно определить» и «когда»).

Поскольку мониторинг может включать юридические аспекты, разработку мониторинга необходимо проверять, чтобы он не имел юридических последствий.

Для обеспечения реальной эффективности мониторинга важно координировать и проводить конечную разработку всех действий по мониторингу.

Действия по мониторингу

Для поддержания уровня информационной безопасности меры и средства контроля и управления информационной безопасностью, определенные как подходящие, должны правильно применяться; обнаружение инцидентов безопасности и реагирование на них должны производиться своевременно, а функционирование системы менеджмента информационной безопасности должно регулярно отслеживаться. Необходимо проводить регулярные проверки, чтобы определить, все ли меры и средства контроля и управления применяются и внедряются, как запланировано в концепции информационной безопасности. В число этих проверок должны входить

проверки соответствия технических средств управления (например, в отношении конфигурации) и организационных средств управления (например, процессов, процедур и операций). Проверки, прежде всего, должны быть направлены на устранение недостатков. Если проверки подлежат принятию, важно, чтобы эта мотивация осознавалась всеми вовлеченными сотрудниками как цель проверки. Необходимо обсуждать возможные решения проблем с участниками во время проверок и заранее готовить соответствующие средства для устранения недостатков.

Проверки должны тщательно подготавливаться для обеспечения как можно более эффективного достижения их целей, вызывая как можно меньше нарушений в обычной работе организации. Общее осуществление проверок должно заранее координироваться с руководством. Действия по разработке можно заключить в три различные основные формы:

- отчеты об инцидентах;
- подтверждение соответствия или несоответствия функциональности средств управления;
- другие регулярные проверки.

Кроме того, необходимо разработать представление результатов действия в отношении того, как выполняется запись и как информация передается руководству. Необходимо составлять официальную документацию для описания разработки, принципа действий и их цели, а также различных сфер ответственности.

Требования к результатам мониторинга

Результаты должны быть следующими:

a) записи действий по мониторингу с требуемой степенью детализации.

По результатам действий по мониторингу руководству должен быть представлен отчет. Вся информация, которая требуется руководству для выполнения надзорных и управленческих функций, должна быть записана в отчете с требуемой степенью детализации;

b) информация, необходимая руководству для принятия решений, когда это требуется для принятия срочных мер.

Отчет для руководства всегда заканчивается перечнем рекомендуемых действий с четко определенными приоритетами вместе с реальной оценкой предполагаемых затрат на выполнение каждого из этих действий. Это обеспечивает возможность принятия руководством решений без лишних задержек.

Планирование программы измерений, связанных с информационной безопасностью. Обзор разработки программы измерений, связанных с информационной безопасностью.

Процесс измерения должен быть плавно введен в цикл СМИБ проекта или организации и использоваться для непрерывного усовершенствования процессов, связанных с безопасностью, и результатов в рамках этого процесса или организации. Это называется программой измерения информационной безопасности (ISO/IEC 27004:2009). Разработку программы необходимо рассматривать в отношении цикла СМИБ. На рисунке Е.2 показано, как процесс измерения вписывается в цикл СМИБ.

Следующие функции систем управления требуются для обеспечения выполнения требований и ожиданий, таких как структурирование необходимых PDCA, измерение и подтверждение выходных данных и их эффективности, и обеспечение передачи результатов измерений руководителю процесса.

Чтобы провести правильные измерения, необходима ранее полученная информация, особенно:

a) политика СМИБ, включая область действия и границы;
b) результаты оценки риска;
c) выбор средств управления;
d) цели управления;
e) конкретные цели информационной безопасности;
f) заданные процессы и ресурсы и их классификация.

Руководство должно назначить и сохранять обязательства по всему процессу измерения. При осуществлении процесса измерения руководство должно:

a) принять требования к измерениям; подробности см. в стандарте ISO/IEC 27004:2009;
b) уделить внимание потребностям в информации, подробности см. в стандарте ISO/IEC 27004:2009;
c) установить обязательства персонала по следующим критериям:
- организация должна продемонстрировать свои обязательства, например, посредством политики измерений для организации, распределения ответственности и обязанностей, обучения и распределения бюджета и других ресурсов;
- должно быть назначено лицо или подразделение организации, отвечающее за программу измерения;
- должно быть назначено лицо или подразделение организации, отвечающее за обмен информацией по значимости и результатам измерений СМИБ во всей организации для обеспечения их принятия и использования, и это лицо или подразделение должно получать поддержку руководства;
- необходимо обеспечить сбор и анализ данных по измерениям СМИБ и их передачу директору по информационным технологиям и другим заинтересованным сторонам;
- необходимо обучить линейных руководителей программы использованию результатов измерений СМИБ для учреждения политики, распределения ресурсов и принятия решений, касающихся бюджета.

Программа измерения информационной безопасности и ее разработка подразумевают следующие роли:

a) высшее руководство;

b) пользователи программных продуктов, связанных с безопасностью;

c) лица, отвечающие за информационные системы;

d) лица, отвечающие за информационную безопасность.

Программа измерения информационной безопасности учреждается для того, чтобы получить показатели эффективности СМИБ, целей и средств управления. Программа описывается в стандарте ISO/IEC 27004:2009.

Для выполнения этих целей необходимо провести соответствующие измерения в фазе планирования.

Подходящие программы измерения информационной безопасности могут различаться в зависимости от структуры организации, а именно:

- размера;
- сложности;
- общего профиля риска в информационной безопасности.

Чем больше организация и чем сложнее ее структура, тем более обширная программа измерений ей требуется. Но уровень общего риска также влияет на объем программы. Если влияние слабой информационной безопасности серьезно, сравнительно небольшим организациям может потребоваться более обширная программа измерения, чтобы охватить риск, чем для более крупных организаций, не испытывающих такого влияния. Объем программы измерения можно оценить на основе выбора средств управления, которые необходимо охватить, и результатов анализа риска.

Разработка программы измерения информационной безопасности

Лицо, ответственное за программу измерения информационной безопасности, должно принять во внимание следующее:

- область действия;
- измерения;
- выполнение измерений;
- периоды измерений;
- отчетность.

Область действия программы измерения должна охватывать область действия, цели управления и меры и средства контроля и управления СМИБ. В частности, цели и границы измерения СМИБ должны устанавливаться в отношении характеристики организации, самой организации, ее местонахождения, активов и технологий и включать детализацию и обоснование любых исключений из области действия СМИБ. Это может быть одно из средств управления безопасностью, процесс, система, область деятельности, целое предприятие, одно подразделение или организация, состоящая из нескольких подразделений.

При выборе одиночного измерения стандарт ISO/IEC 27004:2009 требует, чтобы начальной точкой выступал объект измерения. Для учреждения программы измерений необходимо определить эти объекты. Этими объектами могут быть процессы или ресурсы. (Дополнительные подробности см. в стандарте ISO/IEC 27004:2009). При разработке программы измерений объекты, определенные областью действия СМИБ, часто расчленяются для выявления конкретных объектов, подлежащих измерению. Этот процесс определения можно проиллюстрировать в виде следующего примера: Организация — это весь объект — процесс в организации А/или система информационных технологий X — это часть объекта, которая сама образует объект — объекты в рамках этого процесса, влияющие на информационную безопасность (люди, правила, сети, программные приложения, оборудование и т. д.), обычно являются объектами измерения, помогающими увидеть эффективность защиты информации.

При выполнении программы измерения информационной безопасности необходимо учитывать, что объекты измерения могут служить для выполнения многих процессов в организации в рамках области СМИБ и, следовательно, могут оказывать более сильное влияние на эффективность СМИБ и цели управления. Обычно в рамках области действия программы следует уделять особое внимание таким объектам, например безопасности организации и связанным с ней процессам, компьютерному залу, коллегам, имеющим отношение к информационной безопасности и т. д.

Интервалы измерений могут различаться, но желательно, чтобы измерения проводились или суммировались с определенными интервалами для включения их в проверки, проводимые руководством в процессе непрерывного усовершенствования СМИБ. Это условие должно быть учтено при разработке программы.

Отчетность по результатам должна быть организована таким образом, чтобы обеспечить передачу информации в соответствии с ISO/IEC 27004:2009.

Разработка программы измерения информационной безопасности должна быть отражена в документе, определяющем процедуру, который должен быть утвержден руководством. Этот документ должен охватывать следующие аспекты:

a) сферы ответственности за программу измерения информационной безопасности;

b) сферы ответственности за осуществление связи;

c) область действия измерений;

d) как должна выполняться программа (основной используемый метод, внешнее и внутреннее выполнение и т. д.);

e) когда должна выполняться программа;

f) как должна осуществляться отчетность.

Если организация разрабатывает собственные цели измерения, они должны быть документированы как часть фазы разработки; дополнительную справочную информацию см. в стандарте ISO/IEC 27004:2009. Этот документ может быть достаточно обширным и не обязательно должен подписываться руководством, поскольку детали могут изменяться при выполнении программы.

Измерение эффективности СМИБ

При установлении области действия программы измерения информационной безопасности, подлежащей выполнению, необходимо обеспечить, чтобы объектов не было слишком много. Если объектов много, имеет смысл разделить программу на разные части. Область действия этих частей может быть представлена как отдельные измерения для сравнения, но преобладает их основная цель: сочетание измерений обеспечивает показания для оценки эффективности СМИБ. Эти вспомогательные области действия обычно представляют собой подразделения организации, которые могут быть определены с четкими границами. Сочетание объектов, которые служат многим процессам в организации и измерениям объектов в рамках этих вспомогательных областей действия, вместе могут образовывать необходимую область действия для программы измерения информационной безопасности. Это сочетание также можно представить в виде серии действий по СМИБ, которые могут рассматриваться как состоящие из двух или более процессов (объектов). Следовательно, эффективность всей системы СМИБ можно измерить на основе измерения результатов этих двух или более процессов (объектов).

Поскольку целью является измерение эффективности СМИБ, важно измерить цели, определить меры и средства контроля и управления. Один аспект — это количество средств управления, а другой аспект — это достаточность этих средств управления для оценки эффективности СМИБ. Эти аспекты измерения эффективности СМИБ с помощью процесса PDCA и примеры процессов внутри организации приведены на рис. Е.2. (Могут быть и другие причины для ограничения области действия программы измерения информационной безопасности, которые упоминаются в ISO/IEC 27004:2009).

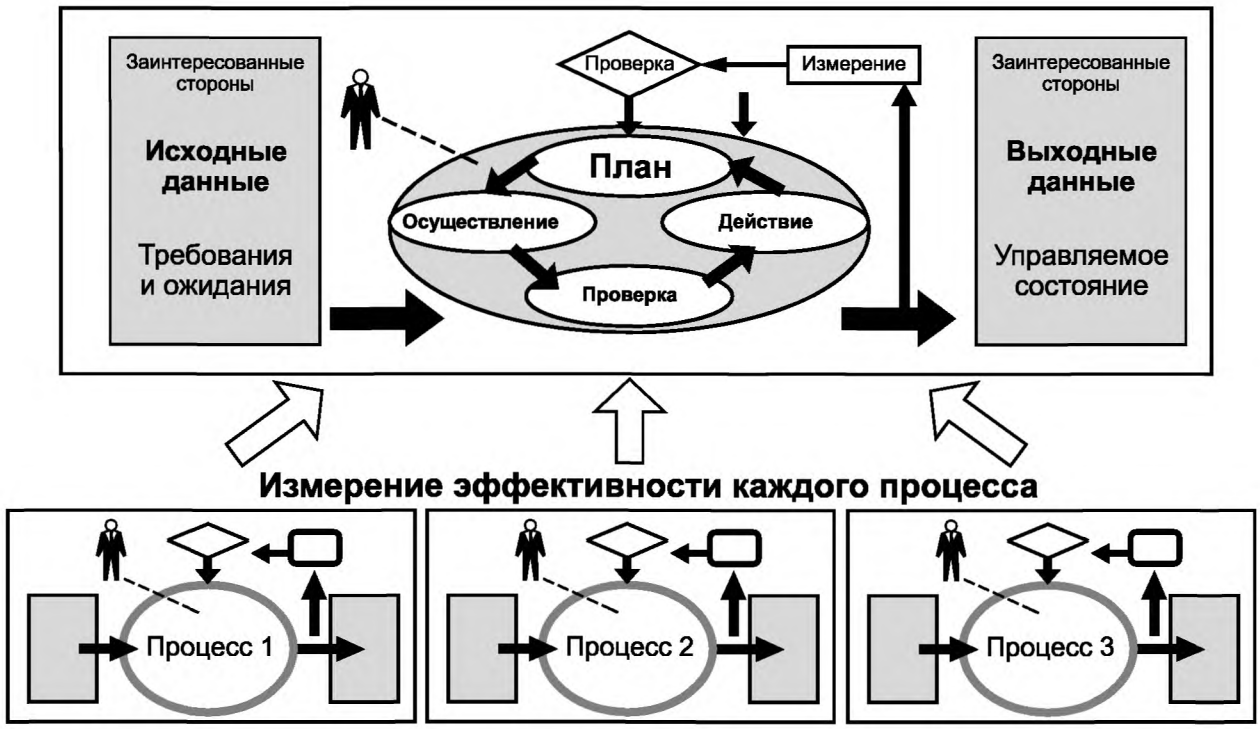



Рисунок Е.2 — Два аспекта измерения эффективности СМИБ с помощью процесса PDCA и примеры процессов внутри организации

При использовании результатов измерения для оценки эффективности СМИБ, целей управления и средств управления необходимо, чтобы руководство было проинформировано об области действия программы измерения информационной безопасности. Лицо, ответственное за программу измерений, должно получить от руководства утверждение области действия программы измерения информационной безопасности перед запуском программы.

Примечания

1 Требование, относящееся к измерению эффективности, в стандарте ISO/IEC 27001:2005 — это «измерение мер и средств контроля и управления или серии средств управления» (см. 4.2.2, d) в ISO/IEC 27001:2005).

2 Требование, относящееся к эффективности всей системы СМИБ, в стандарте ISO/IEC 27001:2005 — это только «проверка эффективности всей системы СМИБ», и «измерение всей системы СМИБ» не требуется (см. 0.2.2 в ISO/IEC 27001:2005).

Фактически проведение измерений может осуществляться работниками организации, специалистами со стороны или теми и другими вместе. Размеры, структура и культура организации — это факторы, которые необходимо принимать во внимание при оценке внутренних или внешних ресурсов. Малые и средние компании имеют больше выгоды от использования поддержки со стороны, чем большие организации. Результаты использования внешних ресурсов могут также обеспечить более надежные результаты в зависимости от культуры организации. Если в организации постоянно проводится внутренний аудит, внутренняя проверка может принести более надежные результаты.

**Приложение ДА**
**(справочное)**

## Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

| Обозначение ссылочного международного стандарта | Степень соответствия | Обозначение и наименование соответствующего национального стандарта |
|---|---|---|
| ISO/IEC 27001:2005 | IDT | ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» |
| ISO/IEC 27006:2007 | IDT | ГОСТ Р ИСО/МЭК 27006—2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности» |
| ISO/IEC 27005:2008 | IDT | ГОСТ Р ИСО/МЭК 27005—2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» |

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

- IDT — идентичные стандарты.

## Библиография


[1] ISO 9001:2008, *Quality management systems — Requirements*
[2] ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*
[3] ISO/IEC 15026 (all parts), *Systems and software engineering — Systems and software assurance*[1)]
[4] ISO/IEC 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*
[5] ISO/IEC 15408-2:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*
[6] ISO/IEC 15408-3:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*
[7] ISO/IEC TR 15443-1:2005, *Information technology — Security techniques — A framework for IT security assurance — Part 1: Overview and framework*
[8] ISO/IEC TR 15443-2:2005, *Information technology — Security techniques — A framework for IT security assurance — Part 2: Assurance methods*
[9] ISO/IEC TR 15443-3:2007, *Information technology — Security techniques — A framework for IT security assurance — Part 3: Analysis of assurance methods*
[10] ISO/IEC 15939:2007, *Systems and software engineering — Measurement process*
[11] ISO/IEC 16085:2006, *Systems and software engineering — Life cycle processes — Risk management*
[12] ISO/IEC 16326:2009, *Systems and software engineering — Life cycle processes — Project management*
[13] ISO/IEC 18045:2008, *Information technology — Security techniques — Methodology for IT security evaluation*
[14] ISO/IEC TR 19791:2006, *Information technology — Security techniques — Security assessment of operational systems*
[15] ISO/IEC 20000-1:2005, *Information technology — Service management — Part 1: Specification*
[16] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*
[17] ISO/IEC 27004:2009, *Information technology — Security techniques — Information security management — Measurement*
[18] ISO/IEC 27005:2008, *Information technology — Security techniques — Information security risk management*
[19] ISO 21500, *Project management — Guide to project management*[2)]
[20] ISO/IEC 27006:2007, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*


[1)] Будет опубликован.
[2)] В процессе подготовки.


УДК 004.91:006.354 ОКС 35.040

Ключевые слова: система менеджмента информационной безопасности, документально оформленная процедура, инцидент информационной безопасности

Редактор *А. В. Барандеев*
Технический редактор *Е. В. Беспрозванная*
Корректор *В. Г. Гришунина*
Компьютерная верстка *Т. Ф. Кузнецовой*

Сдано в набор 09.09.2014. Подписано в печать 27.11.2014. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 6,51. Уч.-изд. л. 5,95. Тираж 81 экз. Зак. 1517.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.

gost.e-ecolog.ru