БРИТАНСКИЙ СТАНДАРТ

BS ISO/IEC 27001:2005
BS 7799-2:2005

Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования

BRITISH STANDARD

BS ISO/IEC
27001:2005
BS 7799-2:2005

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

ICS 35.040

BSI
British Standards

Этот документ является русским переводом британского стандарта BS ISO/IEC 27001:2005 (BS 7799-2:2005), выполненным ООО «GlobalTrust Solutions» с разрешения Британского Института Стандартов (British Standards Institution) по лицензии № 2006AT0005. BSI не несет ответственности за точность перевода. В случае любых разночтений предпочтение должно отдаваться английскому оригиналу.

This document is a translation of BS ISO/IEC 27001:2005 (BS 7799-2:2005) into the Russian language by GlobalTrust Solutions Limited. It is reproduced with the permission of the British Standards Institution under the license number 2006AT0005. BSI takes no responsibility for the accuracy of this translation. In any cases of dispute the English original shall be taken as authoritative.

Национальное предисловие

Этот Британский стандарт дословно воспроизводит ISO/IEC 27001:2005 и вводит его в качестве государственного стандарта Великобритании. Он заменяет собой BS 7799-2:2002, действие которого отменяется.

От лица Великобритании в подготовке этого стандарта участвовал Технический комитет IST/33, Информационные технологии – Методы обеспечения безопасности, в обязанности которого входило следующее:

- Оказание помощи в понимании текста стандарта;
- Предоставление ответственному международному/Европейскому комитету любых справок относительно интерпретации или предложений о внесении изменений, а также защита интересов Великобритании;
- Отслеживание соответствующих международных и Европейских разработок и их распространение в Великобритании.

Список организаций, представленных в Комитете, может быть получен на основании запроса, направленного его секретарю.

Перекрестные ссылки

Британские стандарты, вводящие в действие международные публикации, на которые имеются ссылки в настоящем документе, могут быть найдены в Каталоге стандартов BSI в секции «Индекс соответствия международным стандартам», путем использования функции «Поиск» *Электронного каталога стандартов BSI* или British Standards Online.

Эта публикация не претендует на то, чтобы содержать все положения, необходимые для заключения договоров. Пользователи сами отвечают за ее корректное применение.

Соответствие Британскому стандарту само по себе не предоставляет иммунитета от юридических обязательств.

Сводка страниц

Этот документ состоит из титульного листа, внутренней заглавной станицы, титульного листа ISO/IEC, страниц 3 – 55, задней страницы и задней обложки.

Уведомление об авторском праве BSI, содержащееся в этом документе, указывает на дату его последней публикации.

Этот Британский стандарт был опубликован Комитетом по стратегии и политике в области стандартов (Standards Policy and Strategy Committee) 18 октября 2005 года.

ISBN 0 580 46781 3

INTERNATIONAL STANDARD

ISO/IEC 27001

First edition
2005-10-15

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

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2005(E)

Оглавление

Предисловие

ISO (Международная Организация по Стандартизации) и IEC (Международная Электротехническая Комиссия) формируют специализированную систему всемирной стандартизации. Государственные органы, являющиеся членами ISO или IEC, участвуют в разработке Международных Стандартов через технические комитеты, созданные соответствующей организацией для стандартизации отдельных областей технической деятельности. Технические комитеты ISO и IEC сотрудничают в областях взаимных интересов. Другие международные организации, правительственные и не правительственные, совместно с ISO и IEC, также принимают участие в этой работе. В области информационных технологий, ISO и IEC организован объединенный технический комитет, ISO/IEC JTC 1.

Международные Стандарты проектируются в соответствии с правилами, установленными Директивами ISO/IEC, Часть 2.

Главной задачей объединенного комитета является подготовка Международных Стандартов. Проекты Международных Стандартов, принятые объединенным техническим комитетом, передаются в государственные органы для голосования. Публикация в качестве Международного Стандарта требует одобрения не менее 75 процентов проголосовавших государственных органов.

Обращаем внимание на то, что некоторые элементы этого Международного Стандарта могут быть предметом патентного права. ISO и IEC не несет ответственность за идентификацию любых или всех указанных патентных прав.

ISO/IEC 27001 был подготовлен объединенным техническим комитетом ISO/IEC JTC 1, *Информационные технологии, Подкомитет SC 27, Методы обеспечения безопасности ИТ*.

0 Введение

0.1 Общие положения

Этот Международный стандарт был подготовлен для того, чтобы предоставить модель для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования Системы Управления Информационной Безопасностью (СУИБ). Принятие СУИБ должно являться стратегическим решением для организации. На проектирование и внедрение СУИБ оказывают влияние бизнес цели и потребности организации, вытекающие из них требования безопасности, используемые процессы, а также размер и структура организации. Эти факторы, а также поддерживающие их системы предположительно со временем будут изменяться. Ожидается, что реализация СУИБ будет масштабироваться в соответствии с потребностями организации, например, простая ситуация требует простого решения по построению СУИБ.

Этот Международный стандарт может использоваться заинтересованными внутренними и внешними сторонами для оценки соответствия.

0.2 Процессный подход

Этот Международный стандарт содействует утверждению процессного подхода к созданию, внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ организации.

Организация должна идентифицировать и управлять многими активностями для того, чтобы функционировать эффективно. Любая активность, использующая ресурсы и управляемая с целью обеспечения трансформации входных данных в выходные, может рассматриваться в качестве процесса. Часто выходные данные одного процесса служат входными данными для другого процесса.

Применение системы процессов в организации наряду с идентификацией и взаимодействием этих процессов, а также управление ими, может рассматриваться в качестве «процессного подхода».

Процессный подход к управлению информационной безопасностью, представленный в этом Международном стандарте, подчеркивает важность:

a) Понимания требований информационной безопасности организации и необходимости определения политики и целей информационной безопасности;

b) Внедрения и эксплуатации механизмов контроля для управления рисками информационной безопасности организации в контексте управления общими бизнес рисками организации;

c) Мониторинга и проверки производительности и эффективности СУИБ; и

d) Непрерывное усовершенствование на базе объективных измерений.

В этом Международном стандарте принимается модель Планирование-Реализация-Проверка-Действие (ПРПД), которая применяется для структурирования всех процессов

СУИБ. На рисунке 1 показано как СУИБ получает в качестве входных данных требования информационной безопасности и ожидания заинтересованных сторон и через применение необходимых мер и процессов производит результаты информационной безопасности, которые отвечают этим требованиям и ожиданиям. На рисунке 1 также проиллюстрированы связи в процессах, представленных в разделах 4, 5, 6, 7 и 8.

Принятие модели ПРПД будет также отражать принципы, установленные в руководстве OECD (2002)[1] по управлению безопасностью информационных систем и сетей. Этот Международный стандарт предоставляет четкую модель для реализации определяемых этим руководством принципов оценки рисков, проектирования и внедрения механизмов безопасности, управления безопасностью и ее переоценки.

ПРИМЕР 1

Требование может заключаться в том, чтобы нарушения информационной безопасности не приводили к серьезному финансовому ущербу и/или затруднениям для организации.

ПРИМЕР 2

Ожидание может заключаться в том, что если происходит серьезный инцидент – возможно взлом Web-сайта организации, используемого для ведения электронного бизнеса – должны присутствовать люди, соответствующим образом обученные необходимым процедурам, позволяющим минимизировать ущерб.

ПРИМЕЧАНИЕ: Термин «процедура» в области информационной безопасности обычно обозначает «процесс», который выполняется людьми, в отличие от компьютера или других электронных средств.

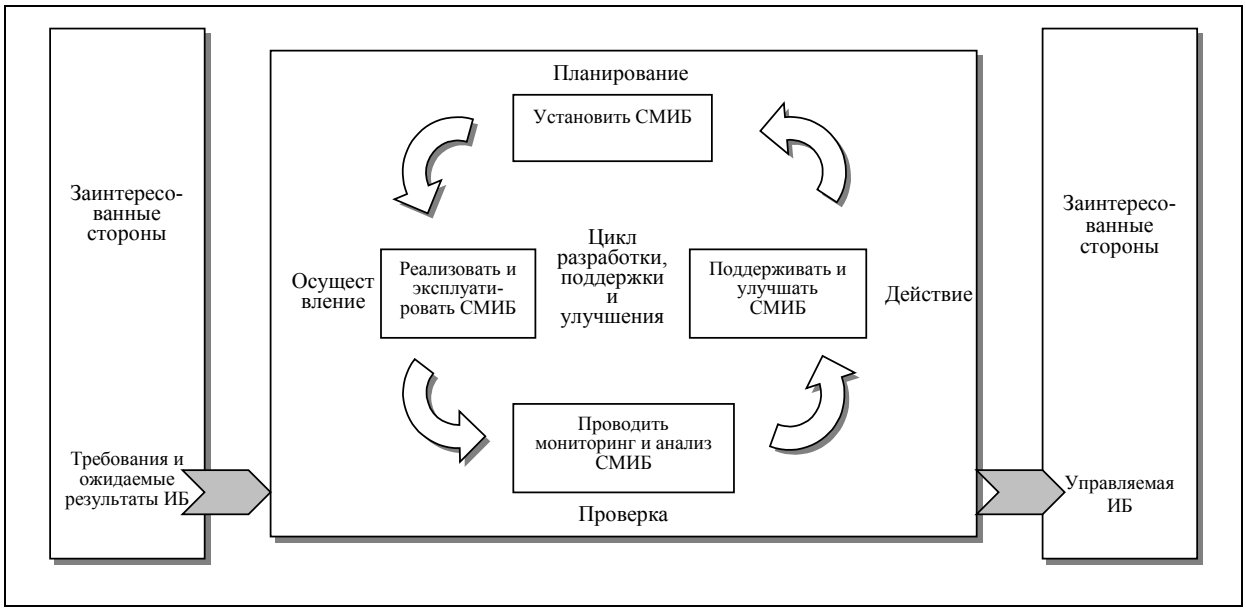

Рисунок 1 Применение модели ПРПД к процессам СУИБ

[1] **OECD Руководство по обеспечению безопасности информационных систем и сетей – На пути к культуре безопасности. Париж: OECD, Июль 2002. www.oecd.org**

Планирование (создание СУИБ)	Определение политики СУИБ, целей, процессов и процедур, относящихся к управлению рисками и совершенствованию информационной безопасности для получения результатов в соответствии с общими политиками и целями организации.
Реализация (внедрение и эксплуатация СУИБ)	Внедрение и эксплуатация политики СУИБ, механизмов контроля, процессов и процедур.
Проверка (мониторинг и анализ СУИБ)	Оценка и, там где это применимо, измерение характеристик исполнения процесса в соответствии с политикой СУИБ, целями и практическим опытом, и предоставление отчетов руководству для анализа.
Действие (сопровождение и совершенствование СУИБ)	Принятие корректирующих и превентивных мер, основанных на результатах внутреннего аудита СУИБ, проверки со стороны руководства или другой относящейся к делу информации, для обеспечения непрерывного совершенствования СУИБ.

0.3 Совместимость с другими системами управления

Этот Международный стандарт приведен в соответствие с ISO 9001:2000 и ISO 14001:2004 с целью поддержки совместимости и интегрированности при внедрении и эксплуатации вместе с другими стандартами в области управления.

Таблица С.1 иллюстрирует взаимосвязь между разделами этого Международного стандарта, ISO 9001:2000 и ISO 14001:2004.

Этот Международный стандарт спроектирован таким образом, чтобы дать возможность организации привести свою СУИБ в соответствие или интегрировать ее с соответствующими требованиями к системам управления.

Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования

ВАЖНО – Эта публикация не претендует на то, чтобы содержать все необходимые положения для контракта. Пользователи сами отвечают за ее корректное применение. Соответствие Международному стандарту само по себе не предоставляет иммунитета от правовых обязательств.

1 Область действия

1.1 Общие положения

Этот Международный охватывает все типы организаций (в том числе коммерческие предприятия, государственные агентства и некоммерческие организации). Этот Международный стандарт определяет требования для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования документированной СУИБ в контексте общих бизнес рисков организации. Он определяет требования к реализации механизмов безопасности, приспособленные к потребностям отдельных организаций или их частей.

СУИБ спроектирована для того, чтобы гарантировать адекватность и пропорциональность механизмов безопасности, которые обеспечивают защиту информационных ресурсов и вызывают доверие у заинтересованных сторон.

ПРИМЕЧАНИЕ 1: Понятие «бизнес» в этом Международном стандарте следует интерпретировать шире, для обозначения активностей, являющихся ключевыми для существования организации.

ПРИМЕЧАНИЕ 2: ISO/IEC 17799 предоставляет руководство по внедрению, которое может использоваться при проектировании механизмов контроля.

1.2 Применение

Требования, изложенные в этом Международном стандарте, носят общий характер и предназначены для применения в любых организациях, независимо от их типа, размера или области деятельности. В том случае, если организация заявляет о соответствии этому Международному стандарту, исключение любых требований, определяемых в разделах 4, 5, 6, 7 и 8, не допустимо.

Любые исключения механизмов контроля, которые сочли необходимыми для удовлетворения критериям принятия рисков, должны быть обоснованы, а также должны

быть предоставлены свидетельства того, что соответствующие риски были приняты ответственными лицами. Там, где были исключены некоторые механизмы контроля, заявления о соответствии этому Международному стандарту неприемлемы до тех пор, пока такие исключения оказывают влияние на способность организации обеспечивать информационную безопасность и/или на ответственность за обеспечение информационной безопасности, которая удовлетворяет требованиям безопасности, определенным на основании оценки рисков, а также требованиям законодательной или нормативной базы.

ПРИМЕЧАНИЕ: Если в организации уже существует работающая система управления бизнес процессами (например, в соответствии с ISO 9001 или ISO 14001), в большинстве случаев предпочтительным является удовлетворение требованиям этого Международного стандарта в рамках этой существующей системы управления.

2 Ссылки на нормативные документы

Перечисленные ниже документы являются необходимыми для применения этого документа. Для документов, датированных определенным числом, применима только указанная редакция. Для недатированных документов, применяется их последняя редакция (включая любые приложения).

ISO/IEC 17799:2005, *Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью*

3 Термины и определения

В этом документе используются следующие термины и определения.

3.1

ресурс

все, что имеет ценность для организации

[ISO/IEC 13335-1:2004]

3.2

доступность

свойство, заключающееся в доступности и применимости для авторизованных субъектов, когда потребуется

[ISO/IEC 13335-1:2004]

3.3

конфиденциальность

свойство, заключающееся в недоступности информации или не раскрытии ее содержания для неавторизованных лиц, субъектов или процессов

[ISO/IEC 13335-1:2004]

3.4

информационная безопасность

обеспечение конфиденциальности, целостности и доступности информации; дополнительно также могут подразумеваться другие свойства, такие как аутентичность, подотчетность, неотказуемость и надежность

[ISO/IEC 17799:2005]

3.5

событие информационной безопасности

идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности

[ISO/IEC TR 18044:2004]

3.6

инцидент информационной безопасности

одно или серия нежелательных или неожиданных событий информационной безопасности, имеющих значительную вероятность нарушения бизнес операций или представляющих угрозу для информационной безопасности

[ISO/IEC TR 18044:2004]

3.7

система управления информационной безопасностью

СУИБ

та часть общей системы управления, основанной на оценке бизнес рисков, которая предназначена для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности

ПРИМЕЧАНИЕ: Система управления включает в себя организационную структуру, политики, действия по планированию, распределение ответственности, практики, процедуры, процессы и ресурсы.

3.8

целостность

свойство, заключающееся в обеспечении точности и полноты ресурсов

[ISO/IEC 13335-1:2004]

3.9

остаточный риск

риск, остающийся после принятия мер по обработке рисков

[ISO/IEC Guide 73:2002]

3.10

принятие риска

решение о принятии риска

[ISO/IEC Guide 73:2002]

3.11

анализ рисков

систематическое использование информации для идентификации источников и оценки величины рисков

[ISO/IEC Guide 73:2002]

3.12

оценка рисков

общий процесс анализа и оценивания рисков

[ISO/IEC Guide 73:2002]

3.13

оценивание рисков

процесс сравнения оценочной величины риска с установленным критерием с целью определения уровня значимости риска

[ISO/IEC Guide 73:2002]

3.14

управление рисками

скоординированные действия по управлению и контролю организации в отношении рисков

[ISO/IEC Guide 73:2002]

3.15

обработка риска

процесс выбора и реализации мер по модификации риска

[ISO/IEC Guide 73:2002]

ПРИМЕЧАНИЕ: В этом Международном стандарте термин «механизм контроля» используется в качестве синонима слова «мера».

3.16

декларация о применимости

документированное заявление, описывающее цели и механизмы контроля, которые имеют отношение и применимы к СУИБ организации

ПРИМЕЧАНИЕ: Цели и механизмы контроля базируются на результатах и выводах, полученных в процессе оценки рисков и обработки рисков, законодательных требованиях и требованиях нормативной базы, договорных обязательствах и бизнес требованиях организации к информационной безопасности.

4 Система управления информационной безопасностью

4.1 Общие требования

Организация должна создать, внедрить, эксплуатировать, осуществлять мониторинг, анализировать, сопровождать и совершенствовать документированную СУИБ в контексте общих бизнес активностей и рисков организации. В этом Международном стандарте используется процесс, основанный на модели ПРПД, показанной на рисунке 1.

4.2 Создание и управление СУИБ

4.2.1 Создание СУИБ

Организация должна делать следующее:

a) Определить область действия и границы СУИБ в терминах характеристик бизнеса, организации, ее расположения, ресурсов и технологий, а также включая детальную информацию и обоснование для любых исключений из области действия (см. 1.2).

b) Определить политику СУИБ в терминах характеристик бизнеса, организации, ее расположения, ресурсов и технологий, которая:

   1) включает в себя основу для определения ее целей и устанавливает общее направление и принципы деятельности по отношению к информационной безопасности;

   2) учитывает требования бизнеса и требования законодательной или нормативной базы, а также контрактные обязательства в области безопасности;

   3) объединяется со стратегическим контекстом управления рисками в организации, в котором будет происходить создание и сопровождение СУИБ;

   4) устанавливает критерии для оценивания рисков (см. 4.2.1c)); и

   5) утверждена руководством.

   ПРИМЕЧАНИЕ: В этом Международном стандарте политика СУИБ рассматривается в качестве надмножества политики информационной безопасности. Эти политики могут быть описаны в одном документе.

c) Определить подход организации к оценке рисков.

   1) Определить методологию оценки рисков, подходящую для СУИБ, а также удовлетворяющую требованиям бизнеса к информационной безопасности, требованиям законодательства и нормативной базы;

   2) Разработать критерии для принятия рисков и определить приемлемые уровни риска (см. 5.1f)).

   Выбранная методология оценки рисков должна обеспечивать получение сопоставимых и воспроизводимых результатов.

   ПРИМЕЧАНИЕ: Существуют различные методологии оценки рисков. Примеры методологий оценки рисков рассматриваются в ISO/IEC TR 13335-3, *Информационные технологии – Руководство по управлению безопасностью ИТ – Методы управления безопасностью ИТ.*

d) Идентифицировать риски.

   1) Идентифицировать ресурсы, находящиеся в области действия СУИБ и владельцев[2] этих ресурсов.

[2] **Термин «владелец» обозначает лицо или сущность, на которую возлагается утвержденная руководством ответственность за производство, разработку, сопровождение, использование и обеспечение безопасности ресурсов. Термин «владелец» не означает, что человек имеет какие-либо имущественные права на ресурс.**

2) Идентифицировать угрозы в отношении этих ресурсов.

3) Идентифицировать уязвимости, которые могут быть использованы для реализации угроз.

4) Идентифицировать последствия нарушения конфиденциальности, целостности и доступности ресурсов.

e) Проанализировать и оценить риски.

1) Оценить ущерб для бизнеса, который может быть причинен в результате нарушения безопасности, принимая во внимание потенциальные последствия нарушения конфиденциальности, целостности или доступности ресурсов.

2) Оценить реалистичную вероятность нарушений безопасности, происходящих в свете существующих угроз, уязвимостей и последствий, связанных с этими ресурсами, а также реализованных в настоящее время механизмов контроля.

3) Оценить уровни рисков.

4) С использованием критерия, установленного в 4.2.1c)2), определить является ли риск приемлемым или требуется его обработка.

f) Идентифицировать и оценить возможности по обработке рисков.

Возможные действия включают в себя следующее:

1) применение подходящих механизмов контроля;

2) осознанное и объективное принятие рисков, при условии, что они строго удовлетворяют политике организации и критериям принятия рисков (см. 4.2.1c)2));

3) избежание рисков; и

4) перенесение объединенных бизнес рисков на другие стороны, например, страховщиков, поставщиков.

g) Выбрать цели и механизмы контроля для обработки рисков.

Цели и механизмы контроля должны быть выбраны и реализованы для обеспечения соответствия требованиям, идентифицированным в процессе оценки и управления рисками. Этот выбор должен учитывать критерии принятия рисков (см. 4.2.1c)2)), а также требования законодательства, нормативной базы и договоров.

Цели и механизмы контроля из Приложения А должны выбираться как часть этого процесса для обеспечения соответствия идентифицированным требованиям.

Цели и механизмы контроля из Приложения А не являются исчерпывающими, поэтому могут быть также выбраны дополнительные цели и механизмы контроля.

ПРИМЕЧАНИЕ: Приложение А содержит всеобъемлющий список целей и механизмов контроля, которые подходят для большинства организаций. Пользователи этого Международного стандарта адресуются к Приложению А как к отправной точке для выбора механизмов контроля, чтобы гарантировать, что важные механизмы контроля не были пропущены.

h) Получить одобрение руководства для предложенных остаточных рисков.

i) Получить разрешение руководства на внедрение и эксплуатацию СУИБ.

j) Подготовить Декларацию о применимости.

Должна быть подготовлена Декларация о применимости, которая включает в себя следующее:

1) Выбранные в 4.2.1g) цели и механизмы контроля и причины их выбора;

2) Цели и механизмы контроля, реализованные в настоящее время (см. 4.2.1e)2)); и

3) Исключение любых целей и механизмов контроля из Приложения А и обоснование их исключения.

ПРИМЕЧАНИЕ: Декларация о применимости предоставляет кратное описание решений по обработке рисков. Обоснование исключений обеспечивает перекрестную проверку того, что механизмы контроля не были пропущены по невнимательности.

4.2.2 Внедрение и эксплуатация СУИБ

Организация должна делать следующее:

a) Разработать план обработки рисков, который определяет соответствующие действия руководства, ресурсы, ответственность и приоритеты по управлению рисками информационной безопасности (см. 5).

b) Реализовать план обработки рисков с целью достижения установленных целей контроля, что включает в себя рассмотрение вопросов финансирования, назначение ролей и распределение ответственности.

c) Реализовать механизмы контроля, выбранные в 4.2.1g), для достижения целей контроля.

d) Определить, как измерять эффективность выбранных механизмов контроля или групп механизмов контроля, и определить, как эти измерения должны использоваться для оценки эффективности механизмов контроля с целью получения сопоставимых и воспроизводимых результатов (см. 4.2.3c)).

ПРИМЕЧАНИЕ: Измерение эффективности механизмов контроля позволяет руководителям и персоналу определить, насколько хорошо механизмы контроля достигают запланированных целей контроля.

e) Реализовать программы обучения и повышения осведомленности (см. 5.2.2).

f) Управлять эксплуатацией СУИБ.

g) Управлять ресурсами СУИБ (см. 5.2).

h) Внедрить процедуры и другие механизмы контроля, пригодные для точного обнаружения событий безопасности и реагирования на инциденты безопасности (см. 4.2.3a)).

4.2.3 Мониторинг и анализ СУИБ

Организация должна делать следующее:

a) Выполнять процедуры мониторинга и анализа, а также применять другие механизмы контроля для того, чтобы:

   1) своевременно обнаруживать ошибки в результатах обработки данных;

   2) своевременно определять неудачные и успешные инциденты и нарушения безопасности;

   3) предоставить руководству возможность определить, выполняются ли должным образом меры безопасности, делегированные людям или реализуемые средствами информационных технологий;

   4) помогать обнаружению событий безопасности и, с помощью этого, предотвращать инциденты безопасности путем использования индикаторов; и

   5) определять, были ли эффективными действия, предпринимаемые для устранения нарушения безопасности.

b) Предпринимать регулярные проверки эффективности СУИБ (включая выполнение требований политики безопасности и достижение целей контроля, а также проверку механизмов контроля), принимая во внимание результаты аудитов безопасности, инциденты, результаты измерения эффективности, предложения и отзывы от всех заинтересованных сторон.

c) Измерять эффективность механизмов контроля, чтобы проверить выполнение требований безопасности.

d) Пересматривать оценки рисков через определенные интервалы, пересматривать остаточные риски и идентифицированные уровни допустимых рисков, принимая во внимание изменения, происходящие в:

   1) организации;

   2) технологиях;

   3) бизнес целях и процессах;

   4) идентифицированных угрозах;

   5) внешних событиях, таких как изменения в законодательной или нормативной среде, изменения контрактных обязательств и изменения социального климата.

e) Проводить внутренний аудит СУИБ через запланированные интервалы времени (см. 6).

   ПРИМЕЧАНИЕ: Внутренние аудиты, иногда называемые аудиты первой стороны, проводятся самой организацией или от лица организации для внутренних целей.

f) Производить анализ СУИБ руководством на регулярной основе для того, чтобы гарантировать, что область действия СУИБ остается адекватной и улучшения в процессах СУИБ идентифицированы (см. 7.1).

g) Обновлять планы обеспечения безопасности, чтобы принять во внимание выводы, полученные в ходе мониторинга и анализа.

h) Протоколировать действия и события, которые могут оказывать влияние на эффективность или поведение СУИБ (см. 4.3.3).

4.2.4 Сопровождение и совершенствование СУИБ

Организация должна регулярно делать следующее:

a) Внедрять идентифицированные усовершенствования в СУИБ.

b) Предпринимать соответствующие корректирующие и превентивные действия согласно 8.2 и 8.3. Использовать собственный опыт и опыт других организаций в области обеспечения безопасности.

c) Сообщать о предпринимаемых мерах и усовершенствованиях всем заинтересованным сторонам со степенью подробности, соответствующей обстоятельствам, и, в случае необходимости, согласовывать свои действия.

d) Обеспечивать достижение поставленных целей в ходе реализации усовершенствований.

4.3 Требования к документированию

4.3.1 Общие требования

Документация должна включать в себя записи о решениях руководства, обеспечивать прослеживаемость действий до решений руководства и политик, а также воспроизводимость запротоколированных результатов.

Важно быть в состоянии продемонстрировать взаимосвязь между выбранными механизмами контроля и результатами процесса оценки и управления рисками, а также в обратную сторону к политике и целям СУИБ.

Документация СУИБ должна включать в себя следующее:

a) документированные положения политики безопасности (см. 4.2.1b)) и цели контроля;

b) область действия СУИБ (см. 4.2.1a));

c) процедуры и механизмы контроля, поддерживающие СУИБ;

d) описание методологии оценки рисков (см. 4.2.1c));

e) отчет об оценке рисков (см. 4.2.1c) – 4.2.1g));

f) план обработки рисков (см. 4.2.2b)).

g) документированные процедуры, которые необходимы организации для обеспечения эффективного планирования, выполнения и контроля процессов информационной безопасности и описывающие как измерять эффективность механизмов контроля (см. 4.2.3c));

h) записи, требуемые этим Международным стандартом (см. 4.3.3); и

i) Декларация о применимости.

ПРИМЕЧАНИЕ 1: Там, где в этом Международном стандарте встречается термин «документированная процедура», это означает, что процедура разработана, документирована, внедрена и сопровождается.

ПРИМЕЧАНИЕ 2: Объем документации СУИБ может различаться от одной организации к другой в зависимости от:

— размера организации и вида ее деятельности; и
— области действия и сложности требований безопасности и системы, которой осуществляется управление.

ПРИМЕЧАНИЕ 3: Документы и записи могут быть представлены в любой форме и на любом типе носителя.

4.3.2 Управление документами

Документы, которые необходимы для СУИБ, должны быть защищены и находится под контролем. Должна быть установлена документированная процедура, определяющая действия руководства, необходимые для:

a) утверждения документов перед опубликованием с точки зрения их достоверности и достаточности;

b) анализа и корректировки документов в случае необходимости, а также повторного утверждения документов;

c) обеспечения идентификации изменений и статуса текущих ревизий документов;

d) обеспечения доступности самых последних версий соответствующих документов в местах их использования;

e) предоставления гарантий того, что документы остаются понятными и легко идентифицируемыми;

f) обеспечения доступности документов для тех, кому они необходимы, а также обеспечения передачи, хранения и, в конечном итоге, уничтожения документов согласно процедурам, соответствующим их классификации;

g) обеспечение идентификации документов, имеющих внешнее происхождение;

h) обеспечения контроля над распространением документов;

i) предотвращения непреднамеренного использования устаревших документов; и

j) применения соответствующей схемы идентификации устаревших документов, если они сохраняются по какой-либо причине.

4.3.3 Управление записями

Должны создаваться и сохраняться записи для предоставления свидетельств соответствия требованиям и эффективности функционирования СУИБ. Они должны контролироваться и быть защищены. СУИБ должна принимать во внимание любые относящиеся к ней требования законодательства или нормативной базы, а также контрактные обязательства.

Записи должны оставаться понятными, легко идентифицируемыми и восстанавливаемыми. Механизмы контроля, необходимые для идентификации, хранения, защиты, восстановления записей, а также период хранения и размещение записей должны быть документированы и реализованы.

Должны вестись записи о выполнении процесса, как изложено в 4.2, а также обо всех значимых инцидентах безопасности, имеющих отношение к СУИБ.

ПРИМЕР

Примерами записей являются: книга посетителей, записи аудита и заполненные формы авторизация доступа.

5 Ответственность руководства

5.1 Приверженность руководства

Руководство должно продемонстрировать свою приверженность созданию, внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ, путем:

a) создания политики СУИБ;

b) обеспечения наличия целей и планов СУИБ;

c) определения ролей и ответственности за информационную безопасность;

d) сообщения организации о важности достижения целей информационной безопасности и соответствия политике информационной безопасности, ее ответственности перед законом и необходимости непрерывного совершенствования;

e) выделения достаточных ресурсов для разработки, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования СУИБ (см. 5.2.1);

f) принятия решения о критериях принятия рисков и допустимом уровне риска;

g) обеспечения проведения внутренних аудитов СУИБ (см. 6); и

h) проведения анализа СУИБ со стороны руководства (см. 7).

5.2 Управление ресурсами

5.2.1 Выделение ресурсов

Организация должна определить и выделить ресурсы, необходимые для:

a) создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования СУИБ;

b) обеспечения поддержки требований бизнеса процедурами информационной безопасности;

c) определения и учета требований законодательства и нормативной базы, а также контрактных обязательств по обеспечению безопасности;

d) поддержания достаточного уровня безопасности путем правильного применения всех реализованных механизмов контроля;

e) проведения проверок, в случае необходимости, и соответствующего реагирования на результаты этих проверок; и

f) там, где это необходимо, повышения эффективности СУИБ.

5.2.2 Обучение, осведомленность и компетентность

Организация должна убедиться в том, что весь персонал, на который возложена определяемая в СУИБ ответственность, обладает необходимой компетенцией для решения требуемых задач, путем:

a) определения необходимых компетенций для персонала, который выполняет работу, оказывающую влияние на СУИБ;

b) предоставления обучения или принятия других мер (например, найма компетентного персонала) для удовлетворения этим потребностям;

c) оценки эффективности предпринимаемых мер; и

d) ведения записей об образовании, обучении, навыках, опыте и квалификациях (см. 4.3.3).

Организация должна также убедиться в том, что весь имеющий отношение к СУИБ персонал осведомлен о важности и необходимости принятия мер по обеспечению информационной безопасности, а также о своем вкладе в достижение целей СУИБ.

6 Внутренние аудиты СУИБ

Организация должна проводить внутренние аудиты СУИБ через запланированные интервалы времени с целью проверки того, что цели контроля, механизмы контроля, процессы и процедуры СУИБ:

a) соответствуют требованиям этого Международного стандарта, а также соответствующим требованиям законодательной или нормативной базы;

b) соответствуют идентифицированным требованиям информационной безопасности;

c) эффективно реализованы и сопровождаются; и

d) выполняются, как ожидалось.

Программа аудита должна быть спланирована с учетом статуса и важности проверяемых процессов и областей, а также результатов предыдущих аудитов. Должны быть определены критерии, область, частота и методы проведения аудита. Выбор

аудиторов и проведение аудитов должны гарантировать объективность и непредвзятость процесса аудита. Аудиторы не должны проверять свою собственную работу.

Ответственность и требования к планированию и проведению аудитов, а также к предоставлению отчетов по результатам и ведению записей (см. 4.3.3) должны быть определены в документированной процедуре.

Руководство, несущее ответственность за проверяемые области аудита, должно обеспечить принятие мер без неоправданных задержек с целью устранения обнаруженных несоответствий и их причин. Действия по усовершенствованию должны включать в себя проверку предпринятых мер и предоставление отчета о результатах проверки (см. 8).

ПРИМЕЧАНИЕ: ISO 19011:2002, *Руководство по аудиту систем управления качеством и/или окружающей средой*, может предоставить полезное руководство по выполнению внутренних аудитов СУИБ.

7 Анализ СУИБ руководством

7.1 Общие положения

Руководство должно анализировать СУИБ организации через запланированные интервалы времени, чтобы убедиться в ее постоянной пригодности, адекватности и эффективности. Эти проверки должны включать в себя оценку возможностей для усовершенствования и необходимости внесения изменений в СУИБ, включая политику информационной безопасности и цели информационной безопасности. Результаты проверок должны быть четко документированы, а также должны вестись записи (см. 4.3.3).

7.2 Входные данные для анализа

Входные данные для анализа СУИБ руководством должны включать в себя следующую информацию:

a) результаты аудитов и анализа СУИБ;

b) отзывы заинтересованных сторон;

c) методики, продукты и процедуры, которые могли бы использоваться в организации для повышения производительности и эффективности СУИБ;

d) статус превентивных и корректирующих мер;

e) уязвимости или угрозы, которые не были в достаточной степени учтены во время предыдущей оценки рисков;

f) результаты измерений эффективности;

g) меры, предпринятые по результатам предыдущих анализов СУИБ руководством;

h) любые изменения, которые могли бы повлиять на СУИБ; и

i) рекомендации по совершенствованию.

7.3 Выходные данные анализа

Выходные данные по результатам анализа СУИБ руководством должны включать в себя любые решения и меры, относящиеся к следующему:

a) Повышение эффективности СУИБ.

b) Корректировка плана оценки и плана обработки рисков;

c) Внесение необходимых изменений в процедуры и механизмы контроля, влияющие на информационную безопасность, в ответ на внутренние или внешние события, которые могут повлиять на СУИБ, включая изменения в:

   1) требованиях бизнеса;

   2) требованиях безопасности;

   3) бизнес процессах, влияющих на существующие требования бизнеса;

   4) требованиях нормативной или законодательной базы;

   5) контрактных обязательствах; и

   6) уровнях риска и/или критериях принятия рисков.

d) Потребности в ресурсах.

e) Совершенствование методов измерения эффективности механизмов контроля.

8 Совершенствование СУИБ

8.1 Непрерывное совершенствование

Организация должна непрерывно повышать эффективность СУИБ путем использования политики информационной безопасности, целей безопасности, результатов аудита, анализа отслеживаемых событий, корректирующих и превентивных мер и анализа со стороны руководства (см. 7).

8.2 Корректирующие меры

Организация должна предпринимать меры по устранению причин несоответствий требованиям СУИБ в целях предотвращения их повторений. Документированная процедура по реализации корректирующих мер должна определять требования для:

a) идентификации несоответствий;

b) определения причин несоответствий;

c) оценки необходимости принятия мер по предупреждению повторения несоответствий;

d) определение и реализация необходимых корректирующих мер;

e) протоколирования результатов принятых мер (см. 4.3.3); и

f) анализ предпринятых корректирующих мер.

8.3 Превентивные меры

Организация должна определить меры по устранению причин потенциальных несоответствий требованиям СУИБ с целью предотвращения их возникновения. Предпринимаемые превентивные меры должны соответствовать последствиям потенциальных проблем. Документированная процедура по реализации превентивных мер должна определять требования для:

a) идентификации потенциальных несоответствий и их причин;

b) оценки необходимости принятия мер для предотвращения возникновения несоответствий;

c) определения и реализации необходимых превентивных мер;

d) протоколирования результатов предпринимаемых мер (см. 4.3.3); и

e) анализа предпринятых превентивных мер.

Организация должна идентифицировать изменившиеся риски и требования к превентивным мерам, сосредоточив внимание на существенно изменившихся рисках.

Приоритетность превентивных мер должна определяться на основе результатов оценки рисков.

ПРИМЕЧАНИЕ: Меры по предотвращению несоответствий часто являются более экономически оправданными, нежели корректирующие меры.

Приложение А
(нормативное)

Цели и механизмы контроля

Цели и механизмы контроля, перечисленные в Таблице А.1, напрямую позаимствованы и приведены в соответствие с теми, которые перечислены в разделах 5 – 15 ISO/IEC 17799:2005. Перечни, приведенные в Таблице А.1, не являются исчерпывающими, и организация может посчитать необходимым применение дополнительных целей и механизмов контроля. Выбор целей и механизмов контроля из этих таблиц должен осуществляться как часть процесса СУИБ, определенного в 4.2.1.

Разделы 5 – 15 ISO/IEC 17799:2005 содержат рекомендации по внедрению и руководство по «лучшей практике» в отношении механизмов контроля, определяемых в А.5 – А.15.

Таблица А.1 – Цели и механизмы контроля

А.5 Политика безопасности		
А.5.1 Политика информационной безопасности		
Цель: Обеспечить управление и поддержку в области информационной безопасности со стороны руководства организации в соответствии с требованиями бизнеса, относящимися к делу законами и нормативными актами.		
А.5.1.1	Документированная политика информационной безопасности	*Механизм контроля* Документированная политика информационной безопасности должна быть утверждена руководством, опубликована и доведена до сведения всех сотрудников организации и имеющих к ней отношение внешних сторон.
А.5.1.2	Пересмотр политики информационной безопасности	*Механизм контроля* Политика информационной безопасности должна пересматриваться через запланированные интервалы времени, а также в случае влияющих на нее существенных изменений, чтобы обеспечить ее непрерывное соответствие реальному положению дел, достаточность и эффективность.

A.6 Организация информационной безопасности

A.6.1 Внутренняя организация

Цель: Управлять информационной безопасностью в организации.

A.6.1.1	Приверженность руководства информационной безопасности	*Механизм контроля* Руководство должно активно поддерживать безопасность в организации путем четкого управления, демонстрируемой приверженности, явного назначения и подтверждения ответственности за информационную безопасность.
A.6.1.2	Координация информационной безопасности	*Механизм контроля* Действия по обеспечению информационной безопасности должны координироваться представителями из различных частей организации с соответствующими ролями и должностными обязанностями.
A.6.1.3	Распределение ответственности за информационную безопасность	*Механизм контроля* Все области ответственности за информационную безопасность должны быть четко определены.
A.6.1.4	Процесс авторизации для средств обработки информации	*Механизм контроля* Должен быть определен и реализован процесс авторизации руководством новых средств обработки информации.
A.6.1.5	Соглашения о конфиденциальности	*Механизм контроля* Требования к соглашениям о конфиденциальности или не разглашении, отражающие потребности организации в защите информации, должны быть определены и должны регулярно пересматриваться.
A.6.1.6	Контакт с органами власти	*Механизм контроля* Должны поддерживаться соответствующие контакты с соответствующими органами власти.
A.6.1.7	Контакт с профессиональными объединениями	*Механизм контроля* Должны поддерживаться необходимые контакты с профессиональными объединениями или другими форумами специалистов по безопасности и профессиональными ассоциациями.
A.6.1.8	Независимая проверка информационной безопасности	*Механизм контроля* Подход организации к управлению информационной безопасностью и ее реализации (т.е. цели контроля,

		механизмы контроля, политики, процессы и процедуры информационной безопасности) должны подвергаться независимой проверке через запланированные интервалы времени или, в случае, если происходят существенные изменения в реализации безопасности.
A.6.2 Внешние стороны		
Цель: Обеспечить безопасность информации организации и средств ее обработки, доступ, обработка, передача или управление которыми осуществляется третьими сторонами.		
A.6.2.1	Идентификация рисков, связанных с внешними сторонами	*Механизм контроля* Риски для информации организации и средств ее обработки со стороны бизнес процессов, в которых задействованы внешние стороны, должны быть идентифицированы и соответствующие механизмы контроля должны быть реализованы, прежде чем будет предоставлен доступ.
A.6.2.2	Учет требований безопасности при работе с клиентами	*Механизм контроля* Должны быть учтены все идентифицированные требования безопасности, прежде чем клиентам будет предоставлен доступ к информации или ресурсам организации.
A.6.2.3	Учет требований безопасности в договорах с третьими сторонами	*Механизм контроля* Соглашения с третьими сторонами, предусматривающие доступ, обработку, передачу или управление информацией организации или средствами ее обработки, или добавление продуктов или сервисов в средства обработки информации должны охватывать все необходимые требования безопасности.
A.7 Управление ресурсами		
A.7.1 Ответственность за ресурсы		
Цель: Обеспечить и поддерживать необходимую защиту ресурсов организации.		
A.7.1.1	Инвентаризация ресурсов	*Механизм контроля* Все ресурсы должны быть четко идентифицированы, а также должна проводиться и поддерживаться инвентаризация всех важных ресурсов.
A.7.1.2	Владение ресурсами	*Механизм контроля* Вся информация и ресурсы, связанные со средствами

		обработки информации, должны находиться во владении[3] назначенной частью организации.
A.7.1.3	Допустимое использование ресурсов	*Механизм контроля* Правила допустимого использования информации и ресурсов, связанных со средствами обработки информации должны быть определены, документированы и реализованы.
A.7.2 Классификация информации		
Цель: Обеспечить необходимый уровень защиты информации.		
A.7.2.1	Руководство по классификации	*Механизм контроля* Информация должна быть классифицирована в терминах ее ценности, требований законодательства, конфиденциальности и критичности для организации.
A.7.2.2	Маркирование и обращение с информацией	*Механизм контроля* Должен быть определен и реализован необходимый набор процедур для маркирования и обращения с информацией, соответствующий схеме классификации, принятой в организации.
A.8 Безопасность людских ресурсов		
A.8.1 Перед наймом[4]		
Цель: Гарантировать, что работники, подрядчики и пользователи третьих сторон понимают свою ответственность и соответствуют своим ролям, а также снизить риск краж, мошенничества или неправомерного использования оборудования.		
A.8.1.1	Роли и ответственность	*Механизм контроля* Роли и обязанности сотрудников, подрядчиков и пользователей третьих сторон по обеспечению безопасности должны быть определены и документированы в соответствии с политикой информационной безопасности организации.

[3] Объяснение: Термин «владелец» обозначает лицо или сущность, на которую возлагается утвержденная руководством ответственность за контроль производства, разработки, сопровождения, использования и обеспечения безопасности ресурсов. Термин «владелец» не означает, что человек имеет имущественные права на ресурс.

[4] Объяснение: Слово «найм» здесь охватывает различные ситуации: прием людей на работу (временную или постоянную), назначение рабочих ролей, изменение рабочих ролей, заключение договоров, а также прекращение все перечисленных договоренностей.

A.8.1.2	Проверка работников	*Механизм контроля* Проверки анкетных данных всех кандидатов на работу, подрядчиков и пользователей третьих сторон должны выполняться в соответствии с действующими законами, правилами и этическими нормами, соразмерно требованиям бизнеса, классификации информации, к которой будет осуществляться доступ, и осознаваемым рискам.
A.8.1.3	Условия найма	*Механизм контроля* Работники, подрядчики и пользователи третьих сторон как часть их контрактных обязательств должны одобрить и подписать свои трудовые договора, в которых устанавливается их ответственность и ответственность организации за информационную безопасность.
A.8.2 В период работы		
Цель: Гарантировать, что все работники, подрядчики и пользователи третьих сторон осведомлены об угрозах и проблемах информационной безопасности, их ответственности и обязательствах и готовы поддерживать политику безопасности организации в своей повседневной деятельности и уменьшать риск человеческой ошибки.		
A.8.2.1	Ответственность руководства	*Механизм контроля* Руководство должно требовать от работников, подрядчиков и пользователей третьих сторон применения мер безопасности в соответствии с установленными в организации политиками и процедурами.
A.8.2.2	Повышение осведомленности, обучение и тренинги в области информационной безопасности	*Механизм контроля* Все сотрудники организации и, в случае необходимости, подрядчики и пользователи третьей стороны, должны проходить необходимое обучение и получать регулярные обновления политик и процедур, принятых в организации и необходимых для выполнения их должностных обязанностей.
A.8.2.3	Дисциплинарный процесс	*Механизм контроля* Должен существовать официальный дисциплинарный процесс в отношении сотрудников, допускающих нарушения безопасности.
A.8.3 Завершение или изменение трудовых отношений		
Цель: Гарантировать, что все сотрудники, подрядчики и пользователи третьих сторон покидают организацию или меняют работу в установленном порядке.		
A.8.3.1	Ответственность при завершении трудовых отношений	*Механизм контроля* Ответственность за выполнение действий по завершению трудовых отношений должна быть четко определена и установлена.

A.8.3.2	Возврат ресурсов	*Механизм контроля* При завершении их трудовых отношений, контракта или соглашения все сотрудники, подрядчики и пользователи третьих сторон должны возвратить все принадлежащие организации ресурсы, находящие в их владении.
A.8.3.3	Отмена прав доступа	*Механизм контроля* При завершении их трудовых отношений, контракта или соглашения права доступа всех сотрудников, подрядчиков и пользователей третьих сторон к информации и средствам ее обработки должны быть отменены или, в случае изменения характера работы, откорректированы.

A.9 Физическая безопасность и безопасность окружающей среды

A.9.1 Защищенные области

Цель: Предотвратить несанкционированный физический доступ и причинение ущерба для помещений и информации организации.

A.9.1.1	Физический периметр безопасности	*Механизм контроля* Для защиты зон, содержащих информацию и средства ее обработки, должны использовать периметры безопасности (различные барьеры, такие как стены, проходные с контролем доступа по картам, приемные с дежурными).
A.9.1.2	Механизмы контроля физического входа	*Механизм контроля* Защищенные области должны быть защищены соответствующими механизмами контроля входа, обеспечивающими возможность доступа только для авторизованного персонала.
A.9.1.3	Защита офисов, комнат и оборудования	*Механизм контроля* Должны проектироваться и применяться механизмы обеспечения физической безопасности офисов, комнат и оборудования.
A.9.1.4	Защита от внешних угроз и угроз окружающей среды	*Механизм контроля* Должна проектироваться и применяться физическая защита от ущерба, вызванного огнем, наводнением, землетрясением, взрывом, гражданскими беспорядками и другими формами природных и антропогенных катастроф.

A.9.1.5	Работа в защищенных областях	*Механизм контроля* Должны проектироваться и применяться механизмы обеспечения физической безопасности и инструкции по работе в защищенных областях.
A.9.1.6	Области общего доступа, доставки и погрузки	*Механизм контроля* Места доступа, такие как области доставки и погрузки и другие места, в которых неавторизованные люди могут входить в помещения организации, должны контролироваться и, если это возможно, должны быть изолированы от средств обработки информации с целью предотвращения несанкционированного доступа.
A.9.2 Безопасность оборудования *Цель:* Предотвратить потерю, повреждение, кражу или компрометацию ресурсов и нарушение деятельности организации.		
A.9.2.1	Размещение и защита оборудования	*Механизм контроля* С целью снижения рисков, связанных с опасными явлениями окружающей среды, и возможностей несанкционированного доступа, должно осуществляться надежное размещение или защита оборудования.
A.9.2.2	Вспомогательные службы	*Механизм контроля* Оборудование должно быть защищено от сбоев электропитания и других нарушений функционирования, вызванных сбоями вспомогательных служб.
A.9.2.3	Безопасность кабельной разводки	*Механизм контроля* Телекоммуникационные и силовые кабели, передающие данные или поддерживающие информационные сервисы должны быть защищены от прослушивания или повреждения.
A.9.2.4	Техническое обслуживание оборудования	*Механизм контроля* В целях обеспечения его непрерывной доступности и целостности оборудование должно правильно обслуживаться.
A.9.2.5	Безопасность оборудования, находящегося вне территории организации	*Механизм контроля* Должна обеспечиваться безопасность оборудования за пределами территории организации, принимая во внимание различные риски, связанные с работой за пределами территории организации.
A.9.2.6	Безопасная утилизация или повторное использование оборудования	*Механизм контроля* Все виды оборудования, содержащие средства хранения информации, должны проверяться, чтобы гарантировать, что все конфиденциальные данные и

		лицензионное программное обеспечение были удалены или надежно перезаписаны перед утилизацией.
A.9.2.7	Перемещение имущества	*Механизм контроля* Оборудование, информация или программное обеспечение без предварительного разрешения не должны выноситься за пределы организации.

A.10 Управление коммуникациями и операциями

A.10.1 Операционные процедуры и распределение ответственности

Цель: Обеспечить корректное и безопасное функционирование средств обработки информации.

A.10.1.1	Документированные операционные процедуры	*Механизм контроля* Операционные процедуры должны быть документированы, поддерживаться в актуальном состоянии и быть доступными для всех пользователей, которым они требуются.
A.10.1.2	Управление изменениями	*Механизм контроля* Изменения средств и систем обработки информации должны контролироваться.
A.10.1.3	Разделение обязанностей	*Механизм контроля* Обязанности и области ответственности должны быть разделены с целью снижения возможностей несанкционированного изменения или злоупотребления ресурсами организации.
A.10.1.4	Разделение разрабатываемых, тестируемых и действующих систем	*Механизм контроля* Средства разработки, тестирования и действующие системы должны быть разделены с целью уменьшения риска несанкционированного доступа или внесения изменений в действующую систему.

A.10.2 Управление сервисами, предоставляемыми третьей стороной

Цель: Реализация и поддержание необходимого уровня информационной безопасности и предоставления сервиса в соответствии с соглашениями о предоставлении сервисов, заключаемыми с третьей стороной.

A.10.2.1	Предоставление сервиса	*Механизм контроля* Необходимо убедиться в том, что механизмы безопасности, определения сервисов и уровни предоставления сервисов, включенные в соглашение о предоставлении сервиса третьей стороной, реализованы, соблюдаются и поддерживаются третьей стороной.

A.10.2.2	Мониторинг и анализ сервисов, предоставляемых третьей стороной	*Механизм контроля* Сервисы, отчеты и записи, предоставляемые третьей стороной, должны регулярно просматриваться и анализироваться, а также должен регулярно проводиться аудит.
A.10.2.3	Управление изменениями в сервисах, предоставляемых третьей стороной	*Механизм контроля* Необходимо управлять изменениями в сервисах, включая сопровождение и совершенствование существующих политик, процедур и механизмов контроля информационной безопасности, с учетом критичности задействованных бизнес систем и процессов, а также результатов переоценки рисков.
A.10.3 Планирование и приемка системы *Цель:* Минимизировать риск сбоя систем.		
A.10.3.1	Управление производительностью	*Механизм контроля* Должно отслеживаться и приспосабливаться использование ресурсов, а также должны прогнозироваться требования к ресурсам на будущее с целью обеспечения требуемой производительности системы.
A.10.3.2	Приемка системы	*Механизм контроля* Должны быть установлены критерии приемки новых информационных систем, их модернизаций и новых версий, а также должно проводиться необходимое тестирование систем(ы) в ходе разработки и перед приемкой в эксплуатацию.
A.10.4 Защита от вредоносного и мобильного кода *Цель:* Обеспечить целостность информации и программного обеспечения.		
A.10.4.1	Механизмы контроля, направленные против вредоносного кода	*Механизм контроля* Для защиты от вредоносного кода должны быть реализованы механизмы обнаружения, предотвращения и восстановления, а также соответствующие процедуры повышения осведомленности пользователей.
A.10.4.2	Механизмы контроля, направленные против мобильного кода	*Механизм контроля* Там, где разрешено использование мобильного кода, конфигурация должна гарантировать, что авторизованный мобильный код исполняется в соответствии с четко определенной политикой безопасности, а выполнение неавторизованного мобильного кода должно предотвращаться.
A.10.5 Резервное копирование		

Цель: Поддерживать целостность и доступность информации и средств ее обработки.		
A.10.5.1	Резервное копирование информации	*Механизм контроля* Резервные копии информации и программного обеспечения должны создаваться и тестироваться регулярно в соответствии с согласованной политикой резервного копирования.
A.10.6 Управление сетевой безопасностью		
Цель: Обеспечить сохранность информации в сетях, а также защиту поддерживающей инфраструктуры.		
A.10.6.1	Сетевые механизмы контроля	*Механизм контроля* Должны быть обеспечены адекватное управление и контроль сети для защиты от угроз и обеспечения безопасности систем и приложений при использовании сети, включая передаваемую информацию.
A.10.6.2	Безопасность сетевых сервисов	*Механизм контроля* Должны быть идентифицированы и включены во все соглашения о предоставлении сетевых сервисов функции безопасности, уровни сервиса и требования руководства для всех сетевых сервисов, независимо от того, предоставляются ли сервисы внутри организации или находятся на аутсорсинге.
A.10.7 Обращение с носителями информации		
Цель: Предотвратить несанкционированное раскрытие, модификацию, удаление или разрушение ресурсов, а также прерывание бизнес деятельности.		
A.10.7.1	Управление сменными носителями информации	*Механизм контроля* Должны быть установлены процедуры для управления сменными носителями информации.
A.10.7.2	Уничтожение носителей информации	*Механизм контроля* Не используемые более носители информации подлежат безопасному и надежному уничтожению с использованием установленных процедур.
A.10.7.3	Процедуры обращения с информацией	*Механизм контроля* Для защиты информации от несанкционированного раскрытия или неправомерного использования, необходимо установить процедуры обращения и хранения информации.
A.10.7.4	Безопасность системной документации	*Механизм контроля* Системная документация должна быть защищена от несанкционированного доступа.
A.10.8 Обмен информацией		

Цель: Поддерживать безопасность информации и программного обеспечения при их обмене внутри организации и с любой внешней стороной.		
A.10.8.1	Политики и процедуры обмена информацией	*Механизм контроля* Должны существовать официальные политики, процедуры и механизмы обмена информацией для защиты информационных обменов, использующих все виды средств коммуникаций.
A.10.8.2	Соглашения об обмене информацией	*Механизм контроля* Между организацией и внешними сторонами должны быть установлены соглашения об обмене информацией и программным обеспечением.
A.10.8.3	Транспортировка физических носителей информации	*Механизм контроля* Носители, содержащие информацию, должны быть защищены от несанкционированного доступа, неправомерного использования или повреждения во время транспортировки за пределы границ организации.
A.10.8.4	Передача электронных сообщений	*Механизм контроля* Информация, участвующая в электронных обменах, должна быть должным образом защищена.
A.10.8.5	Информационные бизнес системы	*Механизм контроля* Для защиты информации, связанной с взаимодействием информационных бизнес систем должны быть разработаны и внедрены соответствующие политики и процедуры.
A.10.9 Сервисы электронной коммерции		
Цель: Обеспечить безопасность сервисов электронной коммерции и их безопасное использование.		
A.10.9.1	Электронная коммерция	*Механизм контроля* Информация, используемая в электронной коммерции и передаваемая по сетям общего пользования, должна быть защищена от мошеннических действий, контрактных споров, а также несанкционированного раскрытия и модификации.
A.10.9.2	Онлайновые транзакции	*Механизм контроля* Информация, используемая в онлайновых транзакциях, должна быть защищена с целью предотвращения незавершенных транзакций, ошибок маршрутизации, несанкционированного изменения сообщений, несанкционированного раскрытия, несанкционированного дублирования и повторного использования сообщений.

A.10.9.3	Общедоступная информация	*Механизм контроля* Целостность информации, которая делается общедоступной в системах общего пользования, должна быть защищена для предотвращения несанкционированных модификаций.
A.10.10 Мониторинг		
Цель: Обнаружение несанкционированных действий по обработке информации.		
A.10.10.1	Регистрация событий аудита	*Механизм контроля* Должны вестись журналы аудита, в которых протоколируются действия пользователей, исключительные ситуации и события информационной безопасности. Они должны храниться в течение установленного периода времени с целью их использования в будущем для проведения расследований и мониторинга доступа.
A.10.10.2	Мониторинг использования системы	*Механизм контроля* Должны быть установлены процедуры мониторинга использования средств обработки информации. Результаты мониторинга должны регулярно анализироваться.
A.10.10.3	Защита данных журналов аудита	*Механизм контроля* Средства регистрации событий и информация журналов аудита должны быть защищены от подделки и несанкционированного доступа.
A.10.10.4	Журналы администратора и оператора	*Механизм контроля* Действия системного администратора и системного оператора должны протоколироваться.
A.10.10.5	Протоколирование сбоев	*Механизм контроля* Сбои должны протоколироваться, анализироваться, и должны предприниматься соответствующие меры.
A.10.10.6	Синхронизация часов	*Механизм контроля* Часы всех важных систем обработки информации в организации или в домене безопасности должны быть синхронизированы с установленным источником точного времени.
A.11 Контроль доступа		
A.11.1 Бизнес требования к контролю доступа		
Цель: Контролировать доступ к информации.		

A.11.1.1	Политика контроля доступа	*Механизм контроля* Политика контроля доступа должна быть установлена, документирована и должна пересматриваться на основании бизнес требований и требований по обеспечению безопасности доступа.
A.11.2 Управление доступом пользователей		
Цель: Обеспечить доступ авторизованных пользователей и предотвратить несанкционированный доступ к информационным системам.		
A.11.2.1	Регистрация пользователей	*Механизм контроля* Должна существовать официальная процедура регистрации и удаления учетных записей пользователей для предоставления и отмены доступа ко всем информационным системам и сервисам.
A.11.2.2	Управление привилегиями	*Механизм контроля* Распределение и использование привилегий должно ограничиваться и контролироваться.
A.11.2.3	Управление паролями пользователей	*Механизм контроля* Контроль распределения паролей должен осуществляться при помощи официального управляющего процесса.
A.11.2.4	Проверка прав доступа пользователей	*Механизм контроля* Руководство должно регулярно производить проверку прав доступа пользователей в рамках соответствующего официального процесса.
A.11.3 Ответственность пользователей		
Цель: Предотвратить несанкционированный доступ пользователей, а также компрометацию или кражу информации и средств ее обработки.		
A.11.3.1	Использование паролей	*Механизм контроля* От пользователей надо требовать, чтобы они следовали стандартам хорошо зарекомендовавшей себя практики в области выбора и использования паролей.
A.11.3.2	Пользовательское оборудование, оставленное без присмотра	*Механизм контроля* Пользователи должны обеспечить необходимый уровень защиты для оборудования, оставляемого без присмотра.
A.11.3.3	Политика чистых столов и чистых экранов	*Механизм контроля* Должна быть принята политика чистых столов для бумаг и съемных устройств хранения информации и политика чистых экранов для средств обработки информации.
A.11.4 Управление доступом к сети		

Цель: Предотвратить несанкционированный доступ к сетевым сервисам.		
A.11.4.1	Политика использования сетевых сервисов	*Механизм контроля* Пользователям должен быть предоставлен доступ только к тем сервисам, использование которых им явным образом разрешено.
A.11.4.2	Аутентификация пользователей при внешних подключениях	*Механизм контроля* Для контроля доступа удаленных пользователей должны использоваться подходящие методы аутентификации.
A.11.4.3	Идентификация оборудования в сетях	*Механизм контроля* В качестве методов аутентификации соединений из конкретных мест и от конкретного оборудования должна рассматриваться автоматическая идентификация оборудования.
A.11.4.4	Защита удаленных диагностических и конфигурационных портов	*Механизм контроля* Физический и логический доступ к диагностическим и конфигурационным портам должен контролироваться.
A.11.4.5	Изоляция в сетях	*Механизм контроля* Группы информационных сервисов, пользователей и информационных систем должны быть изолированы в сетях.
A.11.4.6	Контроль сетевых подключений	*Механизм контроля* В совместно используемых сетях, особенно в тех, которые выходят за границы организации, должны быть ограничены возможности подключения пользователей к сети в соответствии с политикой контроля доступа и требованиями бизнес приложений (см. 11.1).
A.11.4.7	Контроль маршрутизации в сети	*Механизм контроля* В сетях должны быть внедрены механизмы контроля маршрутизации, чтобы гарантировать, что подключение компьютеров и информационные потоки не нарушают политики контроля доступа бизнес приложений.
A.11.5 Контроль доступа в операционных системах		
Цель: Предотвратить несанкционированный доступ к операционным системам.		
A.11.5.1	Безопасные процедуры входа в систему	*Механизм контроля* Доступ к операционным системам должен контролироваться при помощи безопасной процедуры входа в систему.
A.11.5.2	Идентификация и аутентификация	*Механизм контроля*

	пользователя	Все пользователи должны иметь уникальный идентификатор (идентификатор пользователя) исключительно для персонального использования. Для подтверждения заявленного идентификатора пользователя должны выбираться подходящие методы аутентификации.
A.11.5.3	Система управления паролями	*Механизм контроля* Системы управления паролями должны быть интерактивными и обеспечивать выбор качественных паролей.
A.11.5.4	Использование системных утилит	*Механизм контроля* Использование утилит, которые могут обходить механизмы контроля системы и приложений, должно быть ограничено и строго контролироваться.
A.11.5.5	Завершение сессий при превышении лимита времени	*Механизм контроля* Неактивные сессии должны автоматически завершаться при истечении установленного периода неактивности.
A.11.5.6	Ограничение времени подключения	*Механизм контроля* Ограничения времени подключения должно использоваться для обеспечения дополнительного уровня защиты для приложений с высоким риском.
A.11.6 Контроль доступа к приложениям и информации		
Цель: Предотвратить несанкционированный доступ к информации, содержащейся в прикладных системах.		
A.11.6.1	Ограничение доступа к информации	*Механизм контроля* Доступ к информации и к функциям прикладной системы со стороны пользователей и обслуживающего персонала должен быть ограничен в соответствии с установленной политикой контроля доступа.
A.11.6.2	Изоляция критичных систем	*Механизм контроля* Критичные системы требуют создания выделенной (изолированной) компьютерной среды.
A.11.7 Мобильное компьютерное оборудование и работа вне офиса		
Цель: Обеспечить безопасность информации при использовании мобильного компьютерного оборудования и при работе вне офиса.		
A.11.7.1	Мобильное компьютерное оборудование и средства связи	*Механизм контроля* Должна существовать официальная политика и должны быть утверждены соответствующие механизмы контроля для защиты от рисков, связанных с использованием мобильного компьютерного оборудования и средств связи.

A.11.7.2	Работа вне офиса	*Механизм контроля* Должны быть разработаны и реализованы политика, рабочие планы и процедуры для работы вне офиса.

A.12 Приобретение, разработка и сопровождение информационных систем

A.12.1 Требования безопасности для информационных систем

Цель: Гарантировать, что безопасность является составной частью информационных систем.

A.12.1.1	Анализ и спецификация требований безопасности	*Механизм контроля* Требования к механизмам безопасности должны определяться бизнес требованиями для новых систем или требованиями к усовершенствованию для существующих систем.

A.12.2 Корректная обработки информации в приложениях

Цель: Предотвратить ошибки, потерю, несанкционированную модификацию или неправильное использование информации в приложениях.

A.12.2.1	Проверка входных данных	*Механизм контроля* Входные данные приложения должны проверяться на предмет их корректности и приемлемости.
A.12.2.2	Контроль внутренней обработки данных	*Механизм контроля* Для выявления любых искажений обрабатываемых данных в результате ошибок их обработки или умышленных действий в приложения должны быть встроены механизмы проверки их достоверности.
A.12.2.3	Целостность сообщения	*Механизм контроля* Должны быть идентифицированы требования к обеспечению аутентичности и целостности сообщения в приложениях, а также должны быть идентифицированы и реализованы соответствующие механизмы контроля.
A.12.2.4	Проверка выходных данных	*Механизм контроля* Выходные данные приложения должны проверяться для обеспечения корректности обработки хранимой информации и ее соответствия обстоятельствам.

A.12.3 Криптографические механизмы

Цель: Защитить конфиденциальность, аутентичность и целостность информации криптографическими средствами.

A.12.3.1	Политика использования криптографических механизмов	*Механизм контроля* Должна быть разработана и реализована политика использования криптографических механизмов для защиты информации.
A.12.3.2	Управление ключами	*Механизм контроля* Должно осуществляться управление ключами для поддержки применения криптографических методов в организации.
A.12.4 Безопасность системных файлов		
Цель: Обеспечить безопасность системных файлов.		
A.12.4.1	Контроль действующего программного обеспечения	*Механизм контроля* Должны существовать процедуры для контроля установки программного обеспечения в действующих системах.
A.12.4.2	Защита тестовых системных данных	*Механизм контроля* Тестовые данные необходимо аккуратно выбирать, защищать и контролировать.
A.12.4.3	Контроль доступа к исходным текстам программ	*Механизм контроля* Доступ к исходным текстам программ должен быть ограничен.
A.12.5 Безопасность процессов разработки и поддержки		
Цель: Поддерживать безопасность программного обеспечения и информации прикладных систем.		
A.12.5.1	Процедуры контроля изменений	*Механизм контроля* Внесение изменений должно контролироваться путем использования официальных процедур контроля изменений.
A.12.5.2	Технический анализ приложений после изменений операционной системы	*Механизм контроля* После внесения изменений в операционные системы критичные для бизнеса приложения должны анализироваться и тестироваться, чтобы гарантировать отсутствие вредных последствий для работы или безопасности организации.
A.12.5.3	Ограничения на изменения пакетов программного обеспечения	*Механизм контроля* Следует препятствовать внесению изменений в пакеты программного обеспечения, за исключение необходимых изменений, и все изменения должны строго контролироваться.

A.12.5.4	Утечка информации	*Механизм контроля* Следует предотвращать возможности утечки информации.
A.12.5.5	Аутсорсинг разработки программного обеспечения	*Механизм контроля* Аутсорсинг разработки программного обеспечения должен контролироваться и отслеживаться организацией.
A.12.6 Управление техническими уязвимостями		
Цель: Уменьшение рисков, связанных с использованием опубликованных технических уязвимостей.		
A.12.6.1	Контроль технических уязвимостей	*Механизм контроля* Следует своевременно получать информацию о технических уязвимостях используемых информационных систем, оценивать подверженность организации этим уязвимостям и принимать необходимые меры по минимизации, связанного с ними риска.
A.13 Управление инцидентами информационной безопасности		
A.13.1 Информирование о событиях и слабостях информационной безопасности		
Цель: Гарантировать, что информация о событиях информационной безопасности и слабостях, связанных с информационными системами, доводится до сведения уполномоченных лиц в порядке, позволяющем вовремя предпринимать корректирующие действия.		
A.13.1.1	Информирование о событиях информационной безопасности	*Механизм контроля* Информирование о событиях информационной безопасности должно производиться по соответствующим каналам управления как можно быстрее.
A.13.1.2	Информирование о слабостях безопасности	*Механизм контроля* Все сотрудники, подрядчики и пользователи информационных систем и сервисов третьих сторон должны записывать и сообщать обо всех наблюдаемых или предполагаемых слабостях безопасности в системах или сервисах.
A.13.2 Управление инцидентами и усовершенствованиями информационной безопасности		
Цель: Обеспечить использование последовательного и эффективного подхода к управлению инцидентами информационной безопасности.		

A.13.2.1	Ответственность и процедуры	*Механизм контроля* Должны быть установлены ответственность руководства и процедуры для обеспечения быстрой, эффективной и последовательной реакции на инциденты информационной безопасности.
A.13.2.2	Обучение на инцидентах информационной безопасности	*Механизм контроля* Должны существовать механизмы для количественного представления и отслеживания типов, размеров и стоимости инцидентов информационной безопасности.
A.13.2.3	Сбор свидетельств	*Механизм контроля* В тех случаях, когда действия, предпринимаемые после инцидента информационной безопасности против физического лица или организации, предполагают юридические санкции (гражданские или уголовные), должны осуществляться сбор, хранение и предоставление свидетельств для выполнения правил, принятых в соответствующей юрисдикции(ях).

A.14 Управление непрерывностью бизнеса

A.14.1 Аспекты управления непрерывностью бизнеса, связанные с информационной безопасностью

Цель: Препятствовать прерываниям хозяйственной деятельности и защищать критически важные бизнес процессы от влияния крупных сбоев информационных систем или аварий и обеспечить их своевременное возобновление.

A.14.1.1	Включение информационной безопасности в процесс управления непрерывностью бизнеса	*Механизм контроля* Для обеспечения непрерывности бизнеса во всей организации следует разработать и поддерживать управляемый процесс, учитывающий требования информационной безопасности, необходимые для обеспечения непрерывности бизнеса организации.
A.14.1.2	Непрерывность бизнеса и оценка рисков	*Механизм контроля* События, которые могут привести к прерываниям бизнес процессов, должны быть идентифицированы наряду с вероятностью и последствиями таких прерываний и их влиянием на информационную безопасность.

A.14.1.3	Разработка и реализация планов обеспечения непрерывности, включая информационную безопасность	*Механизм контроля* Должны быть разработаны и реализованы планы, которые позволят продолжить или восстановить операции и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя критически важных бизнес процессов.
A.14.1.4	Общая схема планирования непрерывности бизнеса	*Механизм контроля* Необходимо поддерживать единую структуру планов обеспечения непрерывности бизнеса, что позволит гарантировать непротиворечивость всех планов, последовательно учитывать требования информационной безопасности, а также определять приоритеты в области тестирования и сопровождения.
A.14.1.5	Тестирование, поддержка и пересмотр планов обеспечения непрерывности бизнеса	*Механизм контроля* Планы обеспечения непрерывности бизнеса необходимо регулярно тестировать и пересматривать, чтобы гарантировать их эффективность и соответствие текущему положению дел.

A.15 Соблюдение требований

A.15.1 Соблюдение требований законодательства

Цель: Избежать нарушения положений любых обязанностей, установленных действующим законодательством, подзаконными актами и договорными отношениями, а также любых требований безопасности.

A.15.1.1	Определение законодательной базы, применимой к деятельности организации	*Механизм контроля* Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход организации к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии для каждой информационной системы и организации.
A.15.1.2	Право интеллектуальной собственности	*Механизм контроля* Должны быть внедрены соответствующие процедуры для обеспечения соблюдения законодательных ограничений, подзаконных актов и контрактных обязательств по использованию материалов, охраняемых правом интеллектуальной собственности, а также по использованию лицензионного программного обеспечения.

A.15.1.3	Защита документации организации	*Механизм контроля* Важная документация организации должна быть защищена от утери, уничтожения и фальсификации в соответствии с требованиями законодательства, подзаконных актов, контрактных обязательств и бизнес требованиями.
A.15.1.4	Защита данных и персональной информации	*Механизм контроля* Защита данных и персональной информации должна обеспечиваться согласно требованиям действующего законодательства и нормативной базы, а также, если необходимо, положений контрактных обязательств.
A.15.1.5	Предотвращение случаев ненадлежащего использования средств обработки информации	*Механизм контроля* Пользователи должны удерживаться от использования средств обработки информации не целевым образом.
A.15.1.6	Правовое регулирование в области использования криптографических средств	*Механизм контроля* Криптографические механизмы должны использоваться в соответствии со всеми имеющимися соглашениями, законодательными и нормативными актами.
A.15.2 Соблюдение требований политик и стандартов безопасности, а также технических требований		
Цель: Обеспечить соответствие систем политикам и стандартам безопасности организации.		
A.15.2.1	Соблюдение требований политик и стандартов безопасности	*Механизм контроля* Руководители должны обеспечить корректное выполнение всех процедур по обеспечению безопасности в зоне своей ответственности с целью соблюдения требований политик и стандартов безопасности.
A.15.2.2	Проверка соответствия техническим требованиям	*Механизм контроля* Информационные системы должны регулярно проверяться на соответствие стандартам в области реализации механизмов безопасности.
A.15.3 Соображения, относящиеся к аудиту информационных систем		
Цель: Максимизировать эффективность и минимизировать вмешательство в/со стороны процесса аудита информационных систем.		

A.15.3.1	Механизмы аудита информационных систем	*Механизм контроля* Требования и мероприятия аудита, включающие в себя проведение проверок действующих систем, должны быть тщательно спланированы и согласованы с целью сведения к минимуму риска прерывания бизнес процессов.
A.15.3.2	Защита средств аудита информационных систем	*Механизм контроля* Доступ к средствам аудита информационных систем должен быть защищен с целью предотвращения любой возможности ненадлежащего использования или компрометации.

Приложение B
(информативное)

Принципы OECD и этот Международный стандарт

Принципы, определенные в руководстве OECD по Безопасности информационных систем и сетей, применяются ко всем политикам и уровням функционирования, которые управляют безопасностью информационных систем и сетей. Этот Международный стандарт предоставляет структуру системы управления информационной безопасностью для реализации некоторых принципов OECD с использованием модели ПРПД и процессов, описанных в пунктах 4, 5, 6 и 8, как показано в таблице B.1

Таблица B.1 – Принципы OECD и модель ПРПД

Принцип OECD	**Соответствующий процесс СУИБ и стадия ПРПД**
Осведомленность Участники должны быть осведомлены о необходимости обеспечения безопасности информационных систем и сетей, а также о том, что они могут сделать для усиления безопасности.	Эта мера является частью стадии **Реализации** (см. **4.2.2** и **5.2.2**)
Ответственность Все участники несут ответственность за обеспечение безопасности информационных систем и сетей.	Эта мера является частью стадии **Реализации** (см. **4.2.2** и **5.1**)
Реагирование Участники должны действовать своевременно и сообща для предотвращения, обнаружения и реагирования на инциденты безопасности.	Это частично меры по мониторингу стадии **Проверки** (см. **4.2.3** и **6 – 7.3**) и ответные меры стадии **Действия** (см. **4.2.4** и **8.1 – 8.3**). Это также частично может закрываться некоторыми аспектами стадии **Планирования** и **Проверки**.
Оценка рисков Участники должны проводить оценку рисков.	Эта мера является частью стадии **Планирования** (см. **4.2.1**), также оценка рисков является частью стадии **Проверки** (см. **4.2.3** и **6 – 7.3**).
Проектирование и внедрение механизмов безопасности Участники должны встраивать механизмы	По завершению оценки рисков выбираются механизмы контроля для обработки рисков как часть стадии **Планирования** (см. **4.2.1**). Стадия **Реализации** (см. **4.2.2** и **5.2**) затем

безопасности как существенный элемент информационных систем и сетей.	закрывает вопросы внедрения и рабочей эксплуатации этих механизмов контроля.
Управление безопасностью Участники должны принять комплексный подход к управлению безопасностью.	Управления рисками – это процесс, включающий в себя предотвращение, обнаружение и реагирование на инциденты, непрерывное сопровождение, анализ и аудит. Все эти аспекты включены в стадии **Планирования**, **Реализации**, **Проверки** и **Действия**.
Пересмотр Участники должны анализировать и пересматривать безопасность информационных систем и сетей, вносить необходимые изменения в политики безопасности, практики, механизмы и процедуры.	Пересмотр информационной безопасности является частью стадии **Проверки** (см. **4.2.3** и **6 – 7.3**), где должны проводиться регулярные пересмотры с целью проверки эффективности системы управления информационной безопасностью, а совершенствование безопасности является частью стадии **Действия** (см. **4.2.4** и **8.1 – 8.3**).

Приложение С
(информативное)

Взаимосвязь между ISO 9001:2000, ISO 14001:2004 и этим Международным стандартом

В Таблице С.1 показана взаимосвязь между ISO 9001:2000, ISO 14001:2004 и этим Международным стандартом.

Таблица С.1 – Взаимосвязь между ISO 9001:2000, ISO 14001:2004 и этим Международным стандартом

Этот Международный стандарт	**ISO 9001:2000**	**ISO 14001:2004**
0 Введение	**0 Введение**	**Ведение**
0.1 Общие положения	0.1 Общие положения	
0.2 Процессный подход	0.2 Процессный подход	
	0.3 Взаимосвязь с ISO 9004	
0.3 Совместимость с другими системами управления	0.4 Совместимость с другими системами управления	
1 Область действия	**1 Область действия**	**1 Область действия**
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 управления информационной безопасностью	**4 Система управления качеством**	**4 Требования СУОС**
4.1 Общие требования	4.1 Общие требования	4.1 Общие требования
4.2 Создание и управление СУИБ		
4.2.1 Создание СУИБ		
4.2.2 Внедрение и эксплуатация СУИБ		4.4 Внедрение и эксплуатация

4.2.3 Мониторинг и анализ СУИБ 4.2.4 Сопровождение и совершенствование СУИБ	8.2.3 Мониторинг и измерение процессов 8.2.4 Мониторинг и измерение продукта	4.5.1 Мониторинг и измерение
4.3 Требования к документированию 4.3.1 Общие требования 4.3.2 Управление документами 4.3.3 Управление записями	4.2 Требования к документированию 4.2.1 Общие требования 4.2.2 Руководство по качеству 4.2.3 Управление документами 4.2.4 Управление записями	4.4.5 Управление документацией 4.5.4 Управление записями
5 Ответственность руководства 5.1 Приверженность руководства	**5 Ответственность руководства** 5.1 Приверженность руководства 5.2 Фокус на клиента 5.3 Политика качества 5.4 Планирование 5.5 Ответственность, полномочия и взаимодействие	4.2 Политика окружающей среды 4.3 Планирование
5.2 Управление ресурсами 5.2.1 Обеспечение ресурсами 5.2.2 Обучение, осведомленность и компетенция	**6 Управление ресурсами** 6.1 Обеспечение ресурсами 6.2 Людские ресурсы 6.2.2 Компетенция, осведомленность и обучение 6.3 Инфраструктура 6.4 Рабочая среда	4.2.2 Компетенция, обучение и осведомленность
6 Внутренние аудиты СУИБ	**8.2.2 Внутренний аудит**	**4.5.5 Внутренний аудит**
7 Анализ СУИБ со стороны руководства 7.1 Общие положения 7.2 Входные данные анализа 7.3 Выходные данные анализа	**5.6 Анализ со стороны руководства** 5.6.1 Общие положения 5.6.2 Входные данные анализа 5.6.3 Выходные данные анализа	**4.6 Анализ со стороны руководства**

8 Совершенствование СУИБ 8.1 Непрерывное совершенствование 8.2 Корректирующая мера 8.3 Превентивная мера	**8.5 Совершенствование** 8.5.1 Непрерывное совершенствование 8.5.2 Корректирующие меры 8.5.3 Превентивные меры	4.5.3 Несоответствие, корректирующая мера и превентивная мера
Приложение A Цели контроля и механизмы контроля **Приложение B Принципы OECD и этот Международный стандарт** **Приложение C Взаимосвязь между ISO 9001:2000, ISO 14001:2004 и этим Международным стандартом**	**Приложение A Взаимосвязь между ISO 9001 и ISO 14001:1996**	**Приложение A Инструкции по использованию этого Международного стандарта** **Приложение B Взаимосвязь между ISO 14001:2004 и ISO 9001:2000**

Библиография

Публикации стандартов

[1] ISO 9001:2000, *Системы управления качеством - Требования*

[2] ISO/IEC 13335-1:2004, *Информационные технологии – Методы обеспечения безопасности – Управление безопасностью информационных и телекоммуникационных технологий – Часть 1: Концепции и модели для управления безопасностью информационных и телекоммуникационных технологий*

[3] ISO/IEC TR 13335-3:1998, *Информационные технологии - Принципы управления ИТ безопасностью – Часть 3: Методы управления ИТ безопасностью*

[4] ISO/IEC TR 13335-4:2000, *Информационные технологии - Принципы управления ИТ безопасностью – Часть 4: Выбор механизмов защиты*

[5] ISO 14001:2004, *Системы управления окружающей средой – Требования и руководство по применению*

[6] ISO/IEC TR 18044:2004, *Информационные технологии – Методы обеспечения безопасности – Управление инцидентами информационной безопасности*

[7] ISO 19011:2002, *Руководство по аудиту систем управления качеством и/или окружающей средой*

[8] ISO/IEC Guide 62:1996, *Общие требования к оценке деятельности юридических лиц и сертификации/регистрации систем качества*

[9] ISO/IEC Guide 73:2002, *Управление рисками – Словарь – Инструкции по использованию в стандартах*

Другие публикации

[1] OECD, *Принципы обеспечения безопасности информационных систем и сетей – Двигаясь к культуре безопасности. Париж: OECD, Июль 2002. www.oecd.org*

[2] NIST SP 800-30, *Руководство по управлению рисками для информационных систем*

[3] Deming W.E., *Выход из кризиса, Кэмбридж, Mass:MIT, Центр продвинутого инженерного обучения, 1986*

пустая страница

BS ISO/IEC 27001:2005
BS 7799-2:2005

BSI – Британский Институт Стандартов

BSI является независимым государственным учреждением, отвечающим за подготовку Британских стандартов. Он представляет взгляды Объединенного Королевства на стандарты в Европе и на международном уровне. Он образован Королевским указом.

Пересмотры и исправления

Британские стандарты обновляются путем внесения в них исправлений или пересмотров. Пользователям Британских стандартов следует убедиться в том, что они владеют последними исправлениями или редакциями.

Постоянной целью BSI является улучшение качества наших продуктов и услуг. Мы будем признательны, если, обнаружив неточность или неясность при использовании этого Британского стандарта, вы проинформируете об этом Секретаря технического комитета. Тел.: +44 (0)20 8996 9000. Факс: +44 (0)20 8996 7400.

BSI предлагает своим членам индивидуальную службу обновлений, которая называется PLUS и позволяет подписчикам автоматически получать последние редакции стандартов.

Приобретение стандартов

Заказы на все стандарты BSI, международные и иностранные публикации стандартов следует направлять в Клиентские службы. Тел.: +44 (0)20 8996 9001. Факс: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Стандарты также можно приобрести через Web-сайт BSI: http://www.bsi-global.com.

В ответ на заказы международных стандартов политикой BSI является предоставление тех стандартов BSI , которые были опубликованы в качестве Британских стандартов, если не требуется иное.

Информация о стандартах

BSI предоставляет широкий спектр информации о национальных, Европейских и международных стандартов через свою Библиотеку и Службу Технической Помощи Экспортерам. Также имеются различные службы электронной информации, которые предоставляют детальные сведения обо всех продуктах и сервисах BSI. Свяжитесь с Информационным центром. Тел.: +44 (0)20 8996 7111. Факс: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Подписчики BSI своевременно информируются о разрабатываемых стандартах и получают существенные скидки от стоимости стандартов. Для получения более подробной информации об этих и других преимуществах связывайтесь с Администрацией. Тел.: +44 (0)20 8996 7002. Факс: +44 (0)20 8996 7001. Email: membership@bsi-global.com.

Информацию относительно получения доступа к Британским стандартам в интерактивном режиме через British Standards Online можно найти по адресу: http://www.bsi-global.com/bsonline.

Остальную информацию о BSI можно найти на web-сайте BSI: http://www.bsi-global.com.

Авторское право

BSI
389 Chiswick High Road
London
W4 4AL