ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27001— 2006

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Требования

ISO/IEC 27001: 2005
Information technology — Security techniques — Information security management systems — Requirements
(IDT)

Издание официальное

БЗ 1—2007/380

Москва
Стандартинформ
2008

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

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

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (ISO/IEC 27001:2005 «Information technology — Security techniques — Information security management systems — Requirements»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочного международного стандарта соответствующий ему национальный стандарт Российской Федерации, сведения о котором приведены в дополнительном приложении D

5 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2008

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

0 Введение IV
1 Область применения 1
1.1 Общие положения 1
1.2 Применение 1
2 Нормативные ссылки 2
3 Термины и определения 2
4 Система менеджмента информационной безопасности 3
4.1 Общие требования 3
4.2 Разработка системы менеджмента информационной безопасности. Управление системой менеджмента информационной безопасности 3
4.3 Требования к документации 6
5 Ответственность руководства 7
5.1 Обязательства руководства 7
5.2 Управление ресурсами 7
6 Внутренние аудиты системы менеджмента информационной безопасности 8
7 Анализ системы менеджмента информационной безопасности со стороны руководства 8
7.1 Общие положения 8
7.2 Входные данные для анализа системы менеджмента информационной безопасности 8
7.3 Выходные данные анализа системы менеджмента информационной безопасности 8
8 Улучшение системы менеджмента информационной безопасности 9
8.1 Постоянное улучшение 9
8.2 Корректирующие действия 9
8.3 Предупреждающие действия 9
Приложение А (рекомендуемое) Цели и меры управления 10
Приложение В (справочное) Принципы Организации экономического сотрудничества и развития и настоящий стандарт 22
Приложение С (справочное) Сравнение структуры настоящего стандарта со структурами международных стандартов ИСО 9001:2000, ИСО 14001:2004 23
Приложение D (справочное) Сведения о соответствии национального стандарта Российской Федерации ссылочному международному стандарту 25
Библиография 25

0 Введение

0.1 Общие положения

Настоящий стандарт подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности (СМИБ). Внедрение СМИБ является стратегическим решением организации. На проектирование и внедрение СМИБ организации влияют потребности и цели организации, требования безопасности, используемые процессы, а также масштабы деятельности и структура организации. Предполагается, что вышеуказанные факторы и поддерживающие их системы будут изменяться во времени. Предполагается также, что СМИБ будет изменяться пропорционально потребностям организации, т. е. для простой ситуации потребуется простое решение по реализации СМИБ.

Положения настоящего стандарта могут быть использованы как внутри организации, так и внешними организациями для оценки соответствия.

0.2 Процессный подход

Настоящий стандарт предполагает использовать процессный подход для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ организации.

Для успешного функционирования организация должна определить и осуществить менеджмент многочисленных видов деятельности. Деятельность, использующая ресурсы и управляемая в целях преобразования входов в выходы, может быть рассмотрена как процесс. Часто выход одного процесса непосредственно формирует вход для следующего процесса.

Использование внутри организации системы процессов наряду с идентификацией и взаимодействием этих процессов, а также менеджмент процессов могут быть определены как «процессный подход».

Согласно предлагаемому настоящим стандартом процессному подходу применительно к менеджменту информационной безопасности (ИБ) особую значимость для пользователей имеют следующие факторы:

a) понимание требований информационной безопасности организации и необходимости установления политики и целей информационной безопасности;

b) внедрение и использование мер управления для менеджмента рисков ИБ среди общих бизнес-рисков организации;

c) мониторинг и проверка производительности и эффективности СМИБ;

d) непрерывное улучшение СМИБ, основанное на результатах объективных измерений.

В настоящем стандарте представлена модель «Планирование (Plan) — Осуществление (Do) — Проверка (Check) — Действие (Act)» (PDCA), которая может быть применена при структурировании всех процессов СМИБ. На рисунке 1 показано, как СМИБ, используя в качестве входных данных требования ИБ и ожидаемые результаты заинтересованных сторон, с помощью необходимых действий и процессов выдает выходные данные по результатам обеспечения информационной безопасности, которые соответствуют этим требованиям и ожидаемым результатам. Рисунок 1 иллюстрирует также связи между процессами, описанными в разделах 4, 5, 6, 7 и 8.

Принятие модели PDCA также отражает принципы, установленные в Директивах Организации экономического сотрудничества и развития (ОЭСР) и определяющие безопасность информационных систем и сетей [1]. Настоящий стандарт представляет наглядную модель для реализации на практике указанных принципов, которые позволяют осуществить оценку рисков, проектирование и реализацию системы информационной безопасности, ее менеджмент и переоценку.

Примеры

1 Требование может заключаться в том, чтобы нарушения информационной безопасности не приводили к значительному финансовому ущербу для организации и/или к существенным затруднениям в ее деятельности.

2 Ожидаемым результатом может быть наличие в организации достаточно хорошо обученных сотрудников для проведения процедур, позволяющих минимизировать возможные неблагоприятные последствия в случае серьезного инцидента, например несанкционированного проникновения (атаки хакеров) на веб-сайт организации, через который она осуществляет электронную торговлю.

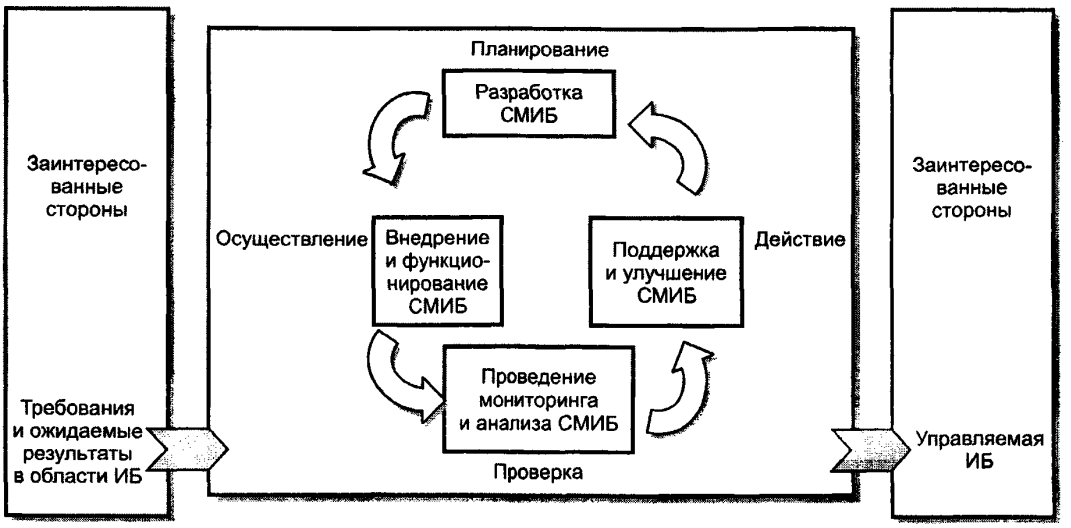


Рисунок 1

Связи между процессами, описанными в разделах 4, 5, 6, 7 и 8, представлены также в таблице 1.

Таблица 1

Планирование (разработка СМИБ)	Разработка политики, установление целей, процессов и процедур СМИБ, относящихся к менеджменту риска и улучшению информационной безопасности, для достижения результатов, соответствующих общей политике и целям организации
Осуществление (внедрение и обеспечение функционирования СМИБ)	Внедрение и применение политики информационной безопасности, мер управления, процессов и процедур СМИБ
Проверка (проведение мониторинга и анализа СМИБ)	Оценка, в том числе, по возможности, количественная, результативности процессов относительно требований политики, целей безопасности и практического опыта функционирования СМИБ и информирование высшего руководства о результатах для последующего анализа
Действие (поддержка и улучшение СМИБ)	Проведение корректирующих и превентивных действий, основанных на результатах внутреннего аудита или другой соответствующей информации, и анализа со стороны руководства в целях достижения непрерывного улучшения СМИБ

0.3 Совместимость с другими системами менеджмента

Настоящий стандарт согласован со стандартами ИСО 9001:2000 «Системы менеджмента качества. Требования» [2] и ИСО 14001:2004 «Системы управления окружающей средой. Требования и руководство по применению» [3] в целях поддержки последовательного и интегрированного внедрения и взаимодействия с другими подобными взаимосвязанными стандартами в области менеджмента. Таким образом, одна правильно построенная система менеджмента в организации может удовлетворять требованиям всех этих стандартов.

Таблица С.1 иллюстрирует взаимосвязь между разделами настоящего стандарта, а также ИСО 9001:2000 и ИСО 14001:2004.

Настоящий стандарт позволяет организации регулировать СМИБ или интегрировать ее с соответствующими требованиями других систем менеджмента.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Требования

Information technology. Security techniques. Information security management systems. Requirements

Дата введения — 2006—02—01

1 Область применения

1.1 Общие положения

Настоящий стандарт предназначен для применения организациями любой формы собственности (например, коммерческими, государственными и некоммерческими организациями). Настоящий стандарт устанавливает требования по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной системы менеджмента информационной безопасности (СМИБ) среди общих бизнес-рисков организации. Кроме этого, стандарт устанавливает требования по внедрению мер управления информационной безопасностью и ее контроля, которые могут быть использованы организациями или их подразделениями в соответствии с установленными целями и задачами обеспечения информационной безопасности (ИБ).

Целью построения СМИБ является выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон.

Примечание — Термин «бизнес», в настоящем стандарте понимаемый в широком смысле, обозначает всю ту деятельность, которая является основой для целей существования организации.

1.2 Применение

Требования, устанавливаемые настоящим стандартом, предназначены для применения во всех организациях независимо от типа, масштабов и сферы их деятельности. Исключение любого из требований, указанных в разделах 4, 5, 6, 7 и 8, не допускается, если организация заявляет о соответствии ее СМИБ настоящему стандарту.

Любой отказ от применения той или иной меры управления, обусловленный необходимостью удовлетворения критериев принятия рисков, должен быть обоснован. Необходимо также наличие адекватных доказательств того, что подобные риски были уже приняты ответственными лицами. При исключении каких-либо мер управления заявления о соответствии организации настоящему стандарту неправомочны, кроме случаев, когда эти исключения не влияют на способность и/или обязанность организации обеспечивать информационную безопасность, которая соответствует требованиям безопасности, установленным соответствующими законодательными актами или определенными на основе оценок рисков.

Примечание — Если организация уже имеет действующую систему менеджмента бизнес-процессов (например, в соответствии с ИСО 9001 [2] или ИСО 14001 [3]), тогда в большинстве случаев предпочтительнее удовлетворить требования настоящего стандарта в рамках этой существующей системы менеджмента.

Издание официальное

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующий стандарт:

ИСО/МЭК 17799:2005 Информационная технология. Методы и средства обеспечения безопасности. Практические правила менеджмента информационной безопасности

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **активы** (asset): Все, что имеет ценность для организации.

[ИСО/МЭК 13335-1:2004] [4]

3.2 **доступность** (availability): Свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта.

[ИСО/МЭК 13335-1:2004] [4]

3.3 **конфиденциальность** (confidentiality): Свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

[ИСО/МЭК 13335-1:2004] [4]

3.4 **информационная безопасность**; ИБ (information security): Свойство информации сохранять конфиденциальность, целостность и доступность.

Примечание — Кроме того, данное понятие может включать в себя также и свойство сохранять аутентичность, подотчетность, неотказуемость и надежность.

[ИСО/МЭК 17799:2005]

3.5 **событие информационной безопасности** (information security event): Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

[ИСО/МЭК ТО 18044:2004] [5]

3.6 **инцидент информационной безопасности** (information security incident): Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Примечание — Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

[ИСО/МЭК ТО 18044:2004] [5]

3.7 **система менеджмента информационной безопасности**; СМИБ (information security management system; ISMS): Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

Примечание — Система менеджмента включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы.

3.8 **целостность** (integrity): Свойство сохранять правильность и полноту активов.

[ИСО/МЭК 13335-1:2004] [4]

3.9 **остаточный риск** (residual risk): Риск, остающийся после его обработки.

[Руководство ИСО/МЭК 73:2002] [6]

3.10 **принятие риска** (risk acceptance): Решение по принятию риска.

[Руководство ИСО/МЭК 73:2002] [6]

3.11 **анализ риска** (risk analysis): Систематическое использование информации для определения источников риска и количественной оценки риска.

[Руководство ИСО/МЭК 73:2002] [6]

3.12 **оценка риска** (risk assessment): Общий процесс анализа риска и его оценивания.

[Руководство ИСО/МЭК 73:2002] [6]

3.13 **оценивание риска** (risk evaluation): Процесс сравнения количественно оцененного риска с заданными критериями риска для определения его значимости.

[Руководство ИСО/МЭК 73:2002] [6]

3.14 **менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией в отношении риска.

Примечание — Обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска и коммуникацию риска.

[Руководство ИСО/МЭК 73:2002] [6]

3.15 **обработка риска** (risk treatment): Процесс выбора и осуществления мер по модификации риска.

[Руководство ИСО/МЭК 73:2002] [6]

Примечания

1 Меры по обработке риска могут включать в себя избежание, оптимизацию, перенос или сохранение риска.

2 В настоящем стандарте термин «мера управления» (control) использован как синоним термина «мера» (measure).

3.16 **положение о применимости** (statement of applicability): Документированное предписание, определяющее цели и меры управления, соответствующие и применимые к системе менеджмента информационной безопасности организации.

Примечание — Цели и меры управления основываются на результатах и выводах процессов оценки и обработки рисков, на требованиях законодательных или нормативных актов, на обязательствах по контракту и бизнес-требованиях организации по отношению к информационной безопасности.

4 Система менеджмента информационной безопасности

4.1 Общие требования

Организация должна разработать, внедрить, обеспечить функционирование, вести мониторинг, анализировать, поддерживать и непрерывно улучшать документированную СМИБ применительно ко всей деловой деятельности организации и рискам, с которыми она сталкивается. С учетом целей настоящего стандарта используемый процесс основан на применении модели PDCA, приведенной на рисунке 1.

4.2 Разработка системы менеджмента информационной безопасности. Управление системой менеджмента информационной безопасности

4.2.1 Разработка системы менеджмента информационной безопасности

Организация должна осуществить следующее:

a) определить область и границы действия СМИБ с учетом характеристик бизнеса, организации, ее размещения, активов и технологий, в том числе детали и обоснование любых исключений из области ее действия (см. 1.2);

b) определить политику СМИБ на основе характеристик бизнеса, организации, ее размещения, активов и технологий, которая:

1) содержит концепцию, включающую в себя цели, основные направления и принципы действий в сфере ИБ;

2) принимает во внимание требования бизнеса, нормативно-правовые требования, а также договорные обязательства по обеспечению безопасности;

3) согласуется со стратегическим содержанием менеджмента рисков организации, в рамках которого будет разрабатываться и поддерживаться СМИБ;

4) устанавливает критерии оценки рисков [см. 4.2.1, перечисление c)];

5) утверждается руководством организации.

Примечание — Для целей настоящего стандарта политика СМИБ имеет приоритет перед политикой ИБ. Эти политики могут быть изложены в одном документе;

c) определить подход к оценке риска в организации, для чего необходимо:

1) определить методологию оценки риска, подходящую для СМИБ, которая должна соответствовать требованиям обеспечения деятельности организации и нормативно-правовым требованиям информационной безопасности;

2) разработать критерии принятия риска и определить приемлемые уровни риска [см. 5.1, перечисление f)].

Выбранная методология оценки риска должна обеспечивать сравнимые и воспроизводимые результаты.

Примечание — Имеются различные методологии оценки риска. Примеры таких методологий даны в ИСО/МЭК ТО 13335-3:1998 «Руководство по управлению безопасностью информационных технологий. Часть 3. Методы управления безопасностью информационных технологий» [7];

d) идентифицировать риски, для чего необходимо:

1) идентифицировать активы в пределах области функционирования СМИБ и определить владельцев[1)] этих активов;

2) идентифицировать угрозы этим активам;

3) идентифицировать уязвимости активов, которые могут быть использованы угрозами;

4) идентифицировать последствия воздействия на активы в результате возможной утраты конфиденциальности, целостности и доступности активов;

e) проанализировать и оценить риски, для чего необходимо:

1) оценить ущерб для деятельности организации, который может быть нанесен в результате сбоя обеспечения безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности или доступности активов;

2) оценить реальную вероятность сбоя обеспечения безопасности с учетом превалирующих угроз, уязвимостей и их последствий, связанных с этими активами, а также с учетом применяемых мер управления безопасностью;

3) оценить уровни рисков;

4) определить, являются ли риски приемлемыми или требуют обработки с использованием критериев допустимости рисков, установленных в 4.2.1, перечисление c);

f) определить и оценить различные варианты обработки рисков.

Возможные действия:

1) применение подходящих мер управления;

2) сознательное и объективное принятие рисков при условии, что они полностью соответствуют требованиям политики и критериям организации в отношении принятия рисков [см. 4.2.1, перечисление, c), 2)];

3) избежание рисков;

4) передача соответствующих деловых рисков сторонним организациям, например страховщикам или поставщикам;

g) выбрать цели и меры управления для обработки рисков.

Цели и меры управления должны быть выбраны и реализованы так, чтобы удовлетворять требованиям, определенным в процессе оценки и обработки рисков. Этот выбор должен учитывать критерии принятия рисков [см. 4.2.1, перечисление c), 2)], а также нормативно-правовые требования и договорные обязательства.

Цели и меры управления должны быть выбраны согласно приложению А как часть процесса оценки и обработки рисков и соответствовать требованиям этого процесса.

Перечень целей и мер управления, приведенный в приложении А, не является исчерпывающим, а потому могут быть выбраны дополнительные цели и меры управления.

Примечание — Приложение А содержит подробный перечень целей и мер управления, обычно используемых в организациях. Рекомендуется использовать этот перечень в качестве исходных данных, позволяющих выбрать рациональный вариант мер управления и контроля;

h) получить утверждение руководством предполагаемых остаточных рисков;

i) получить разрешение руководства на внедрение и эксплуатацию СМИБ;

j) подготовить Положение о применимости, которое включает в себя следующее:

1) цели и меры управления, выбранные в 4.2.1, перечисление g), и обоснование этого выбора;

2) цели и меры управления, реализованные в настоящее время [см. 4.2.1 , перечисление e), 2)];

3) перечень исключенных целей и мер управления, указанных в приложении А, и процедуру обоснования их исключения.

[1)] Здесь и далее термин «владелец» определяет лицо или организацию, которые имеют утвержденные руководством обязательства по контролю за производством, разработкой, поддержкой, использованием и безопасностью активов. Термин «владелец» не означает, что лицо действительно имеет какие-либо права собственности на актив.

Примечание — Положение о применимости содержит итоговые решения, касающиеся обработки рисков. Обоснование исключений предусматривает перекрестную проверку, позволяющую определить, что ни одна мера управления не была случайно упущена.

4.2.2 Внедрение и функционирование системы менеджмента информационной безопасности

Организация должна выполнить следующее:

a) разработать план обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ (см. раздел 5);

b) реализовать план обработки рисков для достижения намеченных целей управления, включающий в себя вопросы финансирования, а также распределение функций и обязанностей;

c) внедрить меры управления, выбранные согласно 4.2.1, перечисление g), для достижения целей управления;

d) определить способ измерения результативности выбранных мер управления или их групп и использования этих измерений для оценки результативности управления с целью получить сравнимые и воспроизводимые данные [см. 4.2.3, перечисление c)].

Примечание — Измерение результативности мер управления позволяет руководителям и персоналу определить, в какой степени меры управления способствуют достижению намеченных целей управления;

e) реализовать программы по обучению и повышению квалификации сотрудников (см. 5.2.2);

f) управлять работой СМИБ;

g) управлять ресурсами СМИБ (см. 5.2);

h) внедрить процедуры и другие меры управления, обеспечивающие быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ [см. 4.2.3, перечисление a)].

4.2.3 Проведение мониторинга и анализа системы менеджмента информационной безопасности

Организация должна осуществлять следующее:

a) выполнять процедуры мониторинга и анализа, а также использовать другие меры управления в следующих целях:

1) своевременно обнаруживать ошибки в результатах обработки;

2) своевременно выявлять удавшиеся и неудавшиеся попытки нарушения и инциденты ИБ;

3) предоставлять руководству информацию для принятия решений о ходе выполнения функций по обеспечению ИБ, осуществляемых как ответственными лицами, так и информационными технологиями;

4) способствовать обнаружению событий ИБ и, таким образом, предотвращать инциденты ИБ путем применения средств индикации;

5) определять, являются ли эффективными действия, предпринимаемые для устранения нарушения безопасности;

b) проводить регулярный анализ результативности СМИБ (включая проверку ее соответствия политике и целям СМИБ и анализ мер управления безопасностью) с учетом результатов аудиторских проверок ИБ, ее инцидентов, результатов измерений эффективности СМИБ, а также предложений и другой информации от всех заинтересованных сторон;

c) измерять результативность мер управления для проверки соответствия требованиям ИБ;

d) пересматривать оценки рисков через установленные периоды времени, анализировать остаточные риски и установленные приемлемые уровни рисков, учитывая изменения:

1) в организации;

2) в технологиях;

3) в целях деятельности и процессах;

4) в выявленных угрозах;

5) в результативности реализованных мер управления;

6) во внешних условиях, например изменения нормативно-правовых требований, требований договорных обязательств, а также изменения в социальной структуре общества;

e) проводить внутренние аудиты СМИБ через установленные периоды времени (см. раздел 6).

Примечание — Внутренние аудиты, иногда называемые аудитами первой стороны, проводятся самой организацией (или внешней организацией от ее имени) для собственных целей;

f) регулярно проводить руководством организации анализ СМИБ в целях подтверждения адекватности ее функционирования и определения направлений совершенствования (см. 7.1);

g) обновлять планы ИБ с учетом результатов анализа и мониторинга;

h) регистрировать действия и события, способные повлиять на результативность или функционирование СМИБ, в соответствии с 4.3.3.

4.2.4 Поддержка и улучшение системы менеджмента информационной безопасности

Организация должна регулярно осуществлять следующее:

a) выявлять возможности улучшения СМИБ;

b) предпринимать необходимые корректирующие и предупреждающие действия в соответствии с 8.2 и 8.3, использовать на практике опыт по обеспечению ИБ, полученный как в собственной организации, так и в других организациях;

c) передавать подробную информацию о действиях по улучшению СМИБ всем заинтересованным сторонам, при этом степень ее детализации должна соответствовать обстоятельствам и, при необходимости, согласовывать дальнейшие действия;

d) обеспечивать внедрение улучшений СМИБ для достижения запланированных целей.

4.3 Требования к документации

4.3.1 Общие положения

Документация должна включать в себя записи решений руководства, позволяющие обеспечивать контроль выполнения решений руководства и политик организации, а также обеспечивать воспроизводимость документированных результатов.

Важно иметь обратную связь выбранных мер управления с результатами процессов оценки и обработки риска, а также последних с политикой СМИБ и целями СМИБ.

Документация СМИБ должна включать в себя следующее:

a) документированные положения политики СМИБ [см. 4.2.1, перечисление b)] и целей СМИБ;

b) область функционирования СМИБ [см. 4.2.1, перечисление a)];

c) процедуры и меры управления, поддерживающие СМИБ;

d) описание методологии оценки риска [см. 4.2.1, перечисление c)];

e) отчет по оценке рисков [см. 4.2.1, перечисления c)—g)];

f) план обработки рисков;

g) документированные процедуры, необходимые организации для обеспечения эффективного планирования, внедрения процессов в области ИБ и управления этими процессами, а также описания путей оценки результативности мер управления [см. 4.2.3, перечисление c)];

h) учетные записи (см. 4.3.3);

i) положение о применимости.

Примечания

1 Согласно настоящему стандарту термин «документированная процедура» означает, что процедура установлена, документально оформлена, реализована и поддерживается на должном уровне.

2 Для разных организаций объем документации СМИБ может быть различным в зависимости:

- от размера организации и вида ее деятельности;
- от области применения и сложности требований безопасности и от управляемой системы.

3 Документы и учетные записи могут существовать в любой форме и на носителях любого типа.

4.3.2 Управление документами

Для разработки, актуализации, использования, хранения и уничтожения документов СМИБ, а также их защиты в организации должна существовать документированная процедура, определяющая действия руководства по:

a) утверждению документов СМИБ перед их изданием;

b) пересмотру и обновлению, при необходимости, документов, а также повторному их утверждению;

c) обеспечению идентификации внесенных изменений и текущего статуса документов;

d) обеспечению наличия версий соответствующих документов в местах их использования;

e) определению порядка просмотра документов и их идентификации;

f) обеспечению доступа к документам авторизованным лицам, а также передачи, хранения и уничтожения в соответствии с процедурами, применимыми к степени их конфиденциальности;

g) идентификации документов, созданных вне организации;

h) обеспечению контроля за распространением документов;

i) предотвращению непреднамеренного использования устаревших документов;

j) использованию соответствующей идентификации устаревших документов в случае их дальнейшего хранения.

4.3.3 Управление записями

Для предоставления свидетельств соответствия требованиям и результативности функционирования СМИБ необходимо вести и поддерживать в рабочем состоянии учетные записи. Учетные записи необходимо контролировать и защищать. СМИБ должна принимать во внимание все нормативно-правовые требования и договорные обязательства, имеющие отношение к ИБ. Записи должны быть четкими, легкоидентифицируемыми и восстанавливаемыми. Меры управления, требуемые для идентификации, хранения, защиты, поиска, определения сроков хранения и уничтожения записей должны быть документированы и реализованы.

Кроме этого, следует вести и хранить записи о выполнении процессов, описанных в 4.2, и обо всех значительных инцидентах информационной безопасности, связанных со СМИБ.

Пример — Примерами записей являются: журнал регистрации посетителей, отчеты о результатах аудитов, заполненные формы авторизации доступа.

5 Ответственность руководства

5.1 Обязательства руководства

Руководство организации должно предоставлять доказательства выполнения своих обязательств в отношении разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ путем осуществления следующих мер:

a) разработки политики СМИБ;

b) обеспечения разработки целей и планов СМИБ;

c) определения функций и ответственности в области ИБ;

d) доведения до всех сотрудников организации информации о важности достижения целей информационной безопасности и соответствия ее требованиям политики организации, об их ответственности перед законом, а также о необходимости непрерывного совершенствования в реализации мер ИБ;

e) выделения необходимых и достаточных ресурсов для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ (см. 5.2.1);

f) установления критериев принятия рисков и уровней их приемлемости;

g) обеспечения проведения внутренних аудитов СМИБ (см. раздел 6);

h) проведения анализа СМИБ со стороны руководства (см. раздел 7).

5.2 Управление ресурсами

5.2.1 Обеспечение ресурсами

Организация должна определить и предоставить ресурсы, необходимые для:

a) разработки, внедрения, обеспечения функционирования, мониторинга, анализа, улучшения и поддержки СМИБ;

b) поддержки требований бизнеса процедурами информационной безопасности;

c) выявления и обеспечения выполнения требований соответствующих законов, нормативных актов, а также договорных обязательств в области информационной безопасности;

d) поддержания адекватной безопасности путем правильного применения всех реализованных мер управления;

e) проведения, при необходимости, анализа и принятия соответствующих мер по его результатам;

f) повышения, при необходимости, результативности СМИБ.

5.2.2 Подготовка, осведомленность и квалификация персонала

Организация должна обеспечить необходимую квалификацию персонала, на который возложены обязанности выполнения задач в рамках СМИБ путем:

a) определения требуемого уровня знаний и навыков для персонала, который выполняет работу, влияющую на СМИБ;

b) организации обучения персонала или принятия других мер (например, наем компетентного персонала) для удовлетворения указанных потребностей;

c) оценки результативности предпринятых действий;

d) ведения записей об образовании, подготовке, навыках, опыте и квалификации сотрудников (см. 4.3.3).

Организация должна также обеспечить понимание всеми соответствующими сотрудниками значимости и важности деятельности в области информационной безопасности, и их роли в достижении целей СМИБ.

6 Внутренние аудиты системы менеджмента информационной безопасности

Организация должна в соответствии с утвержденным графиком проводить внутренние аудиты СМИБ, позволяющие установить, что цели управления, меры управления, процессы и процедуры СМИБ:

a) соответствуют требованиям настоящего стандарта и соответствующим законам или нормативным документам;

b) соответствуют установленным требованиям ИБ;

c) результативно внедряются и поддерживаются;

d) функционируют должным образом.

Программа аудита должна быть спланирована с учетом статуса и важности проверяемых процессов и зон, подлежащих аудиту, а также результатов предыдущих аудитов. Должны быть определены критерии, область, частота и методы аудита. Отбор аудиторов и процедура аудита должны обеспечивать его объективность и беспристрастность. Аудиторы не должны проводить проверку своей собственной работы.

Правила и требования, относящиеся к планированию, проведению аудита, сообщению о его результатах и поддержанию в рабочем состоянии учетных записей (см. 4.3.3), должны быть документированы.

Руководитель, ответственный за проверяемый участок деятельности организации, должен своевременно и без задержки обеспечить проведение проверки в целях устранения обнаруженных несоответствий и их причин. Последующие действия должны включать в себя проверку предпринятых действий и сообщение о результатах проверки (см. раздел 8) [8].

7 Анализ системы менеджмента информационной безопасности со стороны руководства

7.1 Общие положения

Руководство должно в соответствии с утвержденным графиком периодически (не менее одного раза в год) проводить анализ СМИБ организации в целях обеспечения ее постоянной пригодности, адекватности и результативности. Результаты анализа должны содержать предложения по изменению СМИБ и оценку их реализации в интересах обеспечения выполнения требований политики и целей информационной безопасности. Результаты таких проверок должны быть зафиксированы документально, а учетные записи должны быть сохранены (см. 4.3.3).

7.2 Входные данные для анализа системы менеджмента информационной безопасности

Входные данные для анализа СМИБ со стороны руководства должны включать в себя следующую информацию:

a) результаты предыдущих аудитов и анализа СМИБ;

b) результаты взаимодействия с заинтересованными сторонами;

c) методы, средства или процедуры, которые могут быть использованы в организации для совершенствования функционирования и повышения результативности СМИБ;

d) правовое обоснование предупреждающих и корректирующих действий;

e) уязвимости или угрозы, которые не были адекватно учтены в процессе предыдущей оценки рисков;

f) результаты количественной оценки результативности СМИБ;

g) последующие действия, вытекающие из предыдущего анализа со стороны руководства;

h) любые изменения, которые могли бы повлиять на СМИБ;

i) рекомендации по улучшению.

7.3 Выходные данные анализа системы менеджмента информационной безопасности

Выходные данные анализа СМИБ со стороны руководства должны включать в себя все решения и действия, направленные:

a) на повышение результативности СМИБ;

b) на обновление планов оценки и обработки рисков;

c) на модификацию процедур и мер управления и контроля, влияющих на ИБ, с целью обеспечить реагирование на внутренние или внешние события, которые могут оказать воздействие на СМИБ, включая изменения:

1) в бизнес-требованиях;

2) в требованиях безопасности;
3) в бизнес-процессах, влияющих на существующие бизнес-требования;
4) в законах и нормативных документах;
5) в договорных обязательствах;
6) в уровнях риска и/или критериев принятия риска;
d) на потребности в ресурсах;
e) на совершенствование способов оценки результативности мер управления.

8 Улучшение системы менеджмента информационной безопасности

8.1 Постоянное улучшение

Организация должна постоянно повышать результативность СМИБ посредством уточнения политики ИБ, целей ИБ, использования результатов аудитов, анализа контролируемых событий, корректирующих и предупреждающих действий, а также использования руководством результатов анализа СМИБ (см. раздел 7).

8.2 Корректирующие действия

Организация должна проводить мероприятия по устранению причин несоответствий требованиям СМИБ с целью предупредить их повторное возникновение. Документированная процедура корректирующего действия должна устанавливать требования по:

a) выявлению несоответствий;
b) определению причин несоответствий;
c) оцениванию необходимости действий во избежание повторения несоответствий;
d) определению и реализации необходимых корректирующих действий;
e) ведению записей результатов предпринятых действий (см. 4.3.3);
f) анализу предпринятого корректирующего действия.

8.3 Предупреждающие действия

Организация должна определять действия, необходимые для устранения причин потенциальных несоответствий требованиям СМИБ, с целью предотвратить их повторное появление. Предпринимаемые предупреждающие действия должны соответствовать последствиям потенциальных проблем. Документированная процедура предпринятого предупреждающего действия должна устанавливать требования по:

a) выявлению потенциальных несоответствий и их причин;
b) оцениванию необходимости действия с целью предупредить появление несоответствий;
c) определению и реализации необходимого предупреждающего действия;
d) записи результатов предпринятого действия (см. 4.3.3);
e) анализу результатов предпринятого действия.

Организация должна определить изменения в оценках рисков и установить требования к предупреждающим действиям, при этом обращая особое внимание на существенно измененные количественные показатели рисков.

Приоритеты в отношении реализации предупреждающих действий должны быть определены на основе результатов оценки риска.

Примечание — Обычно затраты на проведение мероприятий по предотвращению несоответствий более экономичны, чем на корректирующие действия.

Приложение А
(рекомендуемое)

Цели и меры управления

Цели и меры управления, перечисленные в таблице А.1, непосредственно взяты из перечня целей и мер управления, приведенного в ИСО/МЭК 17799:2005, разделы 5—15, и полностью с ним согласованы. Перечень мер управления, содержащийся в данной таблице, не является исчерпывающим, и организация может рассмотреть необходимость дополнительных целей и мер управления. Выбор целей и мер управления и контроля, приведенных в таблице, должен быть осуществлен в соответствии с разделом 4.

В разделах 5—15 ИСО/МЭК 17799:2005 приведены рекомендации по реализации и указания с точки зрения передовой практики в отношении поддержки мер управления, изложенных в А.5—А.15.

Таблица А.1 — Цели и меры управления

А.5 Политика безопасности		
А.5.1 Политика информационной безопасности		
Цель: Обеспечить участие высшего руководства организации в решении вопросов, связанных с обеспечением информационной безопасности в соответствии с целями деятельности организации (бизнеса), законами и нормативными актами		
А.5.1.1	Документирование политики информационной безопасности	Политика информационной безопасности должна быть руководством утверждена, издана и доведена до сведения всех сотрудников организации, а также сторонних организаций
А.5.1.2	Анализ политики информационной безопасности	Политика информационной безопасности организации должна быть подвергнута анализу и пересмотру через заданные промежутки времени или при появлении существенных изменений характеристик целей безопасности
А.6 Организация информационной безопасности		
А.6.1 Внутренняя организация		
Цель: Обеспечение управления информационной безопасностью в организации		
А.6.1.1	Обязанности руководства по обеспечению информационной безопасности	Руководство организации должно постоянно поддерживать заданный уровень информационной безопасности путем внедрения системы менеджмента, а также путем распределения обязанностей и ответственности персонала за ее обеспечение
А.6.1.2	Координация вопросов обеспечения информационной безопасности	Действия по обеспечению информационной безопасности должны координироваться представителями различных подразделений организации, имеющими соответствующие функции и должностные обязанности
А.6.1.3	Распределение обязанностей по обеспечению информационной безопасности	Обязанности персонала по обеспечению информационной безопасности должны быть четко определены
А.6.1.4	Процедура получения разрешения на использование средств обработки информации	Руководство должно определить и внедрить процедуры получения разрешения на использование новых средств обработки информации
А.6.1.5	Соглашения о соблюдении конфиденциальности	Руководство организации должно определять условия конфиденциальности или вырабатывать соглашения о неразглашении информации в соответствии с целями защиты информации и регулярно их пересматривать
А.6.1.6	Взаимодействие с компетентными органами	Руководство организации должно поддерживать взаимодействие с соответствующими компетентными органами
А.6.1.7	Взаимодействие с ассоциациями и профессиональными группами	Руководство организации должно поддерживать соответствующее взаимодействие с профессиональными группами, ассоциациями и участвовать (организовывать) в конференциях (форумах) специалистов в области информационной безопасности

Продолжение таблицы А.1

А.6.1.8	Независимая проверка (аудит) информационной безопасности	Порядок организации и управления информационной безопасностью и ее реализация (например, изменение целей и мер управления, политики, процессов и процедур обеспечения информационной безопасности) должны быть подвергнуты независимой проверке (аудиту) через определенные промежутки времени или при появлении существенных изменений в способах реализации мер безопасности
А.6.2 Обеспечение безопасности при наличии доступа сторонних организаций к информационным системам Цель: Поддерживать безопасность информации и средств обработки информации организации при наличии доступа к ним сторонних организаций в процессах обработки и передачи этой информации		
А.6.2.1	Определение рисков, связанных со сторонними организациями	Перед предоставлением доступа сторонним организациям к информации и средствам ее обработки в процессе деятельности организации необходимо определять возможные риски для информации и средств ее обработки и реализовывать соответствующие им меры безопасности
А.6.2.2	Рассмотрение вопросов безопасности при работе с клиентами	Перед предоставлением клиентам права доступа к информации или активам организации необходимо определить и внедрить меры безопасности
А.6.2.3	Рассмотрение требований безопасности в соглашениях со сторонними организациями	Соглашения со сторонними организациями должны содержать все требования безопасности, включающие в себя правила доступа к процессам обработки, передачи информации или к управлению информацией или средствами обработки информации организации, а также и в случае приобретения дополнительных программных продуктов или организации сервисного обслуживания средств обработки информации
А.7 Управление активами		
А.7.1 Ответственность за защиту активов организации Цель: Обеспечивать соответствующую защиту активов организации		
А.7.1.1	Инвентаризация активов	Опись всех важных активов организации должна быть составлена и актуализирована
А.7.1.2	Владение активами	Вся информация и активы, связанные со средствами обработки информации, должны иметь назначенного во владение[1)] представителя организации
А.7.1.3	Приемлемое использование активов	Правила безопасного использования информации и активов, связанных со средствами обработки информации, должны быть определены, документированы и реализованы
А.7.2 Классификация информации Цель: Обеспечить уверенность в том, что информация защищена на надлежащем уровне		
А.7.2.1	Основные принципы классификации	Информация должна быть классифицирована исходя из правовых требований, ее конфиденциальности, а также ценности и критичности для организации
А.7.2.2	Маркировка и обработка информации	В соответствии с принятой в организации системой классификации должна быть разработана и реализована совокупность процедур маркировки и обработки информации

[1)] Термин «владелец» (owner) определен как лицо или организация, на которую возложена установленная ответственность управления по контролю производства, разработке, поддержке, использованию и безопасности активов. Термин «владелец» не означает, что данное лицо фактически имеет права собственности на этот актив.

Продолжение таблицы А.1

А.8 Правила безопасности, связанные с персоналом		
А.8.1 Перед трудоустройством[1)] Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации осознают свою ответственность и способны выполнять предусмотренные для них функции и снижать риск от воровства, мошенничества и нецелевого использования оборудования, а также от угроз безопасности информации		
А.8.1.1	Функции и обязанности персонала по обеспечению безопасности	Функции и обязанности персонала по обеспечению безопасности сотрудников, подрядчиков и пользователей сторонней организации должны быть определены и документированы в соответствии с требованиями информационной безопасности
А.8.1.2	Проверка при приеме на работу	Проверка всех кандидатов на постоянную работу, подрядчиков и пользователей сторонней организации должна быть проведена в соответствии с законами, инструкциями и правилами этики, с учетом требований бизнеса, характера информации, к которой будет осуществлен их доступ, и предполагаемых рисков
А.8.1.3	Условия трудового договора	Сотрудники, подрядчики и пользователи сторонней организации должны согласовать и подписать условия своего трудового договора, в котором установлены их ответственность и ответственность организации относительно информационной безопасности
А.8.2 Работа по трудовому договору Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации осведомлены об угрозах и проблемах информационной безопасности, об их ответственности и обязательствах, ознакомлены с правилами и обучены процедурам для поддержания мер безопасности организации при выполнении ими своих служебных обязанностей и для снижения риска человеческого фактора для информационной безопасности		
А.8.2.1	Обязанности руководства	Руководство организации должно требовать, чтобы сотрудники, подрядчики и пользователи сторонней организации были ознакомлены с правилами и процедурами обеспечения мер безопасности в соответствии с установленными требованиями
А.8.2.2	Осведомленность, обучение и переподготовка в области информационной безопасности	Все сотрудники организации и, при необходимости, подрядчики и пользователи сторонних организаций должны проходить соответствующее обучение и переподготовку в целях регулярного получения информации о новых требованиях правил и процедур организации безопасности, необходимых для выполнения ими должностных функций
А.8.2.3	Дисциплинарная практика	К сотрудникам, совершившим нарушение требований безопасности, должна быть применена дисциплинарная практика, установленная в организации
А.8.3 Увольнение или изменение трудового договора Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации уведомлены об увольнении или изменении условий трудового договора в соответствии с установленным порядком		
А.8.3.1	Ответственность по окончании действия трудового договора	Ответственность по окончании действия трудового договора должна быть четко определена и установлена
А.8.3.2	Возврат активов	Сотрудники, подрядчики и пользователи сторонней организации обязаны вернуть все активы организации, находящиеся в их пользовании (владении), по истечении срока действия трудового договора или соглашения (увольнение)
А.8.3.3	Аннулирование прав доступа	Права доступа к информации и средствам обработки информации сотрудников, подрядчиков и пользователей сторонней организации должны быть аннулированы или уточнены по окончании действия трудового договора (увольнение)

[1)] Под словом «трудоустройство» (employment) здесь поняты следующие ситуации: прием на работу (временную или постоянную), назначение на должность или перевод на другую должность, переоформление контрактов или аннулирование каких-либо из этих ситуаций.

Продолжение таблицы А.1

А.9 Физическая защита и защита от воздействия окружающей среды		
А.9.1 Охраняемые зоны Цель: Предотвращать несанкционированные физический доступ, повреждение и воздействия на помещения и информацию организации		
А.9.1.1	Периметр охраняемой зоны	Для защиты зон, где имеются информация и средства обработки информации, должны быть использованы периметры охраняемых зон (барьеры, такие как стены, проходные, оборудованные средствами контроля входа по идентификационным карточкам, или, где предусмотрен, контроль сотрудника регистрационной стойки)
А.9.1.2	Контроль доступа в охраняемую зону	Охраняемая зона должна быть защищена соответствующими средствами контроля входа, предполагающими обеспечить уверенность в том, что только авторизованный персонал может получить доступ в зону
А.9.1.3	Обеспечение безопасности зданий, производственных помещений и оборудования	Требования к обеспечению физической безопасности зданий, производственных помещений и оборудования должны быть разработаны и реализованы
А.9.1.4	Защита от внешних угроз и угроз со стороны окружающей среды	Требования к обеспечению физической защиты зданий, производственных помещений и оборудования от нанесения ущерба в результате пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других природных и антропогенных факторов должны быть разработаны и реализованы
А.9.1.5	Выполнение работ в охраняемых зонах	Требования по физической защите и рекомендации по выполнению работ в охраняемых зонах должны быть разработаны и реализованы в инструкциях
А.9.1.6	Зоны общественного доступа, приема и отгрузки материальных ценностей	Места доступа, такие как зоны приема, отгрузки материальных ценностей и другие места, где неавторизованные лица могут проникнуть в помещения, должны быть под контролем и, по возможности, должны быть изолированы от средств обработки информации во избежание несанкционированного доступа
А.9.2 Безопасность оборудования Цель: Предотвращать потерю, повреждение, хищение или компрометацию активов и прекращение деятельности организации		
А.9.2.1	Размещение и защита оборудования	Оборудование должно быть размещено и защищено так, чтобы уменьшить риски от воздействия окружающей среды и возможности несанкционированного доступа
А.9.2.2	Вспомогательные услуги	Оборудование необходимо защищать от перебоев в подаче электроэнергии и других сбоев, связанных с отказами в обеспечении вспомогательных услуг
А.9.2.3	Безопасность кабельной сети	Силовые и телекоммуникационные кабельные сети, по которым передаются данные или поддерживаются информационные услуги, необходимо защищать от перехвата информации или повреждения
А.9.2.4	Техническое обслуживание оборудования	Должно проводиться надлежащее регулярное техническое обслуживание оборудования для обеспечения его непрерывной работоспособности и сохранности
А.9.2.5	Обеспечение безопасности оборудования, используемого вне помещений организации	При обеспечении безопасности оборудования, используемого вне места его постоянной эксплуатации, должны быть учтены различные риски, связанные с работой вне помещений организации
А.9.2.6	Безопасная утилизация или повторное использование оборудования	Все компоненты оборудования, содержащие носители данных, должны быть проверены с целью удостовериться в том, что любые конфиденциальные данные и лицензионное программное обеспечение были удалены или скопированы безопасным образом до их утилизации (списания)
А.9.2.7	Вынос имущества с территории организации	Оборудование, информацию или программное обеспечение допускается выносить из помещения организации только на основании соответствующего разрешения

Продолжение таблицы А.1

А.10 Управление средствами коммуникаций и их функционированием		
А.10.1 Эксплуатация средств и ответственность Цель: Обеспечить надлежащее и безопасное функционирование средств обработки информации		
А.10.1.1	Документирование операционных процедур эксплуатации	Операционные процедуры должны документироваться, поддерживаться и быть доступными для всех авторизованных пользователей
А.10.1.2	Управление изменениями	Изменения в конфигурациях средств обработки информации и системах должны быть контролируемыми
А.10.1.3	Разграничение обязанностей	Обязанности и области ответственности должны быть разграничены в целях снижения возможностей несанкционированной или непреднамеренной модификации, или нецелевого использования активов организации
А.10.1.4	Разграничение средств разработки, тестирования и эксплуатации	Средства разработки, тестирования и эксплуатации должны быть разграничены в целях снижения риска несанкционированного доступа или изменения операционной системы
А.10.2 Управление поставкой услуг лицами и/или сторонними организациями Цель: Реализовать и поддерживать требуемый уровень информационной безопасности и оказания услуг в соответствии с договорами об оказании услуг сторонними организациями (внешними лицами и/или организациями)		
А.10.2.1	Оказание услуг	Должна быть обеспечена уверенность в том, что меры управления информационной безопасностью, включенные в договор об оказании услуг сторонней организации, реализованы, функционируют и поддерживаются сторонней организацией
А.10.2.2	Мониторинг и анализ услуг, оказываемых сторонними лицами и/или организациями	Необходимо регулярно проводить мониторинг, аудит и анализ услуг, отчетов и актов, обеспечиваемых сторонней организацией
А.10.2.3	Изменения при оказании сторонними организациями услуг по обеспечению безопасности	Изменения при оказании услуг по обеспечению безопасности, включая внедрение и совершенствование существующих требований, процедур и мер обеспечения информационной безопасности, должны быть управляемыми с учетом оценки критичности систем и процессов бизнеса, а также результатов переоценки рисков
А.10.3 Планирование производительности и загрузки систем Цель: Свести к минимуму риск сбоев в работе систем		
А.10.3.1	Управление производительностью	Необходимо осуществлять прогнозирование, мониторинг и корректировку потребности мощности системы для обеспечения требуемой ее производительности
А.10.3.2	Приемка систем	Должны быть определены критерии принятия новых и модернизированных информационных систем, новых версий программного обеспечения, а также проведено тестирование систем в процессе их разработки и приемки
А.10.4 Защита от вредоносного кода и мобильного кода Цель: Защищать целостность программного обеспечения и массивов информации		
А.10.4.1	Меры защиты от вредоносного кода	Должны быть реализованы меры по обнаружению, предотвращению проникновения и восстановлению после проникновения вредоносного кода, а также должны быть установлены процедуры обеспечения соответствующего оповещения пользователей
А.10.4.2	Меры защиты от мобильного кода	Там, где разрешено использование мобильного кода, конфигурация системы должна обеспечивать уверенность в том, что авторизованный мобильный код функционирует в соответствии с четко определенной политикой безопасности, а исполнение операции с использованием неавторизованного мобильного кода будет предотвращено

Продолжение таблицы А.1

А.10.5 Резервирование		
Цель: Поддерживать целостность и доступность информации и средств обработки информации		
А.10.5.1	Резервирование информации	Резервные копии информации и программного обеспечения должны создаваться, проверяться и тестироваться на регулярной основе в соответствии с принятыми требованиями резервирования
А.10.6 Управление безопасностью сети		
Цель: Обеспечить защиту информации в сетях и защиту поддерживающей инфраструктуры		
А.10.6.1	Средства контроля сети	Сети должны быть адекватно управляемыми и контролируемыми в целях защиты от угроз и поддержания безопасности систем и приложений, использующих сеть, включая информацию, передаваемую по сетям
А.10.6.2	Безопасность сетевых сервисов	Меры обеспечения безопасности, уровни обслуживания для всех сетевых услуг и требования управления должны быть определены и включены в любой договор о сетевых услугах независимо от того, предоставляются ли эти услуги своими силами или сторонней организацией
А.10.7 Обращение с носителями информации		
Цель: Предотвратить несанкционированное разглашение, модификацию, удаление или уничтожение активов и прерывание бизнес-процессов		
А.10.7.1	Управление съемными носителями информации	Для управления съемными носителями информации должны существовать соответствующие процедуры
А.10.7.2	Утилизация носителей информации	Носители информации, когда в них больше нет необходимости, должны быть надежно и безопасно утилизированы с помощью формализованных процедур
А.10.7.3	Процедуры обработки информации	Для обеспечения защиты информации от несанкционированного раскрытия или неправильного использования необходимо установить процедуры обработки и хранения информации
А.10.7.4	Безопасность системной документации	Системная документация должна быть защищена от несанкционированного доступа
А.10.8 Обмен информацией		
Цель: Поддерживать безопасность информации и программного обеспечения при обмене внутри организации и со сторонними организациями		
А.10.8.1	Политики и процедуры обмена информацией	Должны существовать формализованные процедуры, требования и меры контроля, обеспечивающие защиту обмена информацией при использовании связи всех типов
А.10.8.2	Соглашения по обмену информацией	Между организацией и сторонними организациями должны быть заключены соглашения по обмену информацией и программным обеспечением
А.10.8.3	Защита физических носителей информации при транспортировке	Носители информации должны быть защищены от несанкционированного доступа, неправильного использования или повреждения во время их транспортировки за пределами территории организации
А.10.8.4	Электронный обмен сообщениями	Информация, используемая в электронном обмене сообщениями, должна быть защищена надлежащим образом
А.10.8.5	Системы бизнес-информации	Требования и процедуры должны быть разработаны и внедрены для защиты информации, связанной с взаимодействием систем бизнес-информации
А.10.9 Услуги электронной торговли		
Цель: Обеспечить безопасность услуг электронной торговли и их безопасное использование		
А.10.9.1	Электронная торговля	Информация, используемая в электронной торговле, проходящая по общедоступным сетям, должна быть защищена от мошенничества, оспаривания контрактов, а также от несанкционированного разглашения и модификации

Продолжение таблицы А.1

А.10.9.2	Трансакции в режиме реального времени (on-line)	Информация, используемая в трансакциях в режиме реального времени (on-line), должна быть защищена для предотвращения неполной передачи, неправильной маршрутизации, несанкционированного изменения сообщений, несанкционированного разглашения, несанкционированного копирования или повторного воспроизведения сообщений
А.10.9.3	Общедоступная информация	Информация, предоставляемая через общедоступную систему, должна быть защищена от несанкционированной модификации
А.10.10 Мониторинг		
Цель: Обнаруживать несанкционированные действия, связанные с обработкой информации		
А.10.10.1	Ведение журналов аудита	Должны быть обеспечены ведение и хранение в течение определенного периода времени журналов аудита, регистрирующих действия пользователей, нештатные ситуации и события информационной безопасности, в целях помощи в будущих расследованиях и проведении мониторинга контроля доступа
А.10.10.2	Мониторинг использования средств обработки информации	Должны быть установлены процедуры, позволяющие вести мониторинг и регулярный анализ результатов мониторинга использования средств обработки информации
А.10.10.3	Защита информации журналов регистрации	Средства регистрации и информация журналов регистрации должны быть защищены от вмешательства и несанкционированного доступа
А.10.10.4	Журналы регистрации действий администратора и оператора	Действия системного администратора и системного оператора должны быть регистрируемыми
А.10.10.5	Регистрация неисправностей	Неисправности должны быть зарегистрированы, проанализированы и устранены
А.10.10.6	Синхронизация часов	Часы всех соответствующих систем обработки информации в пределах организации или охраняемой зоны должны быть синхронизированы с помощью единого источника точного времени
А.11 Контроль доступа		
А.11.1 Бизнес-требования к контролю доступа		
Цель: Контролировать доступ к информации		
А.11.1.1	Политика контроля доступа	Политика контроля доступа должна быть установлена и документирована с учетом потребностей бизнеса и безопасности информации
А.11.2 Управление доступом пользователей		
Цель: Предотвратить несанкционированный доступ пользователей к информационным системам и обеспечить авторизованный доступ пользователей к этим системам		
А.11.2.1	Регистрация пользователей	Должна быть установлена формализованная процедура регистрации и снятия с регистрации пользователей для предоставления и отмены доступа ко всем информационным системам и услугам
А.11.2.2	Управление привилегиями	Предоставление и использование привилегий должно быть ограниченным и контролируемым
А.11.2.3	Управление паролями пользователей	Предоставление паролей должно быть контролируемым посредством формализованного процесса управления
А.11.2.4	Пересмотр прав доступа пользователей	Руководство должно периодически осуществлять пересмотр прав доступа пользователей, используя формализованный процесс
А.11.3 Ответственность пользователей		
Цель: Предотвращать несанкционированный доступ пользователей, а также компрометацию или кражу информации и средств обработки информации		
А.11.3.1	Использование паролей	Пользователи должны соблюдать правила безопасности при выборе и использовании паролей

Продолжение таблицы А.1

А.11.3.2	Оборудование, оставленное пользователем без присмотра	Пользователи должны обеспечивать соответствующую защиту оборудования, оставленного без присмотра
А.11.3.3	Правила «чистого стола» и «чистого экрана»	Должны быть приняты правила «чистого стола» для документов на бумажных носителях и сменных носителей данных, а также правила «чистого экрана» для средств обработки информации
А.11.4 Контроль сетевого доступа Цель: Предотвратить несанкционированный доступ к сетевым сервисам		
А.11.4.1	Политика в отношении использования сетевых услуг	Пользователям следует предоставлять доступ только к тем услугам, по отношению к которым они специально были авторизованы
А.11.4.2	Аутентификация пользователей для внешних соединений	Для контроля доступа удаленных пользователей должны быть применены соответствующие методы аутентификации
А.11.4.3	Идентификация оборудования в сетях	Автоматическая идентификация оборудования должна рассматриваться как средство аутентификации соединений, осуществляемых с определенных мест и с определенным оборудованием
А.11.4.4	Защита диагностических и конфигурационных портов при удаленном доступе	Физический и логический доступ к портам конфигурации и диагностики должен быть контролируемым
А.11.4.5	Принцип разделения в сетях	В сетях должны быть применены принципы разделения групп информационных услуг, пользователей и информационных систем
А.11.4.6	Контроль сетевых соединений	Подключение пользователей к совместно используемым сетям, особенно к тем, которые выходят за территорию организации, необходимо ограничивать в соответствии с политикой контроля доступа и требованиями бизнес-приложений (см. А.11.1)
А.11.4.7	Контроль маршрутизации в сети	Должны быть внедрены средства управления и контроля маршрутизации в сети с целью исключить нарушения правил контроля доступа для бизнес-приложений, вызываемые соединениями и потоками информации
А.11.5 Контроль доступа к операционной системе Цель: Предотвратить несанкционированный доступ к операционным системам		
А.11.5.1	Безопасные процедуры регистрации	Контроль доступа к операционным системам должен быть обеспечен безопасной процедурой регистрации
А.11.5.2	Идентификация и аутентификация пользователя	Все пользователи должны иметь уникальные идентификаторы (ID) только для персонального использования, а для подтверждения заявленной личности пользователя должны быть выбраны подходящие методы аутентификации
А.11.5.3	Система управления паролями	Системы управления паролями должны быть интерактивными и обеспечивать высокое качество паролей
А.11.5.4	Использование системных утилит	Использование системных утилит, которые могут преодолеть средства контроля операционных систем и приложений, необходимо ограничивать и строго контролировать
А.11.5.5	Периоды бездействия в сеансах связи	Необходимо обеспечить завершение сеансов связи после определенного периода бездействия
А.11.5.6	Ограничение времени соединения	Ограничение времени соединения должно быть использовано для обеспечения дополнительной безопасности
А.11.6 Контроль доступа к прикладным системам и информации Цель: Предотвратить несанкционированный доступ к прикладным системам и информации		
А.11.6.1	Ограничения доступа к информации	Доступ к информации и функциям прикладных систем пользователей и обслуживающего персонала должен быть предоставлен только в соответствии с определенными политиками контроля доступа

Продолжение таблицы А.1

А.11.6.2	Изоляция систем, обрабатывающих важную информацию	Системы, обрабатывающие важную информацию, должны иметь выделенную (изолированную) вычислительную среду
А.11.7 Работа с переносными устройствами и работа в дистанционном режиме Цель: Обеспечить информационную безопасность при использовании переносных устройств и средств, необходимых для работы в дистанционном режиме		
А.11.7.1	Работа с переносными устройствами	Необходимо иметь в наличии формализованную политику для защиты от рисков при использовании переносных устройств
А.11.7.2	Работа в дистанционном режиме	Для работы в дистанционном режиме необходимо разработать и реализовать политику, оперативные планы и процедуры
А.12 Разработка, внедрение и обслуживание информационных систем		
А.12.1 Требования к безопасности информационных систем Цель: Обеспечить уверенность в том, что безопасность является неотъемлемым свойством внедряемых информационных систем, и обеспечить выполнение требований безопасности при разработке и эксплуатации систем		
А.12.1.1	Анализ и детализация требований безопасности	В формулировках требований бизнеса для новых информационных систем или совершенствования существующих должны быть детализированы требования безопасности
А.12.2 Правильная обработка данных в приложениях Цель: Предотвратить ошибки, потерю, несанкционированную модификацию или неправильное использование информации в приложениях		
А.12.2.1	Проверка достоверности входных данных	Входные данные для приложений должны быть подвергнуты процедуре подтверждения с целью установления их достоверности
А.12.2.2	Контроль обработки данных в приложениях	Для обнаружения искажений (ошибок или преднамеренных действий) при обработке информации в требования к функциям приложений должны быть включены требования по выполнению контрольных проверок
А.12.2.3	Целостность сообщений	Должны быть определены требования для обеспечения аутентичности и защиты целостности сообщений в приложениях, а также реализованы соответствующие средства контроля
А.12.2.4	Подтверждение достоверности выходных данных	Данные, выводимые из приложения, необходимо подвергать проверке на корректность, чтобы обеспечить уверенность в том, что обработка информации выполнена правильно
А.12.3 Криптографические средства защиты Цель: Защищать конфиденциальность, аутентичность или целостность информации криптографическими средствами		
А.12.3.1	Политика использования криптографических средств защиты	Должны быть разработаны и внедрены правила использования криптографических средств защиты информации
А.12.3.2	Управление ключами	Для реализации организацией криптографических методов защиты должна быть использована система управления ключами
А.12.4 Безопасность системных файлов Цель: Обеспечить безопасность системных файлов		
А.12.4.1	Контроль программного обеспечения, находящегося в промышленной эксплуатации	Необходимо обеспечить контроль за процессом внедрения программного обеспечения в промышленную эксплуатацию
А.12.4.2	Защита данных тестирования системы	Данные тестирования следует тщательно отбирать, защищать и контролировать
А.12.4.3	Контроль доступа к исходным кодам	Доступ к исходным кодам должен быть ограничен

Продолжение таблицы А.1

А.12.5 Безопасность в процессах разработки и поддержки		
Цель: Поддерживать безопасность программного обеспечения прикладных систем и содержащейся в них информации		
А.12.5.1	Процедуры контроля изменений	Внесение изменений должно быть проверено с использованием соответствующих формализованных процедур контроля изменений
А.12.5.2	Технический анализ прикладных систем после внесения изменений в операционные системы	При внесении изменений в операционные системы необходимо провести анализ и тестирование критичных бизнес-приложений с целью удостовериться в отсутствии негативного влияния на работу и безопасность организации
А.12.5.3	Ограничения на внесение изменений в пакеты программ	Необходимо избегать модификаций пакетов программ, а все требуемые изменения должны подлежать строгому контролю
А.12.5.4	Утечка информации	Возможности для утечки информации должны быть предотвращены
А.12.5.5	Разработка программного обеспечения с привлечением сторонних организаций	Разработка программного обеспечения с привлечением сторонних организаций должна проводиться под контролем и при мониторинге организации
А.12.6 Менеджмент технических уязвимостей		
Цель: Снизить риски, являющиеся результатом использования опубликованных технических уязвимостей		
А.12.6.1	Управление техническими уязвимостями	Необходимо получать своевременную информацию о технических уязвимостях используемых информационных систем, оценивать опасность таких уязвимостей и принимать соответствующие меры по устранению связанного с ними риска
А.13 Управление инцидентами информационной безопасности		
А.13.1 Оповещение о нарушениях и недостатках информационной безопасности		
Цель: Обеспечить оперативность оповещения о событиях информационной безопасности и нарушениях, связанных с информационными системами, а также своевременность корректирующих действий		
А.13.1.1	Оповещение о случаях нарушения информационной безопасности	О случаях нарушения информационной безопасности следует сообщать по соответствующим каналам управления незамедлительно, насколько это возможно
А.13.1.2	Оповещение о недостатках безопасности	Все сотрудники, подрядчики и пользователи сторонних организаций, пользующиеся информационными системами и услугами, должны незамедлительно сообщать о любых замеченных или предполагаемых нарушениях безопасности в системах или услугах
А.13.2 Управление инцидентами информационной безопасности и его усовершенствование		
Цель: Обеспечить последовательный и эффективный подход к управлению инцидентами информационной безопасности		
А.13.2.1	Ответственность и процедуры	Должны быть установлены ответственность руководства и процедуры, позволяющие обеспечить быстрое, эффективное и последовательное реагирование на инциденты информационной безопасности
А.13.2.2	Извлечение уроков из инцидентов информационной безопасности	Должны быть определены механизмы, позволяющие вести мониторинг и регистрацию инцидентов информационной безопасности по типам, объемам и стоимостям
А.13.2.3	Сбор доказательств	На случай, если инцидент информационной безопасности может привести к судебному разбирательству (гражданскому или уголовному) против лица или организации, информация должна быть собрана, сохранена и представлена согласно правилам оформления доказательств, изложенным в соответствующих документах

Продолжение таблицы А.1

А.14 Управление непрерывностью бизнеса		
А.14.1 Вопросы информационной безопасности управления непрерывностью бизнеса Цель: На случай, если инцидент информационной безопасности может привести к судебному разбирательству (гражданскому или уголовному) против лица или организации, информация должна быть собрана, сохранена и представлена согласно правилам оформления доказательств, изложенным в соответствующих документах		
А.14.1.1	Включение информационной безопасности в процесс управления непрерывностью бизнеса	Должен быть разработан и поддержан управляемый процесс обеспечения непрерывности бизнеса во всей организации с учетом требований информационной безопасности, необходимых для обеспечения непрерывности бизнеса организации
А.14.1.2	Непрерывность бизнеса и оценка риска	События, которые могут стать причиной прерывания бизнес-процессов, должны быть связаны с оценками вероятности и степени воздействия таких прерываний, а также с их последствиями для информационной безопасности
А.14.1.3	Разработка и внедрение планов непрерывности бизнеса, включающих в себя информационную безопасность	Должны быть разработаны и внедрены планы для поддержки или восстановления работы и обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или отказа критических бизнес-процессов
А.14.1.4	Структура плана обеспечения непрерывности бизнеса	Должна быть создана единая структура планов непрерывности бизнеса, позволяющая обеспечить непротиворечивость всех планов для последовательного выполнения всех требований к информационной безопасности и для расстановки приоритетов при тестировании и обслуживании
А.14.1.5	Тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса	Планы по обеспечению непрерывности бизнеса должны подлежать регулярному пересмотру и обновлению с целью обеспечить их актуальность и эффективность
А.15 Соответствие требованиям		
А.15.1 Соответствие правовым требованиям Цель: Предотвращать любые нарушения норм уголовного и гражданского права, требований, установленных нормативно-правовыми актами, регулирующими органами или договорными обязательствами, а также требований безопасности		
А.15.1.1	Определение применимых норм	Все применимые нормы, установленные законодательством и исполнительными органами власти, требования договорных обязательств и порядок их выполнения следует четко определить, документировать и поддерживать на актуальном уровне для каждой информационной системы и организации
А.15.1.2	Права на интеллектуальную собственность	Должны быть внедрены соответствующие процедуры для применения законодательных, регулирующих и контрактных требований к используемым материалам с учетом прав на интеллектуальную собственность, а также прав на использование программных продуктов, являющихся предметом частной собственности
А.15.1.3	Защита учетных записей организации	Важные учетные записи организации должны быть защищены от утраты, разрушения и фальсификации в соответствии с требованиями, установленными законами, документами органов исполнительной власти, контрактами и требованиями бизнеса
А.15.1.4	Защита данных и конфиденциальность персональной информации	Защита данных и конфиденциальность персональной информации должны быть обеспечены в соответствии с требованиями законов, нормативных актов и, где это применимо, в соответствии с положениями контрактов

Окончание таблицы А.1

А.15.1.5	Предотвращение нецелевого использования средств обработки информации	Должны быть применены меры контроля для предотвращения нецелевого использования средств обработки информации
А.15.1.6	Регулирование использования средств криптографической защиты	Средства криптографической защиты должны быть использованы в соответствии с законами, нормативными актами и соответствующими соглашениями
А.15.2 Соответствие политикам и стандартам безопасности и техническое соответствие требованиям безопасности Цель: Обеспечить соответствие систем организационным политикам и стандартам безопасности		
А.15.2.1	Соответствие политикам и стандартам безопасности	Руководители должны обеспечить, чтобы все процедуры безопасности в их сфере ответственности были выполнены правильно и соответствовали политикам и стандартам безопасности
А.15.2.2	Проверка технического соответствия требованиям безопасности	Информационные системы следует регулярно проверять на соответствие требованиям стандартов безопасности
А.15.3 Вопросы аудита информационных систем Цель: Повышение эффективности процесса аудита информационных систем и снижение негативного влияния, связанного с данным процессом		
А.15.3.1	Меры управления аудитом информационных систем	Требования и процедуры аудита, включающие в себя проверки операционных систем, необходимо тщательно планировать и согласовывать, чтобы свести к минимуму риск прерывания бизнес-процессов
А.15.3.2	Защита инструментальных средств аудита информационных систем	Доступ к инструментальным средствам аудита информационных систем необходимо защищать для предотвращения любой возможности их неправильного использования или компрометации

Приложение В
(справочное)

Принципы Организации экономического сотрудничества и развития и настоящий стандарт

Принципы, представленные в Руководстве ОЭСР по обеспечению безопасности информационных систем и сетей [1], применимы ко всем уровням политики и эксплуатации, которые определяют безопасность информационных систем и сетей. Настоящий стандарт предлагает концептуальную основу системы менеджмента информационной безопасности для реализации некоторых из принципов ОЭСР с использованием модели PDCA и процессов, описанных в разделах 4, 5, 6 и 8. Принципы ОЭСР и модель PDCA приведены в таблице В.1.

Таблица В.1 — Принципы ОЭСР и модель PDCA

Принцип ОЭСР	Соответствующий процесс СМИБ и стадия PDCA
Осведомленность Участники должны быть осведомлены о необходимости обеспечения безопасности информационных систем и сетей и о том, что они могут сделать для повышения уровня безопасности	Данные мероприятия являются частью стадии «Осуществление» (см. 4.2.2 и 5.2)
Ответственность Все участники являются ответственными за безопасность информационных систем и сетей	Данные мероприятия являются частью стадии «Осуществление» (см. 4.2.2 и 5.1)
Реагирование Участники должны действовать совместно и своевременно, чтобы предотвращать, обнаруживать инциденты безопасности и реагировать на них	Является частью стадии «Проверка» деятельности по мониторингу (см. 4.2.3, раздел 6 и 7.3) и мероприятий по реагированию стадии «Действие» (см. 4.2.4, 8.1, 8.2 и 8.3). Данные мероприятия могут быть также охвачены некоторыми элементами стадий «Планирование» и «Проверка»
Оценка риска Участники должны проводить оценку рисков	Этот вид деятельности является частью стадии «Планирование» (см. 4.2.1), а повторная оценка (переоценка) риска является частью стадии «Проверка» (см. 4.2.3, раздел 6 и 7.3)
Разработка и внедрение безопасности Участники должны внедрить безопасность как важный элемент информационных систем и сетей	После выполнения оценки рисков выбирают меры управления для обработки рисков как часть стадии «Планирование» (см. 4.2.1). Стадия «Осуществление» (см. 4.2.2 и 5.2) охватывает затем внедрение и обеспечение функционирования этих мер управления
Менеджмент безопасности Участники должны применять всесторонний подход к менеджменту безопасности	Менеджмент рисков представляет собой процесс, включающий в себя предотвращение, обнаружение инцидентов и реагирование на них, сопровождение, анализ и аудит. Все эти вопросы решают на стадиях «Планирование», «Осуществление», «Проверка» и «Действие»
Повторная оценка Участники должны анализировать и повторно оценивать состояние безопасности информационных систем и сетей, и вносить соответствующие изменения в политику, практику, меры и процедуры безопасности	Переоценка (повторная оценка) информационной безопасности является частью стадии «Проверка» (см. 4.2.3, раздел 6 и 7.3), на которой должны быть предприняты регулярные анализы эффективности системы менеджмента информационной безопасности, а повышение уровня безопасности является частью стадии «Действие» (см. 4.2.4, 8.1, 8.2 и 8.3)

Приложение С
(справочное)

Сравнение структуры настоящего стандарта со структурами международных стандартов ИСО 9001:2000, ИСО 14001:2004

В таблице С.1 приведено сравнение структур ИСО 9001:2000, ИСО 14001:2004 и настоящего стандарта.

Таблица С.1 — Сравнение структур ИСО 9001:2000, ИСО 14001:2004 и настоящего стандарта

Настоящий стандарт	ИСО 9001: 2000	ИСО 14001:2004
Введение	Введение	Введение
Общие положения	Общие положения	
Процессный подход	Процессный подход Связь с ИСО 9004 [9]	
Возможность совместного использования с другими системами управления	Совместимость с другими системами менеджмента	
1 Область применения	1 Область применения	1 Область применения
1.1 Общие положения	1.1 Общие положения	
1.2 Применение	1.2 Применение	
2 Нормативные ссылки	2 Нормативные ссылки	2 Нормативные ссылки
3 Термины и определения	3 Термины и определения	3 Термины и определения
4 Система менеджмента информационной безопасности	4 Система менеджмента качества	4 Требования системы управления в области охраны окружающей среды
4.1 Общие требования	4.1 Общие требования	4.1 Общие требования
4.2 Разработка СМИБ. Управление СМИБ		
4.2.1 Разработка СМИБ		
4.2.2 Внедрение и функционирование СМИБ		4.4 Внедрение и эксплуатация
4.2.3 Проведение мониторинга и анализа СМИБ	8.2.3 Мониторинг и измерение процессов 8.2.4 Мониторинг и измерение продукции	4.5.1 Мониторинг и измерение
4.2.4 Поддержка и улучшение СМИБ	—	—
4.3 Требования к документации	4.2 Требования к документации	
4.3.1 Общие положения	4.2.1 Общие положения 4.2.2 Руководство по качеству	—
4.3.2 Управление документами	4.3.2 Управление документацией	4.4.5 Меры контроля документации
4.3.3 Управление записями	4.2.4 Управление записями	4.5.4 Меры контроля в отношении учетных записей
5 Ответственность руководства	5 Ответственность руководства	
5.1 Обязательства руководства	5.1 Обязательства руководства 5.2 Ориентация на потребителя	
	5.3 Политика в области качества	4.2 Политика в области охраны окружающей среды
	5.4 Планирование	4.3 Планирование
	5.5 Ответственность, полномочия и обмен информацией	

Окончание таблицы С.1

Настоящий стандарт	ИСО 9001: 2000	ИСО 14001:2004
5.2 Управление ресурсами	6 Управление ресурсами	
5.2.1 Обеспечение ресурсами	6.1 Обеспечение ресурсами 6.2 Человеческие ресурсы	
5.2.2 Подготовка, осведомленность и квалификация персонала	6.2.2 Компетентность, осведомленность и подготовка 6.3 Инфраструктура 6.4 Производственная среда	4.4.2 Обучение, осведомленность и компетентность
6 Внутренние аудиты СМИБ	8.2.2 Внутренние аудиты (проверки)	4.5.5 Внутренний аудит
7 Анализ СМИБ со стороны руководства	5.6 Анализ со стороны руководства	4.6 Контрольный анализ со стороны руководства
7.1 Общие положения	5.6.1 Общие положения	
7.2 Входные данные для анализа СМИБ	5.6.2 Входные данные для проведения контрольного анализа	
7.3 Выходные данные анализа СМИБ	5.6.3 Выходные данные контрольного анализа	
8 Улучшение СМИБ	8.5 Совершенствование	
8.1 Постоянное улучшение	8.5.2 Непрерывное совершенствование	
8.2 Корректирующие действия	8.5.3 Корректирующие действия	4.5.3 Несоответствие, коррективные и превентивные действия
8.3 Предупреждающие действия	8.5.4 Превентивные действия	
Приложение А Цели и меры управления	—	Приложение А Руководство по использованию этого стандарта
Приложение В Принципы ОЭСР и настоящий стандарт	—	—
Приложение С Сравнение структуры настоящего стандарта со структурами международных стандартов ИСО 9001:2000, ИСО 14001:2004	Приложение А Соответствие ИСО 9001:2000 и ИСО 14001:2004	Соответствие между ИСО 14001:2004 и ИСО 9001:2000
Приложение D Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам	—	—

Приложение D
(справочное)

Сведения о соответствии национального стандарта Российской Федерации ссылочному международному стандарту

Таблица D.1

Обозначение ссылочного международного стандарта	Обозначение и наименования соответствующего национального стандарта
ИСО/МЭК 17799:2005	ГОСТ Р ИСО/МЭК 17799—2005 Информационная технология. Практические правила управления информационной безопасностью

Библиография

[1] ОЭСР. Руководство по обеспечению безопасности информационных систем и сетей. Совершенствование безопасности. — Париж: ОЭСР, июль 2002
OECD, Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002.

gost.e-ecolog.ru

[2] ИСО 9001—2000 Система менеджмента качества. Требования (Quality management systems — Requirements)

[3] ИСО 14001:2004 Системы управления окружающей средой. Требования и руководство по применению (Environmental management systems — Requirements with guidance for use)

[4] ИСО/МЭК 13335-1:2004 Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационных и телекоммуникационных технологий. Часть 1. Концепция и модели управления безопасностью информационных и телекоммуникационных технологий (Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management)

[5] ИСО/МЭК ТО 18044:2004 Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности (Information technology — Security techniques — Information security incident management)

[6] Руководство ИСО/МЭК 73:2002 Управление риском. Словарь. Руководящие указания по использованию в стандартах (Risk management — Vocabulary — Guidelines for use in standards)

[7] ИСО/МЭК ТО 13335-3:1998 Информационная технология. Рекомендации по управлению безопасностью информационных технологий. Часть 3. Методы управления безопасностью информационных технологий (Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security)

[8] ИСО 19011:2002 Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента (Guidelines for quality and/or environmental management systems auditing)

[9] ИСО 9004:2000 Системы менеджмента качества. Рекомендации по улучшению деятельности (Quality management systems — Guidelines for performance improvements)

УДК 001.4:025.4:006.354 ОКС 35.040 01.040.01 Т00

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

Редактор *Л.В. Афанасенко*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 27.11.2007. Подписано в печать 10.01.2008. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 3,72. Уч.-изд. л. 3,50. Тираж 463 экз. Зак. 1.

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